Some calculations on the action of groups on surfaces

Some calculations on

the action of groups on surfaces

by Emilio Pierro

A thesis submitted to

Birkbeck, University of London

for the degree of
Doctor of Philosophy

Department of Economics, Mathematics and Statistics

Birkbeck, University of London

London

October 17, 2015

Declaration

I warrant that the content of this thesis is the direct result of my own work and that any use made in it of published or unpublished material is fully and correctly referenced.

Signed ....E. Pierro.... Date ....17/10/2015....

Copyright

Abstract

In this thesis we treat a number of topics related to generation of finite groups with motivation from their action on surfaces. The majority of our findings are presented in two chapters which can be read independently. The first deals with Beauville groups which are automorphism groups of the product of two Riemann surfaces with genus $g > 1$, subject to some further conditions. When these two surfaces are isomorphic and transposed by elements of G we say these groups are mixed, otherwise they are unmixed. We first examine the relationship between when an almost simple group and its socle are unmixed Beauville groups and then go on to determine explicit examples of several infinite families of mixed Beauville groups. In the second we determine the Möbius function of the small Ree groups ${}^2G_2(3^{2m+1}) = R(3^{2m+1})$, where $m \geq 0$, and use this to enumerate various ordered generating n-tuples of these groups. We then apply this to questions of the generation and asymptotic generation of the small Ree groups as well as interpretations in other categories, such as the number of regular coverings of a surface with a given fundamental group and whose covering group is isomorphic to $R(3^{2m+1})$.

Acknowledgment

I would like to thank first and foremost my supervisor, Ben Fairbairn, for always being willing to discuss mathematics, for his time, patience and guidance throughout the course of my studies.

I would like to thank (in reverse alphabetical order) Rob Wilson and Gareth Jones for taking the time to read and examine my thesis. I would also like to thank Gareth Jones for making me aware of the Möbius function and for his encouragement throughout my PhD.

I am indebted to Dimitri Leemans for our valuable conversation at SIGMAP 2014, and, after learning that I was working on the Möbius function of the small Ree groups, for announcing this in his talk and insisting that nobody else work on this problem.

I would like to thank the many mathematicians at Queen Mary, Imperial and City who have given me a mathematical community in London beyond that of my own institution. I would also like to thank my lecturers from the University of Birmingham who continue to support me long after my time there.

Last but not least I wish to thank my family and friends for all of their support, in all of its forms, throughout my PhD and my whole life. I would not be here without them.

The financial support I have received from Birkbeck, in particular the School Scholarship, has been life-changing and for which I cannot sufficiently express my gratitude.

Contents

1 Introduction **11**

1.1 Beauville groups . . . 11

1.1.1 Unmixed Beauville groups . . . 12

1.1.2 Mixed Beauville groups . . . 14

1.1.3 Results . . . 14

1.2 The Möbius function of a group . . . 16

1.2.1 Applications of the Eulerian functions of a group . . . 19

1.2.2 Results . . . 20

2 Beauville groups **21**

2.1 Almost simple unmixed Beauville groups . . . 22

2.1.1 Outer automorphism groups that are not 2-generated . . . 23

2.1.2 Non-split extensions . . . 24

2.1.3 Split extensions . . . 26

2.1.4 Examples . . . 27

2.2 Topological invariants of Beauville surfaces . . . 28

2.3 Mixed Beauville groups via mixable Beauville structures . . . 30

2.4 Mixable Beauville structures for the alternating groups . . . 33

2.5 Mixable Beauville structures for low-rank finite groups of Lie type . . . 37

2.5.1 The projective special linear groups $L_2(q)$ . . . 38

2.5.2 The projective special linear groups $L_3(q)$ . . . 41

2.5.3 The projective special unitary groups $U_3(q)$ . . . 44

2.5.4 The projective symplectic groups $S_4(q)$ . . . 47

2.5.5 The Suzuki groups $Sz(2^{2m+1})$ . . . 51

2.5.6 The exceptional groups $G_2(q)$ . . . 51

2.5.7 The small Ree groups $R(3^{2m+1})$ . . . 54

2.5.8 The large Ree groups ${}^2F_4(2^{2m+1})$ . . . 55

2.5.9 The Steinberg triality groups ${}^3D_4(q)$ . . . 56

2.6 Mixable Beauville structures for the sporadic groups . . . 57

3 The Möbius function of the small Ree groups **61**

3.1 The Möbius function of $R(3)$ . . . 63

3.2 The structure of the simple small Ree groups . . . 65

3.2.1 Conjugacy classes and centralisers of elements in $R(q)$ . . . 65

3.2.2 Maximal subgroups . . . 67

3.3 The Möbius function of the simple small Ree groups . . . 70

3.3.1 Conjugacy classes and normalisers of subgroups in $R(q)$ . . . 71

3.3.2 Intersections of maximal subgroups . . . 73

3.4 Eulerian functions of the small Ree groups . . . 85

3.4.1 Enumerations of $\mathrm{Epi}(\Gamma, R(3))$ . . . 87

3.4.2 Free groups & Hecke groups . . . 88

3.4.3 Asymptotic results . . . 91

3.5 General results on the Möbius and Eulerian functions . . . 92

A The genus spectrum of a group **94**

A.1 Program . . . 94

A.2 The genus spectrum of some finite almost simple groups . . . 97

B Future research **111**

B.1 Beauville groups . . . 111

B.1.1 Mixable Beauville groups . . . 111

B.1.2 Beauville p-groups . . . 112

B.1.3 Strongly real Beauville groups . . . 112

B.2 Möbius functions and related problems . . . 113

B.2.1 More Möbius functions . . . 113

B.2.2 Other properties of subgroup lattices . . . 114

B.2.3 Maximal subgroups . . . 115

List of Tables

2.1 Words in the standard generators for the automorphism groups of the sporadic groups and the Tits group. 28

2.2 Power maps for elements of generating triples in Table 2.1. 29

2.3 Mixable Beauville structures for G and $G \times G$ where $G = U_3(q)$, $q = 4, 5$ and 8. 47

2.4 Mixable strucutres $(x_1, y_1; x_2, y_2)$ for G in terms of words in the standard generators. 59

2.5 Types of the mixable Beauville structures for G and $G \times G$ from the words in Table 2.4 and Lemmas 2.87 and 2.88. 60

3.1 Table of values for $\nu_K(H)$ with the isomorphism class of H in the left hand column. 65

3.2 Conjugacy classes of maximal subgroups of the simple small Ree groups $R(q)$. 67

3.3 The disjoint subsets of **MaxInt**. Each subset consists of subgroups of G for all l dividing n unless otherwise stated. 70

3.4 $H \cong R(3^h) \in \boldsymbol{R}(l)$ 75

3.5 $H \cong (3^h)^{1+1+1} : (3^h - 1) \in \boldsymbol{P}(l)$ 75

3.6 $H \cong 2 \times L_2(3^h) \in \boldsymbol{C}_t(l)$ 76

3.7 $H \cong 2 \times (3^h : \frac{3^h-1}{2}) \in \boldsymbol{C}_t^{\omega}(l)$ 77

3.8 $H \cong 3^h - 1 \in \boldsymbol{C}_0(l)$ 79

3.9 $H \cong (2^2 \times D_{(3^h+1)/2}) : 3 \in \boldsymbol{N}_V(l)$ 82

3.10 $H \cong 3^h - 3^{\frac{h+1}{2}} + 1 : 6 \in \boldsymbol{N}_2(l)$ 82

3.11 $H \cong 2^2 \times D_{(3^h+1)/2} \in \boldsymbol{C}_V(l)$ 83

3.12 $H \cong D_{2a_2(h)} \in \boldsymbol{D}_2(l)$ 83

3.13 $H \cong 2 \times L_2(3) \in \boldsymbol{C}_t(1)$ 83

3.14 $H \cong 2^3 \in \boldsymbol{E}$ 84

3.15 $H \cong 2^2 \in \boldsymbol{V}$ 84

3.16 $H \cong \langle tu \rangle \in \boldsymbol{C}_6^*$ 85

3.17 $H \cong \langle u \rangle \in \boldsymbol{C}_3^*$ 85

3.18 $H \cong \langle t \rangle \in \boldsymbol{C}_2$ 86

3.19 $H \in \boldsymbol{I}$ 86

3.20 Values of $|H|_n$ for nontrivial subgroups of $R(3)$ with $\mu_G(H) \neq 0$. 88

3.21 Evaluation of $d_{a,b}(R(3))$. 88

3.22 Values of $|H|_n$ for $n = 2, 3$ or 6. 89

3.23 Values of $|H|_n$ for $n = 7$ or 9. 89

3.24 Values of $d_2(G)$ for $R(q)$, $q \leq 3^9$. 90

3.25 Values of $h_3(G)$ for $R(q)$, $q \leq 3^9$. 91

A.1 Genus spectrum of A_6 98

A.2 Genus spectrum of S_6 98

A.3 Genus spectrum of A_7 99

A.4 Genus spectrum of S_7, continued on Table A.5 100

A.5 Genus spectrum of S_7 continued 101

A.6 Genus spectrum of $P\Gamma L_2(8) \cong R(3)$ 102

A.7 Genus spectrum of $L_2(16){:}2 \cong O_4^-(4)$ 102

A.8 Genus spectrum of $P\Gamma L_2(16)$ 102

A.9 Genus spectrum of $P\Sigma L_2(25)$, continued on Table A.10 103

A.10 Genus spectrum of $P\Sigma L_2(25)$ continued 104

A.11 Genus spectrum of $P\Sigma L_2(27)$ 105

A.12 Genus spectrum of $L_3(3)$ 106

A.13 Genus spectrum of $P\Gamma L_3(3)$ 106

A.14 Genus spectrum of $U_3(3)$ 107

A.15 Genus spectrum of $P\Gamma U_3(3)$ 107

A.16 Genus spectrum of $L_3(4)$ 108

A.17 Genus spectrum of $Sz(8)$ 109

A.18 Genus spectrum of M_{11} 110

Notation & Preliminaries

Groups and subsets of groups will be denoted with upper case italicised Latin or Greek script or modern script font, G, H, Γ, $\mathcal{C}$ etc., whereas surfaces will be denoted with a cursive script font, $\mathscr{S}$, $\mathscr{C}$, etc. Unless otherwise stated, groups appearing in definitions and results will be arbitrary. Elements of a group are denoted with lower case italicised Latin script. For a group G and elements $x, y \in G$ the inverse of x is denoted x^{-1}, the conjugate of x by y is denoted $x^y = y^{-1}xy$ and the commutator of x and y is $[x, y] = x^{-1}y^{-1}xy$. We write $H \leqslant G$ when H is a subgroup of G and $H < G$ if in addition $H \neq G$. If H is a normal subgroup of G we write $H \lhd G$. The index of H in G is denoted $[G : H]$. If $S \subseteq G$ is a subset of elements of G we write $\langle S \rangle$ to mean the subgroup of G generated by the elements of S.

We use the following conventions for notation of elements of certain families of groups. The cyclic group of order n is denoted C_n or more often simply as n, as in [27], when no confusion can arise. We write D_n for the dihedral group of order n and F_n for the free group on n generators. We follow [27] in using Artin's single letter notation, $L_n(q)$, $U_n(q)$, etc. for the simple classical groups. We do this to avoid confusion between the frequently used notation for the alternating groups A_n and the Chevalley notation for the simple linear groups $A_n(q)$ and the simple unitary groups ${}^2A_n(q)$. This does introduce the similar notation S_n for the symmetric group on n letters and $S_n(q)$ for the simple symplectic group in dimension n, however it should be clear from the context which we mean.

We make use of ATLAS [27] notation throughout. References to conjugacy classes of groups follows the ATLAS convention so that nX is a conjugacy class of elements of order n, labelled by a letter X and ordered alphabetically in decreasing order by their centraliser order. Where we write, for example in the case of $L_2(8)$ [27, p.6], $7ABC$, we mean the union of conjugacy classes $7A, 7B$ and $7C$. Where we refer to the standard generators of a group we mean in the sense of [118]. These are taken from [125] and were used extensively for calculations via their GAP package [124]. For two groups, G, H, we denote the set of epimorphisms from G to H by $\mathrm{Epi}(G, H)$. Similarly, we denote the set of homomorphisms from G to H by $\mathrm{Hom}(G, H)$. We say that a group G is n-generated if there exists a subset $S \subseteq G$ of size n such that $\langle S \rangle = G$, but no subset $T \subseteq G$ of size $n-1$ such that $\langle T \rangle = G$. Equivalently, G is n-generated if $\mathrm{Epi}(F_n, G) \neq \varnothing$ and $\mathrm{Epi}(F_{n-1}, G) = \varnothing$.

Chapter 1

Introduction

The topics of this thesis are questions related to generation of finite groups with applications to the theory of surfaces. In Chapter 2 we determine the existence and non-existence of almost simple unmixed Beauville groups and the existence of a number of new infinite families of mixed Beauville groups both of which arise from the construction of Beauville surfaces. In Chapter 3 we determine the Möbius function of the small Ree groups, which, for a given small Ree group $R(q)$ can be used to determine the number of regular coverings of a topological space with covering group isomorphic to $R(q)$. We now discuss these topics in the context from which they arise.

1.1 Beauville groups

The study of Beauville surfaces and Beauville groups is split between algebraic geometers and group theorists respectively. The author is not a specialist in algebraic geometry and we mostly consider the group-theoretic point of view in this thesis, however, since their origin is from the algebraic geometric point of view, the author feels this aspect should not be overlooked.

Beauville surfaces were introduced by Catanese in 2000 [20] motivated by an exercise given by Beauville [12, Exercise X.13 (4)]. They were initially defined by Catanese [20, Definition 3.23] as "rigid surfaces isogenous to a higher product" and their initial interest was to serve as "cheap counterexamples to the Friedman–Morgan speculation" [9, p.3]. They are a class of surfaces of general type, which is to say that they satisfy a technical condition that we shall not state here. We refer the interested reader to [12, Chapters VII–IX] and [65, Section V.6] for the necessary algebraic geometric background and an overview of the Enriques–Kodaira classification of surfaces to which this class belongs. Furthermore we direct the interested reader to the various survey articles from the algebraic geometric point of view that exist on Beauville surfaces [5, 9, 10]. In addition, there are a number of survey articles covering the group theoretic aspect such as [16, 41, 42, 68].

We do not assume the definition of the terms "rigid" or "isogenous to a product" and so we take as our definition that given by Bauer, Catanese and Grunewald in [6] which incorporates definitions of these terms and also clarifies the difference between unmixed and mixed Beauville surfaces.

Definition 1.1. *A **Beauville surface** is a rigid surface which is isogenous to a product. That is, a surface* $\mathscr{S} = (\mathscr{C}_1 \times \mathscr{C}_2)/G$ *where for* $i = 1, 2$*,*

1. $\mathscr{C}_i$ *is a complex algebraic curve of genus at least* 2*,*

2. G *is a finite group acting freely on the product* $\mathscr{C}_1 \times \mathscr{C}_2$ *and faithfully on each* $\mathscr{C}_i$ *and*

3. $\mathscr{C}_i/G \cong \mathbb{P}^1(\mathbb{C})$ *with the projection* $\mathscr{C}_i \to \mathscr{C}_i/G$ *ramified at* 3 *points.*

The two cases are then as follows.

- *Unmixed type* — where the action of G does not interchange the two curves, and

- *Mixed type* — where $\mathscr{C}_1$ and $\mathscr{C}_2$ are isomorphic, the action of G interchanges the two factors and G contains an index 2 subgroup, G^0, not interchanging the factors.

Another reason for their interest arises from condition 3 of Definition 1.1 which, due to a celebrated theorem of Belyĭ [14, Theorem 4], implies that the curves $\mathscr{C}_1$ and $\mathscr{C}_2$ can be defined over $\overline{\mathbb{Q}}$. This then allows us to observe the behaviour of Beauville surfaces under the action of the absolute Galois group, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. A number of interesting results in this direction have been obtained by González-Diez and Torres-Teigell in [59] and extended by González-Diez, Jones and Torres-Teigell in [58]. We highlight the connection to dessins d'enfants since the results of Chapter 3 also apply to them.

These geometric definitions can then be expressed purely in group-theoretic terms and Catanese already observes in [20] that "Classifying all the Beauville surfaces is then a problem in group theory." We begin by defining the following subset of a group, G.

Definition 1.2. *Let* G *be a finite group. For* $x, y \in G$ *we denote by* $\sum(x, y)$ *the set*

$$\sum(x,y) = \bigcup_{g\in G}\bigcup_{i=1}^{|G|}\{(x^i)^g, (y^i)^g, ((xy)^i)^g\}.$$

Remark 1.3. *It is common in the literature to see this set expressed in a variety of different but equivalent forms.*

1.1.1 Unmixed Beauville groups

The geometric conditions in Definition 1.1 can then be translated into the group-theoretic definition of an unmixed Beauville group given in [6, Definition 3.1] as the following.

Definition 1.4. *For* G*, a finite group, if there exists* $x_1, y_1, x_2, y_2 \in G$ *such that*

1. $\langle x_1, y_1\rangle = \langle x_2, y_2\rangle = G$ *and*

2. $\sum(x_1, y_1) \cap \sum(x_2, y_2) = \{1\}$*,*

then we say that $(x_1, y_1; x_2, y_2)$ *is* ***an unmixed Beauville structure for*** G *and that* G ***admits an unmixed Beauville structure****, or simply that* G *is an* ***unmixed Beauville group****.*

Remark 1.5. *The connection between the geometric definition and the group-theoretic definition is roughly as follows. Condition 1. in Definition 1.4 corresponds to Condition 3. in Defintion 1.1. The vital connection is that if a finite group is* 2*-generated then it is a quotient of* F_2*, the free group on* 2*-generators, which is the fundamental group of the thrice-punctured Riemann sphere. Condition 2. in Definition 1.4 corresponds to the condition that* G *acts freely on the product* $\mathscr{C}_1 \times \mathscr{C}_2$*. A more precise account of the motivation behind this definition is given in [6, 7, 9, 21].*

Mixed Beauville groups are defined in an analogous way but, since their definition is a little more involved, we postpone its statement until Chapter 2.

In the unmixed case Catanese proves in [20, Lemma 3.21] that the only abelian unmixed Beauville groups are the groups $C_n \times C_n$ where $n > 1$ is coprime to 6, the case $n = 5$ being Beauville's original example as mentioned above. This then motivates the classification of non-abelian unmixed Beauville groups. In the same paper [6, Section 5.4] Bauer, Catanese and Grunewald prove that the smallest non-abelian simple group, the alternating group A_5, is not an unmixed Beauville group, but for large n, A_n does admit an unmixed Beauville structure [6, Proposition 3.8]. In a later paper [7, Theorem 7.19] the same authors prove that the symmetric group S_n for $n \geq 7$ also admits an unmixed Beauville structure, although it relies on their proof of [7, Lemma 7.27] which does not hold in the case $n = 7$. These results were improved by Fuertes and González-Diez who prove that A_n is an unmixed Beauville group if and only if $n \geq 6$ [49, Theorem 1] and that S_n is an unmixed Beauville group for $n \geq 5$ [49, Theorem 3]. Fuertes and González-Diez in fact prove something stronger, that A_n for $n \geq 7$ and S_n for $n \geq 5$ admit "strongly real" Beauville structures, which we shall not define here.

Remark 1.6. *It should be noted that the generators given for* S_8 *in [49, Proposition 9] contain a typo which appears to have first been picked up in [41] where it is also resolved.*

Following their results, Bauer, Catanese and Grunewald then conjectured [6, Conjecture 1] that with the exception of A_5 all non-abelian finite simple groups admit an unmixed Beauville structure. This conjecture was verified for various families of non-abelian finite simple groups: the alternating groups, as mentioned above; the families $PSL_2(q), Sz(2^n)$ and $R(3^n)$ by Fuertes and Jones [51], before being proved for sufficiently large non-abelian finite simple groups by Garion, Larsen and Lubotzky [54]. These results were then extended to all non-abelian finite simple groups (except for A_5) by Guralnick and Malle [62] (using different methods to those of Garion, Larsen and Lubotzky) and independently by Fairbairn, Magaard and Parker [45], who also extend these results to all non-abelian finite quasi-simple groups, except for A_5 and $SL_2(5)$.

The case of almost simple unmixed Beauville groups, however, has been little explored. The only known families of non-simple almost simple groups admitting Beauville structures are the aforementioned symmetric groups, the groups $PGL_2(q)$ with $q \geq 5$ [53, Theorem E] and the non-simple almost simple groups with socle isomorphic to a sporadic group, except for ${}^2F_4(2)$ [43, Theorem 20].

1.1.2 Mixed Beauville groups

Examples of mixed Beauville groups in general seem to be much more elusive. In order to have an element of order 2 interchanging our curves, all p-groups where $p \neq 2$ are immediately ruled out. Furthermore, the requirement of having an index 2 subgroup rules out all simple groups except for the cyclic group of order C_2 which is visibly not a mixed Beauville group. Furthermore, Bauer, Catanese and Grunewald also show in [6, Theorem 4.3] that such an index 2 subgroup must be non-abelian. Fuertes and González-Diez [49, Lemma 5] proved the following and used it to show that the symmetric groups were also not mixed Beauville groups, but it also prohibits a number of other families of almost simple groups.

Lemma 1.7. *Let $(\mathscr{C} \times \mathscr{C})/G$ be a Beauville surface of mixed type and G^0 the subgroup of G consisting of the elements which preserve each of the factors; then the order of any element $g \in G \backslash G^0$ is divisible by* 4.

Remark 1.8. *Any group isomorphic to H where $G \leqslant H \leqslant Aut(G)$ for G a non-abelian finite simple group where $Out(G)$ has odd order, such as the Suzuki, small Ree or large Ree groups, is also ruled out from being a mixed Beauville group. However $G = P\Sigma L_2(p^2)$ with p prime is not excluded by this result.*

More generally, Bauer, Catanese and Grunewald show [8] that the smallest mixed Beauville group has order 2^8, and additionally that, of the 56092 groups of order 2^8, only two of them are mixed Beauville groups. However, their method is less instructive since it is precisely to check computationally every group of order $\leq 2^8$. Barker, Boston, Peyerimhoff and Vdovina construct five new examples of mixed Beauville 2-groups in [3] and an infinite family in [4]. As far as the author is aware the aforementioned examples account for all previously known mixed Beauville groups. Aside from these, Bauer, Catanese and Grunewald give a construction in [6] which reduces the problem of finding mixed Beauville groups to finding a pair of generating triples for a particular subgroup, H, subject to some modest constraints. The only examples they give are for A_n when n is large, and $SL_2(p)$ for $p \neq 2, 3, 5$ or 17 [6, Proposition 4.6] although their argument also does not apply when $p = 7$.

1.1.3 Results

In Chapter 2 with respect to unmixed Beauville groups, we investigate the following. What is the relationship between non-abelian finite simple groups admitting an unmixed Beauville structure, depending on whether their socle admits an unmixed Beauville group. A sample of these findings are presented in the following table.

G	G unmixed Beauville?	$\mathrm{Aut}(G)$ unmixed Beauville?
A_5	$\times$	✓
A_6	✓	$\times$
A_n, $n \geq 7$	✓	✓
$L_2(p)$, p odd	✓	✓
$L_2(p^2)$, p odd	✓	$\times$
$Sz(8^{2m+1})$	✓	$\times$
$R(243^{2m+1})$	✓	$\times$

In particular, we find that there is little relationship between such a group and its socle, the prototypical example being the case of the alternating group A_6. As we shall see, of the five different isomorphism types of groups with socle isomorphic to A_6 we find that A_6, $S_6 \cong P\Sigma L_2(9)$ and $PGL_2(9)$ are unmixed Beauville groups, whereas $L_2(9)^{\cdot}2 \cong M_{10}$ and $\mathrm{Aut}(A_6) \cong P\Gamma L_2(9)$ are not. We also determine a number of criteria that ensure a non-abelian finite almost simple group does not admit an unmixed Beauville structure.

In the case of mixed Beauville groups, we determine a number of infinite families of new examples of mixed Beauville groups. In order to do this, we introduce the definition of a "mixable Beauville structure", motivated by a construction of mixed Beauville groups due to Bauer, Catanese and Grunewald, and show that given a mixable Beauville structure on a group, G, there is a natural way of building a mixed Beauville group from this structure. We then prove the following.

Theorem 1.9. *If G belongs to any of the following families of finite simple groups,*

- *the alternating groups, A_n, for $n \geq 6$,*
- *the projective special linear groups, $L_2(q)$, for $q \geq 7$ odd,*
- *the projective special linear groups, $L_3(q)$, for $q \geq 2$*
- *the projective unitary groups, $U_3(q)$, for $q \geq 3$,*
- *the projective symplectic groups, $S_4(q)$, for $q \geq 3$,*
- *the Suzuki groups, $Sz(2^{2m+1})$, for $m \geq 1$,*
- *the small Ree groups, $R(3^{2m+1})$, for $m \geq 1$,*
- *the exceptional groups, $G_2(q)$, for $q \geq 3$,*
- *the large Ree groups, ${}^2F_4(2^{2m+1})$, for $m \geq 1$,*
- *the Steinberg triality groups, ${}^3D_4(q)$, for $q \geq 2$,*
- *the sporadic groups, or the Tits group ${}^2F_4(2)'$,*

then G is a mixable Beauville group. In addition, if G belongs to any of these families, or is equal to $L_2(2^n)$ for $n \geq 3$, then $G \times G$ is a mixable Beauville group.

Remark 1.10. *A necessary condition for a group G to admit a mixable Beauville structure is that G can be generated by a pair of elements of even order. The case of $L_2(2^n)$ is a genuine exception which we treat in Section 2.5.1.*

1.2 The Möbius function of a group

The Möbius function of a finite group has its origins in the generalised enumeration principle due to Weisner [115] first and shortly followed by Hall's independent discovery in [63]. Whereas Weisner conisdered the problem in more generality, Hall was primarily concerned with Möbius inversion in the lattice of subgroups of a finite group and so we mostly refer to Hall's work. The motiviating problem of [63] was to enumerate the number of ordered tuples of elements of a finite group, G, which also generate G. We begin with the following definition.

Definition 1.11. *Let G be a finite group and $H \leqslant G$ a subgroup of G. Let $X = \{x_1, \dots, x_n\}$ be an ordered n-tuple of elements of G, satisfying a finite, possibly empty, family of relations, $f_i(X) = 1$, and let $\Gamma = \langle X \mid f_i(X) \rangle$. We call a* ***summatory function of*** *H the function $\sigma_\Gamma(H)$ which counts the number of ordered n-tuples of H satisfying the relations $f_i(X)$, and an* ***Eulerian function of*** *H, $\phi_\Gamma(H)$, the function counting the number of such n-tuples which in addition generate H. In the case where X has size n and there are no other relations, i.e. when $\Gamma \cong F_n$, we write $\sigma_n(H)$ and $\phi_n(G)$ for our summatory and Eulerian functions respectively.*

The principle Hall uses is then as follows. For a finite group, G, given an n-tuple of elements of G, they will generate a subgroup $H \leqslant G$, not necessarily equal to G. From this we can write the following

$$\sigma_n(G) = \sum_{H \leqslant G} \phi_n(H).$$

Since these are two functions defined on a lattice and taking values in an abelian group, we are able to use Möbius inversion to give

$$\phi_n(G) = \sum_{H \leqslant G} \sigma_n(H)\mu_G(H)$$

where the Möbius function $\mu_G(H)$ is given by the formula

$$\sum_{K \geqslant H} \mu_G(K) = \begin{cases} 1 & \text{if } H = G \\ 0 & \text{otherwise.} \end{cases}$$

Definition 1.12. *The function $\mu_G(H)$ is called the* ***Möbius function of*** *H. We refer to the collection of $\mu_G(H)$ for all $H \leqslant G$ as the* ***Möbius function of*** *G and $\mu_G(1)$ as the* ***Möbius***

number *of G. The* ***inversion formula*** *for G is the general form of the Eulerian function*

$$\phi(G) = \sum_{H \leqslant G} \sigma(H)\mu_G(H)$$

where $\sigma(H)$ stands for the summatory function of H.

Remark 1.13. *In the case that G is a cyclic group, $\phi_1(G)$ is precisely the Euler totient function $\phi(|G|)$. We denote this as usual by $\phi(n)$ for a positive integer n.*

A priori, it seems as though we might have to work through the entire subgroup lattice of G, but since it is clear that $\mu_G(H) = \mu_G(H')$ if H and H' are conjugate in G, we need only determine $\mu_G(H)$ on a set of conjugacy class representatives of subgroups. In fact, due to the following theorem of Hall, we need only determine $\mu_G(H)$ on a set of conjugacy class representatives of subgroups which occur as the intersection of maximal subgroups.

Theorem 1.14 (Hall)**.** *If $H \leqslant G$ then $\mu_G(H) = 0$ unless $H = G$ or H is an intersection of maximal subgroups of G.*

The theory of Möbius functions and enumeration in a general poset was later developed extensively by Rota in [99] and this was shortly followed by a paper due to Crapo [29] which extends Rota's work by introducing the use of complements. In the specific case of the Möbius function of a finite group we also draw the reader's attention to the works of Kratzer and Thévenaz [75], Hawkes, Isaacs and Özaydin [66] and Pahlings [90].

In general, determining the Möbius function of a finite group is a lengthy process, however, a number of results are known which facilitate its determination. One must have a large amount of information about the subgroup structure of G, including knowledge of its classes of maximal subgroups. The following, which can already be found in Weisner [116, Theorem 1], is an immediate consequence of the fact that if N is a normal subgroup of G, the subgroup lattice of the quotient G/N is in bijective correspondence with the lattice of subgroups of G containing N.

Theorem 1.15 (Weisner, 1935)**.** *Let G be a group and let $N \lhd G$ be a normal subgroup of G. Then*

$$\mu_G(N) = \mu_{G/N}(1).$$

In the case that G is a soluble group, Kratzer and Thévenaz take this idea to its extreme conclusion by relating $\mu_G(H)$ to the complements of factors of a fixed chief series of G [75, Theorem 2.6]. In the case of nilpotent groups specifically, a combination of results due to Weisner [116, Section 3] and Hall [63, Sections 2.7 and 2.8] essentially gives the Möbius function of any nilpotent group. These results seem to have been reproved independently by Kratzer and Thévenaz in [75, Proposition 2.4], generalising the work of Delsarte [31].

Theorem 1.16. *Let G be a nilpotent group and $H \leqslant G$ a subgroup of G.*

1. *If H is not a normal subgroup of G, then $\mu_G(H) = 0$.*

2. *If $H \lhd G$ and G/H is not a product of elementary abelian groups, then $\mu_G(H) = 0$.*

3. *If $H \lhd G$ and*

$$G/H = \prod_{i=1}^{r} C_{p_i}^{n_i}$$

(with p_i prime), then

$$\mu_G(H) = \prod_{i=1}^{r} (-1)^{n_i} p_i^{\binom{n_i}{2}}.$$

Remark 1.17. *Kratzer and Thévenaz cite Rota and Delsarte in their paper, but neither Kratzer and Thévenaz nor Delsarte make mention of the work of Weisner or Hall.*

As well as the lattice of subgroups of a finite group, G, one can also consider the poset of conjugacy classes of subgroups of G with ordering determined as follows. If $[H]$ and $[K]$ are conjugacy classes of subgroup of G we have $[H] \leq [K]$ if and only if K contains a conjugate of H in G. The Möbius function of this poset is usually written $\lambda_G(H)$ and the following result due to Pahlings [90] generalises an earlier result due to Hawkes, Isaacs and Özyadin [66, Theorem 7.2].

Theorem 1.18. *If G is a soluble group and H a subgroup, then*

$$\mu_G(H) = [N_{G'}(H) : H \cap G']\lambda_G(H).$$

Remark 1.19. *As mentioned in [90], it was conjectured by Isaacs that this also holds in the case that G is not soluble, however counterexamples were shown to exist by Bianchi, Mauri and Verardi [15].*

Kratzer and Thévenaz also prove the following result which has implications for the Möbius number of G [75, Theorem 3.1].

Theorem 1.20. *If G is a group and $H \leqslant G$, then*

$$\mu_G(H) \frac{[G : G']_0}{[N_G(H) : H]} \in \mathbb{Z}$$

where, for a positive integer n, n_0 is the largest positive divisor of n without square factors. In particular, $\mu_G(1)$ is a multiple of $|G|/[G : G']_0$.

However, as they point out at the end of their paper: “It results from Theorem 3.1 that $\mu_G(1)$ is a multiple of $|G|$ if G is perfect. For example, $\mu_{A_5}(1) = 60 = |A_5|$, $\mu_{A_6}(1) = 720 = |A_6|$, but $\mu_{L_2(7)}(1) = 0$. Thus, contrary to the case of soluble groups, the behaviour of the Möbius function of simple groups seems more difficult to comprehend.” Their interest in Möbius numbers stems from two sources: idempotents in the Burnside ring and their relation with certain homology groups, however, that is not to say the two are not connected cf. the work of Bouc [17]. We note that the connection between Möbius numbers and Lefschetz numbers is also considered in Shareshian's thesis [101] to which we direct the interested reader, particularly, the reader who does not read French.

The connection to the Burnside ring of a group, G, is related via the table of marks of G, originally introduced by Burnside [19], whose definition [90] we recall.

Definition 1.21. *Let G be a group, let n be the number of conjugacy classes of subgroups of G and fix a set of conjugacy class representatives of subgroups of G $\{H_1 = 1, H_2, \dots, H_n = G\}$ ordered such that $|H_i| \leq |H_j|$ when $i \leq j$. The* ***table of marks of*** *G is the $n \times n$ matrix where the (i, j)-the entry is $|\mathrm{Fix}_{G/H_i}(H_j)|$ where*

$$\mathrm{Fix}_{G/H_i} = \{gH_i \mid g \in G,\, xgH_i = gH_i \text{ for all } x \in H_j\}.$$

As one might expect, there is a deep connection between the Möbius function of G and the table of marks of G [90, 91]. This relationship then extends to properties of the Burnside ring of G for which we direct the interested reader to the aforementioned paper of Kratzer and Thévenaz [75] and Solomon [106]. Their relation to the homology and homotopy comes from considering the lattice of subgroups of a finite group, G, as a simplicial complex. For more on the algebraic topological considerations we direct the reader to the aforementioned papers and the references therein.

1.2.1 Applications of the Eulerian functions of a group

The Eulerian functions of a group are of natural interest to group theorists since they can be used to answer questions of generation of G. However, the scope of this function was first broadened, as far as the author is aware, through the work of Downs and Jones [33–38] in their application of it to other categories. Recall the observation that for a finitely presented group, Γ, the Eulerian function $\phi_\Gamma(G)$ counts the number of epimorphisms from Γ into G. A generating n-tuple of G satisfying the relations of Γ is called a Γ-basis of G and corresponds to a normal subgroup $N \lhd \Gamma$ whose quotient $\Gamma/N \cong G$. Hall shows [63, Theorem 1.4] that since the automorphism group of G acts semiregularly on Γ-bases of G, the number of distinct normal subgroups $N \lhd \Gamma$ whose quotient is isomorphic to G is given by $d_\Gamma(G) = \phi_\Gamma(G)/|\mathrm{Aut}(G)|$.

Following this line of reasoning, Downs and Jones observed that if the normal subgroups of Γ were in one-to-one correspondence with the regular objects of some category, $\mathfrak{K}$, then $d_\Gamma(G)$ could be used to count the number of distinct regular objects in that category whose automorphism group is isomorphic to G. For example, if X is a topological space with covering space $\tilde{X}$ and fundamental group $\pi_1(X) \cong \Gamma$, then d_Γ is the number of distinct regular covers of X having covering group isomorphic to G [37].

One important case is when X is the thrice-punctured Riemann sphere $\mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$ which has $\pi_1(X) \cong F_2$, the free group on 2 generators, and which, through Grothendieck's dessins d'enfants programme [61], is also related to the absolute Galois group. The quantity $d_2(G)$ then counts the number of distinct regular dessins having automorphism group isomorphic to G.

A number of other categories of maps are considered by Downs and Jones in [36]. In addition, Jones uses a partial Möbius function of the small Ree groups to show that they are Hurwitz groups for all $q > 3$ [67]. These were independently proved to be Hurwitz groups for all $q > 3$ originally by Malle [83] using different techniques. In addition to this, Downs and Jones determine Eulerian functions corresponding to Hecke groups, such as the modular group $PSL_2(\mathbb{Z})$, and apply them to the problem of probabilistic generation of groups in [37].

1.2.2 Results

As far as the author is aware, the only families of finite simple groups for which the Möbius function is known are as follows. The Möbius function of the simple groups $L_2(p)$, for $p \geq 5$, were originally determined by Hall [63]. This was extended to the Möbius function of $L_2(q)$ and $PGL_2(q)$, for all prime powers $q \geq 5$, by Downs [33]. Recently, Downs and Jones [38] have determined the Möbius function for the simple Suzuki groups $Sz(2^{2m+1})$, where $m > 0$. It seems natural to then determine the Möbius function of the small Ree groups, $R(q)$, where $q \geq 3$ and the following is our main result of Chapter 3.

Theorem 1.22. *Let $G = R(3^n)$ be a simple small Ree group for a positive odd integer $n > 1$. If $H \leqslant G$, then $\mu_G(H) = 0$ unless H belongs to one of the following classes of subgroups of G.*

Isomorphism type of $H \leqslant G$	*for $h \mid n$ and s.t.*	$[G\colon N_G(H)]$	$\mu_G(H)$
$R(3^h)$	–	$\lvert G\rvert/3^{3h}(3^{3h}+1)(3^h-1)$	$\mu(n/h)$
$3^h+\sqrt{3^{h+1}}+1\colon 6$	–	$\lvert G\rvert/6(3^h+\sqrt{3^{h+1}}+1)$	$-\mu(n/h)$
$3^h-\sqrt{3^{h+1}}+1\colon 6$	$h>1$	$\lvert G\rvert/6(3^h-\sqrt{3^{h+1}}+1)$	$-\mu(n/h)$
$(3^h)^{1+1+1}\colon(3^h-1)$	–	$\lvert G\rvert/3^{3h}(3^h-1)$	$-\mu(n/h)$
$2\times L_2(3^h)$	$h>1$	$\lvert G\rvert/3^h(3^{2h}-1)$	$-\mu(n/h)$
$2\times(3^h\colon \frac{3^h-1}{2})$	$h>1$	$\lvert G\rvert/3^h(3^h-1)$	$\mu(n/h)$
$(2^2\times D_{(3^h+1)/2})\colon 3$	$h>1$	$\lvert G\rvert/6(3^h+1)$	$-\mu(n/h)$
$2^2\times D_{(3^h+1)/2}$	$h>1$	$\lvert G\rvert/6(3^h+1)$	$3\mu(n/h)$
$2\times L_2(3)$	–	$\lvert G\rvert/24$	$-2\mu(n)$
2^3	–	$\lvert G\rvert/168$	$21\mu(n)$

In addition to this we determine the Möbius function for $R(3)$ and use these results to derive a number of Eulerian functions for $R(q)$ which we use to prove a number of results on generation and asymptotic generation of the small Ree groups.

Chapter 2

Beauville groups

In order to determine Beauville structures of either kind for a finite group G we give the following definitions and lemmas which will be integral to our discussions. The following will be key.

Definition 2.1. *Let G be a finite group and let $x, y, z \in G$. A **generating triple** for G is a triple $(x, y, z) \in G \times G \times G$ such that*

1. *$xyz = 1$, and;*
2. *$\langle x, y, z \rangle = G$.*

*The **type** of a generating triple (x, y, z) is the triple $(o(x), o(y), o(z))$ and we define $\nu(x, y) := o(x)o(y)o(xy)$. If in addition we have that*

$$\frac{1}{o(x)} + \frac{1}{o(y)} + \frac{1}{o(z)} < 1,$$

*then we say that (x, y, z) is a **hyperbolic** generating triple for G.*

Remark 2.2. *Bauer, Catanese and Grunewald prove in [6, Proposition 3.2] that, if a group G admits an unmixed Beauville structure $(x_1, y_1; x_2, y_2)$, then the generating triple $(x_i, y_i, (x_i y_i)^{-1})$, for $i = 1, 2$, must be hyperbolic.*

Definition 2.3. *Let G be a group and let (x_i, y_i, z_i) be a generating triple for G for $i = 1, 2$. We call these two triples **equivalent** if there exists an automorphism $g \in Aut(G)$ such that $x_1^g = x_2$, $y_1^g = y_2$ and $z_1^g = z_2$. If a pair of triples for G are not equivalent, they are **inequivalent**.*

Remark 2.4. *We recall from [63] that in order to find a generating triple for G^n, it is sufficient to find n inequivalent generating triples for G.*

We now prove a series of lemmas which will aid us in determining the generation or non-generation of finite groups.

Lemma 2.5. *Let G be a group. If (x, y, z) is a generating triple for G, then so are (y, z, x) and (y, x^y, z).*

Proof. The proof of this follows immediately from the fact that $z = y^{-1}x^{-1}$ and that $x^y = y^{-1}xy$. $\square$

Lemma 2.6. *Let G be a group and let (x, y, z) be a generating triple for G. If $gcd(o(x), o(y)) = 1$, then $((x, y), (y, x^y), (z, z))$ is a generating triple for $G \times G$.*

Proof. By Lemma 2.5, since (x, y, z) is a generating triple for G, then so is (y, x^y, z). Then, since the orders of x and y are coprime, we can generate the elements $(x, 1_G), (y, 1_G), (1_G, y)$ and $(1_G, x^y)$ which generate $G \times G$. $\square$

Remark 2.7. *The proof of the preceding lemma naturally generalises to any subset of elements in a generating set whose orders are mutually coprime.*

More generally we can prove the following.

Lemma 2.8. *Let G be a group and let (x_i, y_i, z_i) be a generating triple for G of type (l_i, m_i, n_i) for $i = 1, 2$. If $\{l_1, m_1, n_1\} \neq \{l_2, m_2, n_2\}$ then (x_1, y_1, z_1) and (x_2, y_2, z_2) are inequivalent generating triples.*

Proof. This follows from the fact that automorphisms preserve the order of an element. $\square$

Structure of the chapter

In Section 2.1 we examine the relationship between an almost simple group and its socle admitting an unmixed Beauville structure. In Section 2.2 we briefly discuss topological invariants of Beauville surfaces which can be recovered from their Beauville structure. In Section 2.3 we generalise the construction due to Bauer, Catanese and Grunewald in [6, Lemma 4.4] of a mixed Beauville structure that arises from a mixable Beauville structure for a perfect group. In Sections 2.4, 2.5 and 2.6 we then determine mixable Beauville structures for various families of characteristically simple groups. The main results of Sections 2.3–2.6 appear in [46].

2.1 Almost simple unmixed Beauville groups

As mentioned in Section 1, Beauville groups are either of unmixed or mixed type. Mixed Beauville groups are treated in a later section, while in this section we deal exclusively with unmixed Beauville structures. As such, any reference in this section to Beauville groups or Beauville structures are understood to mean unmixed Beauville groups and unmixed Beauville structures. We now recall a few necessary definitions.

Definition 2.9. *Let G be a group. A* ***minimal normal subgroup*** *of G is a nontrivial normal subgroup of G which does not contain any proper nontrivial subgroups which are normal in G. The* ***socle*** *of G, $soc(G)$, is the subgroup generated by all minimal normal subgroups of G.*

Definition 2.10. *We say that a group G is* ***almost simple*** *if there exists a non-abelian simple group, H, such that $H \leqslant G \leqslant Aut(H)$.*

We state the following lemma for completeness.

Lemma 2.11. *Let G be a group and let $H < G$. If (x, y, z) is a generating triple for G, then at least two elements of (x, y, z) must come from $G \setminus H$.*

Proof. Without loss of generality, if $x, y \in H$, then $z = (xy)^{-1} \in H$ and so $\langle x, y, z\rangle \leqslant H < G$. It follows that at most one element of (x, y, z) can belong to H. □

In the following sections we exploit properties of the outer automorphism groups of finite simple groups of Lie type to show that their corresponding almost simple groups do not admit unmixed Beauville structures. The outer automorphism groups of the finite simple groups of Lie type can be found in [120] and are summarised in [27, pg. xvi].

2.1.1 Outer automorphism groups that are not 2-generated

A necessary condition for a group, G, to admit a Beauville structure of unmixed type is that G must be 2-generated.

Lemma 2.12. *Let G be finite group and let $N \lhd G$. If G/N is n-generated, then G is m-generated where $m \geq n$.*

Proof. Let G/N be n-generated and for a contradiction suppose that G is m-generated where $m < n$. Let $\{x_1, \ldots, x_m\}$ be a generating set for G. The set $\{x_1N, \ldots, x_mN\}$ is then a generating set for G/N and so G/N is m-generated, a contradiction, hence $m \geq n$. □

Corollary 2.13. *Let G be an almost simple group. If $G/soc(G)$ is not 2-generated, then G does not admit an unmixed Beauville structure.*

In order to show that an almost simple group, G, does not admit an unmixed Beauville structure, by the preceding lemma and corollary it suffices to show that there exists an epimorphic image of $G/\mathrm{soc}(G)$ that is not 2-generated. In particular, in the following we show that the elementary abelian group of order 8 is an epimorphic image of G. It is clear that this group is not 2-generated, but since the Möbius function is the subject of Chapter 3, we point out that the Möbius function of 2^3 can be determined by hand and used to show that $|\mathrm{Epi}(F_2, 2^3)| = 0$, where F_2 is the free group on 2 generators. For a more general result we refer the reader to the discussion in [43, p.55].

Lemma 2.14. *If H is a classical group of type*

1. *$L_n(p^{2f})$ with $n > 3$ even and $p \neq 2$,*
2. *$O^+_{2n}(p^{2f})$ with $n > 4$ even and $p \neq 2$, or,*
3. *$O^+_{2n}(p^{2f})$ with $n > 4$ odd and $p \neq 2$,*

then $Aut(H)$ does not admit an unmixed Beauville structure.

Proof. If H is as in case (1), then $\mathrm{Out}(H) \cong 2f \times D_{2d}$ [120, Theorem 3.2] where $d = \gcd(n+1, p^{2f}-1)$. If n and p are odd, then d is even and $\mathrm{Out}(H)$ contains a normal subgroup of shape $f \times \frac{d}{2}$ whose quotient is isomorphic to 2^3, which is not 2-generated. By Lemma 2.12, since since 2^3 is not 2-generated, neither is $\mathrm{Out}(H)$ nor $\mathrm{Aut}(H)$.

If H is as in cases (2) or (3), $\mathrm{Out}(H) \cong 2f \times D_8$ [120, p.75] and contains a normal subgroup of shape $f \times 2 \cong f \times Z(D_8)$ whose quotient is isomorphic to 2^3. As in case (1), this implies that $\mathrm{Aut}(H)$ is not 2-generated. $\square$

Remark 2.15. *After obtaining this result the author was made aware of the work of Dalla Volta and Lucchini where they prove this result along with the converse [30, Corollary on p. 195]. Namely, they show that if an almost simple group is* 3*-generated, then its socle must be isomorphic to one of the groups listed in Lemma 2.14.*

2.1.2 Non-split extensions

As discussed in Section 1.1, the determination of which alternating and symmetric groups admit unmixed Beauville structures is due to Bauer, Catanese and Grunewald [6, 7] and independently by Fuertes and González-Diez in [49], apart from the errors discussed in Chapter 1. The automorphism groups of the alternating groups A_n when $n \geq 4$ are given in [120, Section 2.4.1] and with the exception of A_6 we have $\mathrm{Aut}(A_n) \cong S_n$ and $\mathrm{Out}(A_n) \cong C_2$. For completeness we mention the smallest nontrivial alternating group is $A_3 \cong C_3$ for which $\mathrm{Aut}(A_3) \cong \mathrm{Out}(A_3) \cong C_2$. In the case of A_6 there is an exceptional outer automorphism and $\mathrm{Out}(A_6)$ is isomorphic to the Klein four-group, see [27, p. 4] and the discussion in [120, Section 2.4.2], with full automorphism group isomorphic to $P\Gamma L_2(9)$. This can be seen from the exceptional isomorphism between A_6 and $L_2(9)$ [120, p.52], however this exceptional isomorphism is just as non-obvious. This gives us the following three non-conjugate maximal normal subgroups of $P\Gamma L_2(9)$ with socle isomorphic to A_6:

- the symmetric group $S_6 \cong P\Sigma L_2(9)$;
- the projective general linear group $PGL_2(9)$, and;
- the non-split extension $L_2(9)^{\cdot}2$, isomorphic to the Mathieu group M_{10}.

As also previously mentioned, it is known from the work of Garion [53] that $PGL_2(q)$ is an unmixed Beauville group for $q \geq 5$; but what about M_{10} and the general case of the non-split extension of $L_2(p^{2n})^{\cdot}2$ for $p \neq 2$ and $n \geq 1$? The following lemma is necessary.

Lemma 2.16. *Let $G = L_2(p^{2n})^{\cdot}2$ for $p \neq 2$ and $n \geq 1$. If $g \in G$ is an involution, then $g \in soc(G)$.*

Proof. Let $N = \mathrm{soc}(G)$ and $g \in G \setminus N$ be an outer automorphism of N. Note that g is the composition of a field automorphism of order 2 and a diagonal automorphism. If g is an involution, then conjugation by g is equivalent to conjugation by the square of an element in $PGL_2(p^{2n})$. Since the square of an element in $PGL_2(p^{2n})$ belongs to N, $g \in N$. $\square$

Lemma 2.17. *If $G = L_2(p^{2n})^{\cdot}2$ for $p \neq 2$ and $n \geq 1$, then G does not admit an unmixed Beauville structure.*

Proof. Let (x, y, z) be a generating triple for G. By Lemmas 2.5 and 2.11 we can suppose without loss of generality that $x \in G \setminus L_2(p^{2n})$. Since x has even order, some power of x belongs to the unique conjugacy class of involutions in G. Hence G cannot admit an unmixed Beauville structure. $\square$

Remark 2.18. *In the case where $p = 2$ the only non-trivial outer automorphisms of $L_2(2^n)$, where $n \geq 1$ is either odd or even, come from the field automorphisms. As such, any almost simple group, G, with socle isomorphic to $L_2(2^n)$ is isomorphic to the semi-direct product $L_2(2^n){:}\,m$, with m dividing n. Thus, when m is even there exist involutions in $G \backslash soc(G)$ and hence we cannot extend the preceding lemmas in this section to the case $p = 2$. We discuss the case when m is odd in the following section.*

Corollary 2.19. *The Mathieu group M_{10} does not admit an unmixed Beauville structure.*

We can extend this to show that for $L_2(p^{2n})^{\cdot}2^2$ for $p \neq 2$ is not an unmixed Beauville group.

Lemma 2.20. *If $\Gamma = L_2(p^{2n})^{\cdot}2^2$ where $p \neq 2$ and $n \geq 1$, then Γ does not admit an unmixed Beauville structure.*

Proof. We suggestively denote the normal subgroups of Γ as follows. Let $L \cong L_2(p^{2n})$, $G \cong PGL_2(p^{2n})$, $\Sigma \cong L_2(p^{2n}){:}\,2 \leqslant P\Sigma L_2(p^{2n})$ and $M \cong L_2(p^{2n})^{\cdot}2$. By Lemma 2.11 at least two elements of any generating triple for Γ must come from $\Gamma \setminus L$. A similar argument applies to each of G, Σ and M. By Lemma 2.5, if (x, y, z) is a generating triple for Γ, then we can assume $x \in G \setminus L$, $y \in \Sigma \setminus L$ and $z \in M \setminus L$. Finally, by Lemma 2.16, since $z \in M \setminus L$, then some power of z belongs to the unique conjugacy class of involutions in L, hence Γ cannot admit an unmixed Beauville structure. $\square$

Remark 2.21. *The preceding lemmas exploit the combination of all involutions being conjugate in $L_2(q)$ and there not existing involutions outside of the socle of $L_2(p^{2n})^{\cdot}2$. In general this situation does not occur elsewhere with other finite simple groups of Lie type. For instance, the outer automorphism group of $L_3(9)$ is the Klein four-group, but each of the three maximal normal subgroups of $P\Gamma L_3(9)$ are split extensions by a cyclic group of order 2 and contain involutions outside of the socle [27, p. 78].*

Remark 2.22. *There appears to be little in the literature on the non-split extension of $L_2(p^{2n})$, where $p \neq 2$. Gardiner, Praeger and Zhou describe them in detail in [52, Section 2] and also prove that they act 3-transitively on their natural permutation representation of degree $q+1$ [52, Theorem 2.1]. The first appearance in the literature of their maximal subgroups appears to be due to Giudici in [56].*

2.1.3 Split extensions

Lemma 2.23. *Let $G = H\colon f$ be an almost simple group with soc$(G) = H$, $f \cong Out(H)$ and $f > 1$ a positive integer. If the order of H is coprime to f, then G does not admit an unmixed Beauville structure.*

Proof. In order to generate G, at least two elements must come from outside of H by Lemma 2.11 and must generate $\mathrm{Out}(H)$. Since cyclic subgroups of prime order dividing f are conjugate in G by Sylow's theorems, G does not admit an unmixed Beauville structure. □

Remark 2.24. *A more general result of the preceding lemma and its proof are due to unpublished works of Magaard.*

For the families of finite simple groups of Lie type without graph automorphisms, it is possible to isolate cases of cyclic outer automorphism groups and make the following easy corollary.

Corollary 2.25. *Let H be a finite simple group of Lie type isomorphic to $L_2(2^f)$; $O_{2n+1}(2^f) \cong S_n(2^f)$ where $n \geq 3$; $E_7(2^f)$; $E_8(p^f)$ for all $p \geq 2$; $F_4(p^f)$, where $p \neq 2$, or; $G_2(p^f)$, where $p \neq 3$. If $f > 1$ is coprime to $|H|$ and G is such that $H < G \leqslant Aut(H)$, then G does not admit an unmixed Beauville structure.*

Proof. In each case $\mathrm{Out}(H)$ consists only of field automorphisms and is cyclic of order f. □

If in addition the type and characteristic of H are specified, it is straightforward to write down such an f immediately. For example, since the order of a Suzuki group $Sz(2^{2m+1})$ is always coprime to 3, the order of a small Ree group $R(3^{2m+1})$ is always coprime to 5 and the order of a large Ree group ${}^2F_4(2^{2m+1})$ is always coprime to 17, we have the following corollary.

Corollary 2.26. *Let G be an almost simple group and $n \geq 1$. Suppose one of the following holds:*

1. *the order of G is divisible by 3 and soc(G) is isomorphic to the Suzuki group $Sz(2^{3n})$,*
2. *the order of G is divisible by 5 and soc(G) is isomorphic to the small Ree group $R(3^{5n})$, or;*
3. *the order of G is divisible by 17 and soc(G) is isomorphic to the large Ree group ${}^2F_4(2^{17n})$.*

Then G does not admit an unmixed Beauville structure.

Remark 2.27. *We cannot extend this corollary to general automorphism groups of simple Suzuki, small Ree or large Ree groups since, for example, $Sz(2^5)\colon 5$ is an unmixed Beauville group.*

Remark 2.28. *In the previous section we mention in Remark 2.18 that $L_2(p^n)\colon m$ does not admit an unmixed Beauville structure when m is even and divides n. In the case that m is odd and coprime to $|L_2(p^{2n})|$ we can apply Lemma 2.23 to show that $L_2(2^n)\colon m$ does not admit an unmixed Beauville structure when $m > 1$.*

Lemma 2.29. *Let $G = P\Gamma L_2(p^p)$ where $p \neq 2$. Then G does not admit an unmixed Beauville structure.*

Proof. Let $H = \mathrm{soc}(G) \cong L_2(p^p)$. In order to generate G it is necessary to generate $\mathrm{Out}(H) \cong 2p$, hence some element of a generating triple (x, y, z) must project onto an element of order p in $\mathrm{Out}(H)$. By Lemma 2.5, we can assume that x is such an element, so that p divides $o(x)$. If $x_1, x_2 \in G \setminus H$ are elements of order p, then there exists $g \in G$ and $1 \leq i \leq p-1$ such that $(x_1^i)^g = x_2$. Therefore, there cannot exist an unmixed Beauville structure for G. □

2.1.4 Examples

We conclude this section by determining unmixed Beauville structures for non-simple almost simple groups whose socle is isomorphic to one of the sporadic groups or the Tits group. For each of these groups we present in Table 2.1 words in their standard generators which can be checked in GAP [111] to generate each group. That they are also unmixed Beauville structures can also be checked in GAP, or from their character tables in [27].

Lemma 2.30. *Let H be of one of the* 12 *sporadic groups with nontrivial outer automorphism group or the Tits group, ${}^2F_4(2)'$. If $G = Aut(H)$, then G admits an unmixed Beauville structure.*

Proof. Of the 26 sporadic groups, those which admit non-trivial outer automorphisms are as follows: the Mathieu groups M_{12}, M_{22}; the Janko groups J_2, J_3; HS; M^cL; He; Suz; $O'N$; HN; and the Fischer groups Fi_{22}, Fi_{24}'. In Table 2.1 we present words in the standard generators which provide generating triples for the groups listed. In addition to their type we record the conjugacy classes to which these elements belong, as given in [27]. In Table 2.2 we record the prime power maps of elements in each generating triple from which it can be checked that such generating triples admit an unmixed Beauville structure.

It can be quickly checked in GAP that the generating triples given for $M_{12}\!:\!2$, $M_{22}\!:\!2$, $J_2\!:\!2$, ${}^2F_2(2)'.2$, $HS\!:\!2$, $J_3\!:\!2$, $M^cL\!:\!2$, $He\!:\!2$, $Suz\!:\!2$ and $Fi_{22}\!:\!2$ generate their respective groups, and that the elements have centraliser order as given in the table. It remains to prove generation of $O'N\!:\!2$, $HN\!:\!2$ and $Fi_{24}'\!:\!2$. From the list of maximal subgroups of $O'N\!:\!2$ we see that the only subgroups containing elements of order 31 are isomorphic to $O'N$ or $31\!:\!30$, neither of which contain elements of order 22, and the only subgroups containing elements of order 19 are isomorphic to $O'N$ or $J_1 \times 2$, neither of which contain elements of order 56. From the list of maximal subgroups of $HN\!:\!2$ we see the only subgroups containing elements of order 19 are isomorphic to HN or $U_3(8)\!:\!6$, neither of which contain elements of order 42, and the only subgroups containing elements of order 11 are isomorphic to HN, S_{12} or $4^{\cdot}HS\!:\!2$, none of which contains elements of order 44. Generation by the elements x_1, y_1 for $Fi_{24}'\!:\!2$ can be checked in GAP in a reasonable amount of time and from the list of maximal subgroups of $Fi_{24}'\!:\!2$ we have that the only subgroups that contain elements of order 29 are isomorphic to Fi_{24}' or $29\!:\!28$, neither of which contains elements of order 54.

To check that $g \in \{x_i, y_i, x_iy_i\}$ for $i = 1, 2$ in each case belongs to the stated conjugacy class, either there is an unambiguous choice for elements of order $o(g)$, or the order of $C_G(g^n)$ for some $n \geq 1$ can be computed in GAP in a reasonable amount of time. This completes the proof. $\square$

G	x_1	y_1	x_2	y_2	Type
$M_{12}:2$	cd	dc	$(cd)^3d$	$(x_2^3)^d$	$(12A, 12A, 3A; 10BC, 10BC, 8AB)$
$M_{22}:2$	d	d^c	$(cd)^2d$	$(x_2^2)^c$	$(4C, 4C, 11AB; 10A, 5A, 14AB)$
$J_2:2$	c	d	dcd	$(x_2^3)^c$	$(2C, 5AB, 14A; 24AB, 8B, 8A)$
${}^2F_2(2)'.2$	d	d^c	$(cd)^2d$	$(x_2)^d$	$(4F, 4F, 6A; 16EF, 16EF, 16AD)$
$HS:2$	c	d	$(cd)^2c$	$(x_2)^{dd}$	$(2C, 5C, 30A; 20DE, 20DE, 8A)$
$J_3:2$	c	$((cd)^3d)^{cdd}$	cd	dc	$(2B, 34AB, 9AC; 24AB, 24AB, 3A)$
$M^cL:2$	cd	dc	$cd((cd)^2d)^3$	$(x_2)^d$	$(22AB, 22AB, 3B; 20AB, 20AB, 15AB)$
$He:2$	c	cd^2cd	d	d^c	$(2B, 16AB, 16AB; 6C, 6C, 15A)$
$Suz:2$	c	d	$cd^2(cd)^4$	$(x_2)^{cdc}$	$(2C, 3B, 28A; 24F, 24F, 13AB)$
$O'N:2$	c	dc	$cd(dc)^2d^2$	$(x_2^5)^c$	$(2B, 22A, 31AB; 56AD, 56AD, 19AC)$
$Fi_{22}:2$	c	$(cd)^5dcd$	d	d^c	$(2A, 8H, 18H; 18E, 18E, 21A)$
$HN:2$	cd	$((cd)^5)^{dd}$	$d^2(cd)^8dc$	$(x_2)^c$	$(42A, 42A, 19AB; 44AB, 44AB, 11A)$
$Fi_{24}':2$	$d(dc)^4$	$(d(dc)^4)^c$	cd^3cd^2	$(x_2)^c$	$(28CD, 28CD, 35A; 54A, 54A, 29AB)$

Table 2.1: Words in the standard generators for the automorphism groups of the sporadic groups and the Tits group.

Remark 2.31. *It has subsequently been shown in [43] that the non-simple almost simple sporadic groups (but not ${}^2F_4(2)$) admit a strongly real Beauville structure, a slightly stronger condition.*

2.2 Topological invariants of Beauville surfaces

Catanese's original remark that "Classifying all the Beauville surfaces is then a problem in group theory" extends not just to Beauville surfaces themselves, but to their topological invariants as well. Although we are largely concerned with the group-theoretic properties of Beauville groups, any discussion would be incomplete without consideration of the geometric and topological properties of the surfaces to which they give rise. Here we determine a number of topological invariants which can easily be determined from their Beauville structure.

Since many of these invariants are defined as dimensions of certain homology or cohomology rings of various sheaves and divisors we make no attempt to define them here. Definitions can be found in any standard text on the subject, such as [11] or [65]. Throughout we let $\mathscr{S} = (\mathscr{C}_1 \times \mathscr{C}_2)/G$ be a Beauville surface of either unmixed or mixed type and for $i = 1, 2$ let (x_i, y_i, z_i) be a generating triple for G of type (l_i, m_i, n_i) which admits such a construction as necessary.

G	Prime classes of $g \in \sum(x_1, y_1)$	Prime classes of $g \in \sum(x_2, y_2)$
$M_{12}:2$	$2A, 3A, 3B$	$2B, 2C, 5A$
$M_{22}:2$	$2A, 11A, 11B$	$2B, 2C, 5A, 7A, 7B$
$J_2:2$	$2C, 5A, 5B, 7A$	$2A, 3A$
${}^2F_2(2)'.2$	$2B, 3A$	$2A$
$HS:2$	$2C, 3A, 5B, 5C$	$2A, 5A$
$J_3:2$	$2B, 3B, 17A, 17B$	$2A, 3A$
$M^cL:2$	$2B, 3B, 11A, 11B$	$2A, 3A, 5A$
$He:2$	$2B$	$2C, 3A, 5A$
$Suz:2$	$2B, 2C, 3B, 7A$	$2A, 3A, 13A, 13B$
$O'N:2$	$2B, 11A, 31A, 31B$	$2A, 7A, 19A, 19B, 19C$
$Fi_{22}:2$	$2A, 2C, 2E, 3D$	$2D, 3A, 3B, 7A$
$HN:2$	$2C, 3A, 7A, 19A, 19B$	$2A, 11A$
$Fi_{24}':2$	$2B, 5A, 7A, 7B$	$2C, 3B, 29A, 29B$

Table 2.2: Power maps for elements of generating triples in Table 2.1.

One of the most fundamental topological invariants of a curve $\mathscr{C}$ is its genus $g(\mathscr{C})$. Given our Beauville surface $\mathscr{S} = (\mathscr{C}_1 \times \mathscr{C}_2)/G$, the genus $g_i = g(\mathscr{C}_i)$ for $i = 1, 2$ can be determined from the Riemann–Hurwitz formula [50, Section 2] and is given by

$$2g_i - 2 = |G| \left(1 - \left(\frac{1}{l_i} + \frac{1}{m_i} + \frac{1}{n_i}\right)\right).$$

The Euler–Poincaré characteristic $\chi(\mathscr{S})$ can then be determined, in turn giving the Euler number $e(\mathscr{S})$ and the self-intersection number $K^2_{\mathscr{S}}$ of $\mathscr{S}$ as follows [20, Theorem 3.4]

$$\chi(\mathscr{S}) = \frac{e(\mathscr{S})}{4} = \frac{K^2_{\mathscr{S}}}{8} = \frac{(g_1 - 1)(g_2 - 1)}{|G|}.$$

The irregularity q of any Beauville surface is known to be 0 [3, Section 2] and from this the geometric genus p_g of $\mathscr{S}$ can be determined and is given by [50, Section 4]

$$1 - q + p_g = \chi(\mathscr{S}).$$

Remark 2.32. *We make mention here of the fact that several Beauville surfaces provide examples of fake quadrics, roughly a surface whose Betti numbers are the same as $\mathbb{P}^1(\mathbb{C}) \times \mathbb{P}^1(\mathbb{C})$ and have geometric genus $p_g = 0$ [107, Section 7]. The classification of Beauville surfaces that are also fake quadrics was completed by Bauer, Catanese and Grunewald in [8, Sections 3 and 4]. The corresponding groups are the unmixed Beauville group 5^2 and the two mixed Beauville groups of order*

256*, which are described in detail in the same article.*

The genus spectrum of a Beauville group, G, of either unmixed or mixed type was introduced by Fuertes, González-Diez and Jaikin-Zapirain in [50] from which we take the following definition.

Definition 2.33. *Let G be a finite group. Denote by* $\mathrm{Spec}(G)$ *the set of pairs of integers* (g_1, g_2) *such that* $g_1 \leq g_2$ *and there exist curves* $\mathscr{C}_1, \mathscr{C}_2$ *with* $g(\mathscr{C}_i) = g_i$ *for* $i = 1, 2$ *which admit an action of* G *such that* $\mathscr{S} = (\mathscr{C}_1 \times \mathscr{C}_2)/G$ *is a Beauville surface.*

The authors of [50] also determine theoretically $\mathrm{Spec}(G)$ for $L_2(7)$, S_5 and all abelian unmixed Beauville groups [50, Section 4]. However, they mention that a similar theoretical determination of $\mathrm{Spec}(G)$ for general G "will take too long to be included here". From results of Garion [53, Theorems D and E] it is also possible to recover $\mathrm{Spec}(G)$ for $L_2(q)$ where $q \geq 7$ and $PGL_2(q)$ where $q \geq 5$.

It is not too hard to see that $\mathrm{Spec}(G)$ is always finite. The authors of [50] make the observation that $g_i \leq 1 + \frac{|G|}{2}$ by the Riemann–Hurwitz formula and also show [50, Theorem 9] that $g_i \geq 6$. This bounds the size of $\mathrm{Spec}(G)$ by

$$|\mathrm{Spec}(G)| \leq \min\left\{\frac{(|G|-5)^2}{8}, \frac{d_2(G)^2}{2}\right\}$$

where $d_2(G)$ is the number of inequivalent generating pairs for G which is also finite.

It is possible to write a computer program to determine $\mathrm{Spec}(G)$. In Appendix A we include such a program for determining the genus spectrum of an unmixed Beauville group along with the genus spectrum for various simple and almost simple groups, G, in the case where $\mathrm{Spec}(G)$ is of a modest size. For reference, we mention that it was possible to determine $\mathrm{Spec}(G)$ for the Mathieu group M_{23}, where $|G| = 10,200,960$, in approximately 94 hours of computer time. The computer in question uses an Intel i5/2.7GHz processor with 8GB of RAM. Since $|\mathrm{Spec}(M_{23})| = 2518$ we do not present its genus spectrum in this thesis but the author can provide, on request, $\mathrm{Spec}(G)$ where G is isomorphic to: the alternating group A_n for $6 \leq n \leq 10$; the symmetric group S_n for $6 \leq n \leq 10$; the linear groups $L_2(16){:}2$, $P\Sigma L_2(25)$, $P\Sigma L_2(27)$, $L_3(3)$, $P\Gamma L_3(3)$, $L_3(4)$, or $P\Gamma L_2(q)$ where $q \in \{7, 8, 11, 13, 16, 17, 19, 23, 29\}$; the unitary groups $U_3(3)$, $U_3(4)$, $U_4(2)$ as well as $U_3(3){:}2$; the Suzuki group $Sz(8)$; the Mathieu groups M_{11}, M_{12}, M_{22}, M_{23} as well as $M_{12}{:}2$ and $M_{22}{:}2$; or the Janko groups J_1 and J_2.

2.3 Mixed Beauville groups via mixable Beauville structures

Throughout this section we may refer to a mixed Beauville group or a mixed Beauville structure as simply a Beauville structure. The examples we eventually construct will require the definition of a perfect group, which we recall here, along with that of a mixed Beauville group as given by Bauer, Catanese and Grunewald in [6, Definition 4.1].

Definition 2.34. *Let G be a group. The* ***derived subgroup*** *of G, denoted G', is the subgroup of G generated by all commutators in G. A group is* ***perfect*** *if it equals its derived subgroup.*

Definition 2.35. *Let G be a finite group and let $x, y \in G$. A* ***mixed Beauville quadruple*** *for G is a quadruple $(G^0; x, y; g)$ consisting of a subgroup G^0 of index 2 in G; of elements $x, y \in G^0$ and of an element $g \in G$ such that*

M1 G^0 *is generated by x and y;*

M2 $g \notin G^0$;

M3 *for every $\gamma \in G^0$ we have that $(g\gamma)^2 \notin \Sigma(x, y)$ and*

M4 $\Sigma(x, y) \cap \Sigma(x^g, y^g) = \{1\}$.

If G has a mixed Beauville quadruple we say that G is a ***mixed Beauville group*** *and call $(G^0; x, y; g)$ a* ***mixed Beauville structure*** *for G.*

Remark 2.36. *The motivation for this definition is akin to that described in Remark 1.5. The subgroup G^0 consists of the elements of G which do not interchange the two curves, while conditions $M3$. and $M4$. are those which ensure a free action of G on the product [6, Section 4].*

In order to construct examples of mixed Beauville groups, Bauer, Catanese and Grunewald proved the following [6, Lemma 4.5].

Lemma 2.37. *Let H be a perfect finite group and let $x_1, y_1, x_2, y_2 \in H$. Assume that*

1. *$o(x_1)$ and $o(y_1)$ are even;*
2. *$\langle x_1, y_1 \rangle = H$;*
3. *$\langle x_2, y_2 \rangle = H$;*
4. *$\nu(x_1, y_1)$ is coprime to $\nu(x_2, y_2)$.*

Set $G := (H \times H) : \langle g \rangle$ where g is an element of order 4 that acts by interchanging the two factors; $G^0 = H \times H \times \langle g^2 \rangle$; $x := (x_1, x_2, g^2)$ and $y := (y_1, y_2, g^2)$. Then $(G^0; x, y; g)$ is a mixed Beauville structure for G.

Remark 2.38. *Bauer, Catanese and Grunewald actually proved a similar result for any finite group, H, but stronger conditions on x_1 and y_1 are needed when H is not perfect.*

From this we make the following definition.

Definition 2.39. *Let H be a perfect group. If there exists $x_1, y_1, x_2, y_2 \in H$ such that*

1. *$o(x_1)$ and $o(y_1)$ are even;*
2. *$\langle x_1, y_1 \rangle = \langle x_2, y_2 \rangle = H$, and;*

3. $\nu(x_1, y_1)$ *is coprime to* $\nu(x_2, y_2)$,

then we say that H *is a* ***mixable Beauville group*** *and that* $(x_1, y_1; x_2, y_2)$ *is a* ***mixable Beauville structure*** *for* H *of* ***type*** $(o(x_1), o(y_1), o(x_1y_1); o(x_2), o(y_2), o(x_2y_2))$. *We say that* $(x_1, y_1, (x_1y_1)^{-1})$ *is an* ***even triple*** *for* H *and that* $(x_2, y_2, (x_2y_2)^{-1})$ *is an* ***odd triple*** *for* H.

In order to generalise Lemma 2.37 we recall the following. For a positive integer k let Q_{4k} be the dicyclic group of order $4k$ with presentation

$$Q_{4k} = \langle p, q \mid p^{2k} = q^4 = 1, p^q = p^{-1}, p^k = q^2 \rangle.$$

Let $G = (H \times H) : Q_{4k}$ with the action of Q_{4k} defined as follows. For $(g_1, g_2) \in H \times H$ let $(g_1, g_2)^p = (g_1, g_2)$ and $(g_1, g_2)^q = (g_2, g_1)$. Then $G^0 = H \times H \times \langle p \rangle$ is a subgroup of index 2 inside G.

Theorem 2.40. *Let* H *be a perfect finite group and let* $x_1, y_1, x_2, y_2 \in H$. *Assume that*

1. $(x_1, y_1, (x_1y_1)^{-1})$ *is an even triple for* H*;*

2. $(x_2, y_2, (x_2y_2)^{-1})$ *is an odd triple for* H*, and;*

3. $(x_1, y_1; x_2, y_2)$ *is a mixable Beauville structure for* H.

Set $k > 1$ *to be any integer that divides gcd*$(o(x_1), o(y_1)), G := (H \times H) : Q_{4k}$ *with the action defined above,* $G^0 := H \times H \times \langle p \rangle$*,* x*:=*(x_1, x_2, p) *and* $y := (y_1, y_2, p^{-1})$. *Then* $(G^0; x, y; q)$ *is a mixed Beauville structure for* G.

Proof. We verify that the conditions of Definition 2.35 are satisfied. Since k divides $\nu(x_1, y_1)$ it is coprime to $\nu(x_2, y_2)$ so we can generate the elements $(1, x_2, 1)$ and $(1, y_2, 1)$ allowing us to generate the second factor. We can then produce the elements $x' = (x_1, 1, p)$ and $y' = (y_1, 1, p^{-1})$ allowing us to generate, since H is perfect, the first factor. Since we can generate $H \times H$ we can also generate the third factor, hence we satisfy condition $M1$.

Now let $g \in G \setminus G^0$ and $\gamma \in G^0$. Then $g\gamma$ is of the form $(h_1, h_2, q^i p^j)$ for some $h_1, h_2 \in H$, $i = 1, 3$ and $1 \leq j \leq 2k$. Then

$$(g\gamma)^2 = (h_1h_2, h_2h_1, (q^ip^j)^2) = (h_1h_2, h_2h_1, p^k).$$

For a contradiction, suppose that $(g\gamma)^2 \in \Sigma(x, y)$. Then since h_1h_2 has the same order as h_2h_1 condition 4 implies that $(g\gamma)^2 = (1, 1, p^k) \in \Sigma(x, y)$ if and only if k does not divide $o(x)$ or k does not divide $o(y)$. Note that if $(g\gamma)^2$ were a power of xy by construction it would be 1_G. Since by hypothesis k divides $\gcd(o(x_1), o(y_1))$ we satisfy conditions $M2$ and $M3$.

Finally, to show that condition $M4$ is satisfied, suppose $g' \in \Sigma(x, y) \cap \Sigma(x^g, y^g)$ for $g \in G \setminus G^0$. Since conjugation by such an element g interchanges the first two factors of any element, we again have from condition 4 that g' is of the form $(1, 1, p^i)$ for some power of p, but from our previous remarks it is clear that $p^i = 1_H$ and so $g' = 1_G$. $\square$

Remark 2.41. *The proof of Theorem 2.40 is also a generalisation of the proof of Lemma 2.37. In our proof we chose* $x := (x_1, x_2, p)$ *and* $y := (y_1, y_2, p^{-1})$ *but in principle we could have chosen the third factor of* x *or* y *to be* 1 *and the third factor in their product* xy *to be* p *or* p^{-1} *as appropriate. If we then require* k *to divide* $gcd(o(x), o(xy))$ *or* $gcd(o(xy), o(y))$ *as necessary this gives rise to further examples of mixed Beauville groups.*

Remark 2.42. *Any mixable Beauville group is automatically an unmixed Beauville group and gives rise to a mixed Beauville group by Lemma 2.37.*

In the remaining sections of this chapter we determine mixable Beauville structures for various families of perfect groups. In particular, we consider families of characteristically simple groups whose definition, and important characterisation in the finite case, we state for completeness.

Definition 2.43. *A* ***characteristic subgroup*** *of* G *is a subgroup* $H \leqslant G$ *such that* $H^g = H$ *for all* $g \in Aut(G)$*. A group* G *is* ***characteristically simple*** *if it has no proper nontrivial characteristic subgroups. A finite group is characteristically simple if and only if it is a direct product of isomorphic simple groups [97, p. 85].*

The study of unmixed Beauville structures for such groups was initiated by Jones in [70, 71].

2.4 Mixable Beauville structures for the alternating groups

We always consider A_n, the alternating group of degree n, under its natural permutation representation of degree n. We make heavy use of the following theorem due to Jordan.

Theorem 2.44 (Jordan)**.** *Let* G *be a primitive permutation group of finite degree* n*, containing a cycle of prime length fixing at least three points. Then* $G \geqslant A_n$*.*

Remark 2.45. *A recent extension of this result due to Jones, along with a brief history of this result, can be found in [69].*

We recall that 2-transitivity implies primitivity and in general aim to show 2-transitivity towards proving generation.

Lemma 2.46. *The alternating group* A_6 *and* $A_6 \times A_6$ *are mixable.*

Proof. For our even triples we take the following elements of A_6

$$x_1 = (1,2)(3,4,5,6), \quad y_1 = (1,5,6,4)(2,3), \quad y_1' = (1,5,6).$$

It can easily be checked in GAP that $\langle x_1, y_1 \rangle = A_6$ and these elements provide an even triple of type $(4,4,4)$ for A_6. Similarly, $\langle x_1, y_1' \rangle = A_6$, yielding a triple of type $(4,4,3)$, and the elements $(x_1, x_1), (y_1, y_1') \in A_6 \times A_6$ form an even triple of type $(4,4,12)$ for $A_6 \times A_6$.

For our odd triples let

$$x_2 = (1,2,3,4,5), \quad y_2 = x_2^{(1,3,6)} = (2,6,4,5,3), \quad y_2' = x_2^{(1,2,3,4,6)} = (2,3,4,6,5).$$

It can similarly be checked that $\langle x_2, y_2\rangle = \langle x_2, y_2'\rangle = A_6$ and these elements provide in a similar way odd triples for A_6 and $A_6 \times A_6$ both of type $(5,5,5)$. We then have a mixable Beauville structure of type $(4,4,4;5,5,5)$ for A_6 and of type $(4,12,12;5,5,5)$ for $A_6 \times A_6$. $\square$

Lemma 2.47. *The alternating group A_7 and $A_7 \times A_7$ are mixable.*

Proof. For our even triples we take the following elements of A_7

$$\begin{aligned} x_1 =& (1,2)(3,4)(5,6,7), \quad y_1 = (1,2,3)(4,5)(6,7), \\ x_1' =& (1,6)(2,4,5)(3,7), \quad y_1' = (1,6,2)(3,7,4). \end{aligned}$$

It can easily be checked in GAP that x_1, y_1 provide an even triple for A_7 of type $(6,6,5)$ and that $(x_1, x_1'), (y_1, y_1')$ provide an even triple for $A_7 \times A_7$ of type $(6,6,5)$.

For our odd triples let

$$x_2 = (1,2,3,4,5,6,7), \quad y_2 = x_2^{(1,2,3)} = (1,4,5,6,7,2,3), \quad y_2' = x_2^{(1,3,2)} = (1,2,4,5,6,7,2).$$

Again, it can be checked that x_2, y_2 provide an odd triple of type $(7,7,7)$ for A_7 and that $(x_2, x_2), (y_2, y_2')$ provide an odd triple also of type $(7,7,7)$ for $A_7 \times A_7$. We then have mixable Beauville structures for A_7 and $A_7 \times A_7$ both of type $(6,6,5;7,7,7)$. $\square$

Lemma 2.48. *The alternating group A_{2m} and $A_{2m} \times A_{2m}$ are mixable for $m \geq 4$.*

Proof. For $m \geq 4$ let $G = A_{2m}$ and consider the following elements of G

$$\begin{aligned} x_1 &= (1,2)(3,\dots,2m), \\ y_1 &= x_1^{(1,3,4)} = (1,5,6,\dots,2m,4)(2,3), \\ x_1 y_1 &= (1,3)(2,5,7,\dots,2m-3,2m-1,4,6,8,\dots,2m). \end{aligned}$$

The subgroup $H_1 = \langle x_1, y_1\rangle$ is visibly transitive and the elements

$$x_1^2 = (3,5,\dots,2m-1)(4,6,\dots,2m), \quad y_1^2 = (1,6,8,\dots,2m)(5,7,\dots,2m-1,4),$$

fix the point 2 and act transitively on the remaining points. Finally, $x_1^2 y_1^{-2} = (1,2m,2m-1,3,4)$ is a cycle of length 5, which is prime, fixing at least three points for all m and so by Jordan's Theorem $H_1 = G$. This gives us our first even triple for G of type $(2m-2, 2m-2, 2m-2)$. For our second, we show that there is a similar even triple which is inequivalent to the first under the action of

$\mathrm{Aut}(G) = S_{2m}$. Consider the elements

$$x_1' = (1,2)(3,\dots,2m),$$
$$y_1' = x_1'^{(1,4,3)} = (1,3,5,6,\dots,2m)(2,4),$$
$$x_1'y_1' = (1,4,6,\dots,2m,5,7,\dots,2m-1)(2,3)$$

and note that $x_1' = x_1$. For the same argument as before we have that $\langle x_1', y_1' \rangle = G$. Now suppose that (x_1, y_1, x_1y_1) is equivalent to $(x_1', y_1', x_1'y_1')$ for some $g \in \mathrm{Aut}(G)$. This gives the equalities $\langle x_1^2, y_1^2 \rangle^g = \langle x_1'^2, y_1'^2 \rangle$ and $\langle x_1^2, (x_1y_1)^2 \rangle^g = \langle x_1'^2, (x_1'y_1')^2 \rangle$. From our previous arguments the first equality implies that $g\colon 2 \mapsto 2$, while the second equality implies that $g\colon 1 \mapsto 2$, a contradiction. Hence these two even triples are inequivalent under the action of the automorphism group of G and so $(x_1, x_1'), (y_1, y_1')$ provide an even triple for $G \times G$ of type $(2m-2, 2m-2, 2m-2)$.

For our first odd triple consider the elements

$$x_2 = (1,2,\dots,2m-1),$$
$$y_2 = x_2^{(1,2m,3)} = (1,4,5,\dots,2m-1,2m,2),$$
$$x_2y_2 = (2,3,5,7,\dots,2m-1,4,6,8,\dots,2m-2,2m)$$

and let $H_2 = \langle x_2, y_2 \rangle$. We clearly have transitivity and 2-transitivity, hence H_2 is primitive. Since $x_2y_2^{-1} = (1,2m,2m-1,2,3)$ is a cycle of length 5, which is prime, fixing at least three points for all m, we can apply Jordan's Theorem and we have that $H_2 = G$. For our second odd triple consider the elements

$$x_2' = (1,2,\dots,2m-1),$$
$$y_2' = x_2'^{(1,3,2m)} = (2,2m,4,\dots,2m-1,3),$$
$$x_2'y_2' = (1,2m,4,6,\dots,2m-2,3,5,\dots,2m-1)$$

and note that $x_2' = x_2$. It follows from a similar argument as before that $\langle x_2', y_2' \rangle = G$ and so now we show that (x_2, y_2, x_2y_2) is inequivalent to (x_2', y_2', x_2y_2'). Let $g \in \mathrm{Aut}(G)$ and suppose that $x_2^g = x_2'$. Since $x_2 = x_2'$, $g \in \langle x_2 \rangle$ and from inspection of the fixed points of the elements of our odd triples we have $g\colon 3 \mapsto 1$ and $g\colon 1 \mapsto 2$. But no such g exists in $\langle x_2 \rangle$ and so $(x_2, y_2, (x_2y_2)^{-1})$ and $(x_2', y_2', (x_2'y_2')^{-1})$ are inequivalent generating triples for G both of type $(2m-1, 2m-1, 2m-1)$. Since $\gcd(2m-2, 2m-1) = 1$ we have a mixable Beauville structure of type

$$(2m-2, 2m-2, 2m-2; 2m-1, 2m-1, 2m-1)$$

for both G and $G \times G$. $\square$

Lemma 2.49. *The alternating group A_{2m+1} and $A_{2m+1} \times A_{2m+1}$ are mixable for $m \geq 4$.*

Proof. For $m \geq 4$ let $G = A_{2m+1}$ and consider the elements

$$\begin{aligned} x_1 &= (1,2)(3,4)(5,\dots,2m+1), \\ y_1 &= (1,2,\dots,2m-3)(2m-2,2m-1)(2m,2m+1), \\ x_1y_1 &= (1,3,5,\dots,2m-1,2m+1,6,8,\dots,2m-4). \end{aligned}$$

By considering the orbit of the point 5 the subgroup $H_1 = \langle x_1, y_1 \rangle$ is visibly transitive and the elements

$$\begin{aligned} y_1x_1^2y_1^{-1} &= (4,6,8,\dots,2m,5,7,\dots,2m-5,2m-1,2m+1), \\ x_1y_1^2x_1^{-1} &= (2,4,2m+1,6,8,\dots,2m-4,1,3,\dots,2m-5) \end{aligned}$$

fix the point $2m-3$ and act transitively on the remaining points; hence H_1 acts primitively. Finally, the element $x_1y_1^{-1} = (2,2m-3,2m-1,2m+1,4)$ is a cycle of length 5, which is prime, fixing at least three points for all $m \geq 4$ and so by Jordan's Theorem $H_1 = G$. This gives our first even triple of type $(2(2m-3), 2(2m-3), 2m-3)$ for G. For our second even triple, we manipulate the first in the following way. Let

$$\begin{aligned} x_1' &= (1,2m-4,\dots,6,2m+1,2m-1,\dots,3), \\ y_1' &= (1,2)(3,4)(5,\dots,2m+1), \\ x_1'y_1' &= (1,2m-3,\dots,2)(2m-2,2m-1)(2m,2m+1). \end{aligned}$$

Since $y_1' = x_1$ and $x_1'y_1' = y_1^{-1}$ it is clear that $\langle x_1', y_1' \rangle = G$. Note also that $x_1' = y_1^{-1}x_1^{-1}$. Since conjugation preserves cycle types we see that (x_1, y_1, x_1y_1) and $(x_1', y_1', x_1'y_1')$ are inequivalent. Then, $(x_1, x_1'), (y_1, y_1')$ provide an even triple for $G \times G$ of type $(2(2m-3), 2(2m-3), 2(2m-3))$.

For our first odd triple consider the elements

$$\begin{aligned} x_2 &= (1,2,\dots,2m+1), \\ y_2 &= x_2^{(1,2,3)} = (1,4,5,\dots,2m,2m+1,2,3), \\ x_2y_2 &= (1,3,5,\dots,2m-1,2m+1,4,6,\dots,2m-2,2m,2). \end{aligned}$$

The subgroup $H_2 = \langle x_2, y_2 \rangle$ is visibly transitive while the elements

$$y_2^{-1}x_2^2 = (1,5,6,\dots,2m+1)(3,4), \quad x_2y_2^{-1} = (1,2m+1,3)$$

fix the point 2 and act transitively on the remaining points, hence H_2 is primitive. Since H_2 also contains a cycle of length 3, which is prime, fixing at least three points, by Jordan's Theorem we have that $H_2 = A_{2m+1}$. This gives us an odd triple of type $(2m+1, 2m+1, 2m+1)$ for G and so since $\gcd(2(2m-3), 2m+1) = 1$ it follows that $(x_1, y_1; x_2, y_2)$ is a mixable Beauville structure for A_{2m+1} of type $(2(2m-3), 2(2m-3), 2m-3; 2m+1, 2m+1, 2m+1)$. For our second odd triple consider the cycles

$$\begin{aligned} x_2 &= (1, 2, \ldots, 2m-1), \\ y_2 &= x_2^{(1,2m,2,2m+1,3)} = (1, 4, 5, \ldots, 2m-1, 2m, 2m+1), \\ x_2 y_2 &= (1, 2, 3, 5, \ldots, 2m-1, 4, 6, \ldots, 2m, 2m+1) \end{aligned}$$

and let $H_2 = \langle x_2, y_2 \rangle$. We visibly have transitivity and since the elements $[x_2, y_2] = (1, 2m, 4, 5, 2)$, $x_2[x_2, y_2] = (2, 3, 5, 6, \ldots, 2m-1, 2m, 4)$ stabilise the point $2m+1$ and act transitively on the remaining points we also have 2-transitivity, hence primitivity. Since $[x_2, y_2]$ is a cycle of length 5, which is prime, fixing at least three points for $m \geq 4$ Jordan's Theorem implies that $H_2 = G$ and this gives us an odd triple for G of type $(2m-1, 2m-1, 2m-1)$. Since the types of our odd triples are distinct, by Lemma 2.8 they are inequivalent and so we have an odd triple for $G \times G$. Since $2(2m-3)$ is coprime to both $2m-1$ and $2m+1$ we then have a mixable Beauville structure of type

$$(2(2m-3), 2(2m-3), 2(2m-3); 4m^2-1, 4m^2-1, 4m^2-1)$$

for $G \times G$. $\square$

2.5 Mixable Beauville structures for low-rank finite groups of Lie type

We make use of theorems due to Zsigmondy (generalising a theorem of Bang), Frobenius and Gow which we include here for reference. Throughout this section $q = p^f$ will denote a prime power for a positive integer $f \geq 1$.

Theorem 2.50 (Zsigmondy [127] or Bang [1], as appropriate)**.** *For any positive integer $a > 1$ and $n > 1$ there is a prime number that divides $a^n - 1$ and does not divide $a^k - 1$ for any positive integer $k < n$, with the following exceptions:*

1. *$a = 2$ and $n = 6$; and*

2. *$a + 1$ is a power of 2, and $n = 2$.*

We denote a prime with such a property $\Phi_n(a)$.

Remark 2.51. *The case where $a = 2$, $n > 1$ and not equal to 6 was proven by Bang in [1] while the general case was proven by Zsigmondy in [127]. We shall refer to this as Zsigmondy's Theorem. A* *more recent account of a proof is given by Lüneburg in [82]. An even more recent account in English is given by Roitman in [98].*

The following well-known structure constant formula will be used extensively.

Theorem 2.52 (Frobenius [48])**.** *Let G be a finite group and C_1, C_2, C_3 be conjugacy classes of G. The number of $(x, y, z) \in C_1 \times C_2 \times C_3$ such that $xyz = 1$ is denoted $n(C_1, C_2, C_3)$ and is equal to*

$$n(C_1, C_2, C_3) = \frac{|C_1||C_2||C_3|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\chi(z)}{\chi(1)}$$

where x, y and z are representatives of C_1, C_2 and C_3 repectively.

Definition 2.53. *Let G be a group of Lie type defined over a field of characteristic $p > 0$, prime. A* ***semisimple*** *element is one whose order is coprime to p. A semisimple element is* **regular** *if p does not divide the order of its centraliser in G.*

Theorem 2.54 (Gow [60])**.** *Let G be a finite simple group of Lie type of characteristic p, and let g be a non-identity semisimple element in G. Let L_1 and L_2 be any conjugacy classes of G consisting of regular semisimple elements. Then g is expressible as a product xy, where $x \in L_1$ and $y \in L_2$.*

Remark 2.55. *A slight generalisation of this result to quasisimple groups appears in [45, Theorem 2.6].*

2.5.1 The projective special linear groups $L_2(q)$

The projective special linear groups $L_2(q)$ are defined over fields of order q. They are simple when $q \geq 4$ and have order $q(q+1)(q-1)/d$ where $d = \gcd(2, q+1)$. Their maximal subgroups are found in Dickson [32] based on the work of Moore [87] and Wiman [126]. They are also treated by Mitchell in [85]. Throughout this section we let

$$d = \gcd(2, q+1), \quad q^+ = \frac{q+1}{d} \quad \text{and} \quad q^- = \frac{q-1}{d}.$$

There exists an exceptional isomorphism between the groups $L_2(4)$, $L_2(5)$ and A_5 [120, Section 3.3.5]. It is known that A_5 is not an unmixed Beauville group [6, Section 5.4] and so we begin with the case $q = 7$.

Lemma 2.56. *Let $G = L_2(7)$. Then G^n admits a mixable Beauville structure if and only if $n = 1$ or 2.*

Proof. The maximal subgroups of G are known [27, p.2] and these are subgroups isomorphic to S_4 or point stabilisers in the natural representation of G on eight points of shape $7{:}3$. Hyperbolic generating triples cannot have type $(3, 3, 3)$, since $\frac{1}{3} + \frac{1}{3} + \frac{1}{3} \not< 1$ and similarly for generating triples of types $(2, 2, 2)$, $(2, 2, 4)$ and $(2, 4, 4)$. The number of generating triples of type $(7, 7, 7)$ can be computed using GAP, but since it is equal to the order of $\mathrm{Aut}(G)$ we see from [63] that there is no generating triple of type $(7,7,7)$ for G^n when $n > 1$. Therefore, in order to generate G^n where $n > 1$ an odd triple must consist of elements of orders 3 and 7 and an even triple must have type $(4,4,4)$. Any such even triple generates G since elements of order 4 are not contained in point stabilisers and inside a subgroup isomorphic to S_4 the product of three elements of order 4 cannot be equal to the identity. We can compute the number of such triples from the structure constants and since this is twice the order of $\mathrm{Aut}(G)$ we have that there exist even triples of type $(4,4,4)$ for G and for $G \times G$. We then see that this is the maximum number of direct copies of G for which there exists a mixable Beauville structure.

For our odd triple we then take a triple of elements of type $(7,7,3)$ which can be shown to exist by computing their structure constants and are seen to generate G since if they were to belong to a maximal subgroup then the product of two elements of order 7 would again have order 7. This gives a mixable Beauville structure of type $(4,4,4;7,7,3)$ for G. Finally, we then have mixable Beauville structures for $G \times G$ of type $(4,4,4;7,7,21)$ by Lemma 2.8 or alternatively of type $(4,4,4;7,21,21)$ by Lemma 2.6. $\square$

Lemma 2.57. *Let $G = L_2(2^n)$ where $n \geq 3$. Then G does not admit a mixable Beauville structure.*

Proof. The only elements of even order in G belong to the unique conjugacy class of involutions. If $x, y \in G$ are involutions, then $\langle x, y \rangle$ is isomorphic to a dihedral group. In particular, there do not exist even triples for G. $\square$

Remark 2.58. *The restriction in the previous lemma does not apply to $L_2(2^n)^m$ where $m > 1$.*

Lemma 2.59. *Let $G = L_2(8)$. Then $G \times G$ admits a mixable Beauville structure.*

Proof. It can easily be checked in GAP that for G there exist generating triples of types $(2,7,7)$, $(3,3,9)$ and $(3,9,9)$. The two odd triples are inequivalent by Lemma 2.8 and by Lemma 2.6 we have that there exists a mixable Beauville structure of type $(14,14,7;3,9,9)$ for $G \times G$. $\square$

Lemma 2.60. *Let $G = L_2(9)$. Then both G and $G \times G$ admit a mixable Beauville structure.*

Proof. This follows directly from the exceptional isomorphism $L_2(9) \cong A_6$ [120, Section 3.3.5] and Lemma 2.46. $\square$

We make use of the following Lemmas:

Lemma 2.61. *Let $G = L_2(q)$ for $q = 7, 8$ or $q \geq 11$ and $q = p^f$. Then, under the action of $Aut(G) \cong P\Gamma L_2(q)$ the number of conjugacy classes of elements of order q^+ in G is $\phi(q^+)/2f$.*

Proof. Elements of order q^+ are conjugate to their inverse so there are $\phi(q^+)/2$ conjugacy classes of elements of order q^+ in $L_2(q)$. The only outer automorphisms of G come from the diagonal automorphisms and the field automorphisms, but since diagonal automorphisms do not fuse conjugacy classes of semisimple elements we examine the field automorphisms. These come from the action of the Frobenius automorphism on the elements of the field $\mathbb{F}_q$ sending each entry of the matrix to its p-th power. The only fixed points of this action are the elements of the prime subfield $\mathbb{F}_p$ and so, since the entries on the diagonal of the elements of order q^+ are not both contained in the prime subfield, we have that the orbit under this action has length f, the order of the Frobenius automorphism. We then get f conjugacy classes of elements of order q^+ inside G fusing under this action. Hence under the action of the full automorphism group there are $\phi(q^+)/2f$ conjugacy classes of elements of order q^+ in G. □

Lemma 2.62. *Let $q = p^f \geq 13$, $q \neq 27$ be a prime power. Then $\phi(q^+) > 2f$.*

Proof. Let $S = \{p^i, q^+ - p^i \mid 0 \leq i \leq f-1\}$. This set consists of $2f$ positive integers less than and coprime to q^+ and whose elements are distinct when $q \geq 13$. To this set we add k which depends on q.

- When $p = 2$ we let $k = 7$ since for all $f > 3$, $7 \notin S$ and $\gcd(7, 2^f + 1) = 1$.
- When $p = 3$ we let $k = 11$ since for $f > 3$, $11 \notin S$ and $\gcd(11, 3^f + 1) = 1$.
- When $p \neq 3$ and $q \equiv 1 \bmod 4$ we let $k = q^+ - 2$. Since $p \neq 3$ we have $k \notin S$ and since q^+ is odd we have $\gcd(k, q^+) = 1$.
- When $p \neq 3$ and $q \equiv 3 \bmod 4$ then f must be odd. In the case $f = 1$, $q^+ = 2^i m$ where $i > 0$ and m is odd so that $\phi(q^+) = \phi(2^i)\phi(m) = 2^{i-1}\phi(m) > 2$ since $p > 11$. In the case $f > 2$, $k = \frac{p-1}{2} \notin S$ and is coprime to q^+.

This completes the proof. □

Lemma 2.63. *Let G be the projective special linear group $L_2(q)$ where $q \geq 7$. Then,*

1. *there is a mixable Beauville structure for $G \times G$, and;*
2. *when $p \neq 2$ there is also a mixable Beauville structure for G.*

Proof. In light of Lemmas 2.56–2.60 we can assume that $q \geq 11$. Jones proves in [71] that generating triples of type (p, q^-, q^-) exist for G when $q \geq 11$ and since $\gcd(p, q^-) = 1$ we immediately have, by Lemma 2.6, a generating triple for $G \times G$. We proceed to show that there exists a generating triple (x, y, z) for G of type (q^+, q^+, q^+). Note that p, q^- and q^+ are mutually coprime. The only maximal subgroups containing elements of order q^+ are the dihedral groups of order $2q^+$ which we denote by D_{q^+}. By Gow's Theorem, for a conjugacy class C of elements of order q^+ there exist $x, y, z \in C$ such that $xyz = 1$. Since inside D_{q^+} any conjugacy class of elements of order q^+ contains only two elements, x, y and z can not all be contained in the same maximal subgroup of G. Hence (x, y, z) is a generating triple for G of type (q^+, q^+, q^+). When the number of conjugacy classes of elements of order q^+ in G under the action of $\mathrm{Aut}(G)$ is strictly greater than 1 we can apply Gow's Theorem a second time to give a generating triple of type (q^+, q^+, q^+) for $G \times G$. This follows from Lemmas 2.61 and 2.62 with the exceptions of $q = 11$ or 27. For $G = L_2(11)$ we have that a generating triple of type (p, q^-, q^-) exists by [71] or alternatively the words ab and $[a, b]$ in the standard generators for G give an odd triple of type $(11, 5, 5)$. In both cases we have, by Lemma 2.6, an odd triple of type $(55, 55, 5)$ for $G \times G$. For our even triple, there exists a single conjugacy class of elements of order 6 [27, p. 7]. The structure constant $n(6A, 6A, 6A)$ can easily be computed and is equal to twice the order of $\mathrm{Aut}(G)$ so there exist even triples for G and $G \times G$. For $G = L_2(27)$ we take the words in the standard generators $(ab)^2(abb)^2$ and a^{b^2}, yielding an even triple of type $(2, 14, 7)$, and the words b^2, b^a, yielding an odd triple of type $(3, 3, 13)$. Again, by Lemma 2.6, these give a mixable Beauville structure for $G \times G$. Finally, we remark that when $q \equiv \pm 1 \bmod 4$ we have that q^- and q^+ have opposite parity and this determines the parity of our triples. When $q \equiv 1 \bmod 4$, (p, q^-, q^-) becomes our even triple, (q^+, q^+, q^+) our odd triple, and vice versa when $q \equiv 3 \bmod 4$. □

2.5.2 The projective special linear groups $L_3(q)$

The projective special linear groups $L_3(q)$ are defined over fields of order q. They are simple for $q \geq 2$ and have order $q^3(q^3 - 1)(q^2 - 1)/d$ where $d = (3, q - 1)$. The classification of their maximal subgroups is due to Mitchell [85] in the case q is odd and to Hartley [64] in the case q is even. Their character table was determined by Simpson and Sutherland Frame [105] whose results and notation are used throughout. In particular, throughout this section we let

$$d = \gcd(3, q - 1), \quad t' = (q^2 + q + 1)/d \quad \text{and} \quad r = q - 1.$$

Lemma 2.64. *Let $G = L_3(q)$ and $q = p^f \geq 3$. Then the number of conjugacy classes of elements of order t' in G under the action of Aut(G) is $\phi(t')/6f$ where $\phi(n)$ is Euler's totient function.*

Proof. From the character table of $L_3(q)$ we see that if $g \in G$ is an element of order t', then g is conjugate to g^q and g^{q^2}, hence there are $\phi(t')/3$ conjugacy classes of elements of order t' in G. The outer automorphism group of G is generated by a field automorphism of order f, a diagonal automorphism of order $d =\gcd(3, q - 1)$ and a graph automorphism of order 2. Since elements of order t' are semisimple, and therefore diagonalisable, their conjugacy is preserved by the action of the diagonal automorphism. The actions of the field and graph automorphisms then fuse $2f$ conjugacy classes of elements of order t'. Under the action of $\mathrm{Aut}(G)$ there are thus $\phi(t')/6f$ conjugacy classes of elements of order t' in G. □

Lemma 2.65. *Let $G = L_3(q)$ for $q = 3$ or $q \geq 5$. Then there exists a generating triple of type (t', t', t') for G and for $G \times G$.*

Proof. From the list of maximal subgroups of G we see elements of order t' are contained only in subgroups of order $3t'$ in which they generate a cyclic normal subgroup of order t'. If C is a conjugacy class of elements of order t' and $g \in C$, then $C \cap \langle g \rangle = \{g, g^q, g^{q^2}\}$, partitioning C into $|C|/3$ disjoint subsets of size 3. We now examine the structure constant. The contribution to $n(C, C, C)$ from triples which belong to a maximal subgroup of G is as follows. For each of the $|C|/3$ subsets of C of size 3, there are 6 possible combinations of these elements whose product is equal to the identity, so we require that $n(C, C, C) - 2|C| > 0$. From the character table of G we have that

$$n(C, C, C) = \frac{|C|^3}{|G|}\left(1 - \frac{1}{q(q+1)} + \frac{1}{q^3} + \sum_{u=1}^{t'-1} \frac{(\zeta_{t'}^u + \zeta_{t'}^{uq} + \zeta_{t'}^{uq^2})^3}{3(q-1)^2(q+1)}\right)$$

where $\zeta_{t'}$ is a primitive t'-th root of unity. From the triangle inequality we have $|(\zeta_{t'}^u + \zeta_{t'}^{uq} + \zeta_{t'}^{uq^2})|^3 \leq 27$ so we can bound $n(C, C, C)$ from below and for $q = 7$ or $q \geq 11$ we have

$$n(C, C, C) \geq \frac{|C|^3}{|G|}\left(1 - \frac{1}{q(q+1)} + \frac{1}{q^3} - \frac{9(t'-1)}{(q-1)^2(q+1)}\right) > 2|C|.$$

For $q = 3, 5, 8$ or 9 direct computation of the structure constants in GAP shows that we can indeed find a generating triple of the desired type for G.

In order to find an odd triple of type (t', t', t') for $G \times G$, by Lemma 2.64 it remains to show that for $q = 3$ or $q \geq 5$, we have $\phi(t')/6f > 1$. The case $q = 3$ can be checked by hand and for $q \geq 5$ we have $t' \geq 19$ and $\gcd(6, t') = 1$, so that $2^{3i}, 3^{2i}, 6^i < p^{2i} + p^i + 1$. The set

$$\{1\} \cup \bigcup_{i=1}^{f} \{2^i, 2^{2i}, 2^{3i}, 3^i, 3^{2i}, 6^i\}$$

then consists of $6f + 1$ distinct positive integers less than and coprime to t'. This completes the proof. ∎

Lemma 2.66. *Let $G = L_3(q)$ and $q > 4$ even. Then,*

1. *there exists a mixable Beauville structure for G of type $(2, 4, s; t', t', t')$, and;*
2. *there exists a mixable Beauville structure for $G \times G$ of type $(2, 4s, 4s; t', t', t')$,*

where s divides $q^2 - 1$ and is divisible by $q + 1$.

Proof. The existence of our odd triples for G and $G \times G$ was proven in Lemma 2.65, while the existence of our even triples is due to [45, Lemma 4.5] and Lemma 2.6. ∎

Lemma 2.67. *Let $G = L_3(q)$ and $q \geq 3$ odd. Then, there exists a mixable Beauville structure for G of type*

$$\left(p, \frac{q^2-1}{d}, \frac{q^2-1}{d}; t', t', t'\right).$$

This also yields a mixable Beauville structure for $G \times G$.

Proof. By Lemma 2.65 it remains to determine the existence of our even triples for G and $G \times G$. From the list of maximal subgroups [85] elements of order $(q^2 - 1)/d$ belong only to the stabilisers of a point, the stabilisers of a line, or possibly one of a number of maximal subgroups of fixed order. From the point-line duality of $\mathbb{P}^2(q)$ point stabilisers and line stabilisers are isomorphic, but they are not conjugate in G, hence we just consider maximal subgroups conjugate to point stabilisers. Consider the following elements in their canonical representation as given in [105]

$$x = \begin{bmatrix} \rho^k & . & . \\ . & \sigma^{-k} & . \\ . & . & \sigma^{-qk} \end{bmatrix}, \quad y = \begin{bmatrix} 1 & . & . \\ 1 & 1 & . \\ . & 1 & 1 \end{bmatrix}, \quad xy = \begin{bmatrix} \rho^k & . & . \\ \sigma^{-k} & \sigma^{-k} & . \\ . & \sigma^{-qk} & \sigma^{-qk} \end{bmatrix},$$

where $\rho, \sigma \in \mathbb{F}_{q^2}$, $\rho^{q-1} = 1$, $\sigma^{q+1} = \rho$, k is chosen so that x has order $(q^2-1)/d$ and y has order p. From the character of the natural permutation representation of G of degree q^2+q+1, denoted $\chi_1 + \chi_{qs}$ in [105], we see that x and y each fix a single point. Let x and y act on the left of $\mathbb{P}^2(q)$ and note that x contains a minor which is diagonalisable over $\mathbb{F}_{q^2}$ but not over $\mathbb{F}_q$, hence does not stabilise points of the form $[0\colon a\colon b]$ or $[1\colon a\colon b]$ where $a, b \in \mathbb{F}_q$. We then see that x stabilises the point $[1\colon 0\colon 0]$ and y stabilises the point $[0\colon 0\colon 1]$, hence x and y are not contained in the same point stabiliser of G. The characteristic polynomial of their product xy is

$$1 - x(\rho^k + \sigma^k + \sigma^{qk}) + x^2(\rho^k + \sigma^{-k} + \sigma^{-qk}) - x^3$$

which is identical to that of x, from which we see that x and xy have the same order. It remains to show that elements of order $(q^2-1)/d$ are not contained in any subgroup of G of fixed order. These maximal subgroups exist for certain q and are isomorphic to $L_2(7)$, A_6, M_{10} or A_7. Since any element of these groups has order at most 8, and for $q \geq 3$ odd, $(q^2-1)/d \geq 13$, we have that (x, xy, y^{-1}) is a generating triple for G of type $((q^2-1)/d, p, (q^2-1)/d)$. Since it is clear that $q+1$ and p are both coprime to t', by Lemma 2.6 this then yields an even generating triple for G of type $((q^2-1)/d, p(q^2-1)/d, p(q^2-1)/d)$. $\square$

Lemma 2.68. *The projective special linear group $L_3(q)$ and $L_3(q) \times L_3(q)$ admit a mixable Beauville structure for $q \geq 2$.*

Proof. We note the exceptional isomorphism between $L_3(2)$ and $L_2(7)$ [120, Section 3.12], which was dealt with in Lemma 2.59. By Lemmas 2.66 and 2.67 it remains to prove our statement for $q = 4$. Since explicit words in the standard generators for $L_3(4)$ do not appear on [125], we take the following

$$a := (3,4,5)(7,9,8)(10,14,18)(11,17,20)(12,15,21)(13,16,19);$$

$$b := (1,2,6,7,11,3,10)(4,14,8,15,16,20,13)(5,18,9,19,21,17,12);$$

which are easily checked in GAP to generate G. The triple (a, b, ab) is then of type $(3,7,7)$ which by

Lemma 2.6 also yields an odd triple for $G \times G$ of type $(21, 21, 7)$. For our even triple we let $x := ab^2$, $y := [a, b^2]$, which gives a generating triple of type $(2, 4, 5)$ for G and a generating triple of type $(2, 20, 20)$ for $G \times G$. This completes the proof. $\square$

2.5.3 The projective special unitary groups $U_3(q)$

The projective special unitary groups $U_3(q)$ are defined over fields of order q^2. They are simple for $q \geq 3$ and have order $q^3(q^3+1)(q^2-1)/d$ where $d = (3, q+1)$. The classification of their maximal subgroups is due to Mitchell [85] for q odd and to Hartley [64] for q even. Their character table was determined by Simpson and Sutherland Frame [105] whose results and notation are used throughout. In particular, throughout this section we let

$$d = \gcd(3, q+1), \quad t' = (q^2 - q + 1)/d \quad \text{and} \quad r = q + 1.$$

Lemma 2.69. *Let $G = U_3(q)$ for $q \geq 3$. Then the number of conjugacy classes of elements of order t' in G under the action of $Aut(G)$ is $\phi(t')/6f$.*

Proof. Let $g \in G$ have order t', then g is conjugate to g^{-q} and g^{q^2} and so the number of conjugacy classes of order t' in G is $\phi(t')/3$. Since elements of order t' are semisimple, and therefore diagonalisable, diagonal automorphisms preserve their characteristic polynomials, and so preserve conjugacy. The unitary groups do not admit outer graph automorphisms, and so only field automorphisms fuse conjugacy classes of elements of order t' since their diagonal entries do not all belong to the prime subfield. Since the action of the field automorphism has orbit length $2f$ we have the desired result. $\square$

Lemma 2.70. *Let $G = U_3(q)$ for $q = 7$ or $q \geq 9$. Then there exists a generating triple of type (t', t', t') for G and for $G \times G$.*

Proof. Let C be a conjugacy class of elements of order t' in G. When $q \geq 7$, elements of order t' are contained only in maximal subgroups of order $3t'$ in which they generate a cyclic normal cyclic subgroup. All other nontrivial elements of such a subgroup have order 3. In particular, cyclic subgroups of order t' belong to a unique maximal subgroup. We use the structure constants for G to show that there exists a triple not contained entirely in a maximal subgroup of G. If $g \in C$, then $C \cap \langle g \rangle = \{g, g^{-q}, g^{q^2}\}$ and so C is partitioned into $|C|/3$ subsets of size 3. In particular, the intersection of a maximal subgroup of order $3t'$ and C has order 3 and if $(x, y, z) \in \{g, g^{-q}, g^{q^2}\}^3$ is such that $xyz = 1$, then x, y and z are mutually distinct. The contribution to $n(C, C, C)$ from triples contained in maximal subgroups is then $2|C|$. Using the formula for structure constants as found in [48] we have that

$$n(C, C, C) = \frac{|C|^3}{|G|} \left(1 - \frac{1}{q(q-1)} - \frac{1}{q^3} - \sum_{u=1}^{t'-1} \frac{(\zeta_{t'}^{u} + \zeta_{t'}^{-uq} + \zeta_{t'}^{uq^2})^3}{3(q+1)^2(q-1)} \right)$$

where $\zeta_{t'}$ is a primitive t'-th root of unity. From the triangle inequality we have $|(\zeta_{t'}^{u}+\zeta_{t'}^{-uq}+\zeta_{t'}^{uq^2})|^3 \leq 27$ so we can bound $n(C,C,C)$ from below and for $q \geq 8$ the following inequality holds

$$n(C,C,C) \geq \frac{|C|^3}{|G|}\left(1 - \frac{1}{q(q-1)} - \frac{1}{q^3} - \frac{9(t'-1)}{(q+1)^2(q-1)}\right) > 2|C|.$$

For $q = 7$ direct computation of the structure constants shows that we can indeed find a generating triple of the desired type.

By Lemma 2.69, in order to show there exists a generating triple of type (t', t', t') for $G \times G$, it remains to show that $\phi(t') > 6f$, since we can select generating triples for G belonging to two conjugacy classes which are not equivalent by an automorphism of G to generate $G \times G$. For $q = 7, 9$ it can be verified directly that $\phi(t') > 6f$ so we can assume $q \geq 11$. Note also that t' is coprime to 6. In the case $d = 1$ we have $2^6 < (p^f - 1)^2 < t'$, hence the set $\{1, 2, \ldots, 2^{6f}\}$ consists of $6f + 1$ positive integers less than and coprime to t', giving our inequality. In the case $d = 3$ we have $2^{3f} < p^f(p^f - 1)/3 < t'$ and $3^{4f-1} < (p^f - 1)^2/3 < t'$, hence the set $\{1, 3, \ldots, 3^{4f-1}, 2, \ldots, 2^{3f}\}$ consists of $7f$ positive integers less than and coprime to t', giving our inequality. This completes the proof. □

Lemma 2.71. *Let $G = U_3(q)$ and $q > 8$ even. Then there exists a mixable Beauville structure for G of type*

$$\left(2, 4, \frac{q^2-1}{c}; t', t', t'\right),$$

where $c = gcd(3, q^2 - 1)$. This also yields a mixable Beauville structure for $G \times G$.

Proof. The existence of odd triples for G and for $G \times G$ is shown by Lemma 2.70. Our even triple for G is due to [45, Lemma 4.20 and Theorem 4.22] and, by Lemma 2.6, since $q^2 - 1$ is odd this yields an even triple for $G \times G$. □

Lemma 2.72. *Let $G = U_3(q)$ for $q \geq 7$ odd. Then there exists a mixable Beauville structure for G of type $(p, r, \frac{rs}{d}; t', t', t')$, where $s = q - 1$. This also yields a mixable Beauville structure for $G \times G$.*

Proof. By Lemma 2.70 we have an odd triple for G and $G \times G$ of type (t', t', t') so we proceed to show the existence of our even triples. Let C_7 be a conjugacy class of elements of order rs/d in G. From the list of maximal subgroups of G, elements of order rs/d belong only to those corresponding to stabilisers of isotropic points, stabilisers of non-isotropic points and possibly one of the maximal subgroups of a fixed order which can occur is $U_3(q)$ for certain q. Stabilisers of isotropic points have order q^3rs/d whereas stabilisers of non-isotropic points have order qr^2s/d. There exist $1 + d$ conjugacy classes of elements of order p in G which are as follows. The unique conjugacy class, C_2, of elements whose centralisers have order q^3r/d; and d conjugacy classes, $C_3^{(l)}$ for $0 \leq l \leq d - 1$, of elements whose centralisers have order q^2. Since an element g of order p which stabilises a non-isotropic point belongs to a subgroup of G isomorphic to $SL_2(q)$, the order of $C_G(g)$ is divisible by

$2p$, hence $g \in C_2$. In particular, elements of C_3^0 do not belong to stabilisers of non-isotropic points. There exists a conjugacy class, C_6, of elements of order r whose centralisers have order r^2/d. An element of order r contained in the stabiliser of an isotropic point is contained in a cyclic subgroup of order rs/d, hence rs/d must divide the order of its centraliser and so elements of C_6 are not contained in the stabilisers of isotropic points. If $(x, y, z) \in C_3^0 \times C_6 \times C_7$, then $\langle x, y, z\rangle = G$. We now determine the structure constant $n(C_3^0, C_6, C_7)$ from the character table for G and we find

$$n(C_3^0, C_6, C_7) = \frac{|C_3^0||C_6||C_7|}{|G|}\left(1 + \sum_{u=1}^{\frac{r}{d}-1} \frac{\epsilon^{3u}(\epsilon^{3u} + \epsilon^{6u} + \epsilon^{(r-3)u})}{t}\right)$$

where ϵ is a primitive r-th root of unity. Using the triangle inequality we can bound the absolute value of the summation by $\frac{3q}{q^2-q+1}$ which, for $q \geq 7$, is strictly less than 1. In order to show that such an (x, y, z) is not contained in any of the possible maximal subgroups of order 36, 72, 216 or isomorphic to $L_2(7)$, A_6, M_{10} or A_7 we note that any element of such a group has order at most $8 < r$ unless $r = 7$. When $r = 7$, $rs/d = 16$ and so indeed $\langle x, y, z\rangle = G$. It remains to show that $\gcd(\frac{prs}{d}, t') = 1$. Since it is clear that $\gcd(p, t') = 1$ it suffices to show that $\gcd(rs, t') = 1$. We have that $t'd - s = q^2$ so t' is coprime to s and since $r^2 - t'd = 3q$ and t' is coprime to 3 we have that t' is coprime to r. By Lemma 2.6 this then yields an even triple of type $(p(q+1), p(q+1), \frac{q^2-1}{d})$ on $G \times G$. □

Lemma 2.73. *The projective special unitary group $U_3(q)$ and $U_3(q)\times U_3(q)$ admit a mixable Beauville structure for $q \geq 3$.*

Proof. In light of the preceding Lemmas in this section it remains only to check the cases $U_3(3)$, $U_3(5)$ and $U_3(q) \times U_3(q)$ for $q = 3, 4, 5$ and 8. We present words in the standard generators that can be easily checked to give suitable generating triples for G which, by Lemma 2.6, give mixable Beauville structures for these cases. For $G = U_3(3)$ let

$$x_1 = [a, b^2],\ y_1 = [a, b^2]^b,\ x_1' = (babab^2)^3,\ y_1' = [a, b^2]^b \in G.$$

It can be checked that $G = \langle x_1, y_1\rangle = \langle x_1', y_1'\rangle$ where both triples have type $(4, 4, 8)$ but in the former triple $x_1, y_1 \in 4C$, whereas in the latter, $x_1' \in 4AB, y_1' \in 4C$. Since these two generating triples are then inequivalent under the action of $\mathrm{Aut}(G)$ we have that $(x_1, x_2), (y_1, y_2) \in G \times G$ yields a generating triple of type $(4, 4, 8)$ for $G \times G$. For the odd triples we let $x_2 = ab$ and $y_2 = ba$. These produce a generating triple of type $(7, 7, 3)$ which, by Lemma 2.6, gives a mixable Beauville structure for $G \times G$. For the remaining cases $q = 4, 5$ and 8 we present in Table 2.3 words in the standard generators for G which, by Lemma 2.6, give a mixable Beauville structure for G and $G \times G$ where necessary. □

q	x_1	y_1	x_2	y_2	Type
4	a	$(ab)^2$	b	$[b,a]$	$(2,13,13;3,5,3)$
5	a	ab^2	ab	b^3ab^3	$(3,8,8;7,7,5)$
8	a	$(ab)^2$	$[a,b]$	$[a,b]^{babab}$	$(2,19,19;9,9,7)$

Table 2.3: Mixable Beauville structures for G and $G \times G$ where $G = U_3(q)$, $q = 4, 5$ and 8.

2.5.4 The projective symplectic groups $S_4(q)$

The projective symplectic groups $S_4(q)$ are defined over fields of order q. They are simple for $q \geq 3$ and have order $q^4(q^4-1)(q^2-1)/d$ where $d = \gcd(2, q-1)$. The classification of their maximal subgroups is for q odd is due to Mitchell [86]. The maximal subgroups of the symplectic group $Sp_4(q)$ are given in [18, pp. 383–384] from which the maximal subgroups of the projective symplectic groups $S_4(q)$ are determined by factoring out the centre $Z = Z(Sp_4(q))$. We make use of the character table of $S_4(q)$ for q odd which was determined by Shahabi and Mohtadifar [100] and whose notation we use throughout.

Lemma 2.74. *Let G be the projective symplectic group $S_4(q)$ where $q \geq 8$ is even. Then there exists a mixable Beauville structure for G of type*

$$(4, 4, q^2+1; q^2-1, q^2-1, q+1).$$

This also yields a mixable Beauville structure for $G \times G$.

Proof. The existence of our even triple for G follows from [45, Lemma 4.26] and by Lemma 2.6 for $G \times G$. The existence of our odd triple for G follows from [45, Lemma 4.24] and by Lemma 2.8 for $G \times G$. It is clear that we have $\gcd(4(q^2+1), q^2-1) = 1$ and hence these are indeed mixable Beauville structures for G and for $G \times G$. □

Lemma 2.75. *Let G be the projective symplectic group $S_4(q)$ where $q \geq 5$ is odd. Then there exists an odd triple of type*

$$\left(\frac{q^2+1}{2}, \frac{q^2+1}{2}, \frac{q^2+1}{2}\right)$$

for G and for $G \times G$.

Proof. From the list of maximal subgroups of G elements of order $(q^2+1)/2$ belong only to maximal subgroups isomorphic to $L = L_2(q^2){:}2 \leqslant P\Sigma L_2(q)$. Let B_1 denote a conjugacy class of elements of order $(q^2+1)/2$ in G. We use the structure constants to determine $n(B_1, B_1, B_1)$. We then subtract from this the number of triples of elements from B_1 contained in maximal subgroups isomorphic to L, denoted $n(B_1, B_1, B_1)_L$. Our aim is then to show that

$$\frac{n(B_1, B_1, B_1) - [G:L]n(B_1, B_1, B_1)_L}{|\mathrm{Aut}(G)|} \geq 2,$$

where $[G : L] = [G : N_G(L)]$ is the number of subgroups conjugate to L in G, in which case there are at least 2 inequivalent generating triples, and hence there exist generating triples for G and $G \times G$ of the desired type. Let ζ be a primitive (q^2+1)-th root of unity and let R_1 be the set of $(q^2-1)/4$ distinct positive integers, i, such that $\zeta^i, \zeta^{-i}, \zeta^{qi}$ and ζ^{-qi} are all distinct. We see from the character table of G that the irreducible characters which take non-zero values on the conjugacy class B_1 are those denoted θ_9; θ_{10}; $\chi_1(j)$, where $j \in R_1$ is even; and the linear character, which is not printed in the tables. We have that

$$n(B_1, B_1, B_1) = \frac{q^8(q^2-1)^4}{(q^2+1)} \left(1 + \sum_{j \in R_1} \frac{(\zeta^j + \zeta^{-j} + \zeta^{qj} + \zeta^{-qj})^3}{(q^2-1)^2} - \frac{1}{q(1+q)^2} + \frac{1}{q(1-q)^2} + \frac{1}{q^4} \right).$$

From the triangle inequality we can bound this in the following way.

$$n(B_1, B_1, B_1) \geq \frac{q^4(q^2-1)^2}{(q^2+1)} (q^8 + 14q^6 - 10q^4 - 2q^2 + 1).$$

We use CHEVIE [55] to compute the structure constant $n(B_1, B_1, B_1)_L$ from the structure constants of $L_2(q^2)$ in the following way. Let C be a conjugacy class of elements of order $(q^2+1)/2$ inside $L_2(q^2)$ and let C' be the conjugacy class in $L_2(q^2)$ consisting of q-th powers of elements in C. Under the action of L, C fuses with C' and, since the structure constant $n(C, C, C)_{L_2(q^2)} = 4|L_2(q^2)|$ is constant by replacing any number of choices of C with C', we have $n(B_1, B_1, B_1)_L = 2^3 n(C, C, C)_{L_2(q^2)} = 16|L|$. Putting all this together yields

$$\frac{n(B_1, B_1, B_1) - [G : L] n(B_1, B_1, B_1)_L}{|\mathrm{Aut}(G)|} \geq \frac{q^8 + 14q^6 - 26q^4 - 34q^2 - 15}{2f(q^2+1)^2},$$

the right hand side of which is greater than 2 when $q \geq 5$. This gives the desired result. □

Lemma 2.76. *Let G be the projective symplectic group $S_4(q)$ where $q \geq 5$ is odd. Then,*

1. *if $q = p$, then there exists an even triple for G and $G \times G$ of type $(p, q+1, p(q+1))$, and;*
2. *if $q \neq p$, then there exists an even triple for G and $G \times G$ of type $(p^2, q+1, p(q+1))$.*

Proof. Elements belonging to the conjugacy class A_{41} have order p or p^2, depending on whether $q = p$ or not, and their centraliser in G has order q^2. A conjugacy class of elements of order $q+1$ whose centraliser in G has order $(q+1)^2$ can be chosen and is denoted B_4, while a conjugacy class of elements of order $p(q+1)$ can be chosen with centraliser in G of order $q(q+1)$ and is denoted C_{21}.

Let $x \in A_{41}$, $y \in B_4$, $z \in C_{21}$ and $H = \langle x, y, z \rangle$. From examination of the list of maximal subgroups as found in [18, p. 383] we see that maximal subfield subgroups and maximal subgroups isomorphic to $L_2(q)$ or $S_4(q^2){:}2$ do not contain elements of order $p(q+1)$ and, since $p(q+1) \geq 30$ when $q \geq 5$, H is not contained in any of the possible maximal subgroups of fixed order. An element of order $q+1$ belonging to a parabolic subgroup will have centraliser in G of order divisible by q^2-1

and so neither class of parabolic subgroups contain elements conjugate to y in G. Maximal subgroups isomorphic to $(Sp_2(q) \wr 2)/Z$ have centre of order 2 and so do not contain elements conjugate to x in G. Finally, maximal subgroups of shape $GL_2(q).2/Z$ or $GU_2(q).2/Z$ do not contain elements of order p^2 and an element of order p belonging to either group has centraliser in G of order divisible by $(q-1)/2$ or $(q+1)/2$ as appropriate, hence such subgroups do not contain elements conjugate to x in G. It follows that $H = G$.

We now proceed to show that x, y and z can be chosen such their product is the identity and that there are at least 2 inequivalent such triples. For this we compute the structure constant $n(A_{41}, B_4, C_{21})$. Let $k, r \in T_2 = \{1, 2, \ldots, (q-1)/2\}$,

$$s = (-1)^{\frac{q-1}{2}}, \quad \epsilon = -s(s + \sqrt{sq}), \quad \epsilon' = -s(s - \sqrt{sq}), \quad \eta^{q+1} = 1 \quad \text{and} \quad \beta_j = \eta^j + \eta^{-j},$$

where η is a primitive root of unity. Note that $\epsilon + \epsilon' = -2s$ and $\epsilon\epsilon' = (1 - sq)$. The irreducible characters on which all three of these classes take non-zero values are denoted in [100] as θ_3; $\theta_3\theta_4$; $\xi'_{21}(k)$ and $\xi'_{22}(k)$ where k is odd; $-\xi_1(k)$, where k is even; $\chi_4(k, r)$ where $k + r$ is even and $k \neq r$; $-\chi_6(k)$; and the linear character, which is not printed. From the character table we then have

$$g = \frac{|A_{41}||B_4||C_{21}|}{|G|} = \frac{q^5(q-1)^4(q^2+1)^2(q+1)}{8}$$

and

$$\frac{n(A_{41}, B_4, C_{21})}{g} = 1 - 2\frac{\epsilon\epsilon'(-1)^{\frac{q+1}{2}}}{\frac{1}{2}(1+q^2)} +$$

$$+ \sum_{k \text{ odd}} \frac{\epsilon'(s\beta_k - \beta_{k\frac{q-1}{2}})(1 + \beta_k\epsilon)}{\frac{1}{2}(1-q)^2(1+q^2)} + \sum_{k \text{ odd}} \frac{\epsilon(s\beta_k - \beta_{k\frac{q-1}{2}})(1 + \beta_k\epsilon')}{\frac{1}{2}(1-q)^2(1+q^2)} +$$

$$+ \sum_{k \text{ even}} \frac{(\beta_k + \beta_{k\frac{q-1}{2}})(1 + \beta_k)}{(1-q)(q^2+1)} + \sum_{\substack{k+r \text{ even} \\ k \neq r}} \frac{(\beta_k\beta_{r\frac{q-1}{2}} + \beta_r\beta_{k\frac{q-1}{2}})(\beta_k + \beta_r)}{(1-q)^2(1+q^2)} + \sum_k \frac{\beta_k\beta_{k\frac{q-1}{2}}\beta_k}{(1-q)(1+q^2)}$$

where in each summation k sums over all elements of T_2 subject to the stated conditions. This expression can be simplified to the following

$$\frac{8n(A_{41}, B_4, C_{21})}{q^5(q-1)^3(q^2+1)(q+1)} = (q^2+1)(q-1) +$$

$$+ 4(q-s)(q-1) - 4\sum_{k \text{ odd}} \frac{(\beta_k^2 q + \beta_k\beta_{k\frac{q-1}{2}} + \beta_k) - s(\beta_k\beta_{k\frac{q-1}{2}}q + \beta_k^2 + \beta_{k\frac{q-1}{2}})}{(q-1)} +$$

$$+ \sum_{k \text{ even}} (\beta_k + \beta_{k\frac{q-1}{2}})(1 + \beta_k) + \sum_{\substack{k+r \text{ even} \\ k \neq r}} \frac{(\beta_k\beta_{r\frac{q-1}{2}} + \beta_r\beta_{k\frac{q-1}{2}})(\beta_k + \beta_r)}{(q-1)} + \sum_k \beta_k\beta_{k\frac{q-1}{2}}\beta_k$$

which, from noting that $|\beta_j| \leq 2$, in turn gives the bound

$$\frac{n(A_{41}, B_4, C_{21})}{|\mathrm{Aut}(G)|} \geq \frac{q(q-1)(q^3+3q^2-7q-19)}{16f(q+1)}.$$

When $q \geq 5$, the right hand side is at least 2 and so there exist even triples of the stated types for G and for $G \times G$, hence the desired result. $\square$

Lemma 2.77. *Let G be the projective symplectic group $S_4(q)$ where $q \geq 3$. Then G and $G \times G$ admit mixable Beauville structures.*

Proof. In light of the preceding lemmas it remains to show this for the cases $q = 3$ and $q = 4$. In the case $G = S_4(3)$ the maximal subgroups, character table and permutation characters of necessary maximal subgroups are given in [27, pp. 26–27]. From the permutation characters it can be seen that elements from the conjugacy class $5A$ belong only to maximal subgroups isomorphic to $A = 2^4 : A_5$ or $S = S_6 \cong S_4(2)$. In the case of G and S there is a unique conjugacy class of involutions and the structure constants $n(5A, 5A, 5A)_G = 6028992$ and $n(5A, 5A, 5A)_S = 7632$ can be readily computed in GAP. In the case of A there are two conjugacy classes of elements of order 5 and eventually we compute the number of triples of elements of order 5 in A whose product is the identity as $n(5, 5, 5)_A = 49152$. Combining all of this we have

$$\frac{n(5A, 5A, 5A)_G - 27n(5, 5, 5)_A - 120n(5A, 5A, 5A)_S}{|\mathrm{Aut}(G)|} = \frac{427}{5} > 2$$

from which we see that there exist generating triples for G and $G \times G$ of type $(5, 5, 5)$. The number of inequivalent generating triples for G of type $(5, 5, 5)$ can be computed directly in GAP and we see that there are in fact 87 such triples. For our even triples we again turn to the permutation characters and see that no maximal subgroup of G contains elements from each of the classes $4A$, $4B$ and $9A$. Either directly, or in GAP, the structure constant $n(4A, 4B, 9A)/|\mathrm{Aut}(G)| = 3$ can be computed so we have even triples for G and for $G \times G$ of of type $(4, 4, 9)$. Again, this can be verified in GAP and so we have a mixable structure for G and for $G \times G$ of type $(4, 4, 9; 5, 5, 5)$.

In the case $G = S_4(4)$ the maximal subgroups, character table and permutation characters of necessary maximal subgroups can be found in [27, pp. 44–45]. We note that elements of order 17 belong only to maximal subgroups isomorphic to $L = L_2(16) : 2$. The structure constant $n(17A, 17A, 17A)_G = 188985600$ can be computed directly or in GAP while the structure constant $n(17A, 17A, 17A)_L = 32640$ can also be computed directly in GAP. There are two classes of maximal subgroups isomorphic to L in G, of index 120, and so we have

$$\frac{n(17A, 17A, 17A)_G - 240n(17A, 17A, 17A)_L}{|\mathrm{Aut}(G)|} = \frac{185}{4} > 2,$$

hence there exists odd triples for $S_4(4)$ and $S_4(4) \times S_4(4)$ of type $(17, 17, 17)$. For our even triples we again inspect the permutation characters and observe that no maximal subgroup of G contains elements from each of the conjugacy classes $4A$, $10A$ and $15C$. We compute the structure constant $n(4A, 10A, 15C)/|\mathrm{Aut}(G)| = 25$ and see that there then exist generating triples for G and $G \times G$ of type $(4, 10, 15)$. This completes the proof. $\square$

2.5.5 The Suzuki groups $Sz(2^{2m+1})$

The Suzuki groups ${}^2B_2(q) = Sz(q)$ were first constructed by Suzuki in [109] and are defined over fields of order $q = 2^{2m+1}$ for $m \geq 0$. They have order $q^2(q-1)(q^2+1)$ and are simple when $q > 2$. Their maximal subgroups were determined by Suzuki in [110] and can also be found in [120, Section 4.3.2].

Lemma 2.78. *Let G be the Suzuki group $Sz(q)$ for $q > 2$. Then*

1. *G admits a mixable Beauville structure of type $(2, 4, 5; q-1, n, n)$, and;*

2. *$G \times G$ admits a mixable Beauville structure of type $(4, 10, 10; n(q-1), n(q-1), n)$*

where $n = q \pm \sqrt{2q} + 1$, whichever is coprime to 5.

Proof. In the proof of [51, Theorem 6.2] Fuertes and Jones prove that there exist generating triples for G of types $(2, 4, 5)$ and $(q-1, n, n)$. It is clear that $\gcd(10, n) = \gcd(10, q-1) = 1$. Then, by Lemma 2.6, we need only show that $\gcd(q-1, n) = 1$. If $q-1$ and n share a common factor, then so do q^2-1 and q^2+1 and similarly their difference. Hence $\gcd(q-1, n)$ divides 2, but since $q-1$ is odd we have $\gcd(q-1, n) = 1$ as was to be shown. $\square$

2.5.6 The exceptional groups $G_2(q)$

The exceptional groups $G_2(q)$ are defined over fields of order $q \geq 2$ and have order $q^6(q^6-1)(q^2-1)$. They are simple for all prime powers $q \geq 3$ and their maximal subgroups were determined by Cooperstein [28] for q even and Kleidman [73] for q odd. The maximal subgroups are summarised in [120, Section 4.3.7]. Their conjugacy classes were determined by Enomoto [39] in the cases $p = 2, 3$ and Chang [22] in the case $p \geq 5$.

Lemma 2.79. *Let G be the exceptional group $G_2(q)$ where $q \geq 4$ is even. Then,*

1. *if $q = 4$, G admits a mixable Beauville structure of type $(8, 8, 7; 5, 5, 13)$;*

2. *if $q \geq 8$ and $q \equiv 1 \bmod 3$, G admits a mixable Beauville structure of type*

$$\left(4, 4, q^2-q+1; q+1, q+1, q^2+q+1\right),$$

and;

3. if $q \geq 8$ and $q \equiv -1$ mod 3, G admits a mixable Beauville structure of type

$$\left(4, 4, q^2+q+1; q-1, q-1, q^2-q+1\right).$$

Furthermore, each of these cases yields a mixable Beauville structure for $G \times G$.

Proof. We treat the case $q = 4$ independently, since additional maximal subgroups arise in this case, by presenting words in the standard generators of $G_2(4)$ which are easily checked in GAP. For our odd triple $x_1 = b$ and $y_1 = b^a$ gives a generating triple of type $(5, 5, 13)$ for G and $(5, 65, 65)$ for $G \times G$. For our even triple $x_2 = (ab^2(ab)^2b)^b$ and $y_2 = x_2^a$ gives a generating triple of type $(8, 8, 7)$ for G and of type $(8, 56, 56)$ for $G \times G$. These words visibly provide a mixable Beauville structure for G and $G \times G$.

Now suppose that $q \geq 8$. We begin with the odd triples for all $q \geq 8$ and use results from the character tables of $SL_3(q)$ and $SU_3(q)$ [114] throughout. From the list of conjugacy classes of G elements of order $q^2 - q + 1$ exist, are regular semisimple and belong only to maximal subgroups isomorphic to $SU_3(q){:}2$. Elements of order $q-1$ can be chosen so that their centraliser in G has order $(q-1)^2$ in which case they are regular semisimple. Since the order of the centraliser of an element of order $q-1$ in $SU_3(q)$ is divisible by q^2-1 such elements do not belong to maximal subgroups isomorphic to $SU_3(q){:}2$. Triples of type $(q-1, q-1, q^2-q+1)$ exist by Gow's Theorem and by the previous discussion generate G. The proof for generating triples of type $(q+1, q+1, q^2+q+1)$ is identical with the roles of $SL_3(q){:}2$ and $SU_3(q){:}2$ interchanged. Since $\gcd(q-1, q^2-q+1) = 1$ and $\gcd(q+1, q^2+q+1) = 1$ we have our odd triples for G and $G \times G$.

For our even triples we proceed as follows. In the case $q \equiv 1$ mod 3, elements of order $q^2 - q + 1$ exist as before. Elements of order 4 are conjugate in $SU_3(q){:}2$ and so also in G, but G contains three conjugacy classes of elements of order 4. We denote them $4A, 4B$ and $4C$ in decreasing order of the size of their centraliser in G. If we let $n = q^2 - q + 1$, then a calculation in CHEVIE shows that triples of type $(4A, 4C, nA)$ exist. Again, our argument is identical for the case $q \equiv -1$ mod 3 with the roles of $SL_3(q){:}2$ and $SU_3(q){:}2$ interchanged yielding an even triple of type $(q+1, q+1, q^2+q+1)$. Since $q^2 - q + 1$ and $q^2 + q + 1$ are odd, we have our even triples for G and for $G \times G$.

It remains to show that $\gcd(q-1, q^2+q+1) = \gcd(q+1, q^2-q+1) = 1$. In the former case any common factor must divide $(q^2+q+1) - (q-1)^2 = 3q$. Since $q-1$ is odd and since elements of order $q-1$ are chosen when $q \equiv -1$ mod 3, we have that $\gcd(q-1, q^2+q+1) = 1$. The latter case is proven analogously. $\square$

Remark 2.80. *In the case that $q = 2$, there exists an isomorphism $G_2(2) \cong Aut(U_3(3))$ [120, Section 4.4.4], but this group is neither simple nor mixable since it contains an index 2 subgroup.*

Lemma 2.81. *Let G be the exceptional group $G_2(q)$ where $q \geq 9$ is odd. Then G admits a mixable*

Beauville structure of type

$$\left(\frac{q-1}{2},\frac{q-1}{2},\frac{q^2-q+1}{t_1};\frac{q+1}{2},\frac{q+1}{2},\frac{q^2+q+1}{t_2}\right)$$

where $t_1 = gcd(3, q+1)$ *and* $t_2 = gcd(3, q-1)$. *This also yields a mixable Beauville structure for* $G \times G$.

Proof. We follow closely the construction given in [45, Section 5.7] but modify it slightly to ensure we have a mixable Beauville structure. Let

$$k_1 = \frac{q-1}{2}, \quad k_2 = \frac{q+1}{2}, \quad k_3 = \frac{q^2+q+1}{\gcd(3,q-1)} \quad \text{and} \quad k_6 = \frac{q^2-q+1}{\gcd(3,q+1)}.$$

Note that $\gcd(k_1, k_2) = 1$ and that either k_1 or k_2 is even. It is clear that $\gcd(k_3, k_6) = 1$, $\gcd(k_2, k_3) = 1$ and $\gcd(k_1, k_6) = 1$. Both $\gcd(k_1, k_3)$ and $\gcd(k_2, k_6)$ divide 3, but since 9 does not divide k_3 or k_6, from our choices of k_1, k_2, k_3 and k_6 we have that these four numbers are pairwise coprime. From [22] and [39] we see that there exist conjugacy classes of regular semisimple elements of all of these orders for all odd q. From the character tables of $SL_3(q)$ and $SU_3(q)$ elements of orders k_1 and k_2 can be chosen from the conjugacy class denoted C_6 for both in [105]. By Gow's Theorem, there then exists a pair of elements of order k_1 whose product has order k_6, and a pair of elements of order k_2 whose product has order k_3. From the list of maximal subgroups, such triples of elements cannot belong to a single maximal subgroup. Then, by the preceding arguments and Lemma 2.6 we have a mixable Beauville structure for G and for $G \times G$. □

Lemma 2.82. *Let* G *be the exceptional group* $G_2(q)$ *where* $q \geq 3$. *Then* G *and* $G \times G$ *admit mixable Beauville structures.*

Proof. In light of Lemmas 2.79 and 2.81 it remains to consider the cases $q = 3$, 5 or 7.

If $q = 3$ the following explicit words in the standard generators are easily checked in GAP to admit a mixable Beauville structure. Our even triple is given by $x_1 = a$, $y_1 = aba(bab)^2$, of type $(2, 7, 8)$, and our odd triple is given by $x_2 = b$, $y_2 = b^a$, of type $(3, 3, 13)$. By Lemma 2.6 these also give mixable Beauville structures for $G_2(3) \times G_2(3)$.

When $q = 5$ we refer to the character table and permutation characters of $G_2(5)$ as given in [27, p. 114] where the maximal subgroups can also be found. The only maximal subgroups containing elements of order 31 are isomorphic to $L_3(5){:}2$ which does not contain elements of order 7. Since elements of order 7 and of order 31 are both regular semisimple, by Gow's Theorem there exists an odd triple of type $(7, 7, 31)$ for $G_2(5)$. For our even triple we let $x, y \in 6C$ and use the structure constants to show that we can find $z \in 25A$ such that $xyz = 1$. We now prove that such a triple generates $G_2(5)$. Maximal subgroups containing elements of order 25 belong to one of the two classes of parabolic subgroups in $G_2(5)$. We denote their representatives as $P_a \cong q_+^{1+4}{:}GL_2(5)$ and $P_b \cong q^{2+3}{:}GL_2(5)$. We denote the permutation character of P_a as $\chi_a = \chi_1 + \chi_5 + \chi_8 + \chi_{11}$ and that of P_b

as $\chi_b = \chi_1 + \chi_5 + \chi_9 + \chi_{11}$. If $g \in 6C$, then $\chi_a(g) = \chi_b(g) = 0$ and thus elements from $6C$ are not contained in subgroups isomorphic to P_a or P_b, hence we have an even triple of type $(6, 6, 25)$. By Lemma 2.6 this also yields a mixable Beauville structure for $G_2(5) \times G_2(5)$. It can also be verified in GAP that such a triple exists.

Finally, in the case of $q = 7$, there exist conjugacy classes of regular semisimple elements of orders 8 and 19, as well as elements of orders 49 and 43. By Gow's Theorem there exists a pair of elements of order 8 whose product has order 9, and by computation in CHEVIE there exists a pair of elements of order 49 whose product has order 43. From the list of maximal subgroups and by Lemma 2.6 we have that these triples admit mixable Beauville structures for $G_2(7)$ and $G_2(7) \times G_2(7)$, completing the proof. $\square$

2.5.7 The small Ree groups $R(3^{2m+1})$

The small Ree groups ${}^2G_2(q) = R(q)$ were first announced by Ree in [94] and are defined over fields of order $q = 3^{2m+1}$ for $m \geq 0$. They have order $q^3(q^3 + 1)(q - 1)$ and are simple when $q > 3$. Their maximal subgroups were determined by Levchuk and Nuzhin [77] when $q > 3$ and independently by Kleidman [73] for all q. The maximal subgroups for $q > 3$ can also be found in [120, Section 4.5.3]. Their conjugacy classes and character table were determined by Ward [114].

Lemma 2.83. *Let G be the small Ree group $R(q)$ for $q > 3$. Then*

1. *G admits a mixable Beauville structure of type*

$$\left(\frac{q+1}{2}, \frac{q+1}{2}, q + \sqrt{3q} + 1; \frac{q-1}{2}, \frac{q-1}{2}, q - \sqrt{3q} + 1\right),$$

   and;

2. *$G \times G$ admits a mixable Beauville structure of type*

$$\left(\frac{q+1}{2}, \frac{q+1}{2}n^+, \frac{q+1}{2}n^+; \frac{q-1}{2}, \frac{q-1}{2}n^-, \frac{q-1}{2}n^-\right)$$

where $n^+ = q + \sqrt{3q} + 1$ and $n^- = q - \sqrt{3q} + 1$.

Proof. Let G, q, n^+ and n^- be as in the hypotheses. From the character table of G we see that regular semisimple elements of orders $\frac{q+1}{2}$, $\frac{q-1}{2}$, n^+ and n^- exist. By Gow's Theorem we can find elements $x_1, y_1 \in G$, both of order $\frac{q+1}{2}$, whose product has order n^+, and elements $x_2, y_2 \in G$, both of order $\frac{q-1}{2}$, whose product has order n^-.

The only maximal subgroups of G containing elements of order n^+ have order $6n^+$. Similarly, the only maximal subgroups of G containing elements of order n^- have order $6n^-$. Since $n^+ - (q+1) = \sqrt{3q}$ we have $\gcd(\frac{q+1}{2}, n^+) = 1$ as neither is divisible by 3. Then, for $q > 3$ we have $\frac{q+1}{2} > 6$ so (x_1, y_1, x_1y_1) is indeed an even triple for G of type $(\frac{q+1}{2}, \frac{q+1}{2}, q + \sqrt{3q} + 1)$. Similarly, for $q > 3$ we have $\frac{q-1}{2} > 6$ and $n^+n^- + (q-1) = q^2$, hence $\gcd(\frac{q-1}{2}, n^-) = 1$ as both are coprime to 3. Note this also implies that $\gcd(n^+, \frac{q-1}{2}) = 1$. This gives us an odd triple for G of type $(\frac{q-1}{2}, \frac{q-1}{2}, q - \sqrt{3q} + 1)$.

It is clear that $\gcd(\frac{q+1}{2}, \frac{q-1}{2}) = 1$ since their difference is q and neither is divisible by 3. Similarly, $\gcd(n^+, n^-) = 1$ since their difference is $2\sqrt{3q}$ and both are clearly coprime to 6. Since we have already shown that $\gcd(n^+, \frac{q-1}{2}) = 1$ it remains to show that $\gcd(n^-, \frac{q+1}{2}) = 1$. We have $(q+1) - n^- = \sqrt{3q}$ and since neither is divisible by 3 we have a mixable Beauville structure for G. Finally, by Lemma 2.6, since $\gcd(\frac{q+1}{2}, n^+) = 1$ and $\gcd(\frac{q-1}{2}, n^-) = 1$, we also have a mixable Beauville structure for $G \times G$. □

2.5.8 The large Ree groups ${}^2F_4(2^{2m+1})$

The large Ree groups ${}^2F_4(q)$ were first announced by Ree in [95] and are defined over fields of order $q = 2^{2m+1}$ for $m \geq 0$. They have order $q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$ and are simple except for the case $q = 2$ which has simple derived subgroup ${}^2F_4(2)'$, known as the Tits group. We consider the Tits group along with the sporadic groups in the next section. The maximal subgroups of the large Ree groups were determined by Malle in [84] and can also be found in [120, Section 4.9.3]. Their conjugacy classes were determined by Shinoda [104].

Lemma 2.84. *Let G be the large Ree group ${}^2F_4(q)$ for $q > 2$. Then*

1. *G admits a mixable Beauville structure of type*

$$\left(10, 10, n^+; \frac{q^2-1}{3}, n^-, n^-\right),$$

and;

2. *$G \times G$ admits a mixable Beauville structure of type*

$$\left(10, 10n^+, 10n^+; \frac{q^2-1}{3}n^-, \frac{q^2-1}{3}n^-, n^-\right)$$

where $n^+ = q^2 + q + 1 + \sqrt{2q}(q+1)$ and $n^- = q^2 + q + 1 - \sqrt{2q}(q+1)$.

Proof. Let G, q, n^+ and n^- be as in the hypotheses. Elements of order 10 exist since G contains maximal subgroups of the form $Sz(q) \wr 2$, as do elements of order $\frac{q^2-1}{3}$ since G contains maximal subgroups isomorphic to $SU_3(q){:}2$ and since $\gcd(3, q+1) = 3$. The only maximal subgroups containing elements of order n^+ have order $12n^+$. Similarly, elements of order n^- are only contained in maximal subgroups of order $12n^-$.

Using the computer program CHEVIE it is possible to determine the structure constant for a pair of elements of order 10 whose product is n^+ and we see that such triples exist. Since $n^+n^- = q^4 - q^2 + 1$ and $q \equiv \pm 2 \bmod 5$ we have that $\gcd(10, n^-) = \gcd(10, n^+) = 1$. Then, since no maximal subgroup contains both elements of order 10 and of order n^+ this is indeed an even triple for G. From the list of conjugacy classes we see that elements of order $\frac{q^2-1}{3}$ are semisimple and elements of order n^- are regular semisimple. Then by Gow's Theorem there exists a pair of elements of order n^- whose product has order $\frac{q^2-1}{3}$. Since $(n^+n^-) + (q^2-1) = q^4$ any common factor of n^- and $\frac{q^2-1}{3}$ must be a power of 2, but since n^- and q^2-1 are both odd we have $\gcd(\frac{q^2-1}{3}, n^-) = 1$. Note that this also implies $\gcd(n^+, \frac{q^2-1}{3}) = 1$. Then, since $\frac{q^2-1}{3} > 12$ for $q > 2$, we see that no maximal subgroup contains both elements of order n^- and of $\frac{q^2-1}{3}$. Hence odd triples of type $(\frac{q^2-1}{3}, n^-, n^-)$ exist for G. By Lemma 2.6 are also odd and even triples for $G \times G$.

We have already shown that $\gcd(10, n^-) = 1$, $\gcd(n^+, q^2-1) = 1$ and it is clear that $\gcd(10, \frac{q^2-1}{3}) = 1$. Finally, let $c = \gcd(n^+, n^-)$ and note that c is odd. Since $n^+ - n^- = 2\sqrt{2q}(q+1)$, c must divide $q+1$. Also, since $n^+ + n^- = 2(q^2+q+1)$, c must also divide q^2+q+1. Therefore c must divide q^2 and hence $c = 1$ so we have our desired mixable Beauville structures for G and $G \times G$. □

2.5.9 The Steinberg triality groups ${}^3D_4(q)$

The Steinberg triality groups ${}^3D_4(q)$ are defined over fields of order $q \geq 2$ and are all simple. They have order $q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$ and their maximal subgroups were determined by Kleidman [74]. Their maximal subgroups can also be found in [120, Section 4.6.5].

Lemma 2.85. *Let G be the Steinberg triality group ${}^3D_4(2)$. Then both G and $G \times G$ admit a mixable Beauville structure.*

Proof. It can be verified using GAP that $(a, (ab)^3b^2; ab, b^{ab^2})$, where a and b are the standard generators, is a mixable Beauville structure of type $(2, 7, 28; 13, 9, 13)$ and by Lemma 2.6 this yields a mixable Beauville structure of type $(14, 14, 28; 117, 117, 13)$ for $G \times G$. □

Lemma 2.86. *Let G be the Steinberg triality group ${}^3D_4(q)$ for $q \geq 3$. Then*

1. *for $p = 2$ there exists a mixable Beauville structure for G of type*

$$(6, 6, \Phi_{12}(q); \Phi_3(q), \Phi_3(q), \Phi_6(q)),$$

and;

2. *for $p \neq 2$ there exists a mixable Beauville structure for G of type*

$$\left(\frac{q^2-1}{d}, \frac{q^2-1}{d}, \Phi_{12}(q); \Phi_3(q), \Phi_3(q), \Phi_6(q)\right).$$

where $d = gcd(3, q+1)$. These also yield mixable Beauville structures for $G \times G$.

Proof. Let G and d be as in the hypothesis. By [45, Lemma 5.24] for $q > 2$ there exists a generating triple of type $(\Phi_3(q), \Phi_3(q), \Phi_6(q))$. We now turn to the even triples.

For $p = 2$ one can verify using CHEVIE to compute the structure constants that there exist pairs of elements of order 6 whose product has order $\Phi_{12}(q)$ and it is clear from the list of maximal subgroups that this is indeed an even triple for G. For $p \neq 2$ elements of order $\frac{q^2-1}{d}$ exist since G contains subgroups isomorphic to $SU(3,q)$. It can then be shown using CHEVIE that triples of type $(\frac{q^2-1}{d}, \frac{q^2-1}{d}, \Phi_{12}(q))$ exist and from the list of maximal subgroups it can be shown that they generate G. By Zsigmondy's Theorem it is also clear that we have coprimeness for both Beauville structures.

By Lemma 2.6 we need only verify that $\gcd(6, \Phi_{12}(q)) = 1$ for $p = 2$ to show that these yield mixable Beauville structures for $G \times G$. This is clear since $\Phi_{12}(q)$ is both odd and coprime to $q^2 - 1$ which is divisible by 3. $\square$

2.6 Mixable Beauville structures for the sporadic groups

We present in Table 2.4 explicit mixable Beauville structures for the sporadic groups in terms of words in the standard generators, except for the cases of the Baby Monster, $\mathbb{B}$, and the Monster, $\mathbb{M}$, for which we simply show existence of such structures in the following Lemmas. The types of these structures are given in Table 2.5.

Lemma 2.87. *The Baby Monster $\mathbb{B}$ and $\mathbb{B} \times \mathbb{B}$ admit mixable Beauville structures.*

Proof. By [117, Theorem 2] there exists a generating triple of type $(2, 3, 8)$ for $\mathbb{B}$. Let

$$x = (ab)^3(ba)^4b(ba)^2b^2, \quad y = x^{ab^2}$$

be words in the standard generators. They both have order 47 and their product has order 55. From the list of maximal subgroups of $\mathbb{B}$ (these are due to Wilson and can be found in [119] and [120, Table 5.7], however the latter omits the group $O_8^+(3):S_4$) we see that they generate $\mathbb{B}$. This gives a mixable Beauville structure of type $(2, 3, 8; 47, 47, 55)$ for $\mathbb{B}$ and by Lemma 2.6 we have a mixable Beauville structure of type $(6, 6, 8; 47, 2585, 2585)$ for $\mathbb{B} \times \mathbb{B}$. $\square$

Lemma 2.88. *The Monster $\mathbb{M}$ and $\mathbb{M} \times \mathbb{M}$ admit mixable Beauville structures.*

Proof. Norton and Wilson [88, Theorem 21] show that the only maximal subgroups of the Monster which contain elements of order 94 are copies of $2{}^{\cdot}\mathbb{B}$ which do not contain elements of order 71. A computation of the structure constants then shows that an even triple of type $(94, 94, 71)$ exists. Finally, in [40] it is shown that there exists a generating triple of type $(21, 39, 55)$ for $\mathbb{M}$. Therefore we have a mixable Beauville structure of type $(94, 94, 71; 21, 39, 55)$ for $\mathbb{M}$ and of type $(94, 6674, 6674; 21, 2145, 2145)$ on $\mathbb{M} \times \mathbb{M}$. $\square$

Finally, we have the following Lemma which completes the proof of Theorem 1.9.

Lemma 2.89. *Let G be one of the 26 sporadic groups or the Tits group ${}^2F_4(2)'$. Then there exists a mixable Beauville structure for G and $G \times G$.*

Proof. For $G = \mathbb{B}$ or $\mathbb{M}$ the existence of mixable Beauville structures follows from Lemmas 2.87 and 2.88. If G is one of M_{11}, M_{12}, J_1, M_{22}, J_2, M_{23}, ${}^2F_4(2)'$, HS, J_3, M_{24}, McL, He, Ru, Suz, $O'N$, Co_3, Co_2, Fi_{22}, Fi_{23} or Fi_{24}', then it can easily be checked in GAP that $\langle x_1, y_1\rangle = \langle x_2, y_2\rangle = G$ for all words appearing in Table 2.4. The remaining cases are HN, Ly, Th, Co_1 and J_4. With the exception of Th, in all cases x_1 and y_1 are the standard generators, so there is nothing to check. In the case of Th there are no maximal subgroups containing elements of orders 10 and 13 hence $\langle x_1, y_1\rangle = Th$. Now we turn to the generating pairs x_2, y_2. From the list of maximal subgroups appearing in [27] the following is easily checked. No maximal subgroup of HN contains elements of orders 5 and 19; no maximal subgroup of Ly contains elements of orders 37 and 67; no maximal subgroup of Th contains elements of orders 19 and 31; no maximal subgroup of Co_1 contains elements of orders 11, 13 and 23; no maximal subgroup of J_4 contains elements of orders 23 and 43. Hence all pairs (x_2, y_2) generate their respective groups.

With the exceptions of $\mathbb{B}$ and $\mathbb{M}$, the types of all mixable Beauville structures for G as they appear in Table 2.5 can easily be checked in GAP. The type for $\mathbb{B}$ follows from Lemma 2.87 and the type for $\mathbb{M}$ follows from 2.88. In all cases except our even triple for J_2 it follows from Lemma 2.6 that such structures indeed extend to mixable Beauville structures for $G \times G$. In the case of J_2 we let $y_1' = x_1^{(ba)^2b^2}$ and use GAP to show that $o(x_1y_1') = 10$ and $\langle x_1, y_1'\rangle = J_2$. Letting $x = (x_1, x_1), y = (y_1, y_1') \in J_2 \times J_2$ we have by Lemma 2.8 an even triple for $J_2 \times J_2$ of type $(10, 10, 40)$. This completes the proof. $\square$

G	x_1	y_1	x_2	y_2
M_{11}	$ab(ab^2)^2$	$(x_1)^b$	$(ab)^5$	$[a,b]^2$
M_{12}	$(ab)^4ba(bab)^2b$	$x_1^{b^2aba}$	ab	ba
J_1	$(ab)^2(ba)^3b^2ab^2$	b^{aba}	ab	$[a,b]$
M_{22}	$(ab)^3b^2ab^2$	$ba(bab^2)^2a$	ab	$(ab)^4b^2ab^2$
J_2	$ab(abab^2)^2ab^2$	$x_1^{ab^2}$	ab	ba
M_{23}	$abab^2$	$babab$	ab	$(abab)^{ba}$
$^2F_4(2)'$	$(ab)^3bab$	$(x_1^7)^{baba}$	ab	ba
HS	$abab^3$	b^3aba	$(ab)^3b$	$(x_2)^b$
J_3	$(ab)^2(ba)^3b^2$	x_1^b	ab	$(ab)^b$
M_{24}	$(ab)^4b$	$(x_1^3)^b$	ab	ba
McL	ab^2	bab	ab	$(ab)^b$
He	ab^3	ab^4	ab	ba
Ru	b	$b^{(ab)^5}$	$(ab)^2$	$(ba)^2$
Suz	$ab(abab^2)^2$	$x_1^{abab^2}$	ab	ba
$O'N$	$[a,b]$	$([a,b]^2)^{bab}$	ab^2	$(ab^2)^{abab}$
Co_3	ab	$(ab)^{b^2}$	$a(ab)^2b(a^2b)^2b$	$(x_2^3)^{baba}$
Co_2	a	b	$ab(ab^2)^2b$	$(x_2^2)^{bab^2}$
Fi_{22}	$(ab)^3b^3$	$(x_1)^a$	b	b^a
HN	a	b	$[b,a]$	$(ab)^2b((ab)^5(ab^2)^2)^2$
Ly	a	b	$abab^3$	$x_2^{(ab)^7}$
Th	$[a,b]$	$[a,b]^{(ba)^4b^2}$	$ababa$	$(x_2^5)^{bab}$
Fi_{23}	a	b	$((ab)^{11}b)^3$	x_2^a
Co_1	a	b	$[(ab)^3,aba]$	$[(ab)^{23},ab^2]^{babab}$
J_4	a	b	$a(bab)^3(ab)^2b$	x_2^a
Fi'_{24}	ab	$((ab)^6b)^{15}$	$b(ba)^3$	$(x_2^3)^{bab}$

Table 2.4: Mixable strucutres $(x_1, y_1; x_2, y_2)$ for G in terms of words in the standard generators.

G	Type of G	Type of $G \times G$
M_{11}	$(8,8,5;11,3,11)$	$(8,40,40;11,33,33)$
M_{12}	$(8,8,5;11,11,3)$	$(8,40,40;11,33,33)$
J_1	$(10,3,10;7,19,19)$	$(10,30,30;133,133,19)$
M_{22}	$(8,8,5;11,7,7)$	$(8,40,40;77,77,7)$
J_2	$(10,10,8;7,7,3)$	$(10,10,40;7,21,21)$
M_{23}	$(8,8,11;23,23,7)$	$(8,88,88;23,161,161)$
${}^2F_4(2)'$	$(8,8,5;13,13,3)$	$(8,40,40;13,39,39)$
HS	$(8,8,15;7,7,11)$	$(8,120,120;7,77,77)$
J_3	$(8,8,5;19,19,3)$	$(8,40,40;19,57,57)$
M_{24}	$(8,8,5;23,23,3)$	$(8,40,40;23,69,69)$
McL	$(12,12,7;11,11,5)$	$(84,84,12;55,55,11)$
He	$(8,8,5;17,17,7)$	$(8,40,40;17,119,119)$
Ru	$(4,4,29;13,13,7)$	$(4,116,116;13,91,91)$
Suz	$(8,8,7;13,13,3)$	$(8,56,56;13,39,39)$
$O'N$	$(12,6,31;19,19,11)$	$(12,186,186;209,209,19)$
Co_3	$(14,14,5;23,23,9)$	$(14,70,70;23,207,207)$
Co_2	$(2,5,28;23,23,9)$	$(10,10,28;23,207,207)$
Fi_{22}	$(16,16,9;13,13,11)$	$(144,144,16;143,143,13)$
HN	$(2,3,22;5,19,19)$	$(6,6,22;95,95,19)$
Ly	$(2,5,14;67,67,37)$	$(10,10,14;2479,2479,67)$
Th	$(10,10,13;19,19,31)$	$(130,130,10;589,589,19)$
Fi_{23}	$(2,3,28;13,13,23)$	$(6,6,28;299,299,13)$
Co_1	$(2,3,40;11,13,23)$	$(6,6,40;143,143,23)$
J_4	$(2,4,37;43,43,23)$	$(4,74,74;989,989,43)$
Fi'_{24}	$(29,4,20;33,33,23)$	$(116,116,20;759,759,33)$
$\mathbb{B}$	$(2,3,8;47,47,55)$	$(6,6,8;47,2585,2585)$
$\mathbb{M}$	$(94,94,71;21,39,55)$	$(94,6674,6674;21,2145,2145)$

Table 2.5: Types of the mixable Beauville structures for G and $G \times G$ from the words in Table 2.4 and Lemmas 2.87 and 2.88.

Chapter 3

The Möbius function of the small Ree groups

> 'Surely,' said I, 'surely that is
> something at my window lattice;
> Let me see then, what thereat is,
> and this mystery explore —'
>
> *The Raven*, Edgar Allan Poe

The existence of the small Ree groups was first announced in 1960 by Ree [94] who constructed them shortly after in [96]. Ree observed that Suzuki's original construction [109] of the Suzuki groups $Sz(2^{2m+1}) = {}^2B_2(2^{2m+1})$ for $m > 0$ could be interpreted in terms of Lie theory and applied to the Chevalley groups of types G_2 [94] and F_4 [95] in certain characteristics. In the case of G_2 in characteristic 3 the groups which arise are known as the small Ree groups and denoted by ${}^2G_2(q) = R(q)$ where $q = 3^{2m+1}$ and $m \geq 0$.

The small Ree group $R(q)$ can naturally be considered as a subgroup of $L_7(q)$ as in [77] or as a subgroup of $P\Omega_8^+(q)$ as in [73]. For the purpose of determining all possible intersections of maximal subgroups in $R(q)$ this is quite unwieldy. Thankfully, Tits [112] determined the existence of a natural 2-transitive permutation representation of $R(q)$ of degree $q^3 + 1$, and it is with this representation that we work. Tits' construction, however, still relies on the Lie theory. A construction of the small Ree groups that is Lie-free is due to recent work by Wilson [121–123]. In addition to these constructions, the small Ree groups have an interpretation as a finite geometry for which we direct the reader to [113, Section 7.7] and as the automorphism group of a $2-(q^3+1, q+1, 1)$ design [81].

The classical Möbius function

We recall the classical Möbius function from number theory since it will be necessary for our calculations. For a positive integer n we define

$$\mu(n) = \begin{cases} (-1)^d & \text{if } n \text{ is the product of } d \text{ distinct primes} \\ 0 & \text{if } n > 1 \text{ and has a square factor greater than 1.} \end{cases}$$

Remark 3.1. *We recall the following classical fact about the Möbius function of a natural number, since we make heavy use of it in our determination of the Möbius function. If $n > 0$ is a positive integer, then*

$$\sum_{l|n} \mu(l) = \begin{cases} 1 & \textit{if} \quad n = 1 \\ 0 & \textit{if} \quad n > 1 \end{cases}$$

where l sums over all positive divisors of n.

Counting subgroups

In Section 3.3 we follow closely the style used by Downs [34] in order to calculate $\mu_G(H)$ for a subgroup $H \leqslant G$ of a group G. In order to enumerate overgroups conjugate to K in G of a fixed subgroup $H \leqslant G$ we take care since conjugacy in G is not necessarily preserved in K. The following definitions will be necessary.

Definition 3.2. *Let $H \leqslant K$ be subgroups of G. We denote by $\nu_K(H)$ the number of subgroups conjugate to K in G that contain H. This is enumerated using the formula*

$$\sum_{i=1}^{n} \frac{[G : N_G(K)][K : N_K(H_i)]}{[G : N_G(H)]} = \sum_{i=1}^{n} \frac{|K||N_G(H_i)|}{|N_G(K)||N_K(H_i)|}$$

where $\{H_1, \ldots, H_n\}$ is a set of representatives from each conjugacy class in K of subgroups conjugate to H in G.

Structure of the chapter

The classes of maximal subgroups of $R(3)$ are different from those of $R(q)$ when $q > 3$. As such, we determine the Möbius function of $R(3)$ in the first section and that of the simple small Ree groups in the second and third sections. In the fourth section we use the Möbius function to determine various Eulerian functions, as defined in Chapter 1, from which we prove a number of results on the generation and probabilistic generation of the small Ree groups. In the last section we prove some general results on Möbius functions and Eulerian functions. The main result of this chapter, Theorem 1.22, appears in [92].

3.1 The Möbius function of $R(3)$

There exists an exceptional isomorphism between the small Ree group $R(3)$ and $P\Gamma L_2(8) \cong \mathrm{Aut}(L_2(8))$ [120, Section 4.5.4], hence it is possible to consider the permutation representation of $R(3)$ on 9 points. For continuity with the following sections, however, we consider $R(3)$ in its natural permutation representation of degree 28. The table of marks for $R(3)$ exists in the GAP library from which it is possible to recover its Möbius function, however since it is relatively straightforward to determine by hand, and serves to illustrate our method, we include it here. The character table of $L_2(8)$ is given in [27, p.6], and can also be found in the GAP library, from which it is possible to reconstruct the character table for $R(3)$, as well as listing its conjugacy classes of maximal subgroups. They are the following.

1. $R(3)' \cong L_2(8)$, the derived subgroup of $R(3)$;
2. $2^3\!:\!7\!:\!3 \cong A\Gamma L_1(8)$, the normaliser of a Sylow 2-subgroup;
3. $9\!:\!6$, the normaliser of a Sylow 3-subgroup, and;
4. $7\!:\!6$, the normaliser of a Sylow 7-subgroup.

Remark 3.3. *The normaliser of a Sylow* 3*-subgroup is a point stabiliser in the degree* 28 *permutation representation of* $R(3)$ *and hereafter we denote them as such. Similarly, the Sylow* 7*-subgroups correspond to cyclic Hall subgroups of order* $q + \sqrt{3q} + 1$ *in the simple small Ree groups and we denote them as Hall subgroups hereafter.*

We now examine the possible intersections of pairs of maximal subgroups. The following is clear.

Lemma 3.4. *Let* $M \neq R(3)'$ *be a maximal subgroup of* $R(3)$ *and let* $H = M \cap R(3)'$.

1. *If* $M \cong 2^3\!:\!7\!:\!3$, *then* $H \cong 2^3\!:\!7$.
2. *If* $M \cong 9\!:\!6$, *then* $H \cong 9\!:\!2 \cong D_{18}$.
3. *If* $M \cong 7\!:\!6$, *then* $H \cong 7\!:\!2 \cong D_{14}$.

The following is clear from inspection of the orders of the subgroups.

Lemma 3.5. *The intersection of a point stabiliser with either a Sylow* 2*-subgroup normaliser or a Hall subgroup normaliser is contained in a cyclic subgroup of order* 6.

The following is also clear from the fact that the centraliser of an involution in $R(3)$ is isomorphic to $2 \times L_2(3)$.

Lemma 3.6. *The intersection of a Sylow* 2*-subgroup normaliser with a Hall subgroup normaliser is a subgroup of either a group isomorphic to* $7\!:\!3$ *or of a cyclic group of order* 6.

Remark 3.7. *There is an exceptional isomorphism between $L_2(3)$ and A_4 [120, Section 3.3.1], but in this context it is more appropriate to think of groups isomorphic to these as $L_2(3)$, and we denote them as such hereafter.*

The intersection of more than two maximal subgroups is dealt with in one of the cases listed in the preceding lemmas. The only new case is the Hall subgroup itself which can equal the intersection of the derived subgroup, a Sylow 2-subgroup normaliser and a Hall subgroup normaliser. We require one final lemma.

Lemma 3.8. *If $H \leqslant R(3)$ is cyclic of order 3 and occurs as the intersection of a number of maximal subgroups of $R(3)$, then it is generated by an element from the conjugacy class $3B$, that is, an element of order 3 lying in the complement of the derived subgroup.*

Proof. We prove this by contradiction. Assume that H is a cyclic subgroup of order 3 generated by an element from the conjugacy class $3A$ and occurs as the intersection of maximal subgroups in $R(3)$. The only maximal subgroups which contain elements from the conjugacy class $3A$ are the derived subgroup and a unique point stabiliser whose intersection, by Lemma 3.4, is isomorphic to the dihedral group of order 18. Hence the result. □

Remark 3.9. *We denote by $3b$ a cyclic subgroup generated by an element from the conjugacy class $3B$.*

Since the list of conjugacy classes of subgroups of $H \leqslant R(3)$ which occur as intersections of maximal subgroups is relatively small, we can enumerate all containments between such subgroups to determine $\mu_G(H)$. The necessary values are compiled in Table 3.1 from which the Möbius function can be determined. In order to facilitate computation, conjugacy class representatives of subgroups are presented in pairs, with $H \nleqslant R(3)'$ succeeded by $H \cap R(3)'$.

This ultimately gives us the following.

Theorem 3.10. *The inversion formula for $R(3)$ is*

$$\begin{aligned}\phi(R(3)) = \sigma(R(3)) - 9\sigma(2^3\!:\!7\!:\!3) - 28\sigma(9\!:\!6) - 36\sigma(7\!:\!6) + 72\sigma(7\!:\!3) + 504\sigma(6) - 504\sigma(3b)\\ -\sigma(L_2(8)) + 9\sigma(2^3\!:\!7) + 28\sigma(9\!:\!2) + 36\sigma(7\!:\!2) - 72\sigma(7) - 504\sigma(2) + 504\sigma(1).\end{aligned}$$

Remark 3.11. *The Möbius function of $L_2(8)$ is known [34] and can be expressed a posteriori in terms of the Möbius function of $R(3)$ in the following way. For $H \leqslant R(3)$, let $H' = H \cap R(3)'$. Then*

$$\nu_{R(3)}(H)\mu_{R(3)}(H) = \mu([H : H'])\nu_{L_2(8)}(H)\mu_{L_2(8)}(H').$$

This behaviour can be described by Crapo's complementation theorem [29, Theorem 3] and the group-theoretic extension due to Pahlings [90, Lemma 1]. Compare this with the case of A_7 and S_7. Their

K	$R(3)$	$L_2(8)$	$9:6$	$9:2$	$7:6$	$7:2$	$2^3:7:3$	$2^3:7$	$7:3$	7	6	2	$3b$	1
$\mu_G(K)$	1	-1	-1	1	-1	1	-1	1	2	-2	2	-8	-6	504
$R(3)$	1													
$L_2(8)$	1	1												
$9:6$	1	–	1											
$9:2$	1	1	1	1										
$7:6$	1	–	–	–	1									
$7:2$	1	1	–	–	1	1								
$2^3:7:3$	1	–	–	–	–	–	1							
$2^3:7$	1	1	–	–	–	–	1	1						
$7:3$	1	–	–	–	1	–	2	–	1					
7	1	1	–	–	1	1	2	2	1	1				
6	1	–	1	–	1	–	1	–	–	–	1			
2	1	1	4	4	4	4	1	1	–	–	4	1		
$3b$	1	–	1	–	3	–	3	–	3	–	3	–	1	
1	1	1	28	28	36	36	9	9	36	36	252	63	84	1

Table 3.1: Table of values for $\nu_K(H)$ with the isomorphism class of H in the left hand column.

Möbius functions are known [26] and we have the following. There are two conjugacy classes of maximal subgroups isomorphic to $L_2(7)$ in A_7 and so $\mu_{A_7}(L_2(7)) = -1$. However, in $Aut(A_7) \cong S_7$ the two conjugacy classes of subgroups of A_7 isomorphic to $L_2(7)$ fuse into a single class, hence there is no subgroup $H \leqslant S_7$ such that H has an index 2 subgroup isomorphic to $L_2(7)$. Moreover, we have $\mu_{S_7}(L_2(7)) = 0$.

3.2 The structure of the simple small Ree groups

We turn now to the simple small Ree groups. Throughout this section $G = R(q)$ denotes a simple small Ree group, $q = 3^n$ is an odd power of 3 with $n > 1$ and Ω is a set of size $q^3 + 1$ on which $R(q)$ acts 2-transitively.

3.2.1 Conjugacy classes and centralisers of elements in $R(q)$

We begin by describing the conjugacy classes of elements of G and in particular the action of their elements on Ω. We assemble the necessary results from the character table of $R(q)$, due to Ward [114], as well as results from Levchuk and Nuzhin [77] and the summary given by Jones in [67].

The Sylow 2-subgroups of G are elementary abelian of order 8 and the normaliser of $S \in \mathrm{Syl}_2(G)$ in G has shape $2^3:7:3 \cong A\Gamma L_1(8)$. From this it follows that G contains no elements of order 4 and that there is a unique conjugacy class of involutions in G. An involution in G is represented by t and fixes $q+1$ points in Ω, which we denote by Ω^t and refer to as the **block** of t. The centraliser in G of t has shape $2 \times L_2(q)$ and acts 2-transitively on the block of t [81]. Any two distinct blocks can intersect in at most one point and any two points belong to a unique block.

The Sylow 3-subgroups of G have order q^3, exponent 9 and the normaliser of $S \in \mathrm{Syl}_3(G)$ in G has shape $q^{1+1+1}\colon(q-1)$. Elements of order 3 fix a single point in Ω and fall into one of three conjugacy classes, $\mathcal{C}_3^0$, $\mathcal{C}_3^+$ and $\mathcal{C}_3^-$. If $g \in \mathcal{C}_3^0$, then the centraliser of g in G has order q^3 and g is conjugate to its inverse. Elements belonging to $\mathcal{C}_3^+$ are denoted by u and their inverses belong to $\mathcal{C}_3^-$. We denote their union by $\mathcal{C}_3^* = \mathcal{C}_3^+ \cup \mathcal{C}_3^-$ and the centraliser in G of u has order $2q^2$. Elements of order 6 fix a single point in Ω and fall into two conjugacy classes, $\mathcal{C}_6^+$, $\mathcal{C}_6^-$ whose union we denote by $\mathcal{C}_6^*$. They are the commuting product of an involution with an element of $\mathcal{C}_3^*$ and hence we denote them by tu. If $tu \in \mathcal{C}_6^+$, then its centraliser in G has order $2q$ and $tu^{-1} \in \mathcal{C}_6^-$. Elements of order 9 also fix a single point in Ω and fall into three conjugacy classes $\mathcal{C}_9^0$, $\mathcal{C}_9^+$ and $\mathcal{C}_9^-$. Elements belonging to $\mathcal{C}_9^0$ are conjugate to their inverse where the inverse of an element in $\mathcal{C}_9^+$ belongs to $\mathcal{C}_9^-$. If $g \in \mathcal{C}_9^0 \cup \mathcal{C}_9^+ \cup \mathcal{C}_9^-$ then the centraliser in G of g has order 9 and $g^3 \in \mathcal{C}_3^0$.

The remaining elements of G are all semisimple and are best described in terms of the Hall subgroups to which they belong. The Hall subgroups A_i, for $i = 0, 1, 2, 3$, are each cyclic, having the following orders

$$|A_0| = \frac{1}{2}(q-1), \;\; |A_1| = \frac{1}{4}(q+1), \;\; |A_2| = q - \sqrt{3q} + 1, \;\; |A_3| = q + \sqrt{3q} + 1$$

so that G has order

$$|G| = 2^3 q^3 |A_0||A_1||A_2||A_3|.$$

Elements of order $k \neq 2$ dividing $q-1$ are conjugate to some power of tr, the commuting product of an involution, t, with an element, r, belonging to a Hall subgroup A_0. Such an element fixes two points in Ω and $|C_G(tr)| = q-1$. The remaining elements of G do not fix any points in Ω and have order $k \geq 7$ dividing $q^3+1 = (q+1)(q-\sqrt{3q}+1)(q+\sqrt{3q}+1)$. Elements of order 7 are all conjugate and divide one of these three factors of q^3+1 according to the value of q modulo 7. Otherwise there are elements of order $k > 7$ dividing $(q+1)/2$ conjugate to some power of ts, the commuting product of an involution, t, with an element, s of a Hall subgroup, A_1; elements, v, of order dividing $q - \sqrt{3q} + 1$; and elements, w, of order dividing $q + \sqrt{3q} + 1$. Their centralisers in G have the following orders: $|C_G(ts)| = q+1$, $|C_G(v)| = q - \sqrt{3q} + 1$ and $|C_G(w)| = q + \sqrt{3q} + 1$.

From Sylow's Theorems and the fact that in $R(q)$ a Hall subgroup is the centraliser of any Sylow p-subgroup which it contains, we have that isomorphic Hall subgroups are conjugate in G. We make the following definition which will be necessary.

Definition 3.12. *Let $q = 3^n$ be an odd power of* 3*. For a positive divisor m of n we define*

$$a_1(m) = 3^m + 1, \;\; a_2(m) = 3^m - 3^{\frac{m+1}{2}} + 1, \;\; a_3(m) = 3^m + 3^{\frac{m+1}{2}} + 1.$$

We may simply write a_i when $m = n$ and if no confusion can arise.

3.2.2 Maximal subgroups

The maximal subgroups of the simple small Ree groups were determined by Levchuk and Nuzhin [77] and independently by Kleidman [73]. They are conjugate to one of those listed in Table 3.2. In order to determine their possible mutual intersections, we describe the action of the maximal subgroups on Ω.

Group	Description
$R(q^{1/p})$, p prime	Maximal subfield subgroups
$q^{1+1+1}:(q-1)$	Parabolic subgroups
$2 \times L_2(q)$	Involution centralisers
$(2^2 \times D_{(q+1)/2}):3$	Four-group normalisers
$q - \sqrt{3q} + 1:6$	Normalisers of a Hall subgroup A_2
$q + \sqrt{3q} + 1:6$	Normalisers of a Hall subgroup A_3

Table 3.2: Conjugacy classes of maximal subgroups of the simple small Ree groups $R(q)$.

Subfield subgroups

As shown by Tits in [112], the group $R(q)$, where $q = 3^n$, can be seen as the group of automorphisms of a certain 6-dimensional projective variety defined over $\mathbb{F}_q$ consisting of $q^3 + 1$ points. A subfield subgroup is then conjugate to the group of automorphisms stabilising the points of this variety defined over a subfield of $\mathbb{F}_q$. If we let Ω denote the underlying set of $3^{3n} + 1$ points of this variety, then a subfield subgroup is isomorphic to $R(3^m)$ and stabilises $3^{3m}+1$ points in Ω, for m dividing n. These subgroups are maximal when they are defined over maximal subfields of $\mathbb{F}_q$, that is, when the n/m is prime. We write G_m for a subgroup isomorphic to $R(3^m)$ and note that any two isomorphic subfield subgroups are conjugate in G [77]. For a subfield subgroup G_m we write $\Omega(m)$ for the set of $3^{3m} + 1$ points in Ω stabilised by the Sylow 3-subgroups of G_m. The fixed points of elements of G_m all belong to $\Omega(m)$ with the exception of the blocks of the involutions in G_m which consist of $3^m + 1$ points in $\Omega(m)$ and $3^n - 3^m$ points in $\Omega \setminus \Omega(m)$.

Parabolic subgroups

The parabolic subgroups of G are the normalisers of the Sylow 3-subgroups. They consist of all elements fixing a point $\omega \in \Omega$. As such we refer to them as point stabilisers, and the stabiliser of the point $\omega \in \Omega$ is denoted by P_ω. Let S be a Sylow 3-subgroup of G. The centre of S is elementary abelian of order q and nontrivial elements belong to the conjugacy class $\mathcal{C}_3^0$. This is contained in an elementary abelian normal subgroup of S of order q^2. The elements of this normal subgroup that do not belong to $Z(S)$ belong to $\mathcal{C}_3^*$. All remaining elements of S have order 9 [114] and all remaining elements of $P_\omega \setminus S$ have order 6 or a divisor of $q-1$.

Involution centralisers

Let $t \in G$ be an involution, $C = C_G(t)$ its centraliser in G and Ω^t the block of t stabilised by C. The action of the derived subgroup $C' \cong L_2(q)$ on Ω^t is the expected 2-transitive action of $L_2(q)$ as its natural degree $q+1$ permutation representation [81]. Elements of C of order 3 belong to $\mathcal{C}_3^*$ and fix a point in Ω^t, elements of order dividing $q-1$ fix two points in Ω^t and elements of order dividing $(q+1)/2$ do not fix any points in Ω^t. It follows that any pair of commuting involutions in G have disjoint blocks. If $t_1 \neq t_2$ are non-commuting involutions in C, then their blocks are also disjoint, since otherwise they would intersect in at most one point in Ω^t and be contained in a point stabiliser. The only dihedral subgroups of a point stabiliser are isomorphic to D_6 and D_{18} which, from the list of maximal subgroups of $L_2(q)$ [32] cannot occur. There can then be at most $(q^3+1)/(q+1) = q^2 - q + 1$ involutions in C. The involutions of $C' \cong L_2(q)$ are all conjugate and so there are three conjugacy classes of involutions in C:

1. $\{t\}$, the central involution,
2. the $q(q-1)/2$ involutions in L, and
3. the $q(q-1)/2$ involutions in the coset tL

so that there are a total of $q^2 - q + 1$ involutions in C and we see that for any $\omega \in \Omega$, ω belongs to the block of one and only one involution in C. The blocks of the involutions in C then form a disjoint partition of Ω.

Four-group normalisers

The four-group normalisers of G can be built in two different ways.

- Let $t_1 \neq t_2$ be commuting involutions in G with $t_3 = t_1 t_2$. The four-group $V = \langle t_1, t_2 \rangle$ is centralised in G by a dihedral subgroup of shape $D_{(q+1)/2}$ and normalised by an element $u \in \mathcal{C}_3^*$ cyclically permuting the involutions in V. The normaliser in G of V is then $N = N_G(V) \cong (2^2 \times D_{(q+1)/2}){:}3$.
- Alternatively, let $\langle s \rangle$ be a Hall subgroup conjugate to A_1. The centraliser of $\langle s \rangle$ in G is a unique four-group, V, and $V \times \langle s \rangle$ is normalised by an element, τu, of order 6, where τ commutes with V and u normalises $\langle s \rangle$.

A counting argument shows that $\langle s \rangle$ belongs to a unique four-group normaliser, whereas a four-group belongs to $1 + 3(q+1)/2$ four-group normalisers. To avoid confusion with the normalisers of the other Hall subgroups, we refer to groups conjugate to N in G as four-group normalisers.

There are four subgroups of N isomorphic to $D_{(q+1)/2}$. One of them is normal in N, which we denote by D_τ, the other three are conjugate in N and we denote a representative by $D_{\tau'}$. The three conjugacy classes of involutions in $N_G(V)$ are then the following:

1. the class consisting of the 3 involutions in V, namely t_1, t_2 and t_3,
2. the class of $(q+1)/4$ involutions in D_τ, whose representative we denote by τ, and;
3. the class of $3(q+1)/4$ involutions in the conjugates of $D_{\tau'}$ in N, whose representative we denote by τ'.

The centraliser of τ in N is $C_N(\tau) \cong 2 \times L_2(3)$; conversely, if L is a subgroup of N isomorphic to $2 \times L_2(3)$, then its central involution is conjugate to τ since the only conjugacy class of involutions whose order is not divisible by 3 is that of τ. The centraliser of τ' in N is a Sylow 2-subgroup of N which is a Sylow 2-subgroup of G and is thus elementary abelian of order 8. If $V_{\tau'} \neq V$ is a four-group in N, then one and only one of its nontrivial involutions belongs to V, at most one of its involutions is conjugate to τ and at most one of its involutions is conjugate to τ' since the order of D_τ is not divisible by 4. Thus, $V_{\tau'}$ is conjugate in N to either $\langle t_i, t_i\tau\rangle$ or $\langle t_i, t_j\tau\rangle$ where $i \neq j$, $1 \leq i, j \leq 3$ and $t_i\tau$ and $t_j\tau$ are both conjugate in N to τ'.

The geometric interpretation of N is then as follows. The nontrivial elements of V fix a mutually disjoint triple of blocks in Ω. In fact, any pair of involutions in N fixes a disjoint pair of blocks in Ω, since all involutions belong to the centraliser of an involution in V. The orbits of s stabilise the blocks of all involutions in N and since elements of order $(q+1)/2$ are conjugate to the commuting product of a nontrivial element of V with an element conjugate to τ' we have that elements of order $(q+1)/2$ are composed of four cycles of length $(q+1)/4$ and $2(q^2-q)$ cycles of length $(q+1)/2$. The fixed point of an element of N conjugate to u or u^{-1} belongs to the block of an involution conjugate to τ and, from above, we have that $C_N(\tau)$ acts doubly transitively on four of the points in Ω^τ. Furthermore, the four conjugate cyclic subgroups of order 3 in $C_N(\tau)$ each stabilise one of these four points. Elements conjugate to τu or τu^{-1} behave similarly to u or u^{-1}.

Normalisers of Hall subgroups A_2, A_3

The cyclic Hall subgroups, A_2, A_3, are normalised by cyclic subgroups of order 6. Let $A = \langle a\rangle$ be conjugate to a Hall subgroup A_2 or A_3, and let N be its normaliser in G; the geometric picture of $N_G(A_2)$ is analogous to that of $N_G(A_3)$. Since nontrivial elements of A do not fix any points in Ω and A is centralised only by the cyclic subgroup it generates, the action of A partitions Ω into $(q^3+1)/|A|$ subsets of size $|A|$. If $u \in \mathcal{C}_3^*$ normalises A, then there are $|A|$ conjugates of u in N and the fixed points of elements conjugate to u belong to a unique subset of this partition. For each conjugate of u there is an involution t with which it commutes and so the fixed point of u belongs to the block of t. The remaining elements in the block of t each belong to a unique orbit of a, since if an orbit of a contained more than one element of Ω^t then t would commute with a. As with the four-group normalisers, elements conjugate to tu behave similarly to the elements conjugate to u.

3.3 The Möbius function of the simple small Ree groups

Throughout this section $G = R(q)$ is a simple small Ree group, $q = 3^n$ is an odd power of 3 and G acts 2-transitively on a set Ω of size $q^3 + 1$, as described in the previous section. In order to facilitate the determination of the Möbius function of G we would like to restrict ourselves to a small number of classes of subgroups of G by proving that any subgroup, H, lying outside these classes has $\mu_G(H) = 0$. From Theorem 1.14 a necessary condition for a subgroup H of G to have $\mu_G(H) \neq 0$ is that H is the intersection of a number of maximal subgroups of G. However, as we shall see, there are various classes of subgroups which can exist as intersections of maximal subgroups that also have $\mu_G(H) = 0$. In anticipation we define the collection of classes of subgroups of G appearing in Table 3.3 as **MaxInt**.

Class	Isomorphism type	Description
$\boldsymbol{R}(l)$	$R(3^l)$	Subfield subgroups
$\boldsymbol{P}(l)$	$(3^l)^{1+1+1}:(3^l-1)$	Parabolic subgroups in $R(3^l)$
$\boldsymbol{C}_t(l)$	$2 \times L_2(3^l)$	Involution centralisers in $R(3^l)$, $l > 1$
$\boldsymbol{C}_t^{\omega}(l)$	$2 \times (3^l : \frac{3^l-1}{2})$	Point stabilisers of elements of $\boldsymbol{C}_t(l)$, $l > 1$
$\boldsymbol{F}(l)$	3^l	Sylow 3-subgroups of elements of $\boldsymbol{C}_t(l)$, $l > 1$
$\boldsymbol{C}_0(l)$	$3^l - 1$	Centralisers of Hall subgroups A_1 in $R(3^l)$, $l > 1$
$\boldsymbol{N}_V(l)$	$(2^2 \times D_{(3^l+1)/2}):3$	Four-group normalisers in $R(3^l)$, $l > 1$
$\boldsymbol{N}_2(l)$	$a_2(l):6$	Normalisers of Hall subgroups A_2 in $R(3^l)$, $l > 1$
$\boldsymbol{N}_3(l)$	$a_3(l):6$	Normalisers of Hall subgroups A_3 in $R(3^l)$
$\boldsymbol{C}_V(l)$	$2^2 \times D_{(3^l+1)/2}$	Four-group centralisers in $R(3^l)$, $l > 1$
$\boldsymbol{D}_2(l)$	$D_{2a_2(l)}$	Normal dihedral subgroups of elements of $\boldsymbol{N}_V(l)$, $l > 1$
$\boldsymbol{D}_3(l)$	$D_{2a_3(l)}$	Normal dihedral subgroups of elements of $\boldsymbol{N}_V(l)$
$\boldsymbol{C}_t(1)$	$2 \times L_2(3)$	Involution centralisers in $R(3)$
$\boldsymbol{E}$	2^3	Sylow 2-subgroups of G
$\boldsymbol{V}$	2^2	Four-groups
$\boldsymbol{C}_6^*$	6	Cyclic subgroups of order 6 generated by $tu \in \mathcal{C}_6^+$
$\boldsymbol{C}_3^*$	3	Cyclic subgroups of order 3 generated by $u \in \mathcal{C}_3^+$
$\boldsymbol{C}_2$	2	Cyclic subgroups of order 2
$\boldsymbol{I}$	1	The identity subgroup

Table 3.3: The disjoint subsets of **MaxInt**. Each subset consists of subgroups of G for all l dividing n unless otherwise stated.

Remark 3.13. *For classes appearing in Table 3.3, where we omit the* (l) *by writing, for example* $\boldsymbol{P}$*, we mean those elements for which* $l = n$ *or in the case of* $\boldsymbol{R}$*, the maximal subfield subgroups. In certain classes we have made exclusions to avoid the following repetitions*

$$\boldsymbol{N}_V(1) = \boldsymbol{C}_t(1), \quad \boldsymbol{C}_V(1) = \boldsymbol{E}, \quad \boldsymbol{C}_t^{\omega}(1) = \boldsymbol{C}_6^*, \quad \boldsymbol{F}(1) = \boldsymbol{C}_3^*, \quad \boldsymbol{D}_2(1) = \boldsymbol{C}_0(1) = \boldsymbol{C}_2.$$

In particular, the list is ordered so that no element of a class appears in more than one class. Furthermore, no element of any class of **MaxInt** *is a subgroup of any element of a successive class in the stated ordering with the possible exceptions of elements of* $\boldsymbol{N}_2(l)$ *being subgroups of elements of* $\boldsymbol{N}_3(l)$ *and elements of* $\boldsymbol{D}_2(l)$ *being subgroups of elements of* $\boldsymbol{D}_3(l)$*.*

Our aim is to then prove the following lemma.

Lemma 3.14. *Let* G *be a simple small Ree group and let* $H \leqslant G$*. If* $\mu_G(H) \neq 0$*, then* $H \in$ **MaxInt***.*

3.3.1 Conjugacy classes and normalisers of subgroups in $R(q)$

An important step in determining the inversion formula of a group is to determine the conjugacy classes of contributing subgroups along with their sizes. The following results are also necessary in enumerating containments between subgroups in **MaxInt**. Since they are logically independent from determining the Möbius function of G and will be used along the way to proving Lemma 3.14, we state them first.

Lemma 3.15. *Elements of* $\boldsymbol{R}(l) \cup \boldsymbol{P}(l) \cup \boldsymbol{C}_t(l) \cup \boldsymbol{C}_t(1) \cup \boldsymbol{C}_t^{\omega}(l) \cup \boldsymbol{N}_V(l) \cup \boldsymbol{N}_2(l) \cup \boldsymbol{N}_3(l)$ *are self-normalising in* G*.*

Proof. If $H \in \boldsymbol{R}(l)$, then H is contained only in larger subfield subgroups, all of which are simple, hence $N_G(H) = H$. If $H \cong (3^h)^{1+1+1}\!:(3^h - 1) \in \boldsymbol{P}(l)$, then H is self-normalising in G for the following reason. The Sylow 3-subgroup $S \leqslant H$ is characteristic in H and since the normaliser in G of S is equal to H, we have $N_G(H) = H$. If $H \cong 2 \times L_2(3^h) \in \boldsymbol{C}_t(l) \cup \boldsymbol{C}_t(1)$ or $H \cong 2 \times (3^h\!:\frac{3^h-1}{2}) \in \boldsymbol{C}_t^{\omega}$, then the normaliser of H in G must fix its central involution and so $N_G(H) \leqslant 2 \times L_2(q)$. Since subfield subgroups are self-normalising in $L_2(q)$ and since subgroups of $L_2(q)$ isomorphic to $3^h\!:\frac{3^h-1}{2}$ are also self-normalising in $L_2(q)$, we have that $N_G(H) = H$ in each case. If $H \in \boldsymbol{N}_V(l) \cup \boldsymbol{N}_2(l) \cup \boldsymbol{N}_3(l)$, then H contains a characteristic subgroup, A, of order $(3^h+1)/4$, $3^h - \sqrt{3^{h+1}} + 1$ or $3^h + \sqrt{3^{h+1}} + 1$ as appropriate, which is normalised by a cyclic subgroup of order 6. The normaliser in G of H must also then normalise the subgroup $A\!:6$, but, since elements whose order is a strict multiple of $|A|$ do not normalise $A\!:6$, we have $N_G(H)$ is equal to H. $\square$

Lemma 3.16. *Elements of* $\boldsymbol{C}_V(l)$ *are normalised in* G *by elements of* $\boldsymbol{N}_V(l)$*.*

Proof. If $H \cong 2^2 \times D_{(3^h+1)/2} \in \boldsymbol{C}_V(l)$, then the normaliser in G of H must fix its characteristic normal subgroup of order $(3^h+1)/4$, as well as its normal four-group. From this it follows that $N_G(H) \cong (2^2 \times D_{(3^h+1)/2})\!:3 \in \boldsymbol{N}_V(l)$. $\square$

Lemma 3.17. *Elements of $\boldsymbol{D}_i(l)$ are normalised in G by a subgroup isomorphic to $(2^2 \times D_{2a_i(l)}):3$, where $i = 2, 3$.*

Proof. If $D \in \boldsymbol{D}_2(l) \cup \boldsymbol{D}_3(l)$ is isomorphic to $D_{2a_2(h)}$ or $D_{2a_3(h)}$ then D is contained in the normal dihedral subgroup of order $(q+1)/2$ in a four-group normaliser, N. Hence, the normal subgroup of D of order $a_2(h)$ or $a_3(h)$, as appropriate, is characteristic in N, and is normalised in N by an element of order 3. The normaliser in G of H is then isomorphic to $(2^2 \times D_{2a_i(l)}):3$, as claimed. □

If $H \in \boldsymbol{E} \cup \boldsymbol{V} \cup \boldsymbol{C}_2 \cup \boldsymbol{I}$, then the normaliser of H in G is clear or has already been established. This leaves the following lemma to prove.

Lemma 3.18. *Let $H \leqslant R(q)$, where $q = 3^n$, and $H \in \boldsymbol{F}(l) \cup \boldsymbol{C}_0(l) \cup \boldsymbol{C}_6^* \cup \boldsymbol{C}_3^*$.*

1. *If $H \cong 3^h \in \boldsymbol{F}(l) \cup \boldsymbol{C}_3^*$, then $N_G(H) \cong q^{1+1}:(3^h - 1)$.*

2. *If $H \cong 3^h - 1 \in \boldsymbol{C}_0(l)$, then $N_G(H) \cong D_{2(q-1)}$.*

3. *If $H \cong 6 \in \boldsymbol{C}_6^*$, then $N_G(H) \cong 2 \times q$.*

Proof. We determine the normaliser in G of H by beginning with its centraliser in G.

1. If $H \cong 3^h \in \boldsymbol{F}(l)$, then the nontrivial elements of H belong to $\mathcal{C}_3^*$ with $|H \cap \mathcal{C}_3^+| = |H \cap \mathcal{C}_3^-| = (3^h - 1)/2$. Let $S \in \mathrm{Syl}_3(G)$ be the unique Sylow 3-subgroup to which H belongs and let $h \in H$ be nontrivial. The centraliser in G of H is contained in $C_G(h)$ which has order $2q^2$. Since H belongs to the elementary abelian normal subgroup of order q^2 in S and since H belongs to an involution centraliser, we have $|C_G(H)| = 2q^2$. The elements normalising but not centralising H in G are of order $(3^h - 1)/2$ and belong to the subgroup of G isomorphic to $L_2(3^h)$ containing H. Hence the full normaliser in G of H has size $q^2(q-1)$.

2. If $H \cong 3^h - 1 \in \boldsymbol{C}_0(l)$, then the normaliser of H in G must fix the unique central involution in H and so $N_G(H) \leqslant 2 \times L_2(q)$. The normaliser in $L_2(q)$ of an element of order $(q-1)/2$ is dihedral of order $q - 1$ from which is follows that $N_G(H) \cong 2 \times D_{q-1} \cong D_{2(q-1)}$.

3. If $H \cong 6 \in \boldsymbol{C}_6^*$, then as in the previous case, the normaliser in G of H must fix the unique involution of H and so $N_G(H) \leqslant 2 \times L_2(q)$. Since the normaliser in $L_2(q)$ of an element of order 3 is its Sylow 3-subgroup, we have $N_G(H) \cong 2 \times q$.

This completes the proof. □

The following will aid us in determining the conjugacy classes of subgroups in **MaxInt**.

Lemma 3.19. *Let G be a simple small Ree group and let $\boldsymbol{R}(l)$ be the set of subfield subgroups of G. If $G_m, G_k \in \boldsymbol{R}(l)$ are isomorphic, then they are conjugate in G.*

Proof. The proof of this can be found in [77]. □

Lemma 3.20. *Isomorphic elements of* **MaxInt** *are conjugate in* G.

Proof. By Lemma 3.19 isomorphic elements of $\boldsymbol{R}(l)$ are conjugate in G. Since maximal subgroups of G are conjugate in G if they are isomorphic it follows that isomorphic elements of $\boldsymbol{P}(l) \cup \boldsymbol{C}_t(l) \cup \boldsymbol{C}_t(1) \cup \boldsymbol{N}_V(l) \cup \boldsymbol{N}_2(l) \cup \boldsymbol{N}_3(l)$ are also conjugate in G. The conjugacy of isomorphic elements of $\boldsymbol{E} \cup \boldsymbol{V} \cup \boldsymbol{C}_2$ is immediate from their conjugacy within the normaliser of a Sylow 2-subgroup of G [114] and from the preceding statements it follows that isomorphic elements of $\boldsymbol{C}_V(l) \cup \boldsymbol{D}_2(l) \cup \boldsymbol{D}_3(l)$ are conjugate. Isomorphic elements of $\boldsymbol{C}_0(l) \cup \boldsymbol{C}_6^* \cup \boldsymbol{C}_3^* \cup \boldsymbol{I}$ are generated by conjugate elements in G and so isomorphic subgroups belonging to these classes are conjugate in G. Elements of $\boldsymbol{C}_t^\omega(l)$ are involution centralisers of elements in $\boldsymbol{P}(l)$ and since involutions are conjugate in each element of $\boldsymbol{P}(l)$, isomorphic elements of $\boldsymbol{C}_t^\omega(l)$ are conjugate in G. Finally, since elements of $\boldsymbol{F}(l)$ are the Sylow 3-subgroups of conjugate elements of $\boldsymbol{C}_t(l)$, we have that isomorphic elements of $\boldsymbol{F}(l)$ are conjugate in G. This completes the proof. □

3.3.2 Intersections of maximal subgroups

We begin by proving a number of auxiliary results which determine how pairs of maximal subgroups intersect. Throughout this section $G = R(q)$ denotes a simple small Ree group acting 2-transitively on Ω, a set of size $q^3 + 1$, as described above. We let $\omega \in \Omega$ and $P_\omega \in \boldsymbol{P}$ denote the stabiliser of ω in G. We let $t \in G$ denote an involution, $C = C_G(t) \in \boldsymbol{C}_t$ its centraliser in G and Ω^t the points in Ω fixed by t. A subfield subgroup is denoted by $G_m \in \boldsymbol{R}(l)$, where m divides n, and $\Omega(m)$ denotes the $3^{3m} + 1$ points in Ω stabilised by the Sylow 3-subgroups of G_m. A four-group of G is denoted by V and the normaliser in G of V is denoted by $N = N_G(V) \in \boldsymbol{N}_V$.

Intersections with parabolic subgroups

From our discussion on the action of elements of G on Ω, intersections with parabolic subgroups are relatively straightforward to determine.

Lemma 3.21. *Let* $P_\omega \in \boldsymbol{P}$*, let* $M \neq P_\omega$ *be a maximal subgroup of* G *and let* $H = M \cap P_\omega$.

1. *If* $M \in \boldsymbol{R}$ *is a maximal subfield subgroup, then* $H \in \boldsymbol{P}(l) \cup \boldsymbol{C}_2 \cup \boldsymbol{I}$.
2. *If* $M \in \boldsymbol{P} \setminus \{P_\omega\}$*, then* $H \in \boldsymbol{C}_0$.
3. *If* $M \in \boldsymbol{C}_t$*, then* $H \in \boldsymbol{C}_t^\omega \cup \boldsymbol{C}_2$.
4. *If* $M \in \boldsymbol{N}_V \cup \boldsymbol{N}_2 \cup \boldsymbol{N}_3$*, then* $H \in \boldsymbol{C}_6^* \cup \boldsymbol{C}_3^* \cup \boldsymbol{C}_2 \cup \boldsymbol{I}$.

Proof. (1) Let $G_m \in \boldsymbol{R}$ be a maximal subfield subgroup. If $\omega \in \Omega(m)$ then the intersection of G_m with P_ω is the stabiliser of ω in G_m, belonging to $\boldsymbol{P}(l)$. If $\omega \notin \Omega(m)$ and $H \notin \boldsymbol{I}$, then ω lies in the block of a unique involution in G_m, in which case $H \in \boldsymbol{C}_2$.
(2) The Sylow 3-subgroups of G have trivial intersection and anything lying in two distinct parabolic

subgroups must pointwise fix two points, hence $H \in \boldsymbol{C}_0$.

(3) If $\omega \in \Omega^t$ then H is isomorphic to the direct product of $\langle t \rangle$ with a point stabiliser in $L_2(q)$, hence $H \cong 2 \times (q\colon \frac{q-1}{2}) \in \boldsymbol{C}_t^{\omega}$. Otherwise, since ω belongs to the block of exactly one involution of M, if $\omega \notin \Omega^t$, then $H \in \boldsymbol{C}_2$.

(4) This follows from comparison of the orders of these groups. $\square$

Intersections with maximal subfield subgroups

In the case of the maximal subfield subgroups, their intersection is a little less well-behaved in certain cases. From analysis using GAP it can be shown that when $G = R(27)$ a number of possibilities arise for the intersection of two subgroups isomorphic to $R(3)$. This list includes subgroups we might not naturally expect, such as those of shape 3, 3^2, 9 or $3 \times S_3$. In order not to have to deal with these cases we prove the following lemmas which allow us to immediately rule out a large class of subgroups $H \leqslant G$ which occur as the intersection of maximal subgroups, but have $\mu_G(H) = 0$. In order to determine them, we use the preceding lemmas in this section to determine the Möbius function of a number of classes of subgroups in **MaxInt**. We first prove the following partial result on the intersection of maximal subfield subgroups.

Lemma 3.22. *Let $G_{m_1}, G_{m_2} \in \boldsymbol{R}$ be maximal subfield subgroups of G. If $|\Omega(m_1) \cap \Omega(m_2)| \geq 3$, then $G_{m_1} \cap G_{m_2} \in \boldsymbol{R}(l)$.*

Proof. Let $\Omega(m_1, m_2) = \Omega(m_1) \cap \Omega(m_2)$, let ω_1, ω_2 and ω_3 be three distinct elements of $\Omega(m_1, m_2)$ and let t_i be the unique involution fixing ω_j and ω_k pointwise where $1 \leq i, j, k \leq 3$ are distinct. The subgroup $T = \langle t_1, t_2, t_3 \rangle$ is not contained in a parabolic subgroup of G and furthermore, since any pair of involutions contained in an involution centraliser or a four-group or Hall subgroup normaliser have disjoint blocks, we have that $L_2(8) \leqslant T \leqslant G_{m_0}$ where m_0 divides $\gcd(m_1, m_2)$. Since subgroups isomorphic to $L_2(8)$ are contained in a unique subgroup isomorphic to $R(3)$, which is a subgroup of both G_{m_1} and G_{m_2}, we have that $H \in \boldsymbol{R}(l)$. $\square$

In the subsequent lemmas we summarise the calculation of each $\mu_G(H)$ in a table where we record the overgroups $K \geqslant H$ contributing to $\mu_G(H)$ according to their isomorphism type. These correspond to the classes of **MaxInt**. The subgroups H generally occur for each positive divisor h of n and their overgroups occur for k dividing n such that h divides k. Any extra conditions are recorded in the table. We record the normaliser in K of H in order to aid computation of $\nu_K(H)$, the number of overgroups of H conjugate to K in G.

Lemma 3.23. *If $H \cong R(3^h) \in \boldsymbol{R}(l)$, then $\mu_G(H) = \mu(n/h)$.*

Proof. Let H be as in the hypotheses. If M is a maximal subgroup of G containing H, then M is a maximal subfield subgroup. A counting argument then shows that for a subfield subgroup $R(3^h)$, the subfield subgroups which contain it are in one-to-one correspondence with the elements of the lattice of positive divisors of n/h. This is summarised in Table 3.4 from which we see that $\mu_G(H) = \mu(n/h)$. $\square$

Isomorphism type of overgroup K	for $k \mid n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	$R(3^k)$	1	$\mu(n/k)$

Table 3.4: $H \cong R(3^h) \in \boldsymbol{R}(l)$

Lemma 3.24. *If $H \cong (3^h)^{1+1+1}:(3^h-1) \in \boldsymbol{P}(l)$, then $\mu_G(H) = -\mu(n/h)$.*

Proof. Let H be as in the hypotheses. Since H contains elements from the conjugacy classes $\mathcal{C}_0$, the only maximal subgroups containing H are maximal subfield subgroups or a unique parabolic subgroup. By Lemma 3.21 and since H is self normalising in G, for each positive divisor $h|k|n$ the only subgroups of G containing H are a unique element in $\boldsymbol{R}(l)$ and a unique element in $\boldsymbol{P}(l)$. We present this in Table 3.5 from which we see that $\mu_G(H) = -\mu(n/h)$. $\square$

Isomorphism type of overgroup K	for $k \mid n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	$(3^h)^{1+1+1}:(3^h-1)$	1	$\mu(n/k)$
$(3^k)^{1+1+1}:(3^k-1)$	$k > h$	$(3^h)^{1+1+1}:(3^h-1)$	1	$-\mu(n/k)$

Table 3.5: $H \cong (3^h)^{1+1+1}:(3^h-1) \in \boldsymbol{P}(l)$

Lemma 3.25. *If $H \leqslant P_\omega$ and $H \cap \mathcal{C}_3^0 \neq \varnothing$, then $\mu_G(H) \neq 0$ if and only if $H \in \boldsymbol{P}(l)$.*

Proof. Let H be as in the hypotheses. By Lemma 3.24 we can assume that $H \notin \boldsymbol{P}(l)$. Note that if $M \neq P_\omega$ is any other maximal subgroup of G containing H, then M is a maximal subfield subgroup. Also note that if H is contained in any subfield subgroup, G_m, not necessarily maximal, then the normaliser of H in G_m is equal to the normaliser of H in $G_m \cap P_\omega \in \boldsymbol{P}(l)$. We proceed by induction on H. Suppose that H is contained in P_ω, but no other element of $\boldsymbol{P}(l)$. This implies that H is not contained in any element of $\boldsymbol{R}(l) \setminus \{G\}$ and the only contributions to the Möbius function of H are those of G and P_ω, which cancel, and so $\mu_G(H) = 0$. Now, suppose H is as in our hypothesis and maximal so that our hypothesis is true for all overgroups of H. A counting argument shows that for each divisor k of n, the number of subgroups of G, conjugate to G_k, that contain H is equal to the number of subgroups $(3^k)^{1+1+1}:(3^k-1) \in \boldsymbol{P}(l)$ that contain H. As such, the Möbius function of H cancels at each divisor and we have $\mu_G(H) = 0$. This completes the induction step. $\square$

Before proving the following lemma we make an important observation. Let G_m be a subfield subgroup of G. A Hall subgroup of G conjugate to A_i, where $1 \leq i \leq 3$, is not necessarily contained in a Hall subgroup of G_m of order $a_i(m)$. We have more to say on this in the sequel, for now consider the particular case when $G = R(3^{3m})$. A subfield subgroup $G_m \leqslant G$ contains elements of Hall subgroups of G_m of orders $a_1(m)/4$, $a_2(m)$ or $a_3(m)$, but each of these elements is contained in some Hall subgroup of G conjugate to A_1 of order $(3^{3m}+1)/4$. The centraliser in G_m of such an element will then either be cyclic of order 6 or conjugate to $2 \times L_2(3)$ depending on whether $i = 1, 2$ or 3.

Lemma 3.26. *The intersection of a maximal subfield subgroup and an involution centraliser belongs to* $\boldsymbol{C}_t(l) \cup \boldsymbol{C}_t(1) \cup \boldsymbol{F}(l) \cup \boldsymbol{D}_2(l) \cup \boldsymbol{D}_3(l) \cup \boldsymbol{V} \cup \boldsymbol{C}_3^* \cup \boldsymbol{C}_2 \cup \boldsymbol{I}$.

Proof. Let $G_m \in \boldsymbol{R}$ and let $H = G_m \cap C$. If $|\Omega^t \cap \Omega(m)| \geq 2$, then $t \in G_m$ and H is the centraliser in G_m of t and belongs to $\boldsymbol{C}_t(l) \cup \boldsymbol{C}_t(1)$. If $\Omega^t \cap \Omega(m) = \{\omega\}$, then H is a subgroup of the Sylow 3-subgroup of C since any other element of C that stabilises more than one point in Ω^t stabilises more than one point in $\Omega(m)$. Hence $H \in \boldsymbol{F}(l) \cup \boldsymbol{C}_3^* \cup \boldsymbol{I}$.

Suppose now that $\Omega^t \cap \Omega(m) = \varnothing$. Then $t \notin G_m$ and H is isomorphic to a subgroup of $L_2(q)$ not containing elements of order 3, or dividing $(q-1)/2$, hence H is a subgroup of D_{q+1} [32]. If H does not contain elements of order $k > 2$ dividing $(q+1)/4$ then $H \leqslant V$ for some $V \in \boldsymbol{V}$ and belongs to our list. If there exists $s \in H$ of order k, then k divides $a_1(m)/4$ or $a_2(m/3)a_3(m/3)$ depending on whether 3 divides m or not. In the former case, the involutions which commute with s belong to G_m, contradicting our assumption, so that $s \notin H$. In the latter case, the involutions which commute with s do not belong to G_m, but $\langle s \rangle$ is normalised in G_m by an element of order 6. The involutions which normalise $\langle s \rangle$ in G_m then belong to H, but not the elements of order 3, hence H is isomorphic to $D_{2a_2(m/3)}$ or $D_{2a_3(m/3)}$. Furthermore, since $\langle s \rangle$ is normalised by an element of order 3, H is contained in the normal dihedral subgroup of order $(q+1)/2$ of a four-group normaliser. □

Lemma 3.27. *If* $H \cong 2 \times L_2(3^h) \in \boldsymbol{C}_t(l)$*, then* $\mu_G(H) = -\mu(n/h)$.

Proof. Let H be as in the hypothesis. The only maximal subgroups of G containing H are those in $\boldsymbol{R}(l)$ and in $\boldsymbol{C}_t(l)$. Since elements of $\boldsymbol{C}_t(l)$ are self-normalising, for each divisor $h|k|n$ there is a unique element in $\boldsymbol{R}(l)$ and in $\boldsymbol{C}_t(l)$ containing H. This is presented in Table 3.6 and from this we have that $\mu_G(H) = -\mu(n/h)$. □

Isomorphism type of overgroup K	for $k\|n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	$2 \times L_2(3^h)$	1	$\mu(n/k)$
$2 \times L_2(3^k)$	$k > h$	$2 \times L_2(3^h)$	1	$-\mu(n/k)$

Table 3.6: $H \cong 2 \times L_2(3^h) \in \boldsymbol{C}_t(l)$

Lemma 3.28. *If* $H \cong 2 \times (3^h : \frac{3^h-1}{2}) \in \boldsymbol{C}_t^{\omega}(l)$*, then* $\mu_G(H) = \mu(n/h)$.

Proof. Let H be as in the hypotheses. Since the order of H is divisible by 9 the only maximal subgroups of G containing H are maximal subfield subgroups, a unique parabolic subgroup and a unique involution centraliser. By Lemmas 3.21, 3.22 and 3.26 if $K \in \mathbf{MaxInt}$ contains H, then $K \in \boldsymbol{R}(l) \cup \boldsymbol{P}(l) \cup \boldsymbol{C}_t(l) \cup \boldsymbol{C}_t^\omega$. Since H is self-normalising in each subgroup which contains it, the enumeration of overgroups of H contributing to its Möbius function is as given in Table 3.7 from which we deduce that $\mu_G(H) = \mu(n/h)$. □

Isomorphism type of overgroup K	for $k\|n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	$2 \times (3^h : \frac{3^h-1}{2})$	1	$\mu(n/k)$
$(3^k)^{1+1+1} : (3^k - 1)$	–	$2 \times (3^h : \frac{3^h-1}{2})$	1	$-\mu(n/k)$
$2 \times L_2(3^k)$	–	$2 \times (3^h : \frac{3^h-1}{2})$	1	$-\mu(n/k)$
$2 \times (3^k : \frac{3^k-1}{2})$	$k > h$	$2 \times (3^h : \frac{3^h-1}{2})$	1	$\mu(n/k)$

Table 3.7: $H \cong 2 \times (3^h : \frac{3^h-1}{2}) \in \boldsymbol{C}_t^\omega(l)$

Lemma 3.29. *If $3^2 \leqslant H < K \cong 2 \times (3^k : \frac{3^k-1}{2}) \in \boldsymbol{C}_t^\omega(l)$, then $\mu_G(H) = 0$.*

Proof. Let $H \leqslant R(3^n)$ be as in the hypotheses. The Sylow 3-subgroup of H has order $2 \leq h \leq k$ for some h not necessarily dividing n and its non-trivial elements belong to $\mathcal{C}_3^*$. If M is a maximal subgroup of G containing H, then M is a maximal subfield subgroup, an involution centraliser or a unique parabolic subgroup. By Lemmas 3.21, 3.22, 3.26, the subgroups which contribute to the Möbius function of H belong to $\boldsymbol{R}(l) \cup \boldsymbol{P}(l) \cup \boldsymbol{C}_t(l) \cup \boldsymbol{C}_t^\omega$. In analogy with the proof of Lemma 3.25, if $P \in \boldsymbol{P}(l)$ and $G_m \in \boldsymbol{R}$ are such that $H \leqslant P \leqslant G_m$, then $N_P(H) = N_{G_m}(H)$. Since $\mu_G(P) = -\mu_G(G_m)$, the contribution from each of these such groups cancel. A similar argument applies to elements of $\boldsymbol{C}_t$ and $\boldsymbol{C}_t^\omega$. From this it follows that $\mu_G(H) = 0$. □

The preceding lemmas give the following corollary which allows us to complete our analysis of the potential intersections between maximal subfield subgroups.

Corollary 3.30. *If $H \leqslant P_\omega \in \boldsymbol{P}$ and $H \notin \boldsymbol{P}(l) \cup \boldsymbol{C}_t^\omega(l) \cup \boldsymbol{C}_0(l) \cup \boldsymbol{E} \cup \boldsymbol{V} \cup \boldsymbol{C}_6^* \cup \boldsymbol{C}_3^* \cup \boldsymbol{C}_2 \cup \boldsymbol{I}$, then $\mu_G(H) = 0$.*

Lemma 3.31. *If $H \leqslant G$ is equal to the intersection of two distinct maximal subfield subgroups and $\mu_G(H) \neq 0$, then $H \in \mathbf{MaxInt}$.*

Proof. Let $G_m \neq G_k$ be maximal subfield subgroups of G and let $d = \gcd(m, k)$. Let $H = G_m \cap G_k$ and let $\Omega(m, k)$ denote the intersection $\Omega(m) \cap \Omega(k)$. We suppose that $H \notin \boldsymbol{I}$ and determine possible intersections according to $|\Omega(m, k)|$. By Lemma 3.22 it remains to prove the case when $|\Omega(m, k)| \leq 2$. If $\Omega(m, k) = \varnothing$, then any nontrivial element of H is an involution and H is a subgroup of an element of $\boldsymbol{E}$, all of which belong to $\mathbf{MaxInt}$. Hence we can assume that $\Omega(m, k) \neq \varnothing$. If $\Omega(m, k) = \{\omega\}$, then $H \leqslant P_\omega$ and by Corollary 3.30 $H \in \mathbf{MaxInt}$.

Now suppose that $|\Omega(m,k)| = 2$. There is a unique Hall subgroup conjugate to A_0 stabilising $\Omega(m,k)$ pointwise and containing H. Note that H does not contain elements which interchange the points in $\Omega(m,k)$ since otherwise H would contain a dihedral subgroup of order $2(3^{d_0}-1)$ where d_0 divides d. Such subgroups are contained only in subfield subgroups, involution centralisers or four-group normalisers, and in either case we would have $|\Omega(m,k)| > 2$. We then have that $H \cong 3^d - 1 \in \boldsymbol{C}_0(l) \cup \boldsymbol{C}_2 \subset \mathbf{MaxInt}$. $\square$

Intersections with involution centralisers, four-group and Hall subgroup normalisers

We now determine the intersections between the remaining possible pairs of maximal subgroups.

Lemma 3.32. *The intersection of two distinct involution centralisers belongs to* $\boldsymbol{C}_V \cup \boldsymbol{F} \cup \boldsymbol{V} \cup \boldsymbol{C}_2 \cup \boldsymbol{I}$.

Proof. Let $t' \neq t$ be an involution in G, let $C_{t'} = C_G(t')$ and let $H = C \cap C_{t'}$. We classify possible intersections according to the bound $|\Omega^t \cap \Omega^{t'}| \leq 1$.

Suppose $\Omega^t \cap \Omega^{t'} = \{\omega\}$. If $h \in H$ is nontrivial, then $h \in \mathcal{C}_3^*$ and belongs to the Sylow 3-subgroup of C stabilising ω. Similarly for $C_{t'}$ and so $H \in \boldsymbol{F} \cup \boldsymbol{I}$.

Now suppose that $\Omega^t \cap \Omega^{t'} = \varnothing$. If $t' \in C$, then $H = C \cap C' = C_G(\langle t, t' \rangle) \in \boldsymbol{C}_V$, so suppose that $t' \notin C$. Elements of order 3 or order dividing $(q-1)/2$ do not then belong to H since such elements fix at least one point in $\Omega^t \cap \Omega^{t'}$. If $s \in C$ is an element of order $k > 2$ dividing $(q+1)/4$, then its centraliser in G is equal to its centraliser in C and is isomorphic to $\langle s \rangle \times 2^2$, then, since $t' \notin C$, elements of order k cannot belong to $C \cap C'$ and H is then a subgroup of a four-group and so $H \in \boldsymbol{V} \cup \boldsymbol{C}_2 \cup \boldsymbol{I}$. $\square$

Lemma 3.33. *The intersection of an involution centraliser with a four-group normaliser belongs to* $\boldsymbol{C}_V \cup \boldsymbol{C}_t(1) \cup \boldsymbol{E} \cup \boldsymbol{C}_3^* \cup \boldsymbol{I}$.

Proof. There are three conjugacy classes of involutions in N and so the intersection $H = N \cap C = C_N(t)$ is equal to the centraliser in N of t. If $t \in V$ then the centraliser of t in N is equal to the centraliser of V in N and belongs to $\boldsymbol{C}_V$. The unique subgroup of order $(q+1)/4$ generated by $\langle s \rangle$ belongs to a unique four-group normaliser and only belongs to H when $t \in V$. Hence, all other cases are isomorphic to subgroups of $N/\langle s \rangle \cong 2 \times L_2(3)$. Recall that we denote a subgroup of N isomorphic to $D_{(q+1)/2}$ by D_τ if it is normal in N and $D_{\tau'}$ otherwise and if $t \in N \setminus V$ then $t \in D_\tau$ or t belongs to a conjugate of $D_{\tau'}$. If $t \in D_\tau$, then $H \in \boldsymbol{C}_t(1)$, otherwise, if $t \in D_{\tau'}$, then $H \in \boldsymbol{E}$. Finally, if $t \notin N$ then H is isomorphic to a subgroup of $2 \times L_2(3)$ which does not contain its central involution or its normal four-group, hence is an element of $\boldsymbol{C}_3^* \cup \boldsymbol{I}$. $\square$

We are now in a position to prove the following.

Lemma 3.34. *If* $H \cong 3^h - 1 \in \boldsymbol{C}_0(l)$, *then* $\mu_G(H) = 0$.

Proof. Let H be as in the hypotheses. If M is a maximal subgroup containing H, then M is a maximal subfield subgroup, unique for each divisor k such that $h|k|n$, one of two parabolic subgroups or a unique involution centraliser. By Lemmas 3.21, 3.26, 3.31 and 3.32, the subgroups which contribute to the Möbius function of H are as they appear in Table 3.8. We see that for each k the contributions from the first pair of classes cancel with one another, as do the contributions from the second pair of classes, giving $\mu_G(H) = 0$. □

Isomorphism type of overgroup K	for $k\|n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	$D_{2(3^k-1)}$	1	$\mu(n/k)$
$2 \times L_2(3^k)$	–	$D_{2(3^k-1)}$	1	$-\mu(n/k)$
$(3^k)^{1+1+1}{:}3^k - 1$	–	$3^k - 1$	2	$-\mu(n/k)$
$2 \times (3^k{:}\frac{3^k-1}{2})$	–	$3^k - 1$	2	$\mu(n/k)$
$3^k - 1$	$k > h$	$3^k - 1$	1	0

Table 3.8: $H \cong 3^h - 1 \in \boldsymbol{C}_0(l)$

We now proceed to determine containments between Hall subgroup normalisers of subfield subgroups. Since $\langle h \rangle$ is cyclic we need only prove the following number theoretic lemma in order to aid the accurate determination of the overgroups of such an intersection.

Lemma 3.35. *Let l be a positive factor of $n > 2$ an odd natural number. Then $a_i(l)$ divides one and only one of $a_1(n)$, $a_2(n)$ or $a_3(n)$ for each $i = 1, 2, 3$.*

Proof. Let l and n be as in the hypothesis and $1 \leq i, j \leq 3$. It is clear that for a fixed l we have $\gcd(a_i(l), a_j(l)) = 1$ for $i \neq j$ and so the $a_i(l)$ divide at most one of the a_i. Also, $a_1(l)$ divides a_1 and if 3 divides n/l then a_1 is divisible by $a_1(l)a_2(l)a_3(l)$, so assume that $i = 2$ or 3 and that $n/l \equiv \pm 1$ mod 3. Consider the values of $a_2(l)$ and $a_3(l)$ modulo $a_{2,3}(l) := a_2(l)a_3(l) = 3^{2l} - 3^l + 1$. We have that $a_1(l)a_{2,3}(l) = 3^{3l} + 1$ and so $3^{3l} \equiv -1 \bmod a_{2,3}(l)$ which gives us the following chain of congruences

$$3^n \equiv (-1)3^{n-3l} \equiv (-1)^2 3^{n-6l} \equiv \cdots \equiv (-1)^k 3^{n-3kl} \bmod a_{2,3}(l)$$

where $0 \leq n - 3kl < 3l$, from which it follows that

$$3^n \equiv \begin{cases} (-1)^{\frac{n-l}{3l}} 3^l = 3^l & \bmod a_{2,3}(l), \quad \text{if } (n/l) \equiv 1 \bmod 3 \\ (-1)^{\frac{n-2l}{3l}} 3^{2l} = -3^{2l} & \bmod a_{2,3}(l), \quad \text{if } (n/l) \equiv -1 \bmod 3. \end{cases}$$

Similarly, we have

$$3^{\frac{n+1}{2}} \equiv \cdots \equiv (-1)^k 3^{\frac{n+1}{2} - 3kl} \bmod a_{2,3}(l)$$

where this time $0 \le \frac{n+1}{2} - 3kl < 3l$. Eventually we find

$$3^{\frac{n+1}{2}} \equiv \begin{cases} (-1)^{\frac{n-l}{6l}} 3^{\frac{l+1}{2}} & \bmod a_{2,3}(l), \quad \text{if } (n/l) \equiv 1 \bmod 3 \\ (-1)^{\frac{n-5l}{6l}} 3^{\frac{5l+1}{2}} & \bmod a_{2,3}(l), \quad \text{if } (n/l) \equiv -1 \bmod 3. \end{cases}$$

It can then be easily verified that

$$\frac{n-l}{6l} \equiv \frac{n-5l}{6l} \equiv \begin{cases} 0 \bmod 2 & \text{if } (n/l) \equiv 1 \bmod 4 \\ 1 \bmod 2 & \text{if } (n/l) \equiv 3 \bmod 4. \end{cases}$$

Assembling these results, along with the observation that

$$\mp 3^{\frac{5l+1}{2}} - 3^{2l} + 1 = (3^l + 1 \pm 3^{\frac{l+1}{2}})(3^{l+1} - 3^l + 1 \mp (3^{\frac{3l+1}{2}} + 3^{\frac{l+3}{2}} - 2.3^{\frac{l+1}{2}})),$$

we finally arrive at the following

$$3^n \pm 3^{\frac{n+1}{2}} + 1 \equiv \begin{cases} 3^l \pm 3^{\frac{l+1}{2}} + 1 & \bmod a_{2,3}(l) \quad \text{if } (n/l) \equiv \pm 1 \bmod 12 \\ 3^l \mp 3^{\frac{l+1}{2}} + 1 & \bmod a_{2,3}(l) \quad \text{if } (n/l) \equiv \pm 5 \bmod 12. \end{cases}$$

This completes the proof. □

Lemma 3.36. *The intersection of an element of $\boldsymbol{N}_V \cup \boldsymbol{N}_2 \cup \boldsymbol{N}_3$ with a maximal subfield subgroup belongs to $\boldsymbol{N}_V(l) \cup \boldsymbol{N}_2(l) \cup \boldsymbol{N}_3(l) \cup \boldsymbol{C}_6^* \cup \boldsymbol{C}_3^* \cup \boldsymbol{C}_2 \cup \boldsymbol{I}$.*

Proof. Let G_m be a maximal subfield subgroup and let a generate any Hall subgroup conjugate to A_i, where $i = 1, 2, 3$. If $a \in G_m$, then the intersection is equal to the normaliser in G_m of a which belongs to $\boldsymbol{N}_V(l) \cup \boldsymbol{N}_2(l) \cup \boldsymbol{N}_3(l)$. If $a \notin G_m$ then, since the centraliser in G of a is uniquely contained in its normaliser in G, we have that the intersection is a subgroup of $N_G(a)/C_G(a) \cong C_6$, and so is a subgroup of an element of $\boldsymbol{C}_6^*$. □

Lemma 3.37. *The intersection of two distinct four-group normalisers belongs to $\boldsymbol{C}_t(1) \cup \boldsymbol{E} \cup \boldsymbol{C}_6^* \cup \boldsymbol{C}_3^* \cup \boldsymbol{C}_2 \cup \boldsymbol{I}$.*

Proof. Recall that the normaliser of a four-group is equal to the normaliser of the unique Hall subgroup conjugate to A_1 with which is commutes and that this Hall subgroup belongs to a unique four-group normaliser. The quotient of a four-group normaliser by its normal Hall subgroup is isomorphic to $2 \times L_2(3)$ and so the intersection of two distinct four-group normalisers is isomorphic to a subgroup of $2 \times L_2(3)$.

Let N be the normaliser of a four-group V in G and let $V' \neq V$ be a four-group in G. If $V \leqslant N$ then $N \cap N_G(V')$ is the normaliser of a four group in N and isomorphic to 2^3 or $2 \times L_2(3)$. If V

is not contained in N then the intersection $N \cap N_G(V')$ is isomorphic to a subgroup of $L_2(3)$ not containing a four-group and is hence a subgroup of a cyclic group of order 6. $\square$

Lemma 3.38. *Let $N \in \boldsymbol{N}_2 \cup \boldsymbol{N}_3$. If $M \in \boldsymbol{C}_t \cup \boldsymbol{N}_V \cup \boldsymbol{N}_2 \cup \boldsymbol{N}_3$, then $N \cap M \in \boldsymbol{C}_6^* \cup \boldsymbol{C}_3^* \cup \boldsymbol{C}_2 \cup \boldsymbol{I}$.*

Proof. This follows from comparison of the orders of the various groups and since distinct cyclic Hall subgroups have trivial intersection and belong to a unique Hall subgroup normaliser in G. $\square$

We have now proved the following.

Lemma 3.39. *If $H \leqslant G$ is equal to the intersection of a pair of maximal subgroups of G and $\mu_G(H) \neq 0$, then $H \in$ **MaxInt**.*

The proof of Lemma 3.14 and the Möbius function of the remaining subgroups

We now proceed to show that arbitrary intersections of maximal subgroups of G do not yield new subgroups by proving Lemma 3.14

Proof of Lemma 3.14. Let $H \notin$ **MaxInt** be a subgroup of G that occurs as the intersection of a number of maximal subgroups of G, let $\mu_G(H) \neq 0$ and let $\mathbf{M}$ be the set of maximal subgroups containing H. From the preceding lemmas we can assume $|\mathbf{M}| > 2$ and by Corollary 3.30 we can assume that H is not contained in a parabolic subgroup of G and so $\mathbf{M} \cap \boldsymbol{P} = \varnothing$.

If $\mathbf{M}$ contains more than two elements from $\boldsymbol{N}_V \cup \boldsymbol{N}_2 \cup \boldsymbol{N}_3$ then, by Lemmas 3.37 and 3.38, H is isomorphic to a subgroup of $2 \times L_2(3)$ and the only such subgroups not already contained in **MaxInt** are isomorphic to $L_2(3)$. Hence we can assume that $\mathbf{M} \cap (\boldsymbol{N}_2 \cup \boldsymbol{N}_3) = \varnothing$. To show that subgroups isomorphic to $L_2(3)$ do not appear on our list, suppose that M is maximal and contains $H \cong L_2(3)$. Then $M \in \mathbf{M} \subset \boldsymbol{R} \cup \boldsymbol{C}_t \cup \boldsymbol{N}_V$. By the argument in the proof of Lemma 3.22, if $\mathbf{M}$ contains at least two maximal subfield subgroups, then their intersection must be an element of $\boldsymbol{R}(l)$ and so we can assume that $\mathbf{M} \cap \boldsymbol{R}$ consists of a single subfield subgroup isomorphic to $R(3)$. By Lemma 3.32 we can assume that $\mathbf{M}$ contains at most one involution centraliser. By Lemma 3.26 we may assume that H is equal to the intersection of $M_0 \cong 2 \times L_2(3)$ with a number of elements from $\boldsymbol{N}_V$. Since the normaliser of a four-group contained in M_0 is either M_0 or is isomorphic to its elementary abelian Sylow 2-group of order 8 we have that $H \notin$ **MaxInt**.

If $\mathbf{M} \subset \boldsymbol{R} \cup \boldsymbol{C}_t \cup \boldsymbol{N}_2$ or $\mathbf{M} \subset \boldsymbol{R} \cup \boldsymbol{C}_t \cup \boldsymbol{N}_3$, then by Lemmas 3.26, 3.36 and 3.38 $H \in$ **MaxInt**. Hence, we can assume that $\mathbf{M} \subset \boldsymbol{R} \cup \boldsymbol{C}_t \cup \boldsymbol{N}_V$ contains at most one element from $\boldsymbol{R}$ and at most one element from $\boldsymbol{N}_V$. Moreover, by Lemma 3.36 again we can assume $\mathbf{M} \subset \boldsymbol{C}_t \cup \boldsymbol{N}_V(l)$. Finally, by Lemmas 3.32 and 3.33, $H \in$ **MaxInt**, a contradiction. This completes the proof. $\square$

It now remains to determine the Möbius function for elements of the remaining classes.

Lemma 3.40. *If $H \cong (2^2 \times D_{(3^h+1)/2}){:}3 \in \boldsymbol{N}_V(l)$, then $\mu_G(H) = -\mu(n/h)$.*

Proof. Let H be as in the hypothesis. The only maximal subgroups of G containing H are maximal subfield subgroups, and the normaliser of the normal four-group in H. From the calculations in Table 3.9 we find that $\mu_G(H) = -\mu(n/k)$. $\square$

Isomorphism type of overgroup K	for $k\|n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	$(2^2 \times D_{(3^h+1)/2}){:}3$	1	$\mu(n/k)$
$(2^2 \times D_{(3^k+1)/2}){:}3$	$k > h$	$(2^2 \times D_{(3^h+1)/2}){:}3$	1	$-\mu(n/k)$

Table 3.9: $H \cong (2^2 \times D_{(3^h+1)/2}){:}3 \in \boldsymbol{N}_V(l)$

Lemma 3.41. *If $H \cong 3^h - 3^{\frac{h+1}{2}} + 1{:}6$ or $3^h + 3^{\frac{h+1}{2}} + 1{:}6 \in \boldsymbol{N}_2(l) \cup \boldsymbol{N}_3(l)$, then $\mu_G(H) = -\mu(n/h)$.*

Proof. Let H be as in the hypothesis. By Lemma 3.35, for each divisor k such that $h|k|n$ there is a unique element from $\boldsymbol{N}_V(l) \cup \boldsymbol{N}_2(l) \cup \boldsymbol{N}_3(l)$ containing H. Similarly, there is a unique element from $\boldsymbol{R}(l)$ for each such k. These contributions cancel and we present the calculations for $H \in \boldsymbol{N}_2(l)$ in Table 3.10, the calculations for $H \in \boldsymbol{N}_3(l)$ are similar. We are then left with $\mu_G(H) = -\mu_G(R(3^h)) = -\mu(n/h)$. $\square$

Isomorphism type of overgroup K	for $k\|n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	H	1	$\mu(n/k)$
$(2^2 \times D_{(3^k+1)/2}){:}3$	$\frac{k}{h} \equiv 0 \bmod 3$	H	1	$-\mu(n/k)$
$3^k + \sqrt{3^{k+1}} + 1{:}6$	$\frac{k}{h} \equiv \pm 5 \bmod 12$	H	1	$-\mu(n/k)$
$3^k - \sqrt{3^{k+1}} + 1{:}6$	$k > h$, $\frac{k}{h} \equiv \pm 1 \bmod 12$	H	1	$-\mu(n/k)$

Table 3.10: $H \cong 3^h - 3^{\frac{h+1}{2}} + 1{:}6 \in \boldsymbol{N}_2(l)$

Lemma 3.42. *If $H \cong 2^2 \times D_{(3^h+1)/2} \in \boldsymbol{C}_V(l)$, then $\mu_G(H) = 3\mu(n/h)$.*

Proof. Let H be as in the hypotheses. For each divisor k such that $h|k|n$, H belongs a unique element of $\boldsymbol{R}(l)$ and a unique element of $\boldsymbol{N}_v(l)$. The contributions from each of these groups cancel, as shown in Table 3.11, and the remaining contributions from the involution centralisers give $\mu_G(H) = 3\mu(n/h)$. $\square$

Lemma 3.43. *If $H \cong D_{2a_2(h)}$ or $D_{2a_3(h)} \in \boldsymbol{D}_2(l) \cup \boldsymbol{D}_3(l)$, then $\mu_G(H) = 0$.*

Proof. Let H be as in the hypotheses and note that these subgroups arise when h is such that $3h|n$. The overgroups of H for a divisor k such that $h|k|n$ are dependent on the parity of $\frac{k}{h}$ modulo 3. We present the case $H \in \boldsymbol{D}_2(l)$ in Table 3.12, the case $H \in \boldsymbol{D}_3(l)$ is similar. From the table it is clear that for each divisor k, the contributions to $\mu_G(H)$ cancel with one another and so $\mu_G(H) = 0$. $\square$

Isomorphism type of overgroup K	for $k\|n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	$(2^2 \times D_{(3^h+1)/2}){:}3$	1	$\mu(n/k)$
$(2^2 \times D_{(3^k+1)/2}){:}3$	–	$(2^2 \times D_{(3^h+1)/2}){:}3$	1	$-\mu(n/k)$
$2 \times L_2(3^k)$	–	$2^2 \times D_{(3^h+1)/2}$	3	$-\mu(n/k)$
$2^2 \times D_{(3^k+1)/2}$	$k > h$	$2^2 \times D_{(3^h+1)/2}$	1	$3\mu(n/k)$

Table 3.11: $H \cong 2^2 \times D_{(3^h+1)/2} \in \boldsymbol{C}_V(l)$

Isomorphism type of overgroup K	for $k\|n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	$\frac{k}{h} \equiv 0 \bmod 3$	$(2^2 \times H){:}3$	1	$\mu(n/k)$
$(2^2 \times D_{(3^k+1)/2}){:}3$	$\frac{k}{h} \equiv 0 \bmod 3$	$(2^2 \times H){:}3$	1	$-\mu(n/k)$
$2 \times L_2(3^k)$	$\frac{k}{h} \equiv 0 \bmod 3$	$2^2 \times H$	3	$-\mu(n/k)$
$2^2 \times D_{(3^k+1)/2}$	$\frac{k}{h} \equiv 0 \bmod 3$	$2^2 \times H$	1	$3\mu(n/k)$
$R(3^k)$	$\frac{k}{h} \equiv \pm 1 \bmod 3$	$H{:}3$	4	$\mu(n/k)$
$3^k + \sqrt{3^{k+1}} + 1{:}6$	$\frac{k}{h} \equiv \pm 5 \bmod 12$	$H{:}3$	4	$-\mu(n/k)$
$3^k - \sqrt{3^{k+1}} + 1{:}6$	$\frac{k}{h} \equiv \pm 1 \bmod 12$	$H{:}3$	4	$-\mu(n/k)$

Table 3.12: $H \cong D_{2a_2(h)} \in \boldsymbol{D}_2(l)$

Lemma 3.44. *If $H \cong 2 \times L_2(3)$, then $\mu_G(H) = -2\mu(n)$.*

Proof. Subgroups isomorphic to H are self-normalising in G and so for each k such that k divides n belong to a unique element of each of $\boldsymbol{R}(l)$, $\boldsymbol{C}_t(l)$ and $\boldsymbol{N}_V(l)$. Since $n > 1$, the summation over the $R(3^k)$ is equal to the summation over positive divisors of k which is equal to 0. For the same reason the remainder of the remaining two classes, as shown in Table 3.13, give $\mu_G(H) = -2\mu(n)$. □

Isomorphism type of overgroup K	for $k\|n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	$2 \times L_2(3)$	1	$\mu(n/k)$
$2 \times L_2(3^k)$	$h > 1$	$2 \times L_2(3)$	1	$-\mu(n/k)$
$(2^2 \times D_{(3^k+1)/2}){:}3$	$h > 1$	$2 \times L_2(3)$	1	$-\mu(n/k)$

Table 3.13: $H \cong 2 \times L_2(3) \in \boldsymbol{C}_t(1)$

Lemma 3.45. *If $H \cong 2^3 \in \boldsymbol{E}$, then $\mu_G(H) = 21\mu(n)$.*

Proof. As presented in Table 3.14, the summation over the $R(3^k)$ equates to 0, as does the total summation of the succeeding three lines. From the final line we then have that $\mu_G(2^3) = 21\mu(n)$. □

Lemma 3.46. *If $H \cong 2^2 \in \boldsymbol{V}$, then $\mu_G(H) = 0$.*

Isomorphism type of overgroup K	for $k\|n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	$2^3\!:\!7\!:\!3$	1	$\mu(n/k)$
$2 \times L_2(3^k)$	$k > 1$	$2 \times L_2(3)$	7	$-\mu(n/k)$
$(2^2 \times D_{(3^k+1)/2})\!:\!3$	$k > 1$	$2 \times L_2(3)$	7	$-\mu(n/k)$
$2 \times L_2(3)$	–	$2 \times L_2(3)$	7	$-2\mu(n)$
$2^2 \times D_{(3^k+1)/2}$	$k > 1$	2^3	7	$3\mu(n/k)$

Table 3.14: $H \cong 2^3 \in \boldsymbol{E}$

Proof. Four-groups are conjugate in G but not necessarily conjugate in subgroups of G. Where this is the case, in the $N_K(H)$ column in Table 3.15 the number in parentheses denotes the number of conjugacy classes of V whose normaliser in K is of the specified isomorphism type. This quantity is incorporated into the entry in the $\nu_K(H)$ column. In order to make verification of the arithmetic a little easier, we have separated contributions from overgroups isomorphic to K according to whether the contribution depends on k or not. In the cases where there is no dependence on k the usual properties of the classical Möbius function leave us a few terms to tidy up and we eventually find that $\mu_G(2^2) = 0$. □

Isomorphism type of overgroup K	for $k\|n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	$(2^2 \times D_{(3^k+1)/2})\!:\!3$	$(3^n+1)/(3^k+1)$	$\mu(n/k)$
$(2^2 \times D_{(3^k+1)/2})\!:\!3$	$k > 1$	$(2^2 \times D_{(3^k+1)/2})\!:\!3$	$(3^n+1)/(3^k+1)$	$-\mu(n/k)$
$2^2 \times D_{(3^k+1)/2}$	$k > 1$	$2^2 \times D_{(3^k+1)/2}$	$(3^n+1)/(3^k+1)$	$3\mu(n/k)$
$2 \times L_2(3^k)$	$k > 1$	$2^2 \times D_{(3^k+1)/2}$	$3(3^n+1)/(3^k+1)$	$-\mu(n/k)$
$(2^2 \times D_{(3^k+1)/2})\!:\!3$	$k > 1$	(2) 2^3	$3(3^n+1)/2$	$-\mu(n/k)$
$2^2 \times D_{(3^k+1)/2}$	$k > 1$	(6) 2^3	$3(3^n+1)/2$	$3\mu(n/k)$
$2 \times L_2(3^k)$	$k > 1$	(1) 2^3, (1) $2 \times L_2(3)$	3^n+1	$-\mu(n/k)$
$2 \times L_2(3)$	–	(2) 2^3, (1) $2 \times L_2(3)$	$7(3^n+1)/4$	$-2\mu(n)$
2^3	–	(7) 2^3	$(3^n+1)/4$	$21\mu(n)$

Table 3.15: $H \cong 2^2 \in \boldsymbol{V}$

Lemma 3.47. *If $H \in \boldsymbol{C}_6 \cup \boldsymbol{C}_3^* \cup \boldsymbol{C}_2 \cup \boldsymbol{I}$, then $\mu_G(H) = 0$.*

Proof. In the case $H \in \boldsymbol{C}_6^* \cup \boldsymbol{C}_3^*$ it is clear, but tedious, from the enumerations in Tables 3.16 and 3.17 that $\mu_G(H) = 0$. In the case that $H \in \boldsymbol{C}_2$, where in some subgroups the elements of order 2 split into multiple conjugacy classes, we present this in Table 3.18 in such a way as to make the calculations easier to check. Eventually, as in the case $H \in \boldsymbol{I}$ in Table 3.19. Again, after some calculation we see that $\mu_G(H) = 0$ in both of these cases. □

Isomorphism type of overgroup K	for $k\|n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	2×3^k	3^{n-k}	$\mu(n/k)$
$(3^k)^{1+1+1}\colon 3^k - 1$	–	2×3^k	3^{n-k}	$-\mu(n/k)$
$2 \times L_2(3^k)$	$k > 1$	2×3^k	3^{n-k}	$-\mu(n/k)$
$2 \times (3^k\colon \frac{3^k-1}{2})$	$k > 1$	2×3^k	3^{n-k}	$\mu(n/k)$
$3^k + \sqrt{3^{k+1}} + 1\colon 6$	–	6	3^{n-1}	$-\mu(n/k)$
$3^k - \sqrt{3^{k+1}} + 1\colon 6$	$k > 1$	6	3^{n-1}	$-\mu(n/k)$
$(2^2 \times D_{(3^k+1)/2})\colon 3$	$k > 1$	6	3^{n-1}	$-\mu(n/k)$
$2 \times L_2(3)$	–	6	3^{n-1}	$-2\mu(n)$

Table 3.16: $H \cong \langle tu \rangle \in \boldsymbol{C}_6^*$

Isomorphism type of overgroup K	for $k\|n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	$3^k \times (3^k\colon 2)$	$3^{2(n-k)}$	$\mu(n/k)$
$(3^k)^{1+1+1}\colon (3^k - 1)$	–	$3^k \times (3^k\colon 2)$	$3^{2(n-k)}$	$-\mu(n/k)$
$2 \times L_2(3^k)$	$k > 1$	2×3^k	3^{2n-k}	$-\mu(n/k)$
$2 \times (3^k\colon \frac{3^k-1}{2})$	$k > 1$	2×3^k	3^{2n-k}	$\mu(n/k)$
$3^k + \sqrt{3^{k+1}} + 1\colon 6$	–	6	3^{2n-1}	$-\mu(n/k)$
$3^k - \sqrt{3^{k+1}} + 1\colon 6$	$k > 1$	6	3^{2n-1}	$-\mu(n/k)$
$(2^2 \times D_{(3^k+1)/2})\colon 3$	$k > 1$	6	3^{2n-1}	$-\mu(n/k)$
$2 \times L_2(3)$	–	6	3^{2n-1}	$-2\mu(n)$

Table 3.17: $H \cong \langle u \rangle \in \boldsymbol{C}_3^*$

Remark 3.48. *It follows that the Möbius number of a small Ree group, G, is equal to 0 when G is simple, or $|G'|$ when $G = R(3)$. This is consistent with Theorem 1.20.*

This completes the proof of Theorem 1.22. In the case when $G = R(27)$ the full subgroup lattice and Möbius function has been determined by Connor and Leemans [25] and, from personal correspondence with Leemans in October 2014, it was noted that apart from a few errors, such as their $\mu_G(2 \times (3^3\colon 13)) = 0$, their calculations agree with ours.

3.4 Eulerian functions of the small Ree groups

In this section we determine various Eulerian functions associated with the small Ree groups and use them to prove a number of results regarding generation and asymptotic generation of the small Ree groups. Recall that $\sigma_n(G)$ denotes the number of ordered n-tuples of elements of G and $\phi_n(G)$ is the number of those n-tuples of elements which also generate G. We introduce another summatory

Isomorphism type of overgroup K	for $k\|n$ and s.t.	$N_K(H)$	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	$2 \times L_2(3^k)$	$3^n(3^{2n}-1)/3^k(3^{2k}-1)$	$\mu(n/k)$
$2 \times L_2(3^k)$	$k>1$	$2 \times L_2(3^k)$	$3^n(3^{2n}-1)/3^k(3^{2k}-1)$	$-\mu(n/k)$
$(3^k)^{1+1+1}:(3^k-1)$	–	$2 \times (3^k:\frac{3^k-1}{2})$	$3^n(3^{2n}-1)/3^k(3^k-1)$	$-\mu(n/k)$
$2 \times (3^k:\frac{3^k-1}{2})$	$k>1$	$2 \times (3^k:\frac{3^k-1}{2})$	$3^n(3^{2n}-1)/3^k(3^k-1)$	$\mu(n/k)$
$(2^2 \times D_{(3^k+1)/2}):3$	$k>1$	$2^2 \times D_{(3^k+1)/2}$	$3^n(3^{2n}-1)/2(3^k+1)$	$-\mu(n/k)$
$2^2 \times D_{(3^k+1)/2}$	$k>1$	(3) $2^2 \times D_{(3^k+1)/2}$	$3^n(3^{2n}-1)/2(3^k+1)$	$3\mu(n/k)$
$2 \times L_2(3^k)$	$k>1$	(2) $2^2 \times D_{(3^k+1)/2}$	$3^n(3^{2n}-1)/(3^k+1)$	$-\mu(n/k)$
$3^k+\sqrt{3^{k+1}}+1:6$	–	6	$3^{n-1}(3^{2n}-1)/2$	$-\mu(n/k)$
$3^k-\sqrt{3^{k+1}}+1:6$	$k>1$	6	$3^{n-1}(3^{2n}-1)/2$	$-\mu(n/k)$
$(2^2 \times D_{(3^k+1)/2}):3$	$k>1$	(1) 2^3, (1) $2 \times L_2(3)$	$3^{n-1}(3^{2n}-1)/2$	$-\mu(n/k)$
$2^2 \times D_{(3^k+1)/2}$	$k>1$	(4) 2^3	$3^{n-1}(3^{2n}-1)/2$	$3\mu(n/k)$
$2 \times L_2(3)$	–	(2) 2^3, (1) $2 \times L_2(3)$	$7.3^{n-1}(3^{2n}-1)/8$	$-2\mu(n)$
2^3	–	(7) 2^3	$3^{n-1}(3^{2n}-1)/8$	$21\mu(n)$

Table 3.18: $H \cong \langle t \rangle \in \boldsymbol{C}_2$

Isomorphism type of overgroup K	for $k\|n$ and s.t.	$\nu_K(H)$	$\mu_G(K)$
$R(3^k)$	–	$\|G\|/3^{3k}(3^{3k}+1)(3^k-1)$	$\mu(n/k)$
$3^k+\sqrt{3^{k+1}}+1:6$	–	$\|G\|/6(3^k+\sqrt{3^{k+1}}+1)$	$-\mu(n/k)$
$3^k-\sqrt{3^{k+1}}+1:6$	$k>1$	$\|G\|/6(3^k-\sqrt{3^{k+1}}+1)$	$-\mu(n/k)$
$(3^k)^{1+1+1}:(3^k-1)$	–	$\|G\|/3^{3k}(3^k-1)$	$-\mu(n/k)$
$2 \times L_2(3^k)$	$k>1$	$\|G\|/3^k(3^{2k}-1)$	$-\mu(n/k)$
$2 \times (3^k:\frac{3^k-1}{2})$	$k>1$	$\|G\|/3^k(3^k-1)$	$\mu(n/k)$
$(2^2 \times D_{(3^k+1)/2}):3$	$k>1$	$\|G\|/6(3^k+1)$	$-\mu(n/k)$
$2^2 \times D_{(3^k+1)/2}$	$k>1$	$\|G\|/6(3^k+1)$	$3\mu(n/k)$
$2 \times L_2(3)$	–	$\|G\|/24$	$-2\mu(n)$
2^3	–	$\|G\|/168$	$21\mu(n)$

Table 3.19: $H \in \boldsymbol{I}$

function and corresponding Eulerian function as follows.

Definition 3.49. *Let G be a finite group and $(k_1, \ldots, k_n)$ be an ordered n-tuple of elements from $\mathbb{N}_{>0}$. The summatory function $\sigma_{k_1,\ldots,k_n}(G)$ counts the number of ordered n-tuples of elements of G, $(x_1, \ldots, x_n) \in G^n$, such that $o(x_i) = k_i$ for $1 \leq i \leq n$. By abuse of notation we may write $k_i = \infty$ to mean we allow any element of G in the i-th position. The corresponding Eulerian function is $\phi_{k_1,\ldots,k_n}(G)$. We say that G is $(k_1, \ldots, k_n)$-**generated** if $\phi_{k_1,\ldots,k_n} \neq 0$.*

Remark 3.50. *Let Γ be the group*

$$\Gamma = \langle x_1, \ldots, x_n \mid x_1^{k_1} = \cdots = x_n^{k_n} = 1 \rangle,$$

where any relation $x_i^{\infty} = 1$ for $1 \leq i \leq n$ is ignored. For a finite group G the quantity $\phi_{k_1,\ldots,k_n}(G)$ corresponds to the number of smooth epimorphisms from Γ to G.

Definition 3.51. *The Hecke group H_n, for $n \in \mathbb{N}_{>0} \cup \{\infty\}$, is the group generated by one element of order 2, one element of order n and no other relations. In particular, the Hecke group H_3 is isomorphic to the modular group $PSL_2(\mathbb{Z})$. We write $\eta_n(G) = \phi_{2,n}(G)$ for their corresponding Eulerian function.*

Definition 3.52. *We use the following to denote the number of torsion-free normal subgroups of the appropriate finitely presented group whose quotient is isomorphic to G.*

$$d_n(G) = \frac{\phi_n(G)}{|\mathrm{Aut}(G)|}, \quad d_{k_1,\ldots,k_n} = \frac{\phi_{k_1,\ldots,k_n}}{|\mathrm{Aut}(G)|} \quad \text{and} \quad h_n = \frac{\eta_n}{|\mathrm{Aut}(G)|}.$$

In order to determine these Eulerian functions we require the following definition.

Definition 3.53. *Let G be a finite group and n a positive integer. We write $|G|_n$ for the number of elements of G having order n. By abuse of notation we write $|G|_\infty = |G|$. We then have the relation*

$$\sigma_{k_1,\ldots,k_n}(G) = \prod_{i=1}^{n} |G|_{k_i}.$$

3.4.1 Enumerations of Epi($\Gamma, R(3)$)

Throughout this subsection $G = R(3)$. We present in Table 3.20 values for $|H|_n$ for all subgroups $H \leqslant G$ such that $\mu_G(H) \neq 0$ and n such that there exists $g \in G$ of order n. In the cases of $R(3)$ and $L_2(8)$ these are determined from their character tables [27, p. 6] whereas for the remaining subgroups these values are easily determined.

From the inversion formula of $R(3)$, as given in Theorem 3.10, and the values in Table 3.20 it is then routine to evaluate certain specific Eulerian functions of G which we give in the following corollary.

Corollary 3.54. *Let G be the small Ree group $R(3)$. Then,*

1. $d_2(G) = 1136$,
2. $h_3(G) = 2$,
3. $h_6(G) = 14$, *and;*
4. $h_9(G) = 12$,

H	$\lvert H\rvert_2$	$\lvert H\rvert_3$	$\lvert H\rvert_6$	$\lvert H\rvert_7$	$\lvert H\rvert_9$	$\nu_G(H)\mu_G(H)$
$R(3)$	63	224	504	216	504	1
$L_2(8)$	63	56	–	216	168	-1
$2^3{:}7{:}3$	7	56	56	48	–	-9
$2^3{:}7$	7	–	–	48	–	9
$9{:}6$	9	8	18	–	18	-28
D_{18}	9	2	–	–	6	28
$7{:}6$	7	14	14	6	–	-36
D_{14}	7	–	–	6	–	36
$7{:}3$	–	14	–	6	–	72
C_7	–	–	–	6	–	-72
C_6	1	2	2	–	–	504
C_2	1	–	–	–	–	-504
C_3^*	–	2	–	–	–	-504

Table 3.20: Values of $|H|_n$ for nontrivial subgroups of $R(3)$ with $\mu_G(H) \neq 0$.

$d_{3,3}(G)$	$d_{3,6}(G)$	$d_{3,7}(G)$	$d_{3,9}(G)$	$d_{6,6}(G)$	$d_{6,7}(G)$	$d_{6,9}(G)$	$d_{7,9}(G)$	$d_{9,9}(G)$
16	50	10	66	140	54	162	48	144

Table 3.21: Evaluation of $d_{a,b}(R(3))$.

in addition we have the values presented in Table 3.21.

Remark 3.55. *We note that G cannot be $(2,7)$-generated or $(7,7)$-generated since all elements of order 2 or 7 belong to $R(3)'$.*

3.4.2 Free groups & Hecke groups

We now turn to the case where $G = R(3^n)$ is an arbitrary simple small Ree group. In Tables 3.22 and 3.23 we present the values of $|H|_n$ for $n \in \{2,3,6,7,9\}$ and $H \leqslant G$ with $\mu_G(H) \neq 0$. These are easily determined from the conjugacy classes of G as found in [114].

From these values it is routine, but tedious, to determine a number of Eulerian functions for a simple small Ree group. We present a number of such functions as the following corollary to Theorem 1.22.

Isomorphism type of $H \leqslant G$	$\lvert H\rvert_2$	$\lvert H\rvert_3$	$\lvert H\rvert_6$
$R(3^h)$	$3^{2h}(3^{2h}-3^h+1)$	$(3^{3h}+1)(3^{2h}-1)$	$3^{2h}(3^{3h}+1)(3^h-1)$
$3^h+\sqrt{3^{h+1}}+1:6$	$3^h+\sqrt{3^{h+1}}+1$	$2(3^h+\sqrt{3^{h+1}}+1)$	$2(3^h+\sqrt{3^{h+1}}+1)$
$3^h-\sqrt{3^{h+1}}+1:6$	$3^h-\sqrt{3^{h+1}}+1$	$2(3^h-\sqrt{3^{h+1}}+1)$	$2(3^h-\sqrt{3^{h+1}}+1)$
$(3^h)^{1+1+1}:3^h-1$	3^{2h}	$3^{2h}-1$	$3^{2h}(3^h-1)$
$2\times L_2(3^h)$	$3^{2h}-3^h+1$	$3^{2h}-1$	$3^{2h}-1$
$2\times(3^h:\frac{3^h-1}{2})$	1	3^h-1	3^h-1
$(2^2\times D_{(3^h+1)/2}):3$	3^h+4	$2(3^h+1)$	$2(3^h+1)$
$2^2\times D_{(3^h+1)/2}$	3^h+4	–	–
$2\times L_2(3)$	7	8	8
2^3	7	–	–

Table 3.22: Values of $|H|_n$ for $n=2,3$ or 6.

Isomorphism	$\lvert H\rvert_7$			
type of $H \leqslant G$	$7\mid a_1(h)$	$7\mid a_2(h)$	$7\mid a_3(h)$	$\lvert H\rvert_9$
$R(3^h)$	$\lvert H\rvert/a_1(h)$	$\lvert H\rvert/a_2(h)$	$\lvert H\rvert/a_3(h)$	$3^{2h}(3^{3h}+1)(3^h-1)$
$(3^h)^{1+1+1}:3^h-1$	–	–	–	$3^{2h}(3^h-1)$
$2\times L_2(3^h)$	$3^{h+1}(3^h-1)$	–	–	–
$(2^2\times D_{(3^h+1)/2}):3$	6	–	–	–
$2^2\times D_{(3^h+1)/2}$	6	–	–	–
$3^h-\sqrt{3^{h+1}}+1:6$	–	6	–	–
$3^h+\sqrt{3^{h+1}}+1:6$	–	–	6	–

Table 3.23: Values of $|H|_n$ for $n=7$ or 9.

Corollary 3.56. *Let $G=R(3^n)$ be a simple small Ree group. Then,*

$$\phi_2(G)=|G|\sum_{l|n}\mu\left(\frac{n}{l}\right)(3^l-1)(3^{6l}-3^{2l}-16),\qquad \phi_{2,2,2}(G)=|G|\sum_{l|n}\mu\left(\frac{n}{l}\right)3^l(3^{2l}-3^l+1)^2,$$

$$\phi_{2,\infty}(G)=|G|\sum_{l|n}\mu\left(\frac{n}{l}\right)(3^l-1)(3^{3l}-3^l-2),\qquad \phi_{3,3}(G)=|G|\sum_{l|n}\mu\left(\frac{n}{l}\right)3^l(3^{2l}+3^l-4),$$

$$\phi_{3,\infty}(G)=|G|\sum_{l|n}\mu\left(\frac{n}{l}\right)(3^l-1)(3^{4l}-3^{3l}-3^l-4),\qquad \eta_3(G)=|G|\sum_{l|n}\mu\left(\frac{n}{l}\right)(3^l-1)^2,$$

$$\phi_{6,\infty}(G)=|G|\sum_{l|n}\mu\left(\frac{n}{l}\right)(3^l-1)(3^{5l}-3^l-6),\qquad \eta_6(G)=|G|\sum_{l|n}\mu\left(\frac{n}{l}\right)3^l(3^{2l}-3^l-2),$$

$$\phi_{9,\infty}(G)=|G|\sum_{l|n}\mu\left(\frac{n}{l}\right)3^{5l}(3^l-1),\qquad \eta_9(G)=|G|\sum_{l|n}\mu\left(\frac{n}{l}\right)3^{2l}(3^l-1)$$

and, for the Hecke group H_7 we have

$$\eta_7(G) = |G| \sum_{l|n} \mu\left(\frac{n}{l}\right) g(l) \quad \textit{where } g(l) = \begin{cases} 3^{2l} a_2(l) - 1 & \textit{if } l \equiv \pm 1 \bmod 12 \\ 3^{3l} - 2.3^{2l} + 5 & \textit{if } l \equiv \pm 3 \bmod 12 \\ 3^{2l} a_3(l) - 1 & \textit{if } l \equiv \pm 5 \bmod 12. \end{cases}$$

Remark 3.57. *The automorphism group of $G = R(3^n)$ has order $n|G|$ from which the values of $d_2(G)$, etc. can easily be determined.*

Remark 3.58. *The quantity $d_2(G)$ has a number of other interpretations, a few of which we mention here.*

- *if G is simple, this is equal to the largest positive integer, d, such that G^d can be 2-generated [63],*
- *in Grothendieck's theory of dessins d'enfants [61] this is equal to the number of distinct regular dessins with automorphism group isomorphic to G,*
- *the number of oriented hypermaps having automorphism group isomorphic to G [36].*

We evaluate $d_2(R(3^n))$ for the first few values of n and give these in Table 3.24.

G	$d_2(G)$
$R(3)$	1 136
$R(3^3)$	3 357 637 312
$R(3^5)$	9 965 130 790 521 984
$R(3^7)$	34 169 987 177 353 651 660 608
$R(3^9)$	127 166 774 444 890 319 085 083 766 720

Table 3.24: Values of $d_2(G)$ for $R(q)$, $q \leq 3^9$.

Remark 3.59. *The quantities $d_2(G), d_{2,\infty}(G)$ and $d_{2,2,2}(G)$ are of interest in the study of regular maps as they correspond to the number of orientably regular hypermaps, orientably regular maps and, respectively, regular hypermaps having automorphism group isomorphic to G. We refer the reader to [36, 37] for more details.*

It is known that the simple small Ree groups are quotients of the modular group $PSL_2(\mathbb{Z})$ [67,83]; with the Möbius function we can say a little more.

Corollary 3.60. *Let $G = R(3^n)$ be a simple small Ree group. If d is a positive integer such that*

$$d \leq h_3(G) = \frac{\eta_3(G)}{|\mathrm{Aut}(G)|} = \frac{1}{n} \sum_{l|n} \mu\left(\frac{n}{l}\right) (3^l - 1)^2,$$

then G^d can be $(2,3)$-generated.

G	$h_3(G)$
$R(3)$	2
$R(3^3)$	224
$R(3^5)$	11 712
$R(3^7)$	682 656
$R(3^9)$	43 042 272

Table 3.25: Values of $h_3(G)$ for $R(q)$, $q \leq 3^9$.

We evaluate $h_3(R(3^n))$ for the first few values of n and give these in Table 3.25.

Remark 3.61. *We note that the Möbius function can also be used to determine the number of Hurwitz triples of G, that is generating sets $\langle x, y, z\rangle$ such that $x^2 = y^3 = z^7 = xyz = 1$. From this, the number of distinct Hurwitz curves with automorphism group isomorphic to $R(3^n)$ can also be found. Groups for which such a generating set occurs are known as Hurwitz groups and their study is well documented, see [23, 24] for Conder's surveys of this area. We shall say no more about them here since it was proven by Malle [83] and independently by Jones [67] using a restricted form of Möbius inversion that the simple small Ree groups are Hurwitz groups.*

3.4.3 Asymptotic results

The Möbius function can also be used to prove results on asymptotic generation of groups. In the case of probabilistic generation of finite simple groups we direct the interested reader to the recent survey by Liebeck [79]. We begin with the following definition.

Definition 3.62. *Let G be a group. We denote by $P_{a,b}(G)$ the probability that a randomly chosen element of order a and a randomly chosen element of order b generate G. More generally we define*

$$P_{k_1,\ldots,k_n}(G) = \frac{\phi_{k_1,\ldots,k_n}(G)}{\sigma_{k_1,\ldots,k_n}(G)}$$

where $k_1, \ldots, k_n \in \mathbb{N}_{>0} \cup \{\infty\}$.

The following result due to Kantor and Lubotzky [72, Proposition 4] was proved using probabilistic arguments to enumerate pairs of elements which are contained in a maximal subgroup. We present an independent proof using the Möbius function.

Corollary 3.63 (Kantor–Lubotzky '90)**.** *Let $G = R(3^n)$ be a small Ree group. Then $P_{\infty,\infty} \to 1$ as $|G| \to \infty$.*

Proof. From Corollary 3.56 we have that

$$P_{\infty,\infty}(G) = \frac{\phi_2(G)}{|G|^2} = \frac{1}{|G|}\sum_{l|n} \mu\left(\frac{n}{l}\right)(3^l - 1)(3^{6l} - 3^{2l} - 16).$$

Since this tends to 1 as $|G| \to \infty$, we have the desired result. □

The following results due to Liebeck and Shalev [80, Theorems 1.1 and 1.2] can be proven using a similar argument.

Corollary 3.64 (Liebeck–Shalev, '96)**.** *Let $G = R(3^n)$ be a simple small Ree group. Then*

1. *$P_{2,\infty}(G) \to 1$ as $|G| \to \infty$ and*
2. *$P_{3,\infty}(G) \to 1$ as $|G| \to \infty$.*

We can prove a number of additional results on asymptotic results using Tables 3.22 and 3.23 and the results in Corollary 3.56.

Corollary 3.65. *Let $G = R(3^n)$ be a simple small Ree group and $(k_1, \dots, k_n)$ an n-tuple of positive integers. Then, each of*

$$P_{2,3}(G), \qquad P_{3,3}(G), \qquad P_{2,2,2}(G),$$

$$P_{2,6}(G), \qquad P_{2,7}(G), \qquad P_{2,9}(G),$$

$$P_{6,\infty}(G) \quad \textit{and} \quad P_{9,\infty}(G),$$

tend to 1 *as* $|G| \to \infty$.

3.5 General results on the Möbius and Eulerian functions

When considering the Möbius function of a group G a natural subgroup to consider is the Frattini subgroup of G whose definition we now recall.

Definition 3.66. *Let G be a finite group. We denote by $\Phi(G)$ the Frattini subgroup of G, that is, the intersection of all maximal subgroups of G.*

Remark 3.67. *The Frattini subgroup of G is a characteristic subgroup of G and so for a subgroup $H \leqslant G$, if $\Phi(G) \leqslant H$, then $\Phi(G) \lhd H$. For brevity we denote $H/\Phi(G)$ by H_Φ.*

From Theorem 1.14 it is immediate that if $H \ngeqslant \Phi(G)$, then $\mu_G(H) = 0$. Hall already makes the point [63, Paragraph 3.7] that given the Möbius functions of A_4, S_4 and A_5, the Möbius functions of their double covers $2.A_4$, $2.S_4$ and $2.A_5$, respectively, can be "written down at once from that of the corresponding factor group". We can generalise this by proving a corollary to the following lemma of Pahlings [90, Lemma 1].

Lemma 3.68 (Pahlings)**.** *If H is a subgroup of G and $N \lhd G$ and*

$$\mathcal{H}_H(G, N) = \{K \leqslant G \mid H \leqslant K, G = KN \textit{ and } K \cap HN = H\}$$

then

$$\mu_G(H) = \mu_{G/N}(HN/N) \sum_{K \in \mathcal{H}_H(G,N)} \mu_G(K).$$

Corollary 3.69. *Let G be a finite group, let $H \leqslant G$ be a subgroup of G and $\Phi(G)$ be the Frattini subgroup of G. Then*

$$\mu_G(H) = \mu_{G_\Phi}(H_\Phi).$$

We can then extend this to give the following result on the relationship between certain Eulerian functions of G and G_Φ.

Corollary 3.70. *Let G be a finite group. Then*

$$\phi_n(G) = \phi_n(G_\Phi)|\Phi(G)|^n.$$

Proof. From our previous observations and from the definition we have the following.

$$\phi_n(G) = \sum_{H \leqslant G} \mu_G(H)\sigma_n(H) = \sum_{H_\Phi \leqslant G_\Phi} \mu_{G_\Phi}(H_\Phi)|H|^n$$

$$= \sum_{H_\Phi \leqslant G_\Phi} \mu_{G_\Phi}(H_\Phi)|H_\Phi|^n|\Phi(G)|^n = \phi_n(G_\Phi)|\Phi(G)|^n.$$

The first and fourth equalities are simply the definition of $\phi_n(G)$, by Lemma 3.68 we have the second equality and the third equality is clear. □

Remark 3.71. *In principle, this corollary can be generalised to Eulerian functions involving $|H|_n$ where n is coprime to $|\Phi(G)|$, but for an arbitrary positive integer $n > 1$, dividing $|G|$, the relationship between $|H|_n$ and $|H_\Phi|_n$ is not as straightforward.*

Appendix A

The genus spectrum of a group

A.1 Program

The following is a computer program for GAP to determine the genus spectrum of a group, G. As a by-product this also determines whether G is an unmixed Beauville group or not.

We begin by declaring in GAP the group whose genus spectrum we wish to determine as `G`. The following declares a few preliminary objects and writes the conjugacy classes of G to memory as lists. It goes without saying that it must be possible to hold the conjugacy classes of G in memory as lists. On a 2.7GHz i5/Intel computer with 8GB of RAM this has been possible for groups as big as M_{23}, whose order is 10,200,960, with a runtime of about 96 hours.

```
g:=Size(G);;
cl:=ConjugacyClasses(G);; n:=Size(cl);;
class:=[];; GenTrips:=[];;

for i in [1..n] do
Add(class,AsList(cl[i]));;
od;
```

Each conjugacy class C_i of G is then stored in some order as `class[i]`. The following loop then determines all ordered triples `(i,j,k)` such that there exists a generating triple (x, y, z) for G with $x \in C_i$, $y \in C_j$ and $z \in C_k$. It then adds these triples to the list `GenTrips`.

```
for i in [1..n] do
catch:=[];
x:=class[i][1];;
        for j in [i..n] do
                for j2 in [1..Size(class[j])] do
                y:=class[j][j2];;
```

```
                z:=Inverse(x*y);;
                        for k in [j..n] do
                        if z in class[k] then trip:=[i,j,k];;
                        if trip in GenTrips then else
                        if g=Size(Group(x,y)) then
                        Add(GenTrips,trip);; Add(catch,k);
                        fi;
                        fi; break;
                        fi;
                        if Difference([j..n],catch)=[] then
                        catch:=[]; break;
                        fi;
                        od;
                od;
        od;
od;
```

The purpose of the "`catch`" is to record when there exists a triple "`(i,j,k)`" for `j` $\leq$ `k` $\leq$ `n` and break when either such a triple already exists or we have representatives for all `k`. Note that we check whether `x` and `y` generate `G` only when necessary to reduce the runtime. The following then writes to memory, for each `(x,y,z)` the ordered pair `BeauS:=[BeauSig,gen]` consisting of the set `BeauSig` of all powers of `x`, `y` and `z` minus the identity and `gen` which is determined from the Riemann–Hurwitz formula as described in Section 2.2. Note that we do not take our actual generating triple, we take the first element from the conjugacy class in which each element of our triple appears. Since we eventually compare conjugacy in `G`, this is sufficient.

```
gt:=Size(GenTrips);;
BeauS:=[];;

for b in [1..gt] do
BeauSigma:=[];;

x:=class[GenTrips[b][1]][1];; l:=Order(x);;
y:=class[GenTrips[b][2]][1];; m:=Order(y);;
z:=class[GenTrips[b][3]][1];; n:=Order(z);;

mu:=1/l+1/m+1/n;; gen:=Size(G)*(1-mu)/2+1;;
```

```
        for i in [1..l-1] do Add(BeauSigma,x^i);; od;
        for i in [1..m-1] do Add(BeauSigma,y^i);; od;
        for i in [1..n-1] do Add(BeauSigma,z^i);; od;

        Add(BeauS,[BeauSigma,gen]);;
od;
```

The following loop compares each generating triple to see whether they determine an unmixed Beauville structure, in which case it adds the ordered pair of their genera to the list `Genera`, omitting repeats, along with the geometric genus. The purpose of the `diver` subloop is as follows. Since for each triple we have taken the first element of the conjugacy class to which that element belongs, this allows us to quickly weed out incompatible structures by simply checking the intersection of their `BeauSigma` sets. If their intersection is empty, we then follow through and check whether any element from one triple is conjugate to an element of the other.

```
Genera:=[];
for p in [1..gt-1] do np:=Size(BeauS[p][1]);
for q in [p+1..gt] do nq:=Size(BeauS[q][1]);

        if Intersection(GenTrips[p],GenTrips[q])=[] then
        if Intersection(BeauS[p][1],BeauS[q][1])=[] then

                diver:=0;
                for i in [1..np] do
                for j in [1..nq] do

                if IsConjugate(G,BeauS[p][1][i],BeauS[q][1][j])=true then
                diver:=1;
                fi;

                od;
                od;

                if diver=0 then
                list:=[BeauS[p][2],BeauS[q][2]]; Sort(list);

                        if Intersection(Genera,[list])=[] then
                        Add(Genera,list);
```

```
                              fi;
                    fi;
          fi;
          fi;
od;
od;
```

The following then prints out the genus spectrum of `G`.

```
Sort(Genera);; N:=Size(Genera);;

for i in [1..N] do
          Add(Genera[i],((Genera[i][1]-1)*(Genera[i][2]-1)/g)-1);
          Print(Genera[i]); Display(" ");
od;
```

Remark A.1. *In the case where G is an almost simple group this program can naturally be modified to exclude the case where two of the generators are chosen from $soc(G)$ to reduce the runtime.*

A.2 The genus spectrum of some finite almost simple groups

The genus spectrum of A_6 can be recovered from [53]. We include it here for comparison along with the genus spectrum of S_6, A_7 and S_7. The orders of the genus specrta of A_8 and S_8 are 259 and 723 respectively and so we do not print them here. For the almost simple groups with socle isomorphic to a finite simple group of Lie type we include a few cases whose genus spectra has a modest size. We note that the genus spectrum of $L_2(q)$ and $PGL_2(q)$ can be reconstructed from the work of Garion [53] and so do not include them here. The genus spectrum of the remaining cases of almost simple groups with socle isomorphic to $L_2(q)$, where $q \leq 32$, admitting an unmixed Beauville structure are presented in this section. Of the almost simple groups with socle isomorphic to a sporadic group we include only the Mathieu Group M_{11} since the genus spectrum of the next smallest sporadic simple group, M_{12}, has order 749.

g_1	16	25	46	46
g_2	73	46	49	73
p_g	2	2	5	8

Table A.1: Genus spectrum of A_6

g_1	49	91	91	121	151
g_2	91	121	169	169	169
p_g	5	14	20	27	34

Table A.2: Genus spectrum of S_6

g_1	136	136	136	169	169	169	169	169	169	169	169	169	169
g_2	169	337	505	241	271	316	346	421	451	481	526	556	586
p_g	8	17	26	15	17	20	22	27	29	31	34	36	38
g_1	169	169	169	169	211	211	211	211	211	211	241	241	241
g_2	631	661	691	721	409	481	505	577	649	721	316	337	379
p_g	41	43	45	47	33	39	41	47	53	59	29	31	35
g_1	241	241	271	271	274	274	316	316	316	316	316	316	316
g_2	442	505	337	505	481	721	337	409	481	505	577	649	721
p_g	41	47	35	53	51	77	41	50	59	62	71	80	89
g_1	337	337	337	337	337	337	337	337	337	337	337	346	379
g_2	346	421	451	481	526	556	586	631	661	691	721	505	481
p_g	45	55	59	63	69	73	77	83	87	91	95	68	71
g_1	379	409	409	409	421	421	421	421	421	442	442	451	481
g_2	721	421	526	631	481	505	577	649	721	481	721	505	484
p_g	107	67	84	101	79	83	95	107	119	83	125	89	91
g_1	481	481	481	481	481	484	505	505	505	505	505	505	505
g_2	505	526	547	589	631	721	526	556	586	631	661	691	721
p_g	95	99	103	111	119	137	104	110	116	125	131	137	143
g_1	526	526	526	547	577	589	631	631					
g_2	577	649	721	721	631	721	649	721					
p_g	119	134	149	155	143	167	161	179					

Table A.3: Genus spectrum of A_7

g_1	169	169	169	169	169	169	169	169	211	211	211	211
g_2	841	901	1051	1261	1321	1471	1681	1741	649	1177	1321	1345
p_g	27	29	34	41	43	48	55	57	26	48	54	55
g_1	211	211	211	271	271	271	271	337	337	337	337	337
g_2	1489	1513	1657	1009	1177	1345	1513	691	841	901	1051	1111
p_g	61	62	68	53	62	71	80	45	55	59	69	73
g_1	337	337	337	337	337	337	421	421	421	421	421	421
g_2	1261	1321	1471	1531	1681	1741	649	1177	1321	1345	1489	1513
p_g	83	87	97	101	111	115	53	97	109	111	123	125
g_1	421	481	481	481	481	481	481	481	481	481	481	481
g_2	1657	757	799	841	1009	1051	1135	1177	1219	1261	1345	1387
p_g	137	71	75	79	95	99	107	111	115	119	127	131
g_1	481	481	481	481	481	481	481	505	505	505	505	505
g_2	1429	1471	1513	1555	1597	1639	1681	841	901	1051	1261	1321
p_g	135	139	143	147	151	155	159	83	89	104	125	131
g_1	505	505	505	631	631	631	631	631	631	631	649	649
g_2	1471	1681	1741	649	1177	1321	1345	1489	1513	1657	841	1051
p_g	146	167	173	80	146	164	167	185	188	206	107	134
g_1	649	649	649	691	691	691	757	757	799	799	841	841
g_2	1261	1471	1681	841	1177	1513	841	1321	841	1321	841	901
p_g	161	188	215	114	160	206	125	197	132	208	139	149

Table A.4: Genus spectrum of S_7, continued on Table A.5

g_1	841	841	841	841	841	841	841	841	841	841	841
g_2	1009	1051	1111	1135	1177	1219	1261	1279	1321	1345	1387
p_g	167	174	184	188	195	202	209	212	219	223	230
g_1	841	841	841	841	841	841	841	841	841	841	841
g_2	1429	1471	1489	1513	1531	1555	1597	1639	1657	1681	1699
p_g	237	244	247	251	254	258	265	272	275	279	282
g_1	841	901	901	901	901	967	1009	1009	1009	1009	1009
g_2	1741	1009	1177	1345	1513	1321	1051	1261	1321	1471	1681
p_g	289	179	209	239	269	252	209	251	263	293	335
g_1	1009	1051	1051	1051	1051	1051	1051	1111	1111	1111	1135
g_2	1741	1177	1321	1345	1489	1513	1657	1177	1345	1513	1321
p_g	347	244	274	279	309	314	344	258	295	332	296
g_1	1177	1177	1177	1177	1177	1177	1219	1261	1261	1261	1261
g_2	1261	1321	1471	1531	1681	1741	1321	1321	1345	1489	1513
p_g	293	307	342	356	391	405	318	329	335	371	377
g_1	1261	1321	1321	1321	1321	1321	1321	1321	1321	1321	1345
g_2	1657	1345	1387	1429	1471	1513	1555	1597	1639	1681	1471
p_g	413	351	362	373	384	395	406	417	428	439	391
g_1	1345	1345	1471	1471	1471	1489	1513	1513	1513	1657	
g_2	1681	1741	1489	1513	1657	1681	1531	1681	1741	1681	
p_g	447	463	433	440	482	495	458	503	521	551	

Table A.5: Genus spectrum of S_7 continued

g_1	127	127	127	253	253	253	271	271	337	337	379	379	397
g_2	337	481	505	337	481	505	337	505	379	397	481	505	505
p_g	27	39	41	55	79	83	59	89	83	87	119	125	131

Table A.6: Genus spectrum of $P\Gamma L_2(8) \cong R(3)$

g_1	681	681	681	1121	1225	1225	1361	1633	1801	1801	1801	1801	1801
g_2	1393	2449	3025	1225	1361	2481	1801	1801	1905	2177	2449	2721	2993
p_g	115	203	251	167	203	371	299	359	419	479	539	599	659

Table A.7: Genus spectrum of $L_2(16)\!:\!2 \cong O_4^-(4)$

g_1	2041	2041	2041	2041	2041	2041	2041	2041	2041	2041	2041	2041
g_2	2721	3265	3537	3601	3809	4081	4625	4897	4961	5169	5441	5985
p_g	339	407	441	449	475	509	577	611	619	645	679	747
g_1	2041	2041	2721	2721	2721	3265	3265	3265	3401	3537	3537	3601
g_2	6257	6321	4081	4489	5641	3401	4081	5641	3601	4081	5641	4081
p_g	781	789	679	747	939	679	815	1127	749	883	1221	899
g_1	3601	3601	3809	3809	4081	4081	4081	4081	4081	4081	4081	4081
g_2	4489	5577	4081	5641	4081	4489	4625	4897	4961	5169	5441	5641
p_g	989	1229	951	1315	1019	1121	1155	1223	1239	1291	1359	1409
g_1	4081	4081	4081	4489	4489	4489	4625	4897	5169	5441	5641	5641
g_2	5985	6257	6321	4961	5441	6321	5641	5641	5641	5641	5985	6257
p_g	1495	1563	1579	1363	1495	1737	1597	1691	1785	1879	2067	2161

Table A.8: Genus spectrum of $P\Gamma L_2(16)$

g_1	651	651	651	1171	1171	1171	1171	1171	1171	1171	1171	1171	1171
g_2	2521	4681	5641	2001	2521	2601	3121	3641	4161	4601	4681	5121	5641
p_g	104	194	234	149	188	194	233	272	311	344	350	383	422

g_1	1301	1301	1301	1351	1351	1351	1351	1351	1821	1821	1821	1951	1951
g_2	2521	4681	5641	2601	3121	3641	4161	4681	2521	4681	5641	2001	2521
p_g	209	389	469	224	269	314	359	404	293	545	657	249	314

g_1	1951	1951	1951	1951	1951	1951	1951	1951	2001	2001	2001	2001	2001
g_2	2601	3121	3641	4161	4601	4681	5121	5641	2341	3121	3511	4291	4681
p_g	324	389	454	519	574	584	639	704	299	399	449	549	599

g_1	2341	2341	2341	2341	2341	2341	2341	2341	2341	2471	2471	2471	2521
g_2	2521	2601	3121	3641	4161	4601	4681	5121	5641	2521	4681	5641	2601
p_g	377	389	467	545	623	689	701	767	845	398	740	892	419

g_1	2521	2521	2521	2521	2521	2521	2521	2521	2521	2521	2521	2521	2521
g_2	2991	3121	3251	3511	3641	3771	3901	4161	4291	4421	4551	4681	4941
p_g	482	503	524	566	587	608	629	671	692	713	734	755	797

Table A.9: Genus spectrum of $P\Sigma L_2(25)$, continued on Table A.10

g_1	2521	2521	2601	2601	2601	2601	2601	2601	2601	2991	2991	3121	3121
g_2	5071	5591	3121	3301	3511	4291	4471	4681	5641	4681	5641	3121	3301
p_g	818	902	519	549	584	714	744	779	939	896	1080	623	659

g_1	3121	3121	3121	3121	3121	3121	3121	3121	3121	3251	3251	3301	3301
g_2	3511	3641	4161	4291	4471	4601	4681	5121	5641	4681	5641	3641	4161
p_g	701	727	831	857	893	919	935	1023	1127	974	1174	769	879

g_1	3301	3511	3511	3511	3511	3511	3511	3641	3641	3641	3641	3771	3771
g_2	4681	3641	4161	4601	4681	5121	5641	4291	4471	4681	5641	4681	5641
p_g	989	818	935	1034	1052	1151	1268	1000	1042	1091	1315	1130	1362

g_1	3901	3901	3951	4161	4161	4161	4161	4291	4291	4291	4291	4421	4421
g_2	4681	5641	4681	4291	4471	4681	5641	4601	4681	5121	5641	4681	5641
p_g	1169	1409	1184	1143	1191	1247	1503	1264	1286	1407	1550	1325	1597

g_1	4471	4551	4551	4601	4681	4681	4681	4681	4681	4681	4941	5071	5591
g_2	4681	4681	5641	4681	4681	4941	5071	5121	5591	5641	5641	5641	5641
p_g	1340	1364	1644	1379	1403	1481	1520	1535	1676	1691	1785	1832	2020

Table A.10: Genus spectrum of $P\Sigma L_2(25)$ continued

g_1	2458	2458	2458	2458	2809	2809	2809	2809	3781
g_2	6553	9361	9829	10333	4096	6553	9829	10333	4096
p_g	545	779	818	860	389	623	935	983	524
g_1	3781	3781	3781	3781	3862	3862	3862	4915	4915
g_2	6553	9361	9829	10414	6553	9829	10333	6553	9361
p_g	839	1199	1259	1334	857	1286	1352	1091	1559
g_1	4915	4915	5266	5266	5266	6238	6238	6238	6319
g_2	9829	10333	6553	9829	10333	6553	9361	9829	6553
p_g	1637	1721	1169	1754	1844	1385	1979	2078	1403
g_1	6319	6319	6553	6553	6553	6553	7372	7372	7372
g_2	9829	10333	7372	7723	8695	8776	9361	9829	10333
p_g	2105	2213	1637	1715	1931	1949	2339	2456	2582
g_1	7723	7723	8695	8695	8776	8776			
g_2	9829	10333	9361	9829	9829	10333			
p_g	2573	2705	2759	2897	2924	3074			

Table A.11: Genus spectrum of $P\Sigma L_2(27)$

g_1	235	235	469	469	586	586	703	703	703
g_2	1441	2161	1441	2161	1441	2161	721	1441	2161
p_g	59	89	119	179	149	224	89	179	269

g_1	721	721	721	721	721	721	721	721	721
g_2	820	937	1054	1171	1288	1405	1522	1639	1756
p_g	104	119	134	149	164	179	194	209	224

g_1	820	820	937	937	1054	1054	1171	1171	1288
g_2	1441	2161	1441	2161	1441	2161	1141	2161	1441
p_g	209	314	239	359	269	404	299	449	329

g_1	1288	1405	1405	1441	1441	1441	1522	1639	1756
g_2	2161	1441	2161	1522	1639	1756	2161	2161	2161
p_g	494	359	539	389	419	449	584	629	674

Table A.12: Genus spectrum of $L_3(3)$

g_1	1405	1405	1405	1441	1441	1441	1441	1441	1441	1441	1441
g_2	1441	1873	3313	1639	1873	2107	2341	2575	2809	3043	3277
p_g	179	233	413	209	239	269	299	329	359	389	419

g_1	1441	1441	1441	1639	1639	1873	1873	1873	1873	1873	1873
g_2	3511	3745	3979	1873	3313	1873	2107	2341	2377	2575	2809
p_g	449	479	509	272	482	311	350	389	395	428	467

g_1	1873	1873	1873	1873	1873	1873	1873	1873	1873	1873	2107
g_2	3043	3079	3277	3313	3511	3745	3781	3979	4015	4249	3313
p_g	506	512	545	551	584	623	629	662	668	707	620

g_1	2341	2575	2809	3043	3277	3313	3313	3313
g_2	3313	3313	3313	3313	3313	3511	3745	3979
p_g	689	758	827	896	965	1034	1103	1172

Table A.13: Genus spectrum of $P\Gamma L_3(3)$

g_1	505	577	577	577	577	577	577	577	577	577	577
g_2	1729	631	883	1009	1135	1261	1387	1513	1639	1765	1891
p_g	143	59	83	95	107	119	131	143	155	167	179

g_1	577	577	577	631	631	757	883	883	1009	1009	1135
g_2	2017	2143	2269	1153	1729	1729	1153	1729	1153	1729	1153
p_g	191	203	215	119	179	215	167	251	191	287	215

g_1	1135	1153	1153	1153	1153	1153	1153	1153	1153	1153	1261
g_2	1729	1261	1387	1513	1639	1765	1891	2017	2143	2269	1729
p_g	323	239	263	287	311	335	359	383	407	431	359

g_1	1387	1513	1639	1729	1729	1729	1729	1729
g_2	1729	1729	1729	1765	1891	2017	2143	2269
p_g	395	431	467	503	539	575	611	647

Table A.14: Genus spectrum of $U_3(3)$

g_1	1153	1153	1153	1153	1153	1153	1153	1153	1153	1153	1153
g_2	1765	2017	2269	2521	2773	3025	3277	3529	3781	4033	4285
p_g	167	191	215	239	263	287	311	335	359	383	407

g_1	1153	1765	1765	2017	2017	2017	2017	2017	2017	2017	2017
g_2	4537	2017	3169	2017	2161	2269	2521	2773	2917	3025	3169
p_g	431	293	461	335	359	377	419	461	485	503	527

g_1	2017	2017	2017	2017	2017	2017	2017	2017	2017	2269	2521
g_2	3277	3529	3673	3781	3925	4033	4177	4285	4537	3169	3169
p_g	545	587	611	629	653	671	695	713	755	593	659

g_1	2773	3025	3169	3169	3169	3169	3169	3169
g_2	3169	3169	3277	3529	3781	4033	4285	4537
p_g	725	791	857	923	989	1055	1121	1187

Table A.15: Genus spectrum of $P\Gamma U_3(3)$

g_1	1009	1009	1009	1081	1081	1081	1345	1345	1345	1345	1345
g_2	1921	3841	5761	1345	2689	4033	2161	2521	3601	4681	5761
p_g	95	191	287	71	143	215	143	167	239	311	383

g_1	1681	1681	1681	1681	1921	1921	1921	1921	2161	2161	2185
g_2	4033	4609	5185	5761	2521	3025	3529	4033	2689	4033	5761
p_g	335	383	431	479	239	287	335	383	287	431	623

g_1	2521	2521	2521	2521	2521	2521	2521	2689	2689	2689	2761
g_2	2689	3265	3841	4033	4609	5185	5761	3601	4681	5761	4033
p_g	335	407	479	503	575	647	719	479	623	767	551

g_1	3025	3025	3529	3529	3601	3841	4033	4033
g_2	3841	5761	3841	5761	4033	4033	4681	5761
p_g	575	863	671	1007	719	767	935	1151

Table A.16: Genus spectrum of $L_3(4)$

g_1	729	729	729	729	1457	1457	1457	1457	1561	1561	1561
g_2	8321	9281	10241	11201	8321	9281	10241	11201	5825	7617	9409
p_g	207	231	255	279	415	463	511	559	311	407	503

g_1	1561	2289	2521	2521	2521	2521	3121	3121	3121	3121	3249
g_2	11201	11201	5825	6657	7489	8321	5825	7617	9409	11201	8321
p_g	599	879	503	575	647	719	623	815	1007	1199	927

g_1	3641	3641	3641	3641	3641	3641	3641	3641	3641	3641	4081
g_2	5825	6657	7489	7617	8321	8449	9281	9409	10241	11201	5825
p_g	727	831	935	951	1039	1055	1159	1175	1279	1399	815

g_1	4369	4369	4369	4369	5041	5041	5041	5041	5097	5097	5097
g_2	8321	9281	10241	11201	5825	6657	7489	8321	8321	9281	10241
p_g	1247	1391	1535	1679	1007	1151	1295	1439	1455	1623	1791

g_1	5097	5201	5201	5201	5201	5825	5825	5825	5825	5825	5825
g_2	11201	5825	7617	9409	11201	6161	6761	7721	8321	8681	9281
p_g	1959	1039	1359	1679	1999	1231	1351	1543	1663	1735	1855

g_1	5825	5825	5929	6161	6161	6161	6657	6657	6761	6761	6761
g_2	10241	11201	11201	6657	7489	8321	8681	11201	7617	9409	11201
p_g	2047	2239	2279	1407	1583	1759	1983	2559	1767	2183	2599

g_1	6889	7489	7489	7617	8321	8321	8321
g_2	8321	8681	11201	8321	8681	9409	11201
p_g	1967	2231	2879	2175	2479	2687	3199

Table A.17: Genus spectrum of $Sz(8)$

g_1	631	694	694	826	826	826	826	859	961	991	991	991	991
g_2	1585	1921	2881	1585	2017	2449	2881	2881	1585	1489	1585	1921	2017
p_g	125	167	251	164	209	254	299	311	191	185	197	239	251
g_1	991	991	1126	1156	1156	1156	1156	1189	1189	1261	1291	1321	1321
g_2	2449	2881	1585	1585	2017	2449	2881	1921	2881	1585	1585	1585	2017
p_g	305	359	224	230	293	356	419	287	431	251	257	263	335
g_1	1321	1321	1354	1387	1387	1486	1486	1486	1486	1486	1486	1489	1489
g_2	2449	2881	2881	1921	2881	1489	1585	1921	2017	2449	2881	1981	2476
p_g	407	479	491	335	503	278	296	359	377	458	539	371	464
g_1	1519	1585	1585	1585	1585	1585	1585	1585	1585	1585	1585	1585	1585
g_2	2881	1621	1651	1786	1816	1921	1951	1981	2116	2146	2251	2281	2311
p_g	551	323	329	356	362	383	389	395	422	428	449	455	461
g_1	1585	1585	1585	1585	1585	1585	1651	1651	1651	1684	1684	1717	1816
g_2	2446	2476	2581	2611	2746	2881	2017	2449	2881	1921	2881	2881	2017
p_g	488	494	515	521	548	575	419	509	599	407	611	623	461
g_1	1816	1816	1849	1882	1882	1921	1921	1921	1981	1981	1981	2014	2017
g_2	2449	2881	2881	1921	2881	1981	2179	2476	2017	2449	2881	2881	2146
p_g	560	659	671	455	683	479	527	599	503	611	719	731	545
g_1	2017	2017	2146	2146	2179	2311	2311	2449	2476				
g_2	2311	2476	2449	2881	2881	2449	2881	2476	2881				
p_g	587	629	662	779	791	713	839	764	899				

Table A.18: Genus spectrum of M_{11}

Appendix B

Future research

B.1 Beauville groups

B.1.1 Mixable Beauville groups

The results of Chapter 2 naturally throw open a number of questions and conjectures for further work related to Beauville groups. In light of Theorem 1.9 it seems natural to conjecture the following.

Conjecture B.1. *If G is a non-abelian finite simple group not isomorphic to $PSL_2(2^n)$ for $n \geq 2$, then G is a mixable Beauville group.*

The remaining cases to consider are finite simple groups of Lie type having rank $n \geq 3$ with the exceptions of types ${}^2F_4(2^n)$ and ${}^3D_4(q)$. The main obstructions faced in proving Theorem 1.9 were scarcity of prime divisors, notably in the cases J_2 and $L_2(q)$, and determining even triples in the even characteristic cases. As the rank of n grows the order obstruction should disappear; in the cases of ${}^2F_4(2^n)$ and ${}^3D_4(2^n)$ the existence of elements of even order which were not 2-elements facilitated the determination of even triples. Furthermore the existence and properties of Singer cycles suggest that in even or odd characteristic one can always find a generating triple consisting of Singer cycles. It seems plausible, then, that this conjecture should be true. A related question is then the following.

Question B.2. *If G is a simple group then for which n is G^n a mixable Beauville group?*

Here, n is clearly bounded by $d_2(G)$; moreover, the author suspects the real bound is significantly lower. A case in point is $G = L_2(7)$; by Lemma 2.56 G^n is a mixable Beauville group only for $n = 1, 2$. This falls far short of $d_2(G) = 57$ which can be calculated in GAP or derived from its Möbius function [63]. This is most certainly largely due to the coprimeness restriction which raises the following question.

Question B.3. *Can the coprimeness condition in Theorem 2.40 be weakened?*

In [70, 71] Jones uses the notion of p-fullness in order to determine unmixed Beauville structures where the products of the orders of each generating triple are not coprime. Could p-fullness be utilised to provide a construction compatible with Theorem 2.40? Moreover, can the original construction itself be generalised?

Question B.4. *In the "mixable" construction $G := (H^n) : Q_{4k}$, where H is a perfect group, $n = 2$ and k depends on the mixable structure of H can either of these conditions be generalised?*

It is certainly true that H can be generalised, as in Bauer, Catanese and Grunewald's original construction, but for which n and $K \cong G/H^n$ can a mixed Beauville group be constructed. From the necessary condition that G must be 2-generated we can at least say that K must be 2-generated.

Beyond the topics raised in the thesis, there is a plethora of open questions in the wider world of Beauville groups. We draw a few questions, largely chosen for their interest to the author, from the various existing survey articles [2, 41, 68].

B.1.2 Beauville p-groups

As far as the author is aware, all hitherto known mixed Beauville groups are those discussed in Chapter 1. We mention that the infinite family of mixed Beauville 2-groups appearing in [4] also yields an infinite family of unmixed Beauville 2-groups. We now turn to the unmixed case. It is immediate from the definition that for a group G to admit an unmixed Beauville structure it is sufficient for there to exist a pair of generating triples $(x_1, y_1, (x_1y_1)^{-1})$ and $(x_2, y_2, (x_2y_2)^{-1})$ for G such that $\nu(x_1, y_1)$ is coprime to $\nu(x_2, y_2)$. This reduces the case of determining which nilpotent groups are unmixed Beauville groups to determining which p-groups are unmixed Beauville groups. Unmixed Beauville p-groups of order at most p^4 have been classified in addition to a number of results regarding those of order at most p^6 by Barker, Boston and Fairbairn [2]. In addition, they construct an infinite family of unmixed Beauville groups of order p^3 for $p \geq 7$ with an explicit presentation. Since, as mentioned in Chapter 1, the abelian unmixed Beauville groups are known [20, Lemma 3.21], we turn to non-abelian unmixed Beauville groups. A number of infinite families of unmixed Beauville groups are known due to the work of Fernández-Alcober and Gül [47], González-Diez and Jaikin-Zapirain [57] and Stix and Vdovina [108].

A more striking question to explore is the relationship between the position of a p-group in the so-called 'O'Brien tree' [89] and its status as an unmixed Beauville group. Boston has initiated the study in this vein but as far as the author is aware there are yet to be any conclusive results. We direct the reader to Boston's survey article [16] for further information.

B.1.3 Strongly real Beauville groups

One last problem is that of determining 'strongly real' Beauville groups which are unmixed Beauville groups whose Beauville structure satisfies an additional technical condition which we take from [49, Criterion B].

Definition B.5. *Let G be a group and let $(x_1, y_1; x_2, y_2)$ be an unmixed Beauville structure for G. We say that G is **strongly real** if there exists $\psi \in Aut(G)$ and $\delta_i \in G$ $(i = 1, 2)$ such that*

$$\psi(x_i)^{\delta_i} = x_i^{-1} \quad \textit{and} \quad \psi(y_i)^{\delta_i} = y_i^{-1}$$

for $i = 1, 2$.

For the geometric significance of this problem we refer the reader to [7, Section 7] and [9]. It was conjectured by Catanese that almost all finite simple groups admit a strongly real Beauville structure [6, Conjecture 3] and much work has been done on the determination of groups admitting strongly real Beauville structures [40, 49, 51]. We refer the interested reader to [41, 43] and the survey article [42, Section 5] for the state of play on this topic.

B.2 Möbius functions and related problems

B.2.1 More Möbius functions

Naturally, one might consider determining the Möbius function for other families of non-abelian finite simple groups and, where possible, their automorphism groups.

- Sporadic groups — The subgroup lattice and table of marks for a large number of sporadic groups, as well as the Tits group, are known. The history of their discovery is documented by Connor and Leemans in [26] who also maintain a website [25] where the list of conjugacy classes of subgroups of all almost simple groups of order less than $1,000,000$ in [27] appears. In some cases this also includes their Möbius function.

- Finite simple groups of Lie type — In the case of the finite simple groups of Lie type, the well tempered nature of the conjugacy classes of their maximal subgroups aids one in determining their Möbius function. Ideally one would like to determine the Möbius function of G in the case where G has a relatively small number of classes of maximal subgroups. Hence, the most natural candidates to tackle next would be the groups $PSU_3(q)$ and $PSL_3(q)$. Despite the large number of classes of maximal subgroups in the large Ree groups [84], many of them are p-local and much of the work can be done based on the greatest common divisor of their orders. However, since their Sylow 2-subgroups do not have trivial intersection, as the Sylow 3-subgroups do in the case of the small Ree groups, it will take some work to determine their possible intersections.

- Alternating groups — In the case of the alternating and symmetric groups a general formula for the Möbius function in terms of n seems completely out of reach due to the wild variation of the maximal subgroups appearing in these groups. Even the determination of the Möbius number of these groups becomes a hard problem when n has at least two prime divisors, as visible in the work of Shareshian [101, 102].

Beyond the determination of more Möbius functions, given the various general results on the Möbius function, one might hope to have more general results on the various Eulerian functions. Although again, as mentioned in Chapter 3, given the disparity between summatory functions of subgroups of G and subgroups of quotients of G, this will be a more awkward problem.

Related to the Möbius function of a lattice is its dual $\bar{\mu}_1(H)$ for a subgroup $H \leqslant G$, which, as far as the author is aware, appears to have been little investigated. The dual of the Möbius function is described in [63, Section 2.4] and we have relations such as $\bar{\mu}_1(1) = \mu_G(G) = 1$, $\mu_G(1) = \bar{\mu}_1(G)$ and $\mu_G(p) = -1$ for cyclic subgroups of prime order. In general, determining this function for a group would be even more awkward than determining the usual Möbius function since one needs to know which subgroups are generated by all pairs of elements of prime order. It is not immediately obvious that there should be any nontrivial connection between the usual Möbius function and its dual, but it seems worth investigating.

B.2.2 Other properties of subgroup lattices

The subgroup lattice of a finite group is by definition a poset and so can be considered as a simplicial complex, hence one can consider its homotopy type and its homology. A corollary to Quillen's Fiber Lemma, which we do not state here and is all but stated in [93], is the following. If a poset contains a unique maximal or minimal element, then it is contractible [93, Section 1.5]. As such, one normally considers the *order complex* of the subgroup lattice, see for example [66, Section 9]. Essentially, if $L(G)$ denotes the lattice of subgroups of a group G, the order complex $\bar{L} = \bar{L}(G)$ is the poset $L \setminus \{1, G\}$. Another corollary of Quillen's Fiber Lemma is that L is homotopy equivalent to the subcomplex consisting of those subgroups which are intersections of a maximal number of subgroups. In order to determine the homotopy type of $\bar{L}$ one needs then only consider nontrivial subgroups which occur as intersections of maximal subgroups. In the case where G is a soluble group the homotopy type of $\bar{L}$ is that of a bouquet of equidimensional spheres [76, Corollaire 4.10]. An extension of this is due to Shareshian [103] where the homotopy type of the minimal simple groups are also determined.

Question B.6. *What is the homotopy type of the subgroup lattice of a small Ree group?*

In this thesis we have determined all subgroups of a small Ree group which can occur as the intersection of a number of maximal subgroups with the exception of those H which occur as the intersection of subfield subgroups which intersect in a parabolic subgroup. However, we know such subgroups have $\mu_G(H) = 0$. If $H \leqslant G$ is not the intersection of a number of maximal subgroups, then $\mu_G(H) = 0$ and there exists $H \leqslant K < G$ where K is the intersection of all maximal subgroups of G containing H. From the Quillen Fiber Lemma, the sublattice of the order complex induced between H and K is contractible, so we can "ignore" H. The author is unaware of a result which states that if $\mu_G(H) = 0$, then H can be "ignored" and suspects it not to be true in general. As such, more work needs to be done on the intersection of maximal subgroups of the small Ree groups before the homotopy type of its order complex can be determined.

B.2.3 Maximal subgroups

Given the natural relationship between the maximal subgroups of a group, G, and its Möbius function, a natural question to explore would be a partial converse.

Question B.7. *Suppose G is a group for which an incomplete list of maximal subgroups is known, is it possible to determine information about the remaining possible maximal subgroups of G using the Möbius function?*

It is an open question whether there exist maximal subgroups of the Monster $\mathbb{M}$ with socle isomorphic to $U_3(8)$, however, if such subgroups were to exist, then their Möbius function would be -1. Could this information be used, in conjunction with a suitable Eulerian function, to constrain the existence of such maximal subgroups? The number of known classes of maximal subgroups make it too infeasible to try to determine as much of the full Möbius function as possible. However, could a sensible choice of Γ be employed so that $\mathrm{Epi}(\Gamma, H) = 0$ for a large number of classes of maximal subgroups of $\mathbb{M}$? If we let $\Gamma = \Delta(19, 19, 21)$, the triangle group with presentation

$$\Delta(19, 19, 21) = \langle x, y, z \mid x^{19} = y^{19} = z^{21} = xyz = 1\rangle,$$

the only maximal subgroups of $\mathbb{M}$, known or unknown, apart from the class in question, containing elements of order 19 and 21 are isomorphic to one of [27, 125]

$$2.\mathbb{B}, \quad 2^2.{}^2E_6(2){:}S_3, \quad S_3 \times Th, \quad (D_{10} \times HN).2 \quad \text{or} \quad (A_5 \times U_3(8){:}3){:}2.$$

We can even rule out the last class since for such groups the structure constant $n(19, 19, 21) = 0$. Moreover, we know that

$$\frac{|\mathrm{Epi}(\Gamma, \mathbb{M})|}{|\mathrm{Aut}(\mathbb{M})|}$$

must be a non-negative integer. Could such information be used to prove the non-existence of maximal subgroups?

Bibliography

[1] A. S. Bang, *Talteoretiske undersøgesler*, Tidsskr. for Math. **4** (1886), no. 5, 130–137.

[2] N. Barker, N. Boston, and B. Fairbairn, *A note on Beauville p-groups*, Exp. Math. **21** (2012), no. 3, 298–306.

[3] N. Barker, N. Boston, N. Peyerimhoff, and A. Vdovina, *New examples of Beauville surfaces*, Monatsh. Math. **166** (2012), no. 3-4, 319–327.

[4] ———, *An infinite family of 2-groups with mixed Beauville structures*, Int. Math. Res. Not. IMRN (2014), available at `http://imrn.oxfordjournals.org/content/early/2014/03/27/imrn.rnu045.full.pdf+html`.

[5] I. C. Bauer, *Product-quotient surfaces: Result and problems* (2012), available at `http://arxiv.org/abs/1204.3409`.

[6] I. C. Bauer, F. Catanese, and F. Grunewald, *Beauville surfaces without real structures*, Geometric methods in algebra and number theory, 2005, pp. 1–42.

[7] ———, *Chebycheff and Belyi polynomials, dessins d'enfants, Beauville surfaces and group theory*, Mediterr. J. Math. **3** (2006), no. 2, 121–146.

[8] ———, *The classification of surfaces with $p_g = q = 0$ isogenous to a product of curves*, Pure Appl. Math. Q. **4** (2008), no. 2, 547–586.

[9] I. C. Bauer, F. Catanese, and R. Pignatelli, *Complex surfaces of general type: some recent progress*, Global aspects of complex geometry, 2006, pp. 1–58.

[10] ———, *Surfaces of general type with geometric genus zero: a survey*, Complex and differential geometry, 2011, pp. 1–48.

[11] A. Beauville, *Surfaces algébriques complexes*, Astérisque **54** (1978).

[12] ———, *Complex algebraic surfaces*, London Math. Soc. Stud. Texts, vol. 34, Cambridge University Press, Cambridge, 1996. Translation of [11].

[13] G. V. Belyĭ, *Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 2, 267–276. (Russian).

[14] ———, *On Galois extensions of a maximal cyclotomic field*, Math. USSR Izv. **14** (1980), no. 2, 247–256. Translation of [13].

[15] M. Bianchi, A. Mauri, and L. Verardi, *On Hawkes–Isaacs–Özaydin's conjecture*, Istit. Lombardo Accad. Sci. Lett. Rend. A **124** (1990), 99–117.

[16] N. Boston, *A survey of Beauville p-groups*, Beauville Surfaces and Groups, 2015, pp. 35–40.

[17] S. Bouc, *Modules de Möbius*, C. R. Acad. Sci. Paris Sér. I Math. **299** (1984), no. 1, 9–12.

[18] J. N. Bray, D. F. Holt, and C. M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*, London Math. Soc. Lecture Note Ser. vol. 407, Cambridge University Press, Cambridge, 2013.

[19] W. Burnside, *Theory of groups of finite order,* 2nd edn, Dover Publications, Inc., New York, 1955. 2d ed.

[20] F. Catanese, *Fibred surfaces, varieties isogenous to a product and related moduli spaces*, Amer. J. Math. **122** (2000), no. 1, 1–44.

[21] ———, *Moduli spaces of surfaces and real structures*, Ann. of Math. (2) **158** (2003), no. 2, 577–592.

[22] B. Chang, *The conjugate classes of Chevalley groups of type* (G_2), J. Algebra **9** (1968), 190–211.

[23] M. Conder, *Hurwitz groups: a brief survey*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 359–370.

[24] ———, *An update on Hurwitz groups*, Groups Complex. Cryptol. **2** (2010), no. 1, 35–49.

[25] T. Connor and D. Leemans, *An atlas of subgroup lattices of finite almost simple groups*, 2014. `http://homepages.ulb.ac.be/ tconnor/atlaslat/`.

[26] ———, *An atlas of subgroup lattices of finite almost simple groups*, Ars Math. Contemp. **8** (2015), no. 2, 259–266.

[27] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *An Atlas of finite groups*, Oxford University Press, Eynsham, 1985.

[28] B. N. Cooperstein, *Maximal subgroups of* $G_2(2^n)$, J. Algebra **70** (1981), no. 1, 23–36.

[29] H. H. Crapo, *The Möbius function of a lattice*, J. Combinatorial Theory **1** (1966), 126–131.

[30] F. Dalla Volta and A. Lucchini, *Generation of almost simple groups*, J. Algebra **178** (1995), no. 1, 194–223.

[31] S. Delsarte, *Fonctions de Möbius sur les groupes abeliens finis*, Ann. of Math. (2) **49** (1948), no. 3, 600–609.

[32] L. E. Dickson, *Linear groups: With an exposition of the Galois field theory*, Dover Publications, Inc., New York, 1958.

[33] M. Downs, *Möbius inversion of some classical groups and an application to the enumeration of regular maps*, Ph.D. Thesis, University of Southampton, Southampton, 1988.

[34] ———, *The Möbius function of* $\mathrm{PSL}_2(q)$*, with application to the maximal normal subgroups of the modular group*, J. Lond. Math. Soc. (2) **43** (1991), no. 1, 61–75.

[35] ———, *Some enumerations of regular hypermaps with automorphism group isomorphic to* $\mathrm{PSL}_2(q)$, Q. J. Math. **48** (1997), no. 189, 39–58.

[36] M. Downs and G. A. Jones, *Enumerating regular objects with a given automorphism group*, Discrete Math. **64** (1987), no. 2-3, 299–302.

[37] ———, *Enumerating Regular Objects associated with Suzuki Groups*, ArXiv e-prints (2013), available at `http://arxiv.org/abs/1309.5215`.

[38] ———, *The Möbius function of the suzuki groups*, ArXiv e-prints (2014), available at `http://arxiv.org/abs/1404.5470`.

[39] H. Enomoto, *The conjugacy classes of Chevalley groups of type* (G_2) *over finite fields of characteristic* 2 *or* 3, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **16** (1969), 497–512 (1970).

[40] B. Fairbairn, *Some exceptional Beauville structures*, J. Group Theory **15** (2012), no. 5, 631–639.

[41] ———, *More on strongly real Beauville groups*, Proceedings of the SIGMAP 2014 Conference, 2015.

[42] ———, *Recent work on Beauville surfaces, structures and groups*, Groups St Andrews 2013, 2015.

[43] ———, *Strongly real beauville groups*, Beauville surfaces and groups, 2015, pp. 41–61.

[44] B. Fairbairn, K. Magaard, and C. Parker, *Corrigendum: Generation of finite quasisimple groups with an application to groups acting on Beauville surfaces*, Proc. Lond. Math. Soc. (3) **107** (2013), no. 5, 1220.

[45] ———, *Generation of finite quasisimple groups with an application to groups acting on Beauville surfaces*, Proc. Lond. Math. Soc. (3) **107** (2013), no. 4, 744–798. Corrigenda appear in [44].

[46] B. Fairbairn and E. Pierro, *New examples of mixed Beauville groups*, J. Group Theory **18** (2015), no. 5, 761–792.

[47] G. A. Fernández-Alcober and Ş. Gül, *Beauville structures in finite p-groups* (2015), available at `http://arxiv.org/abs/1507.02942`.

[48] F. G. Frobenius, *Über Gruppencharaktere*, Sitzungsber. Kön. Preuss. Akad. Wiss. Berlin (1896), 985–1021.

[49] Y. Fuertes and G. González-Diez, *On Beauville structures on the groups S_n and A_n*, Math. Z. **264** (2010), no. 4, 959–968.

[50] Y. Fuertes, G. González-Diez, and A. Jaikin-Zapirain, *On Beauville surfaces*, Groups Geom. Dyn. **5** (2011), no. 1, 107–119.

[51] Y. Fuertes and G. A. Jones, *Beauville surfaces and finite groups*, J. Algebra **340** (2011), 13–27.

[52] A. Gardiner, C. E. Praeger, and S. Zhou, *Cross ratio graphs*, J. Lond. Math. Soc. (2) **64** (2001), no. 2, 257–272.

[53] S. Garion, *On Beauville Structures for $PSL(2, q)$* (2010), available at `http://arxiv.org/abs/1003.2792`.

[54] S. Garion, M. Larsen, and A. Lubotzky, *Beauville surfaces and finite simple groups*, J. Reine Angew. Math. **666** (2012), 225–243.

[55] M. Geck, G. Hiss, F. Lübeck, G. Malle, and G Pfeiffer, CHEVIE – *A system for computing and processing generic character tables for finite groups of Lie type, Weyl groups and Hecke algebras*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), no. 3, 175–210.

[56] M. Giudici, *Maximal subgroups of almost simple groups with socle $PSL(2, q)$* (2007), available at `http://arxiv.org/abs/math/0703685`.

[57] G. González-Diez and A. Jaikin-Zapirain, *The absolute Galois group acts faithfully on regular dessins and on Beauville surfaces*, Proc. Lond. Math. Soc. (3) (2013). (to appear).

[58] G. González-Diez, G. A. Jones, and D. Torres-Teigell, *Arbitrarily large Galois orbits of non-homeomorphic surfaces* (2011), available at `http://arxiv.org/abs/1110.4930`.

[59] G. González-Diez and D. Torres-Teigell, *Non-homeomorphic Galois conjugate Beauville structures on* $\mathrm{PSL}(2, p)$, Adv. Math. **229** (2012), no. 6, 3096–3122.

[60] R. Gow, *Commutators in finite simple groups of Lie type*, Bull. London Math. Soc. **32** (2000), no. 3, 311–315.

[61] A. Grothendieck, *Esquisse d'un programme*, Geometric Galois actions, 1. Around Grothendieck's Esquisse d'un Programme, 1997, pp. 243–283.

[62] R. Guralnick and G. Malle, *Simple groups admit Beauville structures*, J. Lond. Math. Soc. (2) **85** (2012), no. 3, 694–721.

[63] P. Hall, *The Eulerian functions of a group*, Q. J. Math. **7** (1936), no. 1, 134–151.

[64] R. W. Hartley, *Determination of the ternary collineation groups whose coefficients lie in the* $\mathrm{GF}(2^n)$, Ann. of Math. (2) **27** (1925), no. 2, 140–158.

[65] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1977.

[66] T. Hawkes, I. M. Isaacs, and M. Özaydin, *On the Möbius function of a finite group*, Rocky Mountain J. Math. **19** (1989), no. 4, 1003–1034.

[67] G. A. Jones, *Ree groups and Riemann surfaces*, J. Algebra **165** (1994), no. 1, 41–62.

[68] ______, *Beauville surfaces and groups: a survey*, Rigidity and symmetry, 2014, pp. 205–225.

[69] ______, *Primitive permutation groups containing a cycle*, Bull. Aust. Math. Soc. **89** (2014), no. 1, 159–165.

[70] ______, *Characteristically simple Beauville groups, I: Cartesian powers of alternating groups*, Geometry, Groups and Dynamics, 2015, pp. 289–306.

[71] ______, *Characteristically simple Beauville groups, II: low lank and sporadic groups*, Beauville surfaces and groups, 2015, pp. 97–120.

[72] W. M. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata **36** (1990), no. 1, 67–87.

[73] P. B. Kleidman, *The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups*, J. Algebra **117** (1988), no. 1, 30–71.

[74] ———, *The maximal subgroups of the Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups*, J. Algebra **115** (1988), no. 1, 182–199.

[75] C. Kratzer and J. Thévenaz, *Fonction de Möbius d'un groupe fini et anneau de Burnside*, Comment. Math. Helv. **59** (1984), no. 3, 425–438.

[76] ———, *Type d'homotopie des treillis et treillis des sous-groupes d'un groupe fini*, Comment. Math. Helv. **60** (1985), no. 1, 85–106.

[77] V. M. Levchuk and Ya. N. Nuzhin, *Structure of Ree groups*, Algebra and Logic **24** (1985), no. 1, 16–26. Translation of [78].

[78] ———, *The structure of Ree groups*, Algebra i Logika **24** (1985), no. 1, 26–41. (Russian).

[79] M. W. Liebeck, *Probabilistic and asymptotic aspects of finite simple groups*, Probabilistic group theory, combinatorics, and computing, 2013, pp. 1–34.

[80] M. W. Liebeck and A. Shalev, *Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky*, J. Algebra **184** (1996), no. 1, 31–57.

[81] H. Lüneburg, *Some remarks concerning the Ree groups of type ($G2$)*, J. Algebra **3** (1966), no. 2, 256–259.

[82] ———, *Ein Einfacher Beweis für den Satz von Zsigmondy über primitive Primteiler von A^{N-1}*, Geometries and groups, 1981, pp. 219–222.

[83] G. Malle, *Hurwitz groups and $G_2(q)$*, Canad. Math. Bull. **33** (1990), no. 3, 349–357.

[84] ———, *The maximal subgroups of ${}^2F_4(q^2)$*, J. Algebra **139** (1991), no. 1, 52–69.

[85] H. H. Mitchell, *Determination of the ordinary and modular ternary linear groups*, Trans. Amer. Math. Soc. **12** (1911), no. 2, 207–242.

[86] ———, *The subgroups of the quaternary abelian linear group*, Trans. Amer. Math. Soc. **15** (1914), no. 4, 379–396.

[87] E. H. Moore, *The subgroups of the generalized finite modular group*, Dicennial publications of the University of Chicago Press **9** (1904), 141–190.

[88] S. P. Norton and R. A. Wilson, *Anatomy of the Monster. II*, Proc. London Math. Soc. (3) **84** (2002), no. 3, 581–598.

[89] E. A. O'Brien, *The p-group generation algorithm*, J. Symbolic Comput. **9** (1990), no. 5, 677–698.

[90] H. Pahlings, *On the Möbius function of a finite group*, Arch. Math. (Basel) **60** (1993), no. 1, 7–14.

[91] G. Pfeiffer, *The subgroups of M_{24}, or how to compute the table of marks of a finite group*, Experiment. Math. **6** (1997), no. 3, 247–270.

[92] E. Pierro, *The Möbius function of the small Ree groups* (2014), available at `http://arxiv.org/abs/1410.8702`.

[93] D. Quillen, *Homotopy properties of the poset of nontrivial p-subgroups of a group*, Adv. Math. **28** (1978), no. 2, 101–128.

[94] R. Ree, *A family of simple groups associated with the simple Lie algebra of type (G_2)*, Bull. Amer. Math. Soc. (N.S.) **66** (1960), 508–510.

[95] ———, *A family of simple groups associated with the simple Lie algebra of type (F_4)*, Bull. Amer. Math. Soc. (N.S.) **67** (1961), 115–116.

[96] ———, *A family of simple groups associated with the simple Lie algebra of type* (G_2), Amer. J. Math. **83** (1961), 432–462.

[97] D. J. S. Robinson, *A course in the theory of groups*, Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1996.

[98] M. Roitman, *On Zsigmondy primes*, Proc. Amer. Math. Soc. **125** (1997), no. 7, 1913–1919.

[99] G.-C. Rota, *On the foundations of combinatorial theory. I. Theory of Möbius functions*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **2** (1964), 340–368.

[100] M. A. Shahabi and H. Mohtadifar, *The characters of finite projective symplectic group* $\mathrm{PSp}(4, q)$, Groups St. Andrews 2001 in Oxford. Vol. II, 2003, pp. 496–527.

[101] J. Shareshian, *Combinatorial properties of subgroup lattices of finite groups*, Ph.D. Thesis, Rutgers University, New Jersey, 1996.

[102] ———, *On the Möbius number of the subgroup lattice of the symmetric group*, J. Combin. Theory Ser. A **78** (1997), no. 2, 236–267.

[103] J Shareshian, *On the shellability of the order complex of the subgroup lattice of a finite group*, Trans. Amer. Math. Soc. **353** (2001), no. 7, 2689–2703.

[104] K. Shinoda, *The conjugacy classes of the finite Ree groups of type* (F_4), J. Fac. Sci. Univ. Tokyo Sect. IA Math. **22** (1975), 1–15.

[105] W. A. Simpson and J. Sutherland Frame, *The character tables for* SL(3, q)*,* SU(3, q^2)*,* PSL(3, q)*,* PSU(3, q^2), Canad. J. Math. **25** (1973), 486–494.

[106] L. Solomon, *The Burnside algebra of a finite group*, J. Combinatorial Theory **2** (1967), 603–615.

[107] J. Stix and A. Vdovina, *Simply transitive quaternionic lattices of rank* 2 *over* $\mathbb{F}_q(t)$ *and a non-classical fake quadric* (2013), available at `http://arxiv.org/abs/1304.5549`.

[108] ———, *Series of* p*-groups with Beauville structure* (2014), available at `http://arxiv.org/abs/1405.3872`. (to apper in Monatsh. Math.)

[109] M. Suzuki, *A new type of simple groups of finite order*, Proc. Natl. Acad. Sci. USA **46** (1960), 868–870.

[110] ———, *On a class of doubly transitive groups*, Ann. of Math. (2) **75** (1962), 105–145.

[111] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.7.8*, The GAP Group, 2015. `http://www.gap-system.org`.

[112] J. Tits, *Les groupes simples de Suzuki et de Ree*, Séminaire Bourbaki, Vol. 6, 1995, pp. Exp. No. 210, 65–82.

[113] H. Van Maldeghem, *Generalized Polygons*, Monographs in Mathematics, vol. 93, Birkhäuser, 1998.

[114] H. N. Ward, *On Ree's series of simple groups*, Trans. Amer. Math. Soc. **121** (1966), 62–89.

[115] L. Weisner, *Abstract theory of inversion of finite series*, Trans. Amer. Math. Soc. **38** (1935), no. 3, 474–484.

[116] ———, *Some properties of prime-power groups*, Trans. Amer. Math. Soc. **38** (1935), no. 3, 485–492.

[117] R. A. Wilson, *The symmetric genus of the Baby Monster*, Q. J. Math **44** (1993), no. 176, 513–516.

[118] ———, *Standard generators for sporadic simple groups*, J. Algebra **184** (1996), no. 2, 505–515.

[119] ———, *The maximal subgroups of the Baby Monster. I*, J. Algebra **211** (1999), no. 1, 1–14.

[120] ———, *The finite simple groups*, Graduate Texts in Mathematics, vol. 251, Springer-Verlag London, Ltd., London, 2009.

[121] ———, *Another new approach to the small Ree groups*, Arch. Math. (Basel) **94** (2010), no. 6, 501–510.

[122] ———, *A new construction of the Ree groups of type* ${}^2G_2$, Proc. Edinb. Math. Soc. (2) **53** (2010), no. 2, 531–542.

[123] ———, *On the simple groups of Suzuki and Ree*, Proc. Lond. Math. Soc. (3) **107** (2013), no. 3, 680–712.

[124] R. A. Wilson, R. A. Parker, S. Nickerson, J. N. Bray, and T. Breuer, *AtlasRep, A GAP Interface to the Atlas of Group Representations, Version 1.5.0*, 2011. `http://www.math.rwth-aachen.de/ Thomas.Breuer/atlasrep/` Refereed GAP package.

[125] R. A. Wilson, P. Walsh, J. Tripp, I. Suleiman, R. A. Parker, S. P. Norton, S. Nickerson, S. Linton, J. Bray, and R. Abbott, *Atlas of Finite Group Representations*, 2015. `http://brauer.maths.qmul.ac.uk/Atlas/v3/`.

[126] A. Wiman, *Bestimmung aller Untergruppen einer doppelt unendlichen Reihe von einfachen Gruppen*, Stockh. Akad. Bihang **25** (1899), 1–47.

[127] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. **3** (1892), no. 1, 265–284.