GENERATION OF SIMPLE GROUPS BY CONJUGATE INVOLUTIONS

Jonathan Mark Ward

Queen Mary college,
University of London

Thesis submitted to
The University of London
for the degree of
Doctor of Philosophy
2009.

Declaration

The results presented in this thesis, unless otherwise stated, are the unaided work of the author, whilst enrolled in the School of Mathematical Sciences as a candidate for the degree of Doctor of Philosophy. This work has not been submitted for any other degree or award in any other university or educational establishment.

Jonathan Mark Ward

May 2009

Abstract

The following problem was posed by V. D. Mazurov in the Kourovka notebook:

14.69 For every finite simple group, find the minimum number of generating involutions satisfying an additional condition, in each of the following cases:

(a) The product of the generating involutions is 1.

(b) All generating involutions are conjugate.

(c) The conditions (a) and (b) are simultaneously satisfied.

(d) All generating involutions are conjugate and two of them commute.

This thesis is focused on part (c) of the above problem. For a non-abelian finite simple group, the minimum number of generating involutions with this property must be at least five. Hence, for G, a non-abelian simple group, this thesis approaches the above problem by asking whether G has the following property:

1. G can be generated by five conjugate involutions whose product is 1.

Often this is done by asking whether the group G has the following stronger property:

2. G can be generated by three conjugate involutions, with the product of two of them also an involution and conjugate to the other three.

After an introductory chapter, this thesis answers these questions for the following simple groups:

- The simple alternating groups (chapter 2). Standard results about the structure of the alternating groups are used;

- The simple sporadic groups (chapter 3). A method developed by V. D. Mazurov is used along with information from character tables;
- The simple linear groups over fields of odd characteristic with some exceptions (chapter 4). A general method developed by L. Di Martino and N. Vavilov is used which is based on information about irreducible groups generated by transvections.

Chapter 5 concludes the thesis with a discussion of the results and some possible next steps.

Acknowledgments

I would like to begin by thanking my supervisor, Robert Wilson. Thank you for setting me off down this road, for getting me fascinated by the simple groups, for sage advice, good suggestions and for your patience. Also thank you for all the hard work done in preparing the various incarnations of the ATLAS, the first place I looked whenever I was stuck.

I would also like to thank everyone in the School of Mathematical Sciences at Queen Mary College. It has been a pleasant, encouraging and stimulating place to study, and that is down to the people who are there. To the academics (for always being interested and interesting), to my fellow students (for helping to keep me sane) and to the great admin. and support staff (for knowing what's actually going on) - a big Thank you!

I am of course very grateful to the EPSRC for their financial support.

My family have been a great support to me throughout my life, and I do not have the space here to do justice to all the ways in which they have helped me. However, I would like to take this opportunity to thank you all for your love in teaching me and encouraging me to follow Jesus. I would like to extend this thank you to my church family as well, especially those whom I got to know at St. Helen's Bishopsgate. Your love, teaching and example have been of incalculable value. Thank you.

But primarily I would like to thank the God and Father of my Lord Jesus Christ. For all your good gifts, but especially for sending your Son to die the death that my sins deserved, for forgiving me and for your steadfast love toward me.

Thy anger, for what I have done,
The gospel forbids me to fear:
My sins thou hast charg'd on thy Son;
Thy justice to him I refer.
Be mindful of Jesus and me!
My pardon he suffer'd to buy;
And what he procur'd on the tree,
For me he demands in the sky.

A. M. Toplady (1740-1778)

Contents

List of Tables

Chapter 1

Introduction

The following problem was posed by V. D. Mazurov in the Kourovka notebook [MK02]:

14.69 For every finite simple group, find the minimum number of generating involutions satisfying an additional condition, in each of the following cases:

(a) The product of the generating involutions, in some order, is 1.

(b) (Malle-Saxl-Weigel) All generating involutions are conjugate.

(c) (Malle-Saxl-Weigel) The conditions (a) and (b) are simultaneously satisfied.

(d) All generating involutions are conjugate and two of them commute.

1.1 Notation

Before we continue discussing this, however, we shall consider the notation we will be using.

Most of the notation will be quite standard, and it should be clear from context what objects are. Let G be any group. We will denote by 1, the identity element of the group G, and by x^{-1}, the inverse of the element $x \in G$. For two elements, $x, y \in G$, we denote by $x^y = y^{-1}xy$, the conjugate of x by

y. We write $H \leqslant G$ when H is a subgroup of G. For a subset, $X \subseteq G$, and for a list of elements $x_1, \ldots, x_n \in G$, we denote by $\langle X \rangle \leqslant G$, the subgroup of G generated by X, and $\langle x_1, \ldots, x_n \rangle \leqslant G$, the subgroup of G generated by $x_1, \ldots, x_n$.

1.2 Preliminaries

Since the only finite abelian simple groups are the cyclic groups of prime order, the only finite abelian simple group to contain involutions is C_2, the cyclic group of order 2. The answers to the above questions for this group (when they make sense) are obvious. Hence, we will confine ourselves to considering non-abelian simple groups. There are of course lower bounds for these numbers given just from the fact that the groups considered are non-abelian finite simple. If you have a non-abelian group generated by 4 involutions, a, b, c and d whose product is 1, then, since $(ab)^a = ba$, $(ab)^b = ba$ and $(ab)^c = cabc = cd = ba$, the group generated by ab is a normal subgroup of $\langle a, b, c, d \rangle$. Similarly, the group generated by bc is a normal subgroup of $\langle a, b, c, d \rangle$. Hence, if $\langle a, b, c, d \rangle$ is simple, then $ab = bc = 1$ and so $a = b = c = d$. Then, $\langle a, b, c, d \rangle = \langle a \rangle$ is a cyclic group and so is abelian. This gives a lower bound for part (a) and part (c) above, while for part (b) and part(d) we can obtain a lower bound simply by realising that a non-abelian group generated by 2 involutions can only be a dihedral group, which is not simple. The bounds obtained are then, respectively:

(a) 5.

(b) 3.

(c) 5.

(d) 3.

This type of problem often comes down to determining if such bounds are realised for the group in question.

For example, the following questions have, for the most part, been answered:

1. Which finite simple groups can be generated by 3 conjugate involutions?
2. Which finite simple groups can be generated by 3 involutions two of which commute?

A simple group can be generated by 3 conjugate involutions if it can be generated by an involution and an element of order 3, as if $G := \langle a, b \rangle$, with G simple, $a^2 = 1$ and $b^3 = 1$, then $\left\langle a, a^b, a^{b^{-1}} \right\rangle$ forms a normal subgroup of G, and hence must be equal to G. Groups that can be generated in this way are often called '$(2, 3)$-generated' groups. As such, the answer to the first of these questions has mostly been answered, as the following simple and near-simple groups are known to be $(2, 3)$-generated:

- The alternating groups, A_n for $n \neq 6, 7, 8$ ([Mil01]);
- The projective special linear groups $L_2(q)$, $q \neq 9$ ([Mac69]);
- The projective special linear groups $L_3(q)$, $q \neq 4$ ([Gar78],[Coh81]);
- The special linear groups $SL_n(q)$, $n \geqslant 25$ ([Tam88]);
- The special linear groups $SL_n(q)$, $n \geqslant 5$, $q \neq 2, 9$ ([DV94],[DV96]);
- The Chevalley groups $G_2(q)$ of type G_2 and the twisted groups ${}^2G_2(q)$ ([Mal88],[Mal90]);
- The projective symplectic groups $PSp_4(q)$, $q = p^m$, $p \neq 2, 3$ ([CD93]);
- The special linear groups $SL_4(q)$, $q = p^m$, $p \neq 2$ ([TV94]);

- The groups $PSp_{2n}(q)$ and $PSU_{2n}(q^2)$, $n \geqslant 37$, characteristic $\neq 2$ and the groups $P\Omega^+_{2n}(q)$, $n \geqslant 37$ [TWG95];

- All the sporadic simple groups other than M_{11}, M_{22}, M_{23} and McL ([Wol89]). In fact all the sporadic groups can be generated by 3 conjugate involutions ([MSW94]);

The second question, has been answered for the following groups:

- Chevalley groups of rank 1 ([Nuz84]);

- Chevalley groups over a field of characteristic 2 ([Nuz90]);

- The alternating groups ([Nuz92]);

- The classical groups $SL_n(q)$ for $n \geqslant 14$, $Sp_{2n}(q)$ for $n \geqslant 20$ q odd, $\Omega^+_{2n}(q)$ for $n \geqslant 20$, $\Omega_{2n+1}(q)$ for $n \geqslant 20$ q odd, $SU_{2n}(q^2)$ for $n \geqslant 20$ q odd and $SU_{2n+1}(q^2)$ for $n \geqslant 20$ q odd ([TZ97]);

Thus, parts (b) and (d) in the above question have, for the most part, been answered.

My work has been focused on part (c) of the above question. Thus I have been answering the question:

Which of the non-abelian finite simple groups, G, have the following property:

Property 1. *G can be generated by 5 conjugate involutions whose product is the identity.*

i.e. when is the lower bound realised (taking into account that G is simple). Since a large number of the finite simple groups are known to be generated by 3 conjugate involutions, a, b and c say, if this lower bound is not realised, then often it will be possible to generate G with 6 conjugate involutions whose product is the identity, namely a,b,c,c,b and a (as $abccba = 1$).

Of course, it is often easier to prove a stronger property, and as such I have often answered the question:

Which of the non-abelian finite simple groups, G, have the following property:

Property 2. *G can be generated by 3 conjugate involutions a, b and c, 2 of which, a and b, commute and such that ab is also conjugate to a, b and c.*

(From now on I will refer to a group as either 'having' or 'not having' Property 1 and/or Property 2 respectively.) Property 2 is indeed a stronger property than Property 1:

Lemma 1.2.1. *If a group G has Property 2 then it has Property 1.*

Proof. Let a group, G, have Property 2. So $G = \langle a, b, c \rangle$, with $ab = ba$, $o(a) = 2$, and b, c and $ab \in a^G$. Then clearly $G = \langle a, b, c, c, ab \rangle$, and $abcc(ab) = 1$. Hence G has Property 1. □

Hence we will often show that a group has Property 2. It is worth noting at this point that these two properties are not equivalent, the alternating group on 6 symbols, A_6 being an example of a group that has Property 1 but not Property 2. To see that A_6 has Property 1, see Lemma 2.2.7, and to see that it does not have Property 2, see Lemma 2.2.2. In fact, the following Lemma shows that Property 2 is equivalent to a (more intuitively) stronger condition.

Lemma 1.2.2. *Property 2 is equivalent to the property "G can be generated by 5 conjugate involutions whose product is the identity, and 2 of which are equal."*

Proof. From the proof of Lemma 1.2.1, it is easy to see that Property 2 implies this new property. To see that the opposite implication holds, consider a group, G, generated by 5 conjugate involutions, a, b, c, d and e, s.t. $abcde = 1$, and

s.t. 2 of them are equal. Since $abcde = 1$, we can assume, without loss of generality, that either $a = b$ or $a = c$. If $a = b$, then

$$\begin{aligned} G &= \langle a, a, c, d, e \rangle \\ &= \langle a, a, c, d \rangle \text{ since } e = abcd \\ &= \langle a, c, d \rangle \end{aligned}$$

and $cd = bae = aae = e$. Hence G is generated by 3 conjugate involutions, a, c and d, with c and d commuting and having product conjugate to a, c and d. Hence G has Property 2. If $a = c$, then

$$\begin{aligned} G &= \langle a, b, a, d, e \rangle \\ &= \langle a, a, d, e \rangle \text{ since } b = cdea \\ &= \langle a, d, e \rangle \end{aligned}$$

and $de = cba = aba = b^a$. Hence, similarly to above, d and e commute, and their product is conjugate to a, d and e. Hence G has Property 2. □

In answering questions asking whether a group can be generated in a particular way, there are two outcomes:

1. Proving a group CAN be generated in a particular way OR

2. Proving a group CANNOT be generated in a particular way.

To show that a group can be generated in a particular way, we must somehow show that elements with the desired properties exist and generate the group. Often, this consists of finding and exhibiting such elements, and then showing that they generate the desired group.

To show that a group cannot be generated in a particular way, we must somehow show that any elements in the group with the desired properties do not generate the group. As such, the following "non-generation" results are useful:

Theorem 1.2.3 (L. Scott. [Sco77])**.** . *Let G be a group acting linearly on a finite-dimensional vector space V over a field k. For X a subgroup or element of G, let $v(X) = v(X, V)$ denote the codimension of the fixed-point space of X in V. Also let $v(X^*)$ denote $v(X, V^*)$, where V^* is the dual of V. Suppose then that G is generated by elements $x_1, \ldots, x_n$ with $x_1 \cdots x_n = 1$. Then*

$$\sum_{i=1}^{n} v(x_i) \geqslant v(G) + v(G^*).$$

Often, it is easier to use a less general form of this result, such as:

Theorem 1.2.4. *Let x_1, x_2, ... , x_m be elements generating a group G with $x_1 x_2 \cdots x_m = 1$, and let V be an irreducible module for G of dimension n. Let $C_V(x_i)$ denote the fixed point space of $\langle x_i \rangle$ on V, and let d_i be the dimension of $V/C_V(x_i)$. Then*

$$d_1 + d_2 + \cdots + d_m \geqslant 2n.$$

or occasionally, where it was more convenient to use a permutation representation, the following result was used (originally proved by Ree [Ree71], but also a corollary of Theorem 1.2.3):

Theorem 1.2.5 (Ree)**.** . *Let x_1, x_2, ... , x_m be permutations generating a transitive group on n letters, with $x_1 x_2 \cdots x_m = 1$, and let c_i denote the number of orbits of $\langle x_i \rangle$, $1 \leqslant i \leqslant m$. Then*

$$c_1 + c_2 + \cdots + c_m \leqslant (m-2)\, n + 2.$$

1.3 Statement of Results

The results in this thesis are summarised in table 1.1 below:

(Note that the result marked * is not proved in this thesis, but a proof can be found in [Nuz97].)

Table 1.1: Summary of Results

G			Property 1	Property 2
A_n	$n = 6$		✓	×
	$n = 7$		×	×
	$n = 8$		×	×
	$n = 12$		×	×
	$n \geqslant 5$, $n \neq 6, 7, 8, 12$		✓	✓
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}			✓	✓
HN			✓	✓
Ly			✓	✓
Th			✓	✓
Fi_{23}			✓	✓
Co_1			✓	✓
J_4			✓	✓
Fi'_{24}			✓	✓
B			✓	✓
M			✓	✓
$L_n(q)$	$n = 2$	$q = 7$	×	×
		$q = 9$	✓	×
		$q \geqslant 5$, $q \neq 7, 9$	✓	✓
	$n = 3$	$q \equiv 1 \mod 3$	✓	$\times^*$
		$q \equiv 0$ or $2 \mod 3$	×	×
	$n = 6$	$q \equiv 1 \mod 4$, $q \neq 9$	✓	✓
	$n = 6$	$q \equiv 3 \mod 4$,	?	?
	$n \geqslant 4$, $n \neq 6$	$q \neq 9$	✓	✓

Chapter 2

The Alternating Groups

The purpose of this chapter is to determine which of the (finite simple) alternating groups has Property 1. In fact we will prove the following Theorem:

Theorem 2.0.1. *The Alternating group on n symbols for $n \geqslant 5$, A_n, has Property 1 if and only if $n \neq 7, 8, 12$.*

Note that the only non-simple alternating group that contains involutions is A_4, and the involutions in A_4 generate at most $D_4 \lneqq A_4$. Hence for $n < 5$, A_n does not have Property 1.

In fact, to prove Theorem 2.0.1 we will also prove the following:

Theorem 2.0.2. *The Alternating group on n symbols for $n \geqslant 5$, A_n, has Property 2 if and only if $n \neq 6, 7, 8, 12$.*

We will divide this result into four separate cases, corresponding to the four values of n modulo 4. The Theorem can be restated as:

Theorem 2.0.3. *The Alternating group on n symbols for $n \geqslant 5$, A_n, has Property 2 if and only if:*

- $n = 4k + 1$ *and* $k \geqslant 1$.
- $n = 4k + 2$ *and* $k \geqslant 2$.
- $n = 4k + 3$ *and* $k \geqslant 2$.
- $n = 4k$ *and* $k \geqslant 4$.

2.1 Notation and Preliminaries

We use the standard notation for permutations, however as we are looking at general cases, we will want to express the generators and other permutations in a general way. To that end, we have chosen generators that have a discernible pattern, which we will make clear to the reader. For example, for $n = 4k$, $n \geqslant 8$, we denote by:

$$(1,2)\,(3,4)\,\underbrace{(5,8)\,(6,7)\ldots(n-7,n-4)\,(n-6,n-5)}_{(4l-3,4l)(4l-2,4l-1)\ 2\leqslant l\leqslant k-1}\,(n-3,n-2)\,(n-1,n)$$

the permutation in A_n that is the product of the permutations $(1,2)\,(3,4)$, $(n-3,n-2)\,(n-1,n)$ and the sequence of permutations, starting with $(5,8)\,(6,7)$ and ending with $(n-7,n-4)\,(n-6,n-5)$, that take the form $(4l-3,4l)\,(4l-2,4l-1)$ for integers, l, in the desired range (in this case $2 \leqslant l \leqslant k-1$). Note that this product is a product of disjoint cycles and hence the whole permutation described is a valid one. Note also that, for the smallest value of n allowed, we sometimes allow the sequence to have zero length, i.e. we include the permutation $(1,2)\,(3,4)\,(5,6)\,(7,8) \in A_8$ in this example. It should be clear when this is the case.

The following Theorem will be useful:

Theorem 2.1.1. *Let G be a primitive subgroup of S_n. If G contains a 3-cycle, then $G \geqslant A_n$.*

This result is well known, and a proof can be found in any sufficiently advanced book on Permutation Groups, for example in [Cam99]. Clearly, from this result, if we can establish primitivity of a group of even permutations that contains a 3-cycle we will have shown that we have the alternating group.

The following two results will also be useful. Again, they are reasonably well known results and their proofs can be found in a sufficiently advanced book on Permutation Groups, for example in [Pas68].

Lemma 2.1.2. *Let G be a permutation group on $\{1,\ldots,n\}$. If G is 2-transitive on $\{1,\ldots,n\}$ then G is primitive on $\{1,\ldots,n\}$.*

Lemma 2.1.3. *Let G be a permutation group on $\{1,\ldots,n\}$. If G is transitive on $\{1,\ldots,n\}$ and, for some i, $1 \leqslant i \leqslant n$, $G_i := \{g \in G : i^g = i\}$ is transitive on $\{1,\ldots,n\} \setminus \{i\}$, then G is 2-transitive on $\{1,\ldots,n\}$.*

2.2 The Proofs

We will prove the positive assertions by displaying suitable involutions and we now consider these results separately:

Lemma 2.2.1. *Let $n = 4k+1$ with $k \geqslant 1$. Then A_n has Property 2.*

Proof. Let

$a := \underbrace{(1,2)\ldots(n-2,n-1)}_{(2l-1,2l)\ 1\leqslant l\leqslant 2k}$,

$b := \underbrace{(1,4)\,(2,3)\ldots(n-4,n-1)\,(n-3,n-2)}_{(4l-3,4l)(4l-2,4l-1)\ 1\leqslant l\leqslant k}$,

$c := \underbrace{(2,3)\ldots(n-1,n)}_{(2l,2l+1)\ 1\leqslant l\leqslant 2k}$

and so we have

$ab = \underbrace{(1,3)\,(2,4)\ldots(n-4,n-2)\,(n-3,n-1)}_{(4l-3,4l-1)(4l-2,4l)\ 1\leqslant l\leqslant k}$, which is an involution with the same cycle type as a, b and c and so is conjugate to them in A_n. Thus a, b and c have the desired properties. It remains to show that they generate A_n.

Let $G := \langle a, b, c\rangle$.

Clearly G is a subgroup of S_n.

Now, $abcac = \underbrace{(2,7)\,(4,5)\ldots(n-7,n-2)\,(n-5,n-4)}_{(4l-2,4l+3)(4l,4l+1)\ 1\leqslant l\leqslant k-1}(n-3,n-1,n)$ (or just $abcac = (n-3,n-1,n) = (2,4,5)$ when $n = 5$).

Hence $(abcac)^2 = (n-3,n,n-1)$.

Also, G is a primitive subgroup of S_n. It is clearly transitive on $\{1,\ldots,n\}$. We now take $G_n := \{g \in G : n^g = n\}$, the subgroup of G that fixes the point

n. Now a, b and $(abcac)^3 = \underbrace{(2,7)\,(4,5)\ldots(n-7,n-2)\,(n-5,n-4)}_{(4l-2,4l+3)(4l,4l+1)\ 1\leqslant l\leqslant k-1}$ fix n and so are in G_n, and $\left\langle a,b,(abcac)^3\right\rangle \leqslant G_n$ is transitive on $\{1,\ldots,n-1\}$. Hence, by Lemma 2.1.3, G is 2-transitive, and hence primitive on $\{1,\ldots,n\}$, by Lemma 2.1.2.

Hence by Theorem 2.1.1, $G \geqslant A_n$. In fact, as a, b and c are all even permutations, $G \cong A_n$, and so we are done. □

Lemma 2.2.2. *Let $n = 4k+2$ with $k \geqslant 2$. Then A_n has Property 2.*

Proof. Let

$a := \underbrace{(3,4)\ldots(n-1,n)}_{(2l-1,2l)\ 2\leqslant l\leqslant 2k+1}$,

$b := (1,2)\,(3,4)\,\underbrace{(5,8)\,(6,7)\ldots(n-5,n-2)\,(n-4,n-3)}_{(4l-3,4l)(4l-2,4l-1)\ 2\leqslant l\leqslant k}$,

$c := \underbrace{(2,3)\ldots(n-2,n-1)}_{(2l,2l+1)\ 1\leqslant l\leqslant 2k}$

and so we have

$ab = (1,2)\,\underbrace{(5,7)\,(6,8)\ldots(n-5,n-3)\,(n-4,n-2)}_{(4l-3,4l-1)(4l-2,4l)\ 2\leqslant l\leqslant k}\,(n-1,n)$ which is an involution with the same cycle type as a, b and c and so is conjugate to them in A_n. Thus a, b and c have the desired properties. It remains to show that they generate A_n.

Let $G := \langle a,b,c\rangle$.

Clearly G is a subgroup of S_n.

Now, $abcacbc = (1,9,4,7)\,(2,3,5)\,\underbrace{(6,11)\ldots(n-6,n-1)}_{(2l,2l+5)\ 3\leqslant l\leqslant 2k-2}\,(n-4,n)$.

Hence $(abcacbc)^4 = (2,3,5)$.

Also, G is a primitive subgroup of S_n. It is clearly transitive on $\{1,\ldots,n\}$. We now take $G_1 := \{g \in G : 1^g = 1\}$, the subgroup of G that fixes the point 1. Now a and c fix 1 and so are in G_1, and $\langle a,c,\rangle \leqslant G_n$ is transitive on $\{2,\ldots,n\}$. Hence, by Lemma 2.1.3, G is 2-transitive, and hence primitive on $\{1,\ldots,n\}$, by Lemma 2.1.2.

Hence by Theorem 2.1.1, $G \geqslant A_n$. In fact, as a, b and c are all even permutations, $G \cong A_n$, and so we are done. □

Lemma 2.2.3. *Let $n = 4k + 3$ with $k \geqslant 2$. Then A_n has Property 2.*

Proof. Let

$$a := \underbrace{(1,2)\dots(n-4,n-3)}_{(2l-1,2l)\ 1\leqslant l\leqslant 2k},$$

$$b := (3,4)\underbrace{(5,8)(6,7)\dots(n-6,n-3)(n-5,n-4)}_{(4l-3,4l)(4l-2,4l-1)\ 2\leqslant l\leqslant k}(n-2,n-1),$$

$$c := (1,n)(2,n-1)(4,5)\underbrace{(7,10)(8,9)\dots(n-8,n-5)(n-7,n-6)}_{(4l-1,4l+2)(4l,4l+1)\ 2\leqslant l\leqslant k-1}\dots$$

$$\dots(n-3,n-2),$$

and so we have

$ab = (1,2)\underbrace{(5,7)(6,8)\dots(n-6,n-4)(n-5,n-3)}_{(4l-3,4l-1)(4l-2,4l)\ 2\leqslant l\leqslant k}(n-2,n-1)$ which is an involution with the same cycle type as a, b and c and so is conjugate to them in A_n. Thus a, b and c have the desired properties. It remains to show that they generate A_n.

Let $G := \langle a, b, c\rangle$.

Clearly G is a subgroup of S_n.

Now,

$$ac = (1,n-1,2,n)(3,5,6,4)\underbrace{(7,9)(8,10)\dots(n-8,n-6)(n-7,n-5)}_{(4l-1,4l+1)(4l,4l+2)\ 2\leqslant l\leqslant k-1}\dots$$

$$\dots(n-4,n-2,n-3).$$

Hence $(ac)^4 = (n-4,n-2,n-3)$.

Also, G is a primitive subgroup of S_n. It is clearly transitive on $\{1,\dots,n\}$. We now take $G_n := \{g \in G : n^g = n\}$, the subgroup of G that fixes the point n. Now a, b and b^c fix n and so are in G_n, and $\langle a, b, b^c\rangle \leqslant G_n$ is transitive on $\{1,\dots,n-1\}$, as . Hence, by Lemma 2.1.3, G is 2-transitive, and hence primitive on $\{1,\dots,n\}$, by Lemma 2.1.2.

Hence by Theorem 2.1.1, $G \geqslant A_n$. In fact, as a, b and c are all even permutations, $G \cong A_n$, and so we are done. □

Lemma 2.2.4. *Let $n = 4k$ with $k \geqslant 4$. Then A_n has Property 2.*

Proof. Let

$$a := \underbrace{(1,2)\dots(n-5,n-4)}_{(2l-1,2l)\ 1\leqslant l\leqslant 2k-2},$$

$$b := (5,6)\,(7,8)\,\underbrace{(9,12)\,(10,11)\dots(n-7,n-4)\,(n-6,n-5)}_{(4l-3,4l)(4l-2,4l-1)\ 3\leqslant l\leqslant k-1}\dots$$

$$\dots(n-3,n-2)\,(n-1,n),$$

$$c := \underbrace{(2,3)\dots(n-8,n-7)}_{(2l,2l+1)\ 1\leqslant l\leqslant 2k-4}\,(n-4,n-3)\,(n-2,n-1)$$

and so we have

$$ab = (1,2)\,(3,4)\,\underbrace{(9,11)\,(10,12)\dots(n-7,n-5)\,(n-6,n-4)}_{(4l-3,4l-1)(4l-2,4l)\ 3\leqslant l\leqslant k-1}\dots$$

$$\dots(n-3,n-2)\,(n-1,n)$$

which is an involution with the same cycle type as a, b and c and so is conjugate to them in A_n. Thus a, b and c have the desired properties. It remains to show that they generate A_n.

Let $G := \langle a, b, c\rangle$.

Clearly G is a subgroup of S_n.

Now,

$$c\left((bc)^{\frac{n}{2}+3}\right)^{abc} = (1,5,4)\,(2,3)\,\underbrace{(6,7)\dots(n-10,n-9)}_{(2l,2l+3)\ 3\leqslant l\leqslant 2k-5}\dots$$

$$\dots(n-8,n-7,n-3,n-4)\,(n-2,n-1).$$

Hence $\left(c\left((bc)^{\frac{n}{2}+3}\right)^{abc}\right)^4 = (1,5,4)$.

Also, G is a primitive subgroup of S_n. It is clearly transitive on $\{1,\dots,n\}$. We now take $G_n := \{g \in G : n^g = n\}$, the subgroup of G that fixes the point

n. Now a, c and $bcacb$ fix n and so are in G_n, and $\langle a, c, bcacb\rangle \leqslant G_n$ is transitive on $\{1, \ldots, n-1\}$, as $(n-6)^{bcacb} = n-2$. Hence, by Lemma 2.1.3, G is 2-transitive, and hence primitive on $\{1, \ldots, n\}$, by Lemma 2.1.2.

Hence by Theorem 2.1.1, $G \geqslant A_n$. In fact, as a, b and c are all even permutations, $G \cong A_n$, and so we are done. □

Thus, we have that A_n has Property 2 for $n \geqslant 5$ and $n \neq 6, 7, 8, 12$. Thus by Lemma 1.2.1, we have that A_n has Property 1 for $n \geqslant 5$ and $n \neq 6, 7, 8, 12$. Also we have:

Lemma 2.2.5. *A_6 has Property 1.*

Proof. Let
$a := (1,2)(4,5)$,
$b := (2,3)(4,5)$,
$c := (3,4)(5,6)$.
Now

$$\begin{aligned} abc &= (1,4,3,2)(5,6) \\ &= (1,2)(3,4) \cdot (2,4)(5,6) \end{aligned}$$

a product of two involutions. We call these involutions e and d respectively. These involutions a, b, c, d and e all have the same cycle type and so are conjugate in A_6, and by definition of d and e, we have $abcde = 1$. Thus a, b, c, d and e have the desired properties. It remains to show that they generate A_6.

Let $G := \langle a, b, c, d, e\rangle$.
Clearly G is a subgroup of S_6.

Now, $ab = (1,3,2)$.

Also, G is a primitive subgroup of S_6. It is clearly transitive on $\{1,2,3,4,5,6\}$. We now take $G_1 := \{g \in G : 1^g = 1\}$, the subgroup of G that fixes the point 1. Now b and c fix 1 and so are in G_1, and $\langle b, c\rangle \leqslant G_1$

is transitive on $\{2,3,4,5,6\}$. Hence, by Lemma 2.1.3, G is 2-transitive, and hence primitive on $\{1,2,3,4,5,6\}$, by Lemma 2.1.2.

Hence by Theorem 2.1.1, $G \geqslant A_6$. In fact, as a, b, c d and e are all even permutations, $G \cong A_6$, and so we are done. □

We now prove the negative results, namely:

Lemma 2.2.6. *The (simple) alternating groups A_7, A_8 and A_{12} do not have Property 1.*

Proof. The information below can be obtained from the Atlas of finite group representations [CCN+85].

- A_7: Consider the ordinary irreducible deleted 7-point permutation module, V, of dimension 6 and use Theorem 1.2.4. In the terminology of Theorem 1.2.4, $n = 6$, $m = 5$ and $d_i = 2$ for $i = 1,2,3,4,5$, as the x_i are all conjugate. Then we have

  $$d_1 + d_2 + d_3 + d_4 + d_5 = 10 < 12 = 2n.$$

  So, by Theorem 1.2.4, A_7 does not have Property 1.

- A_8: For the $2A$ conjugacy class, of cycle type (2^4) in the natural representation (i.e. with class representative $(1,2)(3,4)(5,6)(7,8)$), we consider the ordinary irreducible deleted 15-point permutation module, V, of dimension 14 and use Theorem 1.2.4. In the terminology of Theorem 1.2.4, $n = 14$, $m = 5$ and $d_i = 4$ for $i = 1,2,3,4,5$, as the x_i are all conjugate. Then we have

  $$d_1 + d_2 + d_3 + d_4 + d_5 = 20 < 28 = 2n.$$

  So, by Theorem 1.2.4, A_8 is not generated by elements with the desired properties from class $2A$. For the $2B$ conjugacy class, of cycle type $(1^4 2^2)$ in the natural representation (i.e. with class representative $(1,2)(3,4)$),

we consider the ordinary irreducible deleted 8-point permutation module, V, of dimension 7 and use Theorem 1.2.4. In the terminology of Theorem 1.2.4, $n = 7$, $m = 5$ and $d_i = 2$ for $i = 1, 2, 3, 4, 5$, as the x_i are all conjugate. Then we have

$$d_1 + d_2 + d_3 + d_4 + d_5 = 10 < 14 = 2n.$$

So, by Theorem 1.2.4, A_8 is not generated by elements with the desired properties from class $2B$. Hence A_8 does not have Property 1.

- A_{12}: For the $2A$ conjugacy class, of cycle type $(1^8 2^2)$ in the natural representation (i.e. with class representative $(1,2)(3,4)$), we consider the ordinary irreducible deleted 12-point permutation module, V, of dimension 11 and use Theorem 1.2.4. In the terminology of Theorem 1.2.4, $n = 11$, $m = 5$ and $d_i = 2$ for $i = 1, 2, 3, 4, 5$, as the x_i are all conjugate. Then we have

$$d_1 + d_2 + d_3 + d_4 + d_5 = 10 < 22 = 2n.$$

So, by Theorem 1.2.4, A_{12} is not generated by elements with the desired properties from class $2A$. For the $2B$ conjugacy class, of cycle type (2^6) in the natural representation (i.e. with class representative $(1,2)(3,4)(5,6)(7,8)(9,10)(11,12)$), we consider one of the irreducible modules, V, of dimension 16 over the field $\mathbb{F}_4$ and use Theorem 1.2.4. In the terminology of Theorem 1.2.4, $n = 16$, $m = 5$ and $d_i = 6$ (as in this representation, each transposition contributes 1 to the dimension of $V/C_V(x_i)$) for $i = 1, 2, 3, 4, 5$, as the x_i are all conjugate. Then we have

$$d_1 + d_2 + d_3 + d_4 + d_5 = 30 < 32 = 2n.$$

So, by Theorem 1.2.4, A_{12} is not generated by elements with the desired properties from class $2B$. For the $2C$ conjugacy class, we consider the ordinary irreducible module, V, of dimension 11 and use Theorem 1.2.4.

In the terminology of Theorem 1.2.4, $n = 11$, $m = 5$ and $d_i = 4$ for $i = 1, 2, 3, 4, 5$, as the x_i are all conjugate. Then we have

$$d_1 + d_2 + d_3 + d_4 + d_5 = 20 < 22 = 2n.$$

So, by Theorem 1.2.4, A_{12} is not generated by elements with the desired properties from class $2C$. Hence A_{12} does not have Property 1. □

Thus we have that the simple alternating groups A_n do not have Property 1 for $n = 7, 8, 12$. Hence Theorem 2.0.1 has been proved. Now by Lemma 1.2.1, we have that A_n does not have Property 2 for $n = 7, 8, 12$. Also we have:

Lemma 2.2.7. *The alternating groups A_6 does not have Property 2.*

Proof. The group A_6 is small enough so that it is possible to perform an exhaustive search in GAP [Gro08] of all triples of involutions satisfying the given restrictions, to see that they do not generate A_6. However we will give an outline of how to prove this result by hand.

Since A_6 has only one conjugacy class of involutions, we only need to show that it is not generated by three involutions such that two of them commute, i.e. that A_6 is not generated by involutions a, b and c such that $ab = ba$.

Without loss of generality, we can take $a = (1, 2)(3, 4) \in A_6$. We must have $b \in a^{A_6} \cap C_{A_6}(a) = \ldots$

$$\ldots = \{(1, 2)(3, 4), (1, 2)(5, 6), (1, 3)(2, 4), (1, 4)(2, 3), (3, 4)(5, 6)\}.$$

Now without loss of generality, we can assume that
$b \in \{(1, 2)(5, 6), (1, 4)(2, 3)\}$ as
$\langle (1, 2)(3, 4), (3, 4)(5, 6)\rangle = \langle (1, 2)(3, 4), (1, 2)(5, 6)\rangle$,
$\langle (1, 2)(3, 4), (1, 3)(2, 4)\rangle = \langle (1, 2)(3, 4), (1, 4)(2, 3)\rangle$ and

$b \neq (1,2)(3,4)$, as then $\langle a,b,c\rangle = \langle a,c\rangle$, a dihedral group, which cannot be equal to A_6.

If $b = (1,4)(2,3)$, then for $\langle a,b,c\rangle$ to be transitive on $\{1,2,3,4,5,6\}$, c must have the form $(x,5)(y,6)$, where $x,y \in \{1,2,3,4\}$, $x \neq y$. There are thus 12 choices for c. However, for each of these choices the group $\langle a,b,c\rangle$ fixes the imprimitivity system $\{\{x,y\},\{u,v\},\{5,6\}\}$, where $\{x,y,u,v\} = \{1,2,3,4\}$. Thus, in this case, $\langle a,b,c\rangle$ cannot be isomorphic to A_6.

If $b = (1,2)(5,6)$, then the group $\langle a,b\rangle$ has 3 orbits on $\{1,2,3,4,5,6\}$, namely $\{1,2\}$, $\{3,4\}$ and $\{5,6\}$. Thus, for $\langle a,b,c\rangle$ to be transitive on $\{1,2,3,4,5,6\}$, c must not fix any of these orbits. There are 24 choices for c which all have the form $(u,v)(x,y)$ with u in one of the above orbits, y in another and v and x in the last one. Now, for any of these choices for c, by simply relabeling the points we can see that the group $\langle a,b,c\rangle$ is isomorphic to the group $\langle (u,s)(v,x),(u,s)(y,t),(2,3)(4,5)\rangle$, where s is in the same orbit from above as u and t is in the same orbit from above as y. Now this group is isomorphic to the group $\langle (1,2)(3,4),(1,2)(5,6),(2,3)(4,5)\rangle$, since by construction the pair $(u,s)(v,x)$ and $(u,s)(y,t)$ are a pair from $\{a,b,ab\}$. Hence, for any choice of c, we have $\langle a,b,c\rangle \cong \langle (1,2)(3,4),(1,2)(5,6),(2,3)(4,5)\rangle$. Now this group is isomorphic to A_5 and so $\langle a,b,c\rangle$ does not generate A_6.

Hence, there does not exist a triple of involutions with the requires properties that generates A_6. □

Hence Theorem 2.0.2 has been proved.

For the Alternating groups, we have now seen when the lower bound of 5 generating conjugate involutions whose product is 1 is obtained. For those groups that do not attain the bound, we can ask how many conjugate involutions whose product is 1 are needed to generate the group.

2.3 Additional Results

Since the original question in the Kourovka notebook [MK02] asks for the minimum number of involutions, with certain conditions, needed to generate the simple groups, we include the following result:

Lemma 2.3.1. *The alternating groups A_7 and A_{12} can be generated by 6 conjugate involutions whose product is 1, while the alternating group A_8 needs 7.*

Proof. We deal with each group separately.

- A_7: It is enough to show that A_7 can be generated by 3 conjugate involutions, a, b and c. Let

  $a := (2,3)(4,5)$

  $b := (3,4)(5,6)$

  $c := (1,6)(2,7)$

  and let $G := \langle a, b, c \rangle$.

  Clearly G is a subgroup of S_7.

  Now, $(bc)^2 = (1,5,6)$.

  Also, G is a primitive subgroup of S_7. It is clearly transitive on $\{1,2,3,4,5,6,7\}$. We now take $G_1 := \{g \in G : 1^g = 1\}$, the subgroup of G that fixes the point 1. Now a, b and $cac = (3,7)(4,5)$ fix 1 and so are in G_1, and $\langle a, b, cac \rangle \leqslant G_1$ is transitive on $\{2,3,4,5,6,7\}$. Hence, by Lemma 2.1.3, G is 2-transitive, and hence primitive on $\{1,2,3,4,5,6,7\}$, by Lemma 2.1.2.

  Hence by Theorem 2.1.1, $G \geqslant A_7$. In fact, as a, b and c are all even permutations, $G \cong A_7$. Now a, b and c all have the same cycle type and so are conjugate in $G \cong A_7$ and so we are done.

- A_8: For the $2A$ conjugacy class, of cycle type (2^4) in the natural representation (i.e. with class representative $(1,2)(3,4)(5,6)(7,8)$), we consider the ordinary irreducible deleted 15-point permutation module, V, of dimension 14 and use Theorem 1.2.4. In the terminology of Theorem 1.2.4, $n = 14$, $m = 5$ and $d_i = 4$ for $i = 1, 2, 3, 4, 5, 6$, as the x_i are all conjugate. Then we have

$$d_1 + d_2 + d_3 + d_4 + d_5 + d_6 = 24 < 28 = 2n.$$

So, by Theorem 1.2.4, A_8 is not generated by elements with the desired properties from class $2A$. For the $2B$ conjugacy class, of cycle type $(1^4 2^2)$ in the natural representation (i.e. with class representative $(1,2)(3,4)$), we consider the ordinary irreducible deleted 8-point permutation module, V, of dimension 7 and use Theorem 1.2.4. In the terminology of Theorem 1.2.4, $n = 7$, $m = 5$ and $d_i = 2$ for $i = 1, 2, 3, 4, 5, 6$, as the x_i are all conjugate. Then we have

$$d_1 + d_2 + d_3 + d_4 + d_5 + d_6 = 12 < 14 = 2n.$$

So, by Theorem 1.2.4, A_8 is not generated by elements with the desired properties from class $2B$. So we need at least 7 conjugate involutions whose product is 1 to generate A_8. In fact, let

$a := (1,2)(3,4)$,

$b := (2,3)(4,5)$,

$c := (3,4)(5,6)$,

$d := (2,8)(6,7)$

and let $G := \langle a, b, c, d \rangle$.

Clearly G is a subgroup of S_8.

Now, $(ad)^2 = (1,2,8)$.

Also, G is a primitive subgroup of S_8. It is clearly transitive on $\{1,2,3,4,5,6,7,8\}$. We now take $G_8 := \{g \in G : 8^g = 8\}$, the subgroup of G that fixes the point 8. Now a, b, c and $dcd = (3,4)(5,7)$ fix 8 and so are in G_1, and $\langle a, b, c, dcd\rangle \leqslant G_1$ is transitive on $\{1,2,3,4,5,6,7\}$. Hence, by Lemma 2.1.3, G is 2-transitive, and hence primitive on $\{1,2,3,4,5,6,7,8\}$, by Lemma 2.1.2.

Hence by Theorem 2.1.1, $G \geqslant A_8$. In fact, as a, b, c and d are all even permutations, $G \cong A_8$.

Now

$$\begin{aligned} abcd &= (1,4,8,2)(3,7,6,5) \\ &= (1,2)(4,8) \cdot (3,5)(6,7) \cdot (2,4)(5,7) \end{aligned}$$

a product of three involutions. We call these involutions g, f and e respectively. These involutions are also even permutations, and so $\langle a, b, c, d, e, f, g\rangle \cong A_8$. Now a, b, c, d, e, f and g all have the same cycle type and so are conjugate in $G \cong A_8$, and by definition of e, f and g, we have $abcdefg = 1$ and so we are done.

- A_{12}: It is enough to show that A_{12} can be generated by 3 conjugate involutions, a, b and c. Let

  $a := (1,2)(7,8)(9,10)(11,12)$

  $b := (2,3)(4,5)(6,7)(8,9)$

  $c := (3,4)(5,6)(7,8)(10,11)$

  and let $G := \langle a, b, c\rangle$.

  Clearly G is a subgroup of S_{12}.

  Now, $(ab)^{10} = (1,3,2)$.

  Also, G is a primitive subgroup of S_{12}. It is clearly transitive on $\{1,2,3,4,5,6,7,8,9,10,11,12\}$. We now take $G_1 := \{g \in G : 1^g = 1\}$,

the subgroup of G that fixes the point 1. Now the elements a, b, $aca = (3,4)(5,6)(7,8)(9,12)$ and $bcb = (2,5)(4,7)(6,9)(10,11)$ fix 1 and so are in G_1, and $\langle a, b, aca, bcb\rangle \leqslant G_1$ is transitive on $\{2,3,4,5,6,7,8,9,10,11,12\}$. Hence, by Lemma 2.1.3, G is 2-transitive, and hence primitive on $\{1,2,3,4,5,6,7,8,9,10,11,12\}$, by Lemma 2.1.2.

Hence by Theorem 2.1.1, $G \geqslant A_{12}$. In fact, as a, b and c are all even permutations, $G \cong A_{12}$. Now a, b and c all have the same cycle type and so are conjugate in $G \cong A_{12}$ and so we are done.

□

Chapter 3

The Sporadic Groups

The aim of this chapter is to determine, for each of the Sporadic groups G, whether G has Property 1 or not. It may be noted at this point that it is known that each of the Sporadic Groups can be generated by 3 conjugate involutions ([MSW94]), and so even if the group does not have Property 1, it can be generated by 6 conjugate involutions whose product is 1.

The aim of this chapter is to prove the following Theorem:

Theorem 3.0.2. *Let G be one of the 26 sporadic simple groups. The group G does not have Property 1, if and only if G is isomorphic to M_{11}, M_{12}, M_{22}, M_{23} or McL.*

In fact we also prove:

Theorem 3.0.3. *Let G be one of the 26 sporadic simple groups. The group G does not have Property 2, if and only if G is isomorphic to M_{11}, M_{12}, M_{22}, M_{23} or McL.*

Since having Property 2 implies having Property 1, proving the positive results from Theorem 3.0.3 will give us that the Sporadic groups other than M_{11}, M_{12}, M_{22}, M_{23} and McL have Property 1. Then, using the "non-generation" results given in the introduction, we will see that M_{11}, M_{12}, M_{22}, M_{23} and McL do not have Property 1. This will complete the proof for Theorem 3.0.2,

and will also complete the proof of Theorem 3.0.3 as not having Property 1 implies not having Property 2.

3.1 Notation and Preliminaries

Now for some notation. We use the standard notation from the ATLAS [CCN+85].

The set of all irreducible ordinary characters of a group G is denoted by $Irr(G)$. If A, B and C are classes of conjugate elements of G and if $g \in C$ then $m_G(A, B, C)$ denotes the number of pairs (x, y) such that $x \in A$, $y \in B$, and $xy = g$. Given an involution, t of G, we denote by $i_G(t)$ the number of involutions different from t in $C_G(t)$.

The following results will also be used:

Lemma 3.1.1. *Let A, B and C be conjugacy classes of a group G and let $a \in A$, $b \in B$ and $c \in C$. Then*

$$m_G(A, B, C) = \frac{|A|\,|B|}{|G|} \sum_{\chi \in Irr(G)} \frac{\chi(a)\,\chi(b)\,\overline{\chi(c)}}{\chi(1)}$$

This Lemma is a standard result from Representation Theory, and a proof can be found in [CR81]. Now for a group G, with conjugacy classes A, B and C, the value $m_G(A, B, C)$ can be calculated in GAP [Gro08] using the command

`ClassMultiplicationCoefficient(X,i,j,k)`,

where `i`, `j` and `k` are the column numbers of A, B and C in the character table `X` of G as it is stored in GAP.

Lemma 3.1.2. *Let $C_1, \ldots, C_s$ be all conjugacy classes of involutions of a group G and let $t \in C_1$. Then*

$$i_G(t) = \sum_{i,j=1}^{s} m_G(C_i, C_j, C_1)$$

Proof. If a is an involution, not equal to t, and $a \in C_G(t)$, then at is an involution and $a \cdot at = t$. Hence

$$i_G(t) \leqslant \sum_{i,j=1}^{s} m_G(C_i, C_j, C_1)$$

On the other hand, if x and y are involutions and $xy = t$, then x must be an involution in $C_G(t)$ that is not equal to t, and so

$$i_G(t) \geqslant \sum_{i,j=1}^{s} m_G(C_i, C_j, C_1)$$

Hence the result is proved. □

The following Lemma will be very important in proving the Theorems. The method that uses this was originated by V. D. Mazurov in [Maz03].

Lemma 3.1.3. *Let a and b be conjugate involutions of a finite group G which generate a subgroup $D \neq G$, and let $M_1, \ldots, M_s$ be all maximal subgroups of G containing D. If*

$$\sum_{j=1}^{s} i_{M_j}(a) < m_G(A, A, A),$$

where A is the conjugacy class with $a, b \in A$, then G has Property 2.

Proof. Since

$$\sum_{j=1}^{s} i_{M_j}(a) < m_G(A, A, A),$$

we can choose t such that $t \in A$, $at \in A$ and $t \notin \bigcup_{j=1}^{s} C_{M_j}(a)$. Then a, b and t are conjugate involutions in G, a and t commute and at is conjugate to a, b and t. Suppose that $H := \langle a, b, t \rangle \neq G$, then H must lie in one of the maximal subgroups, M_j, of G, and so $t \in C_{M_j}(a)$, which contradicts our choice of t. □

In fact we can ocasionally improve on this result:

Lemma 3.1.4. *Using the notation from Lemma 3.1.3, if for a maximal subgroup M_i, some of its involutions are not from the conjugacy class A, then for*

the result of Lemma 3.1.3 to hold, it is enough to show that

$$\sum_{j=1,\, j\neq i}^{s} i_{M_j}(a) + \sum_{k,l=1}^{r} m_{M_i}(C_k, C_l, C_1) < m_G(A, A, A),$$

where the conjugacy classes $C_1, \ldots, C_r$ are those that are contained in the conjugacy class $A \subset G$.

Proof. This holds as we are only trying to show the existence of an involution t such that $t \in A$ and $at \in A$. To show such an involution exists, we only need to count those involutions in M_i that have this property, and these are precisely those counted by $\sum_{k,l=1}^{r} m_{M_i}(C_k, C_l, C_1)$. □

In the method described below, we will need to determine which maximal subgroups contain a given dihedral subgroup. As such the following result will be used:

Lemma 3.1.5. *Let G be a group containing a Sylow p-subgroup, S_p. Let H be a maximal subgroup of G also containing S_p.*

1. *If the normalizer in G of S_p, $N_G(S_p)$, is contained in H, then S_p is contained in only one conjugate of H.*

2. *More generally, if $|N_G(S_p) : N_H(S_p)| = m$, then S_p is contained in at most m conjugates of H.*

Proof.

1. Suppose S_p is contained in more than one conjugate of H, i.e. $S_p \leqslant H$ and $S_p \leqslant H^g$, for some $g \in G$. Then, S_p and $S_p^{g^{-1}}$ are two Sylow p-subgroups of G contained in H, and so must be conjugate in H, i.e. $S_p^{g^{-1}h} = S_p$ for some $h \in H$. Thus, $g^{-1}h \in N_G(S_p) \leqslant H$, and so $g \in H$. Hence $H^g = H$, and so S_p must be contained in only one conjugate of H.

2. Let $|N_G(S_p) : N_H(S_p)| = m$, and take k_i for $i = 1, \ldots, m$ as left-coset representatives of $N_H(S_p)$ in $N_G(S_p)$. Then as above, if S_p is contained

in some conjugate, H^g, of H we have, for some $h \in H$, $g^{-1}h \in N_G(S_p)$. Then, we can write $g^{-1}h = k_i n$, with $n \in N_H(S_p)$ and $i \in \{1, \ldots, m\}$. Hence $H^g = H^{hn^{-1}k_i^{-1}} = H^{n^{-1}k_i^{-1}} = H^{k_i^{-1}}$. So S_p can only be contained in the m conjugates, $H^{k_i^{-1}}$, of H.

□

3.2 Proof of the Theorems

Now we are in a position to prove the Theorems. First, we prove:

Lemma 3.2.1. *If $G \in \{M_{11}, M_{12}, M_{22}, M_{23}, McL\}$, G does not have Property 1 (and hence does not have Property 2).*

Proof. Here we deal with each group separately:

- M_{11}: Consider the permutation representation on 12 points. We use Theorem 1.2.5. In the terminology of Theorem 1.2.5, $n = 12$, $m = 5$ and $c_i = 8$ for $i = 1, 2, 3, 4, 5$, as the x_i are all conjugate. Then we have

$$c_1 + c_2 + c_3 + c_4 + c_5 = 40 > 38 = (m-2)\,n + 2.$$

  So, by Theorem 1.2.5, M_{11} does not have Property 1.

- M_{12}: For conjugacy class $2A$, we consider the ordinary irreducible module, V, of dimension 16 and use Theorem 1.2.4. In the terminology of Theorem 1.2.4, $n = 16$, $m = 5$ and $d_i = 6$ for $i = 1, 2, 3, 4, 5$, as the x_i are all conjugate. Then we have

$$d_1 + d_2 + d_3 + d_4 + d_5 = 30 < 32 = 2n.$$

  So, by Theorem 1.2.4, M_{12} is not generated by elements with the desired properties from class $2A$. For conjugacy class $2B$, we consider the permutation representation on 12 points, and use Theorem 1.2.5.

In the terminology of Theorem 1.2.5, $n = 12$, $m = 5$ and $c_i = 8$ for $i = 1, 2, 3, 4, 5$, as the x_i are all conjugate. Then we have

$$c_1 + c_2 + c_3 + c_4 + c_5 = 40 > 38 = (m-2)\,n + 2.$$

So, by Theorem 1.2.5, M_{12} is not generated by elements with the desired properties from class $2B$. Hence M_{12} does not have Property 1.

- M_{22}: Consider the standard representation on 22 points. We use Theorem 1.2.5. In the terminology of Theorem 1.2.5, $n = 22$, $m = 5$ and $c_i = 14$ for $i = 1, 2, 3, 4, 5$, as the x_i are all conjugate. Then we have

  $$c_1 + c_2 + c_3 + c_4 + c_5 = 70 > 68 = (m-2)\,n + 2.$$

  So, by Theorem 1.2.5, M_{22} does not have Property 1.

- M_{23}: Consider the standard representation on 23 points. We use Theorem 1.2.5. In the terminology of Theorem 1.2.5, $n = 23$, $m = 5$ and $c_i = 15$ for $i = 1, 2, 3, 4, 5$, as the x_i are all conjugate. Then we have

  $$c_1 + c_2 + c_3 + c_4 + c_5 = 75 > 71 = (m-2)\,n + 2.$$

  So, by Theorem 1.2.5, M_{23} does not have Property 1.

- McL: Consider the ordinary irreducible module, V, of dimension 22 and use Theorem 1.2.4. In the terminology of Theorem 1.2.4, $n = 22$, $m = 5$ and $d_i = 8$ for $i = 1, 2, 3, 4, 5$, as the x_i are all conjugate. Then we have

  $$d_1 + d_2 + d_3 + d_4 + d_5 = 40 < 44 = 2n.$$

  So, by Theorem 1.2.4, McL does not have Property 1.

□

Lemma 3.2.2. *In each sporadic simple group G other than M_{11}, M_{12}, M_{22}, M_{23} or McL, there are involutions a and b such that the conditions of Lemma 3.1.3 are satisfied.*

Proof. We use the method implied by Lemma 3.1.3. The process for each individual group, G, proceeds as follows:

1. Pick a conjugacy class in G of involutions, X, and another conjugacy class, Y, such that $m_G(X, X, Y) \neq 0$, and such that Y has a "large" order. Hence we will have a dihedral subgroup, D, of G generated by two involutions, a and b from X, with their product having a "large" order. The idea is to get a dihedral subgroup that is contained in a small number of maximal subgroups of G.

2. Find all the maximal subgroups of G that (may) contain D.

3. Count the values $m_G(X, X, X)$, and $i_{M_i}(a)$ for each maximal subgroup, M_i containing D.

4. Compare $m_G(X, X, X)$ and $\sum_{j=1}^{s} i_{M_j}(a)$.
   If $\sum_{j=1}^{s} i_{M_j}(a) < m_G(X, X, X)$, then the conditions of Lemma 3.1.3 are satisfied, and so the group, G has Property 2 (and hence has Property 1).

The process is summarised in Table 3.1, which can be found on pages 65–67. In it, the column labeled (X, X, Y) indicates the conjugacy classes of G which have been picked such that X is a class of involutions and $m_G(X, X, Y) \neq 0$. We take a and b as the fixed involutions in X, such that ab is in Y. The column labeled s indicates the number of maximal subgroups that contain $D := \langle a, b \rangle$ and we label these subgroups $M_1, \ldots M_s$. The data for this table can be easily extracted by means of the formulas given above from the character tables and the lists of maximal subgroups of sporadic groups. GAP [Gro08] was used for all the calculations, using information from the Web-ATLAS [WNB+05].

We deal with each group separately:

- Let $G \cong J_1$.

1. G has one conjugacy class of involutions, namely class $2A$. Since $m_G(2A, 2A, 11A) \neq 0$ then $\exists\, a, b \in 2A$ s.t. $ab = c \in 11A$.
   Note that $\langle c \rangle$ is a Sylow 11-subgroup of G, and that $C_G(c) = \langle c \rangle$.
2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 11 must be isomorphic to $L_2(11)$ or $11 : 10$. From the character table of $L_2(11)$, we can see that the conjugacy classes of elements of order 11 in this group are not real, and so $L_2(11)$ can not contain a dihedral group of order 22. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ is conjugate with $H \cong 11 : 10$. Since this subgroup is isomorphic to the normalizer in G of a Sylow 11-subgroup, by Lemma 3.1.5, there can only be one maximal subgroup of G conjugate to H containing the Sylow 11-subgroup $\langle c \rangle$. Hence there can only be one maximal subgroup of G conjugate to H containing D.
3. $m_G(2A, 2A, 2A) = 30$.
   H has one class of involutions, namely $2A$, and so $i_H(x) = \ldots$ $\ldots = m_H(2A, 2A, 2A) = 0$ for $x \in 2A$.
4. Now $0 < 30$, hence, in this case, the Lemma holds true.

- Let $G \cong J_2$.

1. G has two conjugacy classes of involutions, namely classes $2A$ and $2B$. Since $m_G(2B, 2B, 7A) \neq 0$ then $\exists\, a, b \in 2B$ s.t. $ab = c \in 7A$.
   Note that $\langle c \rangle$ is a Sylow 7-subgroup of G, and that $C_G(c) = \langle c \rangle$.
2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 7 must be isomorphic to $U_3(3)$ or $L_3(2) : 2$. From the character table of $U_3(3)$, we can see that the conjugacy classes of elements of order 7 in this group are

not real, and so $U_3(3)$ can not contain a dihedral group of order 14. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ is conjugate with $H \cong L_3(2) : 2$. Since this subgroup contains the normalizer in G of a Sylow 7-subgroup, by Lemma 3.1.5, there can only be one maximal subgroup of G conjugate to H containing the Sylow 7-subgroup $\langle c \rangle$. Hence there can only be one maximal subgroup of G conjugate to H containing D.

3. $m_G(2B, 2B, 2B) = 32$.

   H has two classes of involutions, namely $2A$ and $2B$, and if X and Y are involution classes, $m_H(X, Y, 7A) \neq 0$ only if $X = Y = 2B$, and $i_H(x) = 6$ for $x \in 2B$.

4. Now $6 < 32$, hence, in this case, the Lemma holds true.

- Let $G \cong {}^2F_4(2)'$.

  1. G has two conjugacy classes of involutions, namely classes $2A$ and $2B$. Since $m_G(2B, 2B, 13A) \neq 0$ then $\exists\ a, b \in 2B$ s.t. $ab = c \in 13A$.

     Note that $\langle c \rangle$ is a Sylow 13-subgroup of G, and that $C_G(c) = \langle c \rangle$.

  2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 13 must be isomorphic to $L_3(3) : 2$ or $L_2(25)$. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ must be conjugate with $H_1 \cong L_3(3) : 2$, $H_2 \cong L_3(3) : 2$ or $H_3 \cong L_2(25)$. Since H_1 contains the normalizer in G of a Sylow 13-subgroup, H_2 contains the normalizer in G of a Sylow 13-subgroup, and the order of the normalizer in H_3 of a Sylow 13-subgroup is $13 \cdot 2$, by Lemma 3.1.5, there can only be one maximal subgroups conjugate with H_1, one maximal subgroup conjugate to H_2 and three maximal subgroups conjugate to H_3 which contain the Sylow 13-subgroup $\langle c \rangle$. Hence there can

be only one maximal subgroup conjugate to H_1, one maximal subgroup conjugate to H_2 and three maximal subgroups conjugate to H_3, containing D.

3. $m_G(2B, 2B, 2B) = 132$.

   H_1 has two classes of involutions, namely $2A$ and $2B$, and if X and Y are involution classes and Z is a class of order 13, $m_{H_1}(X, Y, Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_1}(x) = 18$ for $x \in 2B$.

   H_2 has two classes of involutions, namely $2A$ and $2B$, and if X and Y are involution classes and Z is a class of order 13, $m_{H_2}(X, Y, Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_2}(x) = 18$ for $x \in 2B$.

   H_3 has one class of involutions, namely $2A$, and so $i_{H_3}(x) = m_{H_3}(2A, 2A, 2A) = 12$ for $x \in 2A$.

4. Now $18 + 18 + 3 \times 12 = 72 < 132$, hence, in this case, the Lemma holds true.

- Let $G \cong HS$.

  1. G has two conjugacy classes of involutions, namely $2A$ and $2B$. Since $m_G(2B, 2B, 7A) \neq 0$ then $\exists\, a, b \in 2B$ s.t. $ab = c \in 7A$. Note that $\langle c \rangle$ is a Sylow 7-subgroup of G, and that $C_G(c) = \langle c \rangle$.

  2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 7 must be isomorphic to M_{22}, $U_3(5).2$, $L_3(4).2_1$, $A_8.2$ or $4^3L_3(2)$. Using Structure constants, it can be seen that the groups M_{22} and $4^3L_3(2)$ do not contain a dihedral group of order 14. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ must be conjugate with either $H_1 \cong U_3(5).2$, $H_2 \cong U_3(5).2$ $H_3 \cong L_3(4).2_1$ or $H_4 \cong A_8.2$. Since H_1 contains the normalizer in G of a Sylow 7-subgroup, H_2 contains the normalizer in G of a Sylow 7-subgroup, H_3 contains the normalizer in G of a Sylow 7-subgroup and H_4 contains the

normalizer in G of a Sylow 7-subgroup, by Lemma 3.1.5, there can only be one maximal subgroups conjugate with H_1, one maximal subgroup conjugate to H_2, one maximal subgroup conjugate to H_3 and one maximal subgroup conjugate to H_4 which contain the Sylow 7-subgroup $\langle c \rangle$. Hence there can only be one maximal subgroups conjugate with H_1, one maximal subgroup conjugate to H_2, one maximal subgroup conjugate to H_3 and one maximal subgroup conjugate to H_4 containing D.

3. $m_G(2B, 2B, 2B) = 72$.

   H_1 has two classes of involutions, namely $2A$ and $2B$, and if X and Y are involution classes and Z is a class of order 7, $m_{H_1}(X, Y, Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_1}(x) = 50$ for $x \in 2B$.

   H_2 has two classes of involutions, namely $2A$ and $2B$, and if X and Y are involution classes and Z is a class of order 7, $m_{H_2}(X, Y, Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_1}(x) = 50$ for $x \in 2B$.

   H_3 has two classes of involutions, namely $2A$ and $2B$, and if X and Y are involution classes and Z is a class of order 7, $m_{H_3}(X, Y, Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_1}(x) = 8$ for $x \in 2B$.

   H_4 has four classes of involutions, namely $2A$, $2B$, $2C$ and $2D$, and if X and Y are involution classes and Z is a class of order 7, $m_{H_4}(X, Y, Z) \neq 0$ only if $X = Y = 2D$, and $i_{H_1}(x) = 42$ for $x \in 2B$.

4. Now $50 + 50 + 8 + 42 = 150 > 72$. However, for H_1 and H_2 we can apply Lemma 3.1.4, and only need to count $m_{H_i}(2B, 2B, 2B)$ in each case, giving $0 + 0 + 8 + 42 < 72$, hence, in this case, the Lemma holds true.

- Let $G \cong J_3$.

1. G has one conjugacy class of involutions, namely class $2A$. Since $m_G(2A, 2A, 17A) \neq 0$ then $\exists\ a, b \in 2A$ s.t. $ab = c \in 17A$.
   Note that $\langle c \rangle$ is a Sylow 17-subgroup of G, and that $C_G(c) = \langle c \rangle$.

2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 17 must be isomorphic to $L_2(16).2$ or $L_2(17)$. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ must be conjugate with $H_1 \cong L_2(16).2$ or $H_2 \cong L_2(17)$. Since the order of the normalizer in H_1 of a Sylow 17-subgroup is $17 \cdot 4$ and H_2 contains the normalizer in G of a Sylow 17-subgroup, by Lemma 3.1.5, there can only be two maximal subgroups conjugate with H_1 and one maximal subgroup conjugate to H_2 which contain the Sylow 17-subgroup $\langle c \rangle$. Hence there can only be two maximal subgroups conjugate with H_1 and one maximal subgroup conjugate to H_2 containing D.

3. $m_G(2A, 2A, 2A) = 130$.
   H_1 has two classes of involutions, namely $2A$ and $2B$, and if X and Y are involution classes and Z is a class of order 17, $m_{H_1}(X, Y, Z) \neq 0$ only if $X = Y = 2A$, and $i_{H_1}(x) = 18$ for $x \in 2A$.
   H_2 has one class of involutions, namely $2A$, and so $i_{H_2}(x) = m_{H_2}(2A, 2A, 2A) = 8$ for $x \in 2A$.

4. Now $2 \times 18 + 8 = 44 < 130$, hence, in this case, the Lemma holds true.

- Let $G \cong M_{24}$.

  1. G has two conjugacy class of involutions, namely classes $2A$ and $2B$. Since $m_G(2B, 2B, 11A) \neq 0$ then $\exists\ a, b \in 2B$ s.t. $ab = c \in 11A$.
     Note that $\langle c \rangle$ is a Sylow 11-subgroup of G, and that $C_G(c) = \langle c \rangle$.

2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 11 must be isomorphic to M_{23}, $M_{22}.2$, $M_{12}.2$ or $L_2(23)$. From the character table of M_{23}, we can see that the conjugacy classes of elements of order 11 in this group are not real, and so M_{23} can not contain a dihedral group of order 22. Therefore, each maximal subgroup containing $D := \langle a, b\rangle$ must be conjugate with $H_1 \cong M_{22}.2$, $H_2 \cong M_{12}.2$ or $H_3 \cong L_2(23)$. Since H_1 contains the normalizer in G of a Sylow 11-subgroup, H_2 contains the normalizer in G of a Sylow 11-subgroup and the order of the normalizer in H_3 of a Sylow 11-subgroup is $11 \cdot 2$, by Lemma 3.1.5, there can be only one maximal subgroup conjugate to H_1, one maximal subgroup conjugate to H_2 and five maximal subgroups conjugate to H_3, which contain the Sylow 11-subgroup $\langle c\rangle$. Hence there can be only one maximal subgroup conjugate to H_1, one maximal subgroup conjugate to H_2 and five maximal subgroups conjugate to H_3, containing D.

3. $m_G(2B, 2B, 2B) = 202$.

   H_1 has three classes of involutions, namely $2A$, $2B$ and $2C$, and if X and Y are involution classes and Z is a class of order 11, $m_{H_1}(X, Y, Z) \neq 0$ only if $X = Y = 2C$, and $i_{H_1}(x) = 70$ for $x \in 2C$.

   H_2 has three classes of involutions, namely $2A$, $2B$ and $2C$, and if X and Y are involution classes and Z is a class of order 11, $m_{H_2}(X, Y, Z) \neq 0$ only if $X = Y = 2C$, and $i_{H_2}(x) = 62$ for $x \in 2C$.

   H_3 has one class of involutions, namely $2A$, and so $i_{H_3}(x) = m_{H_3}(2A, 2A, 2A) = 12$ for $x \in 2A$.

4. Now $70 + 62 + 5 \times 12 = 192 < 202$, hence, in this case, the Lemma

holds true.

- Let $G \cong He$.

  1. G has two conjugacy classes of involutions, namely classes $2A$ and $2B$. Since $m_G(2B, 2B, 17A) \neq 0$ then $\exists\ a, b \in 2A$ s.t. $ab = c \in 17A$.

     Note that $\langle c \rangle$ is a Sylow 17-subgroup of G, and that $C_G(c) = \langle c \rangle$.

  2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 17 must be isomorphic to $S_2(4).2$. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ is conjugate with $H \cong S_2(4).2$. Since H contains the normalizer in G of a Sylow 17-subgroup, by Lemma 3.1.5, there can only be one maximal subgroup of G, conjugate to H which contains the Sylow 17-subgroup $\langle c \rangle$. Hence there can only be one maximal subgroup of G conjugate to H containing D.

  3. $m_G(2B, 2B, 2B) = 364$.

     H has four classes of involutions, namely $2A$, $2B$, $2C$ and $2D$, and if X and Y are involution classes and Z is a class of order 17, $m_H(X, Y, Z) \neq 0$ only if $X = Y = 2C$, and $i_H(x) = 126$ for $x \in 2C$.

  4. Now $126 < 364$, hence, in this case, the Lemma holds true.

- Let $G \cong Ru$.

  1. G has two conjugacy classes of involutions, namely classes $2A$ and $2B$. Since $m_G(2B, 2B, 29A) \neq 0$ then $\exists\ a, b \in 2A$ s.t. $ab = c \in 29A$.

     Note that $\langle c \rangle$ is a Sylow 29-subgroup of G, and that $C_G(c) = \langle c \rangle$.

  2. From the list of maximal subgroups of G, it can be seen that

any maximal subgroup whose order is divisible by 29 must be isomorphic to $L_2(29)$. Therefore, each maximal subgroup containing $D := \langle a, b\rangle$ is conjugate with $H \cong L_2(29)$. Since H contains the normalizer in G of a Sylow 29-subgroup, by Lemma 3.1.5, there can only one maximal subgroup of G, conjugate to H containing the Sylow 29-subgroup $\langle c\rangle$. Hence there can only be one maximal subgroup of G conjugate to H containing D.

3. $m_G(2B, 2B, 2B) = 912$.
   H has one class of involutions, namely $2A$, and so $i_H(x) = m_H(2A, 2A, 2A) = 14$ for $x \in 2A$.
4. Now $14 < 912$, hence, in this case, the Lemma holds true.

- Let $G \cong Suz$.

1. G has two conjugacy classes of involutions, namely classes $2A$ and $2B$. Since $m_G(2B, 2B, 13A) \neq 0$ then $\exists\ a, b \in 2A$ s.t. $ab = c \in 13A$.
   Note that $\langle c\rangle$ is a Sylow 13-subgroup of G, and that $C_G(c) = \langle c\rangle$.
2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 13 must be isomorphic to $G_2(4)$, $L_3(3).2$ or $L_2(25)$. Therefore, each maximal subgroup containing $D := \langle a, b\rangle$ is conjugate with $H_1 \cong G_2(4)$, $H_2 \cong L_3(3).2$, $H_3 \cong L_3(3).2$ or $H_4 \cong L_2(25)$ (note that there are two conjugacy classes of maximal subgroups of G that are isomorphic to $L_3(3).2$). Since H_1 contains the normalizer in G of a Sylow 13-subgroup, H_2 contains the normalizer in G of a Sylow 13-subgroup, H_3 contains the normalizer in G of a Sylow 13-subgroup and the order of the normalizer in H_4 of a Sylow 13-subgroup is $13{\cdot}2$, by Lemma 3.1.5, there can only be one maximal subgroup conjugate to H_1, one maximal subgroup conjugate to H_2, one maximal

subgroup conjugate to H_3 and three maximal subgroups conjugate to H_4 which contain the Sylow 13-subgroup $\langle c \rangle$. Hence, there can only be one maximal subgroup conjugate to H_1, one maximal subgroup conjugate to H_2, one maximal subgroup conjugate to H_3 and three maximal subgroups conjugate to H_4 which contain D.

3. $m_G(2B, 2B, 2B) = 1192$.
   H_1 has two classes of involutions, namely $2A$ and $2B$, and if X and Y are involution classes and Z is a class of order 13, $m_{H_1}(X, Y, Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_1}(x) = 302$ for $x \in 2B$.
   H_2 has two classes of involutions, namely $2A$ and $2B$, and if X and Y are involution classes and Z is a class of order 13, $m_{H_2}(X, Y, Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_2}(x) = 18$ for $x \in 2B$.
   H_3 has two classes of involutions, namely $2A$ and $2B$, and if X and Y are involution classes and Z is a class of order 13, $m_{H_3}(X, Y, Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_3}(x) = 18$ for $x \in 2B$.
   H_4 has one class of involutions, namely $2A$, and so $i_{H_4}(x) = m_{H_4}(2A, 2A, 2A) = 12$ for $x \in 2A$.

4. Now $302 + 18 + 18 + 3 \times 12 = 374 < 1192$, hence, in this case, the Lemma holds true.

- Let $G \cong ON$.

  1. G has one conjugacy class of involutions, namely class $2A$. Since $m_G(2A, 2A, 19A) \neq 0$ then $\exists\, a, b \in 2A$ s.t. $ab = c \in 19A$.
     Note that $\langle c \rangle$ is a Sylow 19-subgroup of G, and that $C_G(c) = \langle c \rangle$.

  2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 19 must be isomorphic to $L_3(7).2$ or J_1. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ is conjugate with $H_1 \cong L_3(7).2$, $H_2 \cong L_3(7).2$

or $H_3 \cong J_1$ (note that there are two conjugacy classes of maximal subgroups of G that are isomorphic to $L_3(7).2$). Since H_1 contains the normalizer in G of a Sylow 19-subgroup, H_2 contains the normalizer in G of a Sylow 19-subgroup and H_3 contains the normalizer in G of a Sylow 19-subgroup, by Lemma 3.1.5, there can only be one maximal subgroup conjugate to H_1, one maximal subgroup conjugate to H_2 and one maximal subgroup conjugate to H_3 which contain the Sylow 19-subgroup $\langle c \rangle$. Hence there can only be one maximal subgroup conjugate to H_1, one maximal subgroup conjugate to H_2 and one maximal subgroup conjugate to H_3 which contain D.

3. $m_G(2A, 2A, 2A) = 1750$.

   H_1 has two classes of involutions, namely $2A$ and $2B$, and if X and Y are involution classes and Z is a class of order 19, $m_{H_1}(X, Y, Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_1}(x) = 98$ for $x \in 2B$.

   H_2 has two classes of involutions, namely $2A$ and $2B$, and if X and Y are involution classes and Z is a class of order 19, $m_{H_2}(X, Y, Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_2}(x) = 98$ for $x \in 2B$.

   H_3 has one class of involutions, namely $2A$, and so $i_{H_3}(x) = m_{H_3}(2A, 2A, 2A) = 30$ for $x \in 2A$.

4. Now $98 + 98 + 30 = 226 < 1750$, hence, in this case, the Lemma holds true.

- Let $G \cong Co_3$.

  1. G has two conjugacy classes of involutions, namely classes $2A$ and $2B$. Since $m_G(2B, 2B, 21A) \neq 0$ then $\exists\ a, b \in 2B$ s.t. $ab = c \in 21A$.

     Note that $\langle c^3 \rangle$ is a Sylow 7-subgroup of G, and that $C_G(c) = \langle c \rangle$.

2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 21 must be isomorphic to $McL.2$, HS, $U_4(3).(2^2)_{133}$, M_{23}, $2.S_6(2)$, $U_3(5):S_3$, $2^4.A_8$, $L_3(4).D_{12}$ or $S_3 \times L_2(8).3$. From their character tables, it can be seen that the groups $McL.2$, HS, $U_4(3).(2^2)_{133}$, M_{23}, $2.S_6(2)$ and $2^4.A_8$ do not contain an element of order 21 and so can not contain a dihedral group of order 42. Therefore, each maximal subgroup containing $D := \langle a, b\rangle$ is conjugate with $H_1 \cong U_3(5):S_3$, $H_2 \cong L_3(4).D_{12}$ or $H_3 \cong S_3 \times L_2(8).3$. Since the order of the normalizer in H_1 of a Sylow 7-subgroup is 126, H_2 contains the normalizer in G of a Sylow 7-subgroup and H_3 contains the normalizer in G of a Sylow 7-subgroup, by Lemma 3.1.5, there can only be two maximal subgroup conjugate to H_1, one maximal subgroup conjugate to H_2 and one maximal subgroup conjugate to H_3 which contain the Sylow 7-subgroup $\langle c^3\rangle$. Hence, there can only be two maximal subgroup conjugate to H_1, one maximal subgroup conjugate to H_2 and one maximal subgroup conjugate to H_3 which contain D.

3. $m_G(2B, 2B, 2B) = 792$.

   H_1 has two classes of involutions, namely $2A$ and $2B$, and if X and Y are involution classes and Z is a class of order 21, $m_{H_1}(X, Y, Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_1}(x) = 50$ for $x \in 2B$.

   H_2 has four classes of involutions, namely $2A$, $2B$, $2C$ and $2D$, and if X and Y are involution classes and Z is a class of order 19, $m_{H_2}(X, Y, Z) \neq 0$ only if $X = Y = 2D$, and $i_{H_2}(x) = 50$ for $x \in 2D$.

   H_3 has three class of involutions, namely $2A$, $2B$ and $2C$, and if X and Y are involution classes and Z is a class of order 19, $m_{H_2}(X, Y, Z) \neq 0$ only if $X = Y = 2C$, and $i_{H_3}(x) = 14$ for

$x \in 2C$.

4. Now $2 \times 50 + 50 + 14 = 164 < 792$, hence, in this case, the Lemma holds true.

- Let $G \cong Co_2$.

1. G has three conjugacy class of involutions, namely classes $2A$, $2B$ and $2C$. Since $m_G(2C, 2C, 28A) \neq 0$ then $\exists\ a, b \in 2C$ s.t. $ab = c \in 28A$.

   Note that $\langle c^4 \rangle$ is a Sylow 7-subgroup of G, and that $C_G(c) = \langle c \rangle$.

2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 28 must be isomorphic to $U_6(2).2$, $2^{10} : M_{22} : 2$, McL, $2^{1+8} : S_6 2$, $HS.2$, $2^{1+4+6}.A_8$, $U_4(3).D_8$ or M_{23}. From their character tables, it can be seen that the groups $U_6(2).2$, $2^{10} : M_{22} : 2$, McL, $HS.2$, $2^{1+4+6}.A_8$, and M_{23} do not contain an element of order 28 and so do not contain a dihedral group of order 56. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ is conjugate with $H_1 \cong 2^{1+8} : S_6 2$ or $H_2 \cong U_4(3).D_8$. Since H_1 contains the normalizer in G of a Sylow 7-subgroup and the order of the normalizer in H_2 of a Sylow 7-subgroup is $7 \cdot 2^2 \cdot 6$, by Lemma 3.1.5, there can only be one maximal subgroup conjugate to H_1 and two maximal subgroups conjugate to H_2 which contain the Sylow 7-subgroup $\langle c^4 \rangle$. Hence there can only be one maximal subgroup conjugate to H_1 and two maximal subgroups conjugate to H_2 which contain D.

3. $m_G(2C, 2C, 2C) = 5832$.

   H_1 has ten classes of involutions, namely $2A$, $2B$, $2C$, $2D$, $2E$, $2F$, $2G$, $2H$, $2I$ and $2J$, and if X and Y are involution classes and Z is a class of order 28, $m_{H_1}(X, Y, Z) \neq 0$ only if $X = Y = 2J$, and $i_{H_1}(x) = 1022$ for $x \in 2J$.

H_2 has six classes of involutions, namely $2A$, $2B$, $2C$, $2D$, $2E$ and $2F$, and if X and Y are involution classes and Z is a class of order 28, $m_{H_2}(X,Y,Z) \neq 0$ only if X is $2E$ or $2F$ and Y is $2E$ or $2F$, and $i_{H_2}(x) = 246$ for $x \in 2E$ and $i_{H_2}(x) = 222$ for $x \in 2F$.

4. Now $1022+2\times 222 = 1466 < 1022+2\times 246 = 1514 < 5832$, hence, in this case, the Lemma holds true.

- Let $G \cong Fi_{22}$.

1. G has three conjugacy class of involutions, namely classes $2A$, $2B$ and $2C$. Since $m_G(2C,2C,13A) \neq 0$ then $\exists\ a,b \in 2C$ s.t. $ab = c \in 13A$.

   Note that $\langle c\rangle$ is a Sylow 13-subgroup of G, and that $C_G(c) = \langle c\rangle$.

2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 13 must be isomorphic to $O_7(3)$ or ${}^2F_4(2)$. Therefore, each maximal subgroup containing $D := \langle a,b\rangle$ is conjugate with $H_1 \cong O_7(3)$, $H_2 \cong O_7(3)$ or $H_3 \cong {}^2F_4(2)$ (note that there are two conjugacy classes of maximal subgroups of G that are isomorphic to $O_7(3)$). Since H_1 contains the normalizer in G of a Sylow 13-subgroup, H_2 contains the normalizer in G of a Sylow 13-subgroup and H_3 contains the normalizer in G of a Sylow 13-subgroup, by Lemma 3.1.5, there can only be one maximal subgroup conjugate to H_1, one maximal subgroup conjugate to H_2 and one maximal subgroup conjugate to H_3 which contain the Sylow 13-subgroup $\langle c\rangle$. Hence, there can only be one maximal subgroup conjugate to H_1, one maximal subgroup conjugate to H_2 and one maximal subgroup conjugate to H_3 which contain D.

3. $m_G(2C,2C,2C) = 5184$.

   H_1 has three classes of involutions, namely $2A$, $2B$ and $2C$, and

if X and Y are involution classes and Z is a class of order 13, $m_{H_1}(X,Y,Z) \neq 0$ only if $X = Y = 2C$, and $i_{H_1}(x) = 750$ for $x \in 2C$.

H_2 has three classes of involutions, namely $2A$, $2B$ and $2C$, and if X and Y are involution classes and Z is a class of order 13, $m_{H_2}(X,Y,Z) \neq 0$ only if $X = Y = 2C$, and $i_{H_2}(x) = 750$ for $x \in 2C$.

H_3 has two classes of involutions, namely $2A$ and $2B$, and if X and Y are involution classes and Z is a class of order 13, $m_{H_3}(X,Y,Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_3}(x) = 174$ for $x \in 2B$.

4. Now $750+750+174 = 1674 < 5184$, hence, in this case, the Lemma holds true.

- Let $G \cong HN$.

1. G has two conjugacy classes of involutions, namely classes $2A$ and $2B$. Since $m_G(2B,2B,21A) \neq 0$ then $\exists\ a,b \in 2B$ s.t. $ab = c \in 21A$.

   Note that $\langle c^3 \rangle$ is a Sylow 7-subgroup of G, and that $C_G(c) = \langle c \rangle$.

2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 21 must be isomorphic to A_{12}, $2.HS.2$, $U_3(8).3_1$, $(D_{10} \times U_3(5)).2$ or $2^3.2^2.2^6.(3 \times L_3(2))$. From their character tables, it can be seen that the groups $2.HS.2$ and $(D_{10} \times U_3(5)).2$ do not contain an element of order 21 and the conjugacy classes of elements of order 21 in the groups $U_3(8).3_1$ and $2^3.2^2.2^6.(3 \times L_3(2))$ are not real, and so these groups do not contain a dihedral group of order 42. Therefore, each maximal subgroup containing $D := \langle a,b \rangle$ is conjugate with $H \cong A_{12}$. Since this subgroup contains the normalizer in G of a Sylow 7-subgroup, by Lemma 3.1.5, there can only be

one maximal subgroup of G, conjugate to H containing the Sylow 7-subgroup $\langle c^3 \rangle$. Hence, there can only be one maximal subgroup of G, conjugate to H containing D.

3. $m_G(2B, 2B, 2B) = 7350$.
   H has three classes of involutions, namely $2A$, $2B$ and $2C$, and if X and Y are involution classes and Z is a class of order 21, $m_H(X, Y, Z) \neq 0$ only if $X = Y = 2C$, and $i_H(x) = 366$ for $x \in 2C$.

4. Now $366 < 7350$, hence, in this case, the Lemma holds true.

- Let $G \cong Ly$.

1. G has one conjugacy class of involutions, namely class $2A$. Since $m_G(2A, 2A, 67A) \neq 0$ then $\exists\ a, b \in 2A$ s.t. $ab = c \in 67A$.
   Note that $\langle c \rangle$ is a Sylow 67-subgroup of G, and that $C_G(c) = \langle c \rangle$.

2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 67 must be isomorphic to $67 : 22$. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ is conjugate with $H \cong 67 : 22$. Since this subgroup is isomorphic to the normalizer in G of a Sylow 67-subgroup, by Lemma 3.1.5, there can only be one maximal subgroup of G, conjugate to H containing the Sylow 67-subgroup $\langle c \rangle$. Hence, there can only be one maximal subgroup of G, conjugate to H containing D.

3. $m_G(2A, 2A, 2A) = 34650$.
   H has one class of involutions, namely $2A$, and so $i_H(x) = m_H(2A, 2A, 2A) = 0$ for $x \in 2A$.

4. Now $0 < 34650$, hence, in this case, the Lemma holds true.

- Let $G \cong Th$.

1. G has one conjugacy class of involutions, namely class $2A$. Since $m_G(2A, 2A, 19A) \neq 0$ then $\exists\ a, b \in 2A$ s.t. $ab = c \in 19A$.
   Note that $\langle c \rangle$ is a Sylow 19-subgroup of G, and that $C_G(c) = \langle c \rangle$.
2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 19 must be isomorphic to $U_3(8).6$ or $L_2(19).2$. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ is conjugate with $H_1 \cong U_3(8).6$, or $H_2 \cong L_2(19).2$. Since H_1 contains the normalizer in G of a Sylow 19-subgroup and H_2 contains the normalizer in G of a Sylow 19-subgroup, by Lemma 3.1.5, there can only be one maximal subgroup conjugate to H_1 and one maximal subgroup conjugate to H_2 which contain the Sylow 19-subgroup $\langle c \rangle$. Hence, there can only be one maximal subgroup conjugate to H_1 and one maximal subgroup conjugate to H_2 which contain D.
3. $m_G(2A, 2A, 2A) = 30510$.
   H_1 has two classes of involutions, namely $2A$, and $2B$, and if X and Y are involution classes and Z is a class of order 19, $m_{H_1}(X, Y, Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_1}(x) = 126$ for $x \in 2B$.
   H_2 has two classes of involutions, namely $2A$, and $2B$, and if X and Y are involution classes and Z is a class of order 19, $m_{H_2}(X, Y, Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_2}(x) = 18$ for $x \in 2B$.
4. Now $126 + 18 = 144 < 30510$, hence, in this case, the Lemma holds true.

- Let $G \cong Fi_{23}$.

1. G has three conjugacy classes of involutions, namely classes $2A$, $2B$ and $2C$. Since $m_G(2C, 2C, 17A) \neq 0$ then $\exists\ a, b \in 2C$ s.t. $ab = c \in 17A$.
   Note that $\langle c \rangle$ is a Sylow 17-subgroup of G, and that $C_G(c) = \langle c \rangle$.

2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 17 must be isomorphic to $S_8(2)$ or $S_4(4).4$. Therefore, each maximal subgroup containing $D := \langle a, b\rangle$ is conjugate with $H_1 \cong S_8(2)$, or $H_2 \cong S_4(4).4$. Since the order of the normalizer in H_1 of a Sylow 17-subgroup is $17\cdot 8$ and H_2 contains the normalizer in G of a Sylow 17-subgroup, by Lemma 3.1.5, there can only be two maximal subgroup conjugate to H_1 and one maximal subgroup conjugate to H_2 which contain the Sylow 17-subgroup $\langle c\rangle$. Hence, there can only be two maximal subgroup conjugate to H_1 and one maximal subgroup conjugate to H_2 which contain D.

3. $m_G(2C, 2C, 2C) = 143370$.

   H_1 has two classes of involutions, namely $2A$, $2B$, $2C$, $2D$, $2E$ and $2F$, and if X and Y are involution classes and Z is a class of order 17, $m_{H_1}(X, Y, Z) \neq 0$ only if $X = Y = 2F$, and $i_{H_1}(x) = 2686$ for $x \in 2F$.

   H_2 has three classes of involutions, namely $2A$, $2B$ and $2C$, and if X and Y are involution classes and Z is a class of order 17, $m_{H_2}(X, Y, Z) \neq 0$ only if $X = Y = 2B$, and $i_{H_2}(x) = 126$ for $x \in 2B$.

4. Now $2 \times 2686 + 126 = 5498 < 143370$, hence, in this case, the Lemma holds true.

- Let $G \cong Co_1$.

  1. G has three conjugacy classes of involutions, namely classes $2A$, $2B$ and $2C$. Since $m_G(2C, 2C, 33A) \neq 0$ then $\exists\ a, b \in 2C$ s.t. $ab = c \in 33A$.

     Note that $\langle c^3\rangle$ is a Sylow 11-subgroup of G, and that $C_G(c) = \langle c\rangle$.

2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 33 must be isomorphic to Co_2, $3.Suz.2$, $2^{11}.M_{24}$, Co_3, $U_6(2).3.2$ or $3^6 : 2M_{12}$. From their character tables, it can be seen that the groups Co_2, $2^{11}.M_{24}$ and Co_3 do not contain elements of order 33 and the conjugacy classes of elements of order 33 in $3^6 : 2M_{12}$ are not real, and so these groups do not contain a dihedral group of order 66. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ is conjugate with $H_1 \cong 3.Suz.2$, or $H_2 \cong U_6(2).3.2$. Since H_1 contains the normalizer in G of a Sylow 11-subgroup and the order of the normalizer in H_2 of a Sylow 11-subgroup is 330, by Lemma 3.1.5, there can only be one maximal subgroup conjugate to H_1 and two maximal subgroups conjugate to H_2 which contain the Sylow 11-subgroup $\langle c^3 \rangle$. Hence, there can only be one maximal subgroup conjugate to H_1 and two maximal subgroups conjugate to H_2 which contain D.

3. $m_G(2C, 2C, 2C) = 60984$.

   H_1 has four classes of involutions, namely $2A$, $2B$, $2C$, and $2D$, and if X and Y are involution classes and Z is a class of order 33, $m_{H_1}(X, Y, Z) \neq 0$ only if $X = Y = 2D$, and $i_{H_1}(x) = 3366$ for $x \in 2D$.

   H_2 has five classes of involutions, namely $2A$, $2B$, $2C$, $2D$ and $2E$, and if X and Y are involution classes and Z is a class of order 33, $m_{H_2}(X, Y, Z) \neq 0$ only if $X = Y = 2E$, and $i_{H_2}(x) = 1502$ for $x \in 2B$.

4. Now $3366 + 2 \times 1502 = 6370 < 60984$, hence, in this case, the Lemma holds true.

- Let $G \cong J_4$.

  1. G has two conjugacy classes of involutions, namely classes $2A$ and

$2B$. Since $m_G(2B, 2B, 43A) \neq 0$ then $\exists\ a, b \in 2B$ s.t. $ab = c \in 43A$.

Note that $\langle c \rangle$ is a Sylow 43-subgroup of G, and that $C_G(c) = \langle c \rangle$.

2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 43 must be isomorphic to $43 : 14$. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ is conjugate with $H \cong 43 : 14$. Since this subgroup is isomorphic to the normalizer in G of a Sylow 43-subgroup, by Lemma 3.1.5, there can only be one maximal subgroup of G, conjugate to H containing the Sylow 43-subgroup $\langle c \rangle$. Hence, there can only be one maximal subgroup of G, conjugate to H containing D.

3. $m_G(2A, 2A, 2A) = 147884$.

   H has one class of involutions, namely $2A$, and so $i_H(x) = m_H(2A, 2A, 2A) = 0$ for $x \in 2A$.

4. Now $0 < 147884$, hence, in this case, the Lemma holds true.

- Let $G \cong Fi'_{24}$.

1. G has two conjugacy classes of involutions, namely classes $2A$ and $2B$. Since $m_G(2B, 2B, 29A) \neq 0$ then $\exists\ a, b \in 2B$ s.t. $ab = c \in 29A$.

   Note that $\langle c \rangle$ is a Sylow 29-subgroup of G, and that $C_G(c) = \langle c \rangle$.

2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 29 must be isomorphic to $29 : 14$. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ is conjugate with $H \cong 29 : 14$. Since this subgroup is isomorphic to the normalizer in G of a Sylow 29-subgroup, by Lemma 3.1.5, there can only be one maximal subgroup of G, conjugate to H containing the Sylow 29-subgroup $\langle c \rangle$. Hence, there can

only be one maximal subgroup of G, conjugate to H containing D.

3. $m_G(2A, 2A, 2A) = 2997162$.
   H has one class of involutions, namely $2A$, and so $i_H(x) = m_H(2A, 2A, 2A) = 0$ for $x \in 2A$.

4. Now $0 < 2997162$, hence, in this case, the Lemma holds true.

- Let $G \cong B$.

1. G has four conjugacy classes of involutions, namely classes $2A$, $2B$, $2C$ and $2D$. Since $m_G(2C, 2C, 19A) \neq 0$ then $\exists\ a, b \in 2C$ s.t. $ab = c \in 19A$.
   Note that $\langle c \rangle$ is a Sylow 19-subgroup of G, and that $|C_G(c)| = 19 \times 2$.

2. From the list of maximal subgroups of G, it can be seen that any maximal subgroup whose order is divisible by 19 must be isomorphic to $2.^2E_6(2) : 2$, Th or $HN : 2$. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ is conjugate with $H_1 \cong 2.^2E_6(2) : 2$, $H_2 \cong Th$ or $H_3 \cong HN : 2$. Since H_1 contains the normalizer in G of a Sylow 19-subgroup, the order of the normalizer in H_2 of a Sylow 19-subgroup is $19 \cdot 18$ and the order of the normalizer in H_3 of a Sylow 19-subgroup is $19 \cdot 18$, by Lemma 3.1.5, there can only be one maximal subgroup conjugate to H_1, two maximal subgroups conjugate to H_2 and two maximal subgroups conjugate to H_3 which contain the Sylow 19-subgroup $\langle c \rangle$. Hence, there can only be one maximal subgroup conjugate to H_1, two maximal subgroups conjugate to H_2 and two maximal subgroups conjuagte to H_3 which contain D.

3. $m_G(2C, 2C, 2C) = 184246272$.
   H_1 has ten classes of involutions, namely $2A$, $2B$, $2C$, $2D$, $2E$, $2F$,

$2G$, $2H$, $2I$ and $2J$, and if X and Y are involution classes and Z is a class of order 19, $m_{H_1}(X,Y,Z) \neq 0$ only if X is $2I$ or $2J$ and Y is $2I$ or $2J$, and $i_{H_1}(x) = 7746558$ for any $x \in 2I \cup 2J$.

H_2 has one class of involutions, namely $2A$, and so $i_{H_2}(x) = m_{H_2}(2A, 2A, 2A) = 30510$ for $x \in 2A$.

H_3 has three classes of involutions, namely $2A$, $2B$ and $2C$, and if X and Y are involution classes and Z is a class of order 19, $m_{H_3}(X,Y,Z) \neq 0$ only if $X = Y = 2C$, and $i_{H_3}(x) = 18990$ for $x \in 2C$.

4. Now $7746558 + 2 \times 30510 + 2 \times 18990 = 7845558 < 184246272$, hence, in this case, the Lemma holds true.

- Let $G \cong M$.

1. G has two conjugacy classes of involutions, namely classes $2A$ and $2B$. Since $m_G(2B, 2B, 41A) \neq 0$ then $\exists\ a, b \in 2B$ s.t. $ab = c \in 41A$.

   Note that $\langle c \rangle$ is a Sylow 41-subgroup of G, and that $C_G(c) = \langle c \rangle$.

2. From the list of maximal subgroups of G [NW02], it can be seen that any maximal subgroup whose order is divisible by 41 must be isomorphic to $3^8.O_8^-(3).2_3$ or $41:40$. Therefore, each maximal subgroup containing $D := \langle a, b \rangle$ is conjugate with $H_1 \cong 3^8.O_8^-(3).2_3$, or $H_2 \cong 41:40$. Since the order of the normalizer in H_1 of a Sylow 41-subgroup is $41 \cdot 8$, and H_2 is isomorphic to the normalizer in G of a Sylow 41-subgroup, by Lemma 3.1.5, there can only be five maximal subgroups conjugate to H_1 and one maximal subgroup conjugate to H_2, which contain D.

3. $m_G(2B, 2B, 2B) = 90717803016750$.

   For H_1 the information needed to calculate $i_{H_1}(x)$ is not as readily available. However, we know that $i_{H_1}(x) \leqslant |C_{H_1}(a)|$. Also, since

the subgroup 41 of H_1 acts on the subgroup 3^8 without fixed points, we have $|C_{3^8}(a)| = 3^4$, and so we have $|C_{H_1}(a)| \leqslant 3^4 2 \left|C_{O_8^-(3)}(x)\right|$, for some involution x in $O_8^-(3)$. This upper bound can then be calculated from the character table of $O_8^-(3)$, which is readily available, but it is enough for our purposes to note that this upper bound gives $i_{H_1}(x) < i_G(a)/100 = 90741673459710/100$.

H_2 has one class of involutions, namely $2A$, and so $i_{H_2}(x) = m_{H_2}(2A, 2A, 2A) = 0$ for $x \in 2A$.

4. Now $5 \times 90741673459710/100 + 0 = 9074167345971/2 < \ldots$ $\ldots < 90717803016750$, hence, in this case, the Lemma holds true. □

Table 3.1: Summary of Results from Lemma 3.2.2

G	(X, X, Y)	$m_G(X, X, X)$	s	M_i	$i_{M_i}(a)$	$\sum_{j=1}^{s} i_{M_j}(a)$	$\sum_{j=1}^{s} i_{M_j}(a) < m_G(X, X, X)$
J_1	$2A, 2A, 11A$	30	1	$11:10$	0	0	✓
J_2	$2B, 2B, 7A$	32	1	$L_3(2):2$	6	6	✓
${}^2F_4(2)'$	$2B, 2B, 13A$	132	5	$L_3(3):2$	18	72	✓
				$L_3(3):2$	18		
				$L_2(25)$, $i = 3, 4, 5$	12		
HS	$2B, 2B, 7A$	72	4	$U_3(5).2$	50	150	× See above for proof in this case
				$U_3(5).2$	50		
				$L_3(4).2_1$	8		
				$A_8.2$	42		
J_3	$2A, 2A, 17A$	130	3	$L_2(16).2$, $i = 1, 2$	18	44	✓
				$L_2(17)$	8		
M_{24}	$2B, 2B, 11A$	202	7	$M_{22}.2$	70	192	✓
				$M_{12}.2$	62		
				$L_2(23)$, $i = 3, \ldots, 7$	12		
He	$2B, 2B, 17A$	364	1	$S_4(4).2$	126	126	✓
Ru	$2B, 2B, 29A$	912	1	$L_2(29)$	14	14	✓
Suz	$2B, 2B, 13A$	1192	6	$G_2(4)$	302	374	✓
				$L_3(3).2$, $i = 2, 3$	18		
				$L_2(25)$, $i = 4, 5, 6$	12		
ON	$2A, 2A, 19A$	1750	3	$L_3(7).2$, $i = 1, 2$	98	226	✓
				J_1	30		

Table 3.1: (continued)

G	(X,X,Y)	$m_G(X,X,X)$	s	M_i	$i_{M_i}(a)$	$\sum_{j=1}^{s} i_{M_j}(a)$	$\sum_{j=1}^{s} i_{M_j}(a) < m_G(X,X,X)$
Co_3	$2B,2B,21A$	792	4	$U_3(5).S_3$, $i=1,2$	50	164	✓
				$L_3(4).6.2$	50		
				$S_3.L_2(8).3$	14		
Co_2	$2C,2C,28A$	5832	3	$2^{1+8}:S_6.2$	1022	$\leqslant 1514$	✓
				$U_4(3).D_8$, $i=2,3$	$\leqslant 246$		
Fi_{22}	$2C,2C,13A$	5184	3	$O_7(3)$, $i=1,2$	750	1674	✓
				${}^2F_4(2)$	174		
HN	$2B,2B,21A$	7350	1	A_{12}	366	366	✓
Ly	$2A,2A,67A$	34650	1	$67:22$	0	0	✓
Th	$2A,2A,19A$	30510	2	$U_3(8).6$	126	144	✓
				$L_2(19).2$	18		
Fi_{23}	$2C,2C,17A$	143370	3	$S_8(2)$, $i=1,2$	2686	5498	✓
				$S_4(4).4$	126		
Co_1	$2C,2C,33A$	60984	3	$3.Suz.2$	3366	6370	✓
				$U_6(2).3.2$, $i=2,3$	1502		
J_4	$2B,2B,43A$	147884	1	$43:14$	0	0	✓
Fi'_{24}	$2B,2B,29A$	2997162	1	$29:14$	0	0	✓
B	$2C,2C,19A$	184246272	5	$2.{}^2E_6(2).2$	7746558	7845558	✓
				Th, $i=2,3$	30510		
				$HN.2$, $i=4,5$	18990		

Table 3.1: (continued)

G	(X, X, Y)	$m_G(X, X, X)$	s	M_i	$i_{M_i}(a)$	$\sum_{j=1}^{s} i_{M_j}(a)$	$\sum_{j=1}^{s} i_{M_j}(a) < m_G(X, X, X)$
M	$2B, 2B, 41A$	90717803016750	6	$3^8.O_8^-(3).2$, $i = 1, \ldots, 5$	$\leqslant \lvert C_{M_i}(a)\rvert$ $< i_G(a)/100$	$< 9074167345971/2$	✓
				$41 : 40$	0		

Chapter 4

The Linear Groups, characteristic $\neq 2$

We now move on to the linear groups. The purpose of this chapter is to determine which of the simple finite linear groups, $L_n(q)$, have Property 1 for q odd (and generally for $q \neq 9$). As such, we will first give some relevant definitions and results.

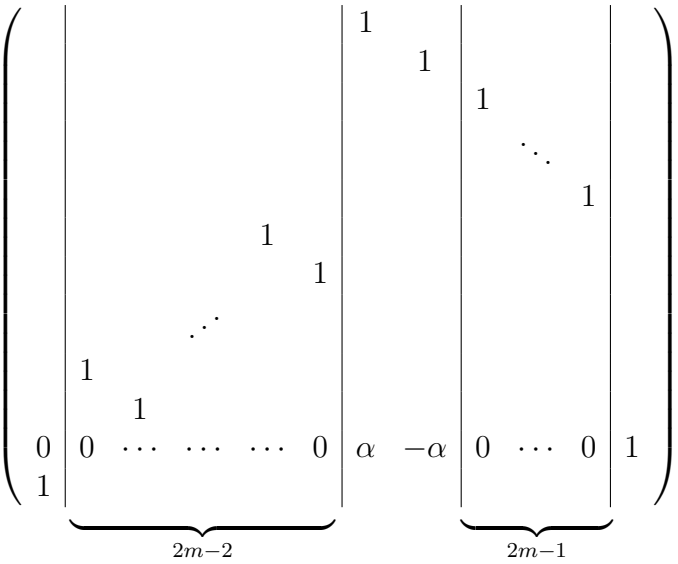
4.1 Preliminaries

First we consider the additional notation used in this chapter. Most of the notation used is fairly standard. For a prime power number, $q = p^k$, (where p is a prime number, and k is a natural number), $\mathbb{F}_q$ will denote the finite field of q elements. A generator of the cyclic group $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ will be called a "primitive element" of $\mathbb{F}_q$, while a generator of $\mathbb{F}_q$ as an algebra over $\mathbb{F}_p$ will be called a "defining element" of $\mathbb{F}_q$. If the field is $\mathbb{F}_p$, a defining element will always be assumed to be non-zero.

Let V be a vector space of dimension n over the finite field, $\mathbb{F}_q$, of order q. The "general linear group", $GL(V)$ is the set of invertible linear maps $V \longrightarrow V$. We may take V as the vector space $\mathbb{F}_q^n$ of n-tuples of elements of $\mathbb{F}_q$, and so the "general linear group", $GL_n(V)$, the set of invertible linear

maps $V \longrightarrow V$, may be identified with the group $GL_n(q)$ of invertible $n \times n$ matrices over $\mathbb{F}_q$. The subgroup of $GL_n(q)$ that consists of all $n \times n$ matrices with determinant 1, is called the "special linear group", and we denote this group by $SL_n(q)$. We denote by I_n the $n \times n$ identity matrix and the centre of the special linear group, $Z(SL_n(q))$, consists of all the scalar matrices, λI_n, of determinant 1. This is a normal subgroup of $SL_n(q)$ and the quotient, $SL_n(q)/Z(SL_n(q))$ is called the "projective special linear group", denoted by $PSL_n(q)$ or $L_n(q)$. We denote the natural surjective homomorphism from $SL_n(q)$ to $L_n(q)$ by ϕ. We will also need to talk about the dual space of row vectors of length n with entries in $\mathbb{F}_q$, and we will denote by ${}^n\mathbb{F}_q$ this space. Also we will denote by e_i the column vector with 1 in the i^{th} position and 0's elsewhere, i.e. $\{e_1, \ldots, e_n\}$ is the standard basis of $\mathbb{F}_q^n$ and so the set of row vectors $\left\{e_1^T, \ldots, e_n^T\right\}$ forms the standard basis of ${}^n\mathbb{F}_q$.

We will generally be working in $SL_n(q)$, and we will want a way to express general $n \times n$ matrices. The generators chosen in this chapter will be relatively close to being permutation matrices, and so will have entries mostly equal to zero, and we follow the standard convention of using blank spaces to represent large numbers of zero entries. Here is an example of a general $n \times n$ matrix for $n = 4m + 1$ with $m \geqslant 2$:



The dots in the matrix indicate that the 'pattern' of matrix entries continues for the number of columns indicated. As the matrix is 'close' to being a permutation matrix, we also indicate the permutation that it is 'close' to (in this case $(1, 2m, n-2, 3, \ldots 2, 2m+1, n-1, n)$). The information given should make it possible to reproduce these matrices for any allowed value of n.

We will require that the involutions we choose as generators for $L_n(q)$ are conjugate. Now, since any involution in $GL_n(q)$ can be diagonalised in $SL_n(q)$ to a diagonal matrix with non-zero entries equal to ± 1 and such matrices are conjugate if they have the same eigenvalues, we can check if two involutions are conjugate in $SL_n(q)$ by comparing their eigenvalues. Also, as $\phi : SL_n(q) \longrightarrow L_n(q)$ is a homomorphism, if x and y are conjugate in $SL_n(q)$, then $\phi(x)$ and $\phi(y)$ are conjugate in $L_n(q)$.

To prove positive results, we will often show that $L_n(q)$ has Property 2, and we will generally be working in $SL_n(q)$. As such we use the fact that ϕ is a surjective homomorphism, and if a set $X \subseteq SL_n(q)$ generates $SL_n(q)$, then $\phi(X) \subseteq L_n(q)$ generates $L_n(q)$.

The following result is due to J. McLaughlin [McL67]:

Lemma 4.1.1. *Let $\mathbb{F}_q$ be any field distinct from $\mathbb{F}_2$, and G be an irreducible linear group generated by root subgroups. Then one of the following holds:*

1. *$G \cong SL_n(q)$;*
2. *n is even and $G \sim Sp_n(q)$.*

which suggests the method outlined below, originated by Di Martino and Vavilov in [DV94] and [DV96].

1. We exhibit elements in $SL_n(q)$, such that they map to elements in $L_n(q)$ with the desired properties (i.e. 5 conjugate involutions whose product is the identity, or 3 conjugate involutions, two of which commute and whose product is also conjugate to the generating involutions) and defined in terms of a variable $\alpha \in \mathbb{F}_q$. We call the group generated by these elements G.

2. We show that there is a non-trivial transvection, g in G. We then show that there is a transvection opposite to g in G. We show, using Dickson's Lemma (Lemma 4.1.2 below) that these two transvections generate a group isomorphic to $SL_2(q)$ (subject to some polynomial in α being a defining element of $\mathbb{F}_q$). Thus we can conclude that G contains the whole root subgroup R, consisting of all transvections with the same centre and the same axis as g.

3. We now consider a subgroup $G_1 \leqslant G$, containing R, and the normal closure $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1} \trianglelefteq G_1$ of the root subgroup R in G_1. Then an analysis of G-invariant subspaces shows that the group G is irreducible (possibly apart from a few values of α). We then show that H_1 is irreducible, and conclude that $H := \langle g \rangle^G = \langle R \rangle^G$ is irreducible.

Thus from the classification of irreducible linear groups generated by root subgroups, H either coincides with $SL(n,q)$, or n is even and H is conjugate to $Sp_n(q)$.

4. We exclude the symplectic case by showing that G does not preserve a non-degenerate symplectic form up to similarity. This implies that, when α satisfies the imposed restrictions, we have that $G \trianglerighteq H = SL_n(q)$. Hence, $G = SL_n(q)$, so by our choice of generators of G, we have that $L_n(q)$ is generated by elements with the desired properties, and so has Property 1 or Property 2, as required.

5. It then remains to check that any restrictions on α can be satisfied.

The following result will be very useful:

Lemma 4.1.2 (Dickson's Lemma)**.** *See [Gor68]. Let $\mathbb{F}_q$ be a finite field with q odd. Also, let λ be a defining element of $\mathbb{F}_q$ and set*

$$L := \left\langle \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

Then we have either

1. *$L = SL_2(q)$, or*

2. *$q = 9$, $|Z(L)| = 2$, $L/Z(L)$ is isomorphic to A_5 and L contains a subgroup isomorphic to $SL_2(3)$.*

Note that, because of the exception in the case of $q = 9$, we do not, in general, deal with this case, as we do not obtain the required root subgroup as described under point 2 in the method above.

4.1.1 Transvections and Root Subgroups

We now give some definitions and results with regard to transvections and root subgroups. This will help us to exhibit the needed properties from point

2 of the method above. These definitions and results are generally fairly well known.

Definition 4.1.3. *For a matrix $x \in GL_n(q)$, the rank of the matrix $x - I_n$ is called the "residue" of x. This is denoted by $res(x)$.*

The general form of a one-dimensional transformation (i.e. a transformation with residue equal to 1) is $x_{ca}(\xi) := I_n + c\xi a$, where $c = (c_1, \ldots, c_n)^T \in \mathbb{F}_q^n$ is a column vector, $a = (a_1, \ldots, a_n) \in {}^n\mathbb{F}_q$ is a row vector and $\xi \in \mathbb{F}_q$ is a scalar.

Definition 4.1.4. *In geometric terminology, c is a generator of the "centre" of $x_{ca}(\xi)$, i.e. the centre is the Image, $Im(x_{ca}(\xi) - I_n)$. The "axis" of $x_{ca}(\xi)$ is the hyperplane in $\mathbb{F}_q^n$ orthogonal to a with respect to the standard scalar product, i.e. the axis is the hyperplane $Ker(x_{ca}(\xi) - I_n)$.*

Definition 4.1.5. *For $i \neq j$, matrices of the form $t_{ij}(\xi) := I_n + \xi e_{ij}$, where e_{ij} is the matrix with 1 in the $(i,j)^{th}$ position and zeros everywhere else, are called "elementary transvections". A matrix is called a "transvection" if it is conjugate in $GL_n(q)$ to an elementary transvection.*

Note that when the characteristic of a field is p, a prime, as in this case, then the order of a transvection is equal to p.

Now we have a simple test to see whether a one-dimensional transformation is a transvection:

Lemma 4.1.6. *The one-dimensional transformation $x_{ca}(\xi)$ is a transvection if and only if $ac = 0$ (i.e. the centre lies on the axis).*

Proof. Assume x is a transvection. Then for some elementary transvection, $t_{ij}(\xi)$, and some $g \in GL_n(q)$, we have

$$\begin{aligned} x &= g^{-1} t_{ij}(\xi)\, g \\ &= g^{-1}(I_n + \xi e_{ij})\, g \end{aligned}$$

$$= \quad I_n + c\xi a$$

where $c = \left(\left(g^{-1}\right)_{1i}, \ldots, \left(g^{-1}\right)_{ni}\right)^T$, the i^{th} column of g^{-1} and $a = (g_{j1}, \ldots, g_{jn})$, the j^{th} row of g. Now since $i \neq j$, we must have $ac = 0$. Conversely, if we have a one-dimensional transformation $x_{ca}(\xi) = I_n + c\xi a$, with $ac = 0$, then there exists a matrix $g \in GL_n(q)$ with c as the 1^{st} column of g^{-1} and with a as the 2^{nd} row of g. Hence, $x_{ca}(\xi)$ is conjugated to the elementary transvection $t_{12}(\xi)$ by g, and so $x_{ca}(\xi)$ is a transvection. □

For a transvection x, the values a and c are defined up to scalar multiples. We normalize x by setting $\xi = 1$, and if $x \neq e$, we let the first non-zero coordinate of a be equal to 1. From now on we denote the normalized a and c of x by $a(x)$ and $c(x)$ respectively.

Definition 4.1.7. *The group $R := \{x_{ca}(\xi) : \xi \in \mathbb{F}_q\}$ is called a "Root Subgroup" of $SL_n(q)$. In particular, the subgroups $X_{ij} := \{t_{ij}(\gamma) : \gamma \in \mathbb{F}_q\}$ are called "elementary root subgroups".*

Note that R is isomorphic to the additive group $\mathbb{F}_q^+$. Also, note that every non-trivial transvection x is contained in a unique root subgroup, $X := \left\{x_{c(x),a(x)}(\gamma) : \gamma \in \mathbb{F}_q\right\}$.

Consider two transvections $x := x_{c(x)a(x)}(1)$ and $x := y_{c(y)a(y)}(1)$. The following fact was first noted in [AS76] by M. Aschbacher and G. Seitz and was used in [Coo79] by B. Cooperstein. A proof may be found in [Vav88].

Lemma 4.1.8. *Any pair (x, y) of transvections can be simultaneously conjugated to a pair of elementary transvections, i.e. $\exists g \in GL_n(q)$ s.t. $x^g = t_{ij}(\gamma)$ and $y^g = t_{hk}(\delta)$, for some $1 \leqslant i, j, h, k \leqslant n$, $i \neq j$, $h \neq k$, $\gamma, \delta \in \mathbb{F}_q$.*

Definition 4.1.9. *For a pair of transvections there are a few possibilities:*

- *Two transvections are called "orthogonal" if the (unique) root subgroups in which they are contained are simultaneously conjugate in $GL_n(q)$ to*

a pair of elementary root subgroups X_{ij} and X_{hk}, with i, j, h and k all distinct.

- *Two transvections are called "commuting" if the (unique) root subgroups in which they are contained are simultaneously conjugate in $GL_n(q)$ to a pair of elementary root subgroups X_{ij} and X_{hk}, with three distinct indices among i, j, h and k, and $i \neq k$, $j \neq h$.*

- *Two transvections are called "non-commuting" if the (unique) root subgroups in which they are contained are simultaneously conjugate in $GL_n(q)$ to a pair of elementary root subgroups X_{ij} and X_{hk}, with three distinct indices among i, j, h and k, and $i \neq h$, $j \neq k$.*

- *If the (unique) root subgroups in which they are contained are simultaneously conjugate in $GL_n(q)$ to a pair of elementary root subgroups X_{ij} and X_{hk}, with $(i,j) = (h,k)$, then the root subgroups coincide.*

- *Two transvections are called "opposite" if the (unique) root subgroups in which they are contained are simultaneously conjugate in $GL_n(q)$ to a pair of elementary root subgroups X_{ij} and X_{hk}, with $(i,j) = (k,h)$.*

Now, under conjugation, the axis and centre of a transformation x behave as follows:

$$\begin{aligned} a\left(g^{-1}xg\right) &= a(x)\,g \text{ and} \\ c\left(g^{-1}xg\right) &= g^{-1}c(x) \end{aligned}$$

Thus, in particular, we have for transformations x and y:

$$\begin{aligned} a\left(g^{-1}xg\right)c\left(g^{-1}yg\right) &= a(x)\,gg^{-1}c(y) \\ &= a(x)\,c(y) \text{ and similarly} \\ a\left(g^{-1}yg\right)c\left(g^{-1}xg\right) &= a(y)\,c(x) \end{aligned}$$

i.e. the values $a(x)\,c(y)$ and $a(y)\,c(x)$ are invariant under conjugation. Also, for two transvections, x and y, collinearity of the row vectors $a(x)$ and $a(y)$ is preserved under simultaneous conjugation (as is the collinearity of the column vectors $c(x)$ and $c(y)$). From these we get the following result:

Lemma 4.1.10. *A necessary and sufficient condition for a pair of transvections x and y to be opposite is that both $\gamma := a(x)\,c(y)$ and $\delta := a(y)\,c(x)$ are distinct from zero. In this case the pair (x, y) is conjugate to the pair $(t_{12}(\gamma), t_{21}(\delta))$.*

Now, since the pair $(t_{12}(\gamma), t_{21}(\delta))$ is conjugate to the pair $(t_{12}(1), t_{21}(\delta\gamma))$, the above result, along with Dickson's Lemma gives us:

Lemma 4.1.11. *Let $K := \mathbb{F}_q$ be a finite field with $\mathrm{char}(K) \neq 2$ and $q \neq 9$. Suppose that x and y are such transvections that the product $\gamma\delta$, where $\gamma := a(x)\,c(y)$ and $\delta := a(y)\,c(x)$, is a defining element of the field $\mathbb{F}_q$. Then the subgroup $\langle x, y\rangle$ contains a root subgroup $X \cong \mathbb{F}_q^+$.*

4.1.2 Irreducibility

We now give some definitions and results to do with showing that a subgroup of $GL_n(q)$ is irreducible over the vector space $V \cong \mathbb{F}_q^n$. Again the majority of these definitions and results are generally fairly well known.

Definition 4.1.12. *Let G be a subgroup of $GL_n(q)$. A subspace $U \subseteq V$ is called "invariant with respect to G" (or "G-invariant") if $gu \in U$ for any $g \in G$ and $u \in U$. A subspace $U \subseteq V$ is called "proper" if it is distinct from V and 0. A subgroup G of $GL_n(q)$ is called "irreducible" if there is no proper G-invariant subspaces in V. A direct sum decomposition $V = U_1 \oplus \cdots \oplus U_t$ is called an "imprimitivity system" for the group G if G permutes the summands U_i, i.e. for every element $g \in G$ and for every i, $1 \leqslant i \leqslant t$, there exists a j, $1 \leqslant i \leqslant t$, s.t. $gU_i = U_j$. The summands, U_i, are called "blocks of*

imprimitivity" of G. G is called "primitive" if it does not admit a non-trivial imprimitivity system, and is called "imprimitive" otherwise.

Note that, if a group, G, is irreducible but imprimitive then all blocks of an imprimitivity system of G have the same dimension s, and G permutes them transitively. In particular, $n = st$.

Definition 4.1.13. *If V is a completely reducible H-module and W is an irreducible submodule of V, then the "homogeneous component" U of V containing W is the sum of all H-submodules of V isomorphic to W.*

Now, we will need a result known as "Clifford's Theorem". The following Lemma summarises the parts of Clifford's Theorem that we will need:

Lemma 4.1.14. *If G is irreducible and $H \trianglelefteq G$ is a normal subgroup of G, then*

1. *V is completely reducible as a H-module;*
2. *The representatives $W_1, \ldots, W_t$ of the isomorphism classes of irreducible H-submodules are G-conjugate;*
3. *Denote by U_i the homogeneous component of V, containing W_i. Then $U_1, \ldots, U_t$ form an imprimitivity system for G;*
4. *In particular, if G is both irreducible and primitive then with respect to an appropriate base of V any element x of H has the form $a(x) \oplus \cdots \oplus a(x)$, for some matrix $a(x) \in GL_s(K)$.*

Now, since we have that

$$res(a_1 \oplus \ldots \oplus a_l) = res(a_1) + \ldots + res(a_l),$$

and we know that for a transvection x, $res(x) = 1$, then we have that a non-trivial transvection cannot be presented as a direct sum $a \oplus \ldots \oplus a$ with

more than one summand. Thus Lemma 4.1.14 implies that if G is a primitive irreducible group which contains a non-trivial transvection x, then the normal closure $H := \langle x \rangle^G$ of x in G is irreducible.

The following result is useful:

Lemma 4.1.15. *Consider a block-monomial matrix of the shape*

$$z = \begin{pmatrix} & a_1 & & \\ & & \ddots & \\ & & & a_{l-1} \\ a_l & & & \end{pmatrix}$$

where $l \geqslant 2$ and $a_1, \ldots, a_l \in GL_m(q)$, $m \geqslant 2$. Then no power of z is a non-trivial transvection.

Proof. We consider the power of z, z^r. If r is not divisible by l, then z^r is a block-monomial matrix which is not block-diagonal. Remember that the residue of a transformation, x, is given by $res(x) = rank(x - I_n)$. Thus, as z^r is not block-diagonal, its residue must be at least m.

Now a simple calculation shows that z^l is a block-diagonal matrix of the form

$$a_1 a_2 \cdots a_{l-1} a_l \oplus a_2 a_3 \cdots a_l a_1 \oplus \cdots \oplus a_l a_1 \cdots a_{l-2} a_{l-1},$$

and these summands are clearly all conjugate. Thus if r is divisible by l, the residue of z^r must be divisible by l.

Thus, as a non-trivial transvection has residue equal to 1, this shows that, for $l \geqslant 2$ and $m \geqslant 2$, z^r can never be a non-trivial transvection. □

We now give the main results for this section:

Proposition 4.1.16. *Let G be a subgroup of $SL_n(q)$ containing two elements, b and c. Suppose some power, $(bc)^r$, of bc is a non-trivial transvection and let $H := \langle (bc)^r \rangle^G$ be the normal subgroup of G generated by $(bc)^r$. Suppose G is irreducible and let $V = U_1 \oplus \cdots \oplus U_l$ be a direct decomposition of V into*

H-homogeneous components. Denote by σ and τ the images of b and c in the action of G on the set $I := \{U_1, \ldots, U_l\}$ of components. Then:

1. *If $l = 1$, then H is irreducible;*
2. *$l \neq n$;*
3. *If $(bc)^r$ acts non-trivially on some $U_i \in I$, then $\sigma\tau U_i = U_i$.*

Proof. 1. Here V is H-homogeneous. If it is not H-irreducible, then any matrix in H is conjugate to a matrix of the form $a \oplus \cdots \oplus a$ for some $a \in GL_m(K)$, $m|n$, $m \neq n$, which makes it impossible for H to contain a transvection.

2. If $l = n$, then H is diagonalizable, so it cannot contain a non-trivial transvection.

3. We may assume $l < n$. Suppose that a subspace U_i is such that $\sigma\tau U_i \neq U_i$. Then U_i is contained in an orbit of cardinality $s \geqslant 2$ with respect to the element $\sigma\tau$ and we let W be the sum of the subspaces U_j from this orbit. Then it follows from Lemma 4.1.15 that $(bc)^r$ must act trivially on W and so on U_i.

□

Proposition 4.1.17. *Let G be a subgroup of $SL_n(q)$ generated by three elements, x, b and c. Suppose some power, $(bc)^r$, of bc is a non-trivial transvection, its conjugate, $((bc)^r)^x$, is opposite to $(bc)^r$ and its conjugates $((bc)^r)^b$ and $((bc)^r)^c$ are both equal to $((bc)^r)^{-1}$. Let $H := \langle (bc)^r \rangle^G$ be the normal subgroup of G generated by $(bc)^r$. If G is irreducible, then H is also irreducible.*

Proof. Let G be irreducible and assume H is not irreducible. We use the notation from Proposition 4.1.16, and we denote by ρ, σ and τ the images of x, b and c in the action of G on the set $I := \{U_1, \ldots, U_l\}$ of components. Now,

from Proposition 4.1.16, we may assume $1 < l < n$. Let U_i be the subspace on which $(bc)^r$ acts non-trivially. Then by Proposition 4.1.16, $\sigma\tau U_i = U_i$. Now U_i must be σ-invariant and τ-invariant as, if not, the transvections $((bc)^r)^b$ and $((bc)^r)^c$ would act non-trivially on some subspace U_j, for some $j \neq i$, and thus must be orthogonal to $(bc)^r$ and then $((bc)^r)^b$ and $((bc)^r)^c$ could not be equal to $((bc)^r)^{-1}$. Now U_i cannot be ρ-invariant, else U_i would form a G-invariant subspace of V, which cannot happen as $l > 1$. But then the transvection $((bc)^r)^x$ acts non-trivially on some subspace U_j for some $j \neq i$, and thus must be orthogonal to $(bc)^r$, and not opposite, contradicting the assumption. Thus, we must have that H is irreducible. □

So, if we can show that a group G, with the properties given in this Proposition, is irreducible, then we will have an irreducible group generated by root subgroups. To show that the group G is irreducible, we will use the following result:

Lemma 4.1.18. *Let G be a subgroup of $GL_n(q)$ containing a transvection g. If U is a G-invariant subspace in V, then either U contains the centre of g, or U is contained in the axis of g.*

Proof. Since U is G-invariant and $g \in G$, we have $(I_n + c(g)\, a(g))\, u \in U$, and so $c(g)\, a(g)\, u \in U$. If U is not contained in the axis of g, then $\exists u \in U$ s.t. $a(g)\, u \neq 0$. Then, as $c(g)\, a(g)\, u \in U$, we have $c(g) \in U$, i.e. the centre of g is contained in U. □

4.1.3 Invariant Forms

If $n = 2l$ is even we denote by $Sp_n(K)$ the symplectic group of degree n over K. $Sp_n(K)$ is defined in terms of a non-degenerate symplectic form $\langle\ ,\ \rangle$ on the space V, and consists of all matrices $g \in GL_n(K)$ s.t. $\langle gu, gv\rangle = \langle u, v\rangle$ for all $u, v \in V$. Since we are dealing with finite fields, $K = \mathbb{F}_q$, we will also write $Sp_n(q)$. We will also consider the corresponding general group $GSp_n(K)$,

consisting of all symplectic similarities, i.e. consisting of all matrices $g \in GL_n(K)$ s.t. for all $u, v \in V$, we have $\langle gu, gv \rangle = \lambda(g) \langle u, v \rangle$, for some scalar $\lambda(g) \in K^*$ dependent on g. We call $\lambda(g)$ the "multiplier" corresponding to g.

This section is concerned with definitions and results to do with symplectic forms. We will need these to exclude the possibility that certain groups are symplectic groups. Again, these definitions and results are fairly well known.

Lemma 4.1.19. *Let $\Gamma := Sp_n(K)$. Then the normalizer of Γ in $GL_n(K)$ coincides with $GSp_n(K)$.*

The intersection of $GSp_n(K)$ with $SL_n(K)$, we denote by $SGSp_n(K)$, and it is the normalizer of $Sp_n(K)$.

From this, we have that to show $H := \langle g \rangle^G = \langle R \rangle^G$ is not conjugate to $Sp_n(q)$ (and hence must be isomorphic to $SL_n(q)$), we will be using the explicit generators of G to show that G does not preserve a non-degenerate symplectic form up to similarity (possibly with some restrictions on α). We will show that any form that is preserved by G up to similarity must be degenerate, i.e. $\langle u, v \rangle = 0 \ \forall u, v \in V$. To do this, we will first consider the multipliers corresponding to the generators of G, and show that they must all be equal to 1. As such the following result will be useful:

Lemma 4.1.20. *Let $g, h_1, h_2 \in GSp_n(K)$, and let $\lambda(g)$, $\lambda(h_1)$ and $\lambda(h_2) \in K^*$ be the multipliers corresponding to g, h_1 and h_2 respectively.*

1. *If $g = 1$, then $\lambda(g) = 1$.*
2. *If $g = h_1 h_2$, then $\lambda(g) = \lambda(h_1)\lambda(h_2)$.*
3. *If g is an element of order n then $\lambda(g)^n = 1$.*
4. *If g is an involution then $\lambda(g) = \pm 1$.*
5. *If h_1 and h_2 are conjugate in $GSp_n(K)$, then $\lambda(h_1) = \lambda(h_2)$.*

Proof. 1. If $g = 1$, then for $u, v \in V$, $\lambda(g)\langle u, v\rangle = \langle gu, gv\rangle = \langle u, v\rangle$, and thus $\lambda(g) = 1$.

2. If $g = h_1 h_2$, then for $u, v \in V$, $\lambda(g)\langle u, v\rangle = \langle gu, gv\rangle = \langle h_1 h_2 u, h_1 h_2 v\rangle = \lambda(h_1)\langle h_2 u, h_2 v\rangle = \lambda(h_1)\lambda(h_2)\langle u, v\rangle$, and thus $\lambda(g) = \lambda(h_1)\lambda(h_2)$.

3. If g is an element of order n, then by the above $\lambda(g)^n = \lambda(g^n) = \lambda(1) = 1$.

4. If g is an involution, then by the above $\lambda(g)^2 = \lambda(g^2) = \lambda(1) = 1$, and so $\lambda(g) = \pm 1$.

5. If $h_1 = h_2^g$ for some $g \in GSp_n(K)$, then for $u, v \in V$, $\lambda(h_1) = \lambda(g^{-1}h_2 g) = \lambda(g^{-1})\lambda(h_2)\lambda(g) = \lambda(g)^{-1}\lambda(g)\lambda(h_2) = \lambda(h_2)$.

□

Another useful result concerning multipliers is given below, but we will first need another definition:

Definition 4.1.21. *For an involution x, we denote by $V^+(x)$ and $V^-(x)$ the eigenspaces of x corresponding to the eigenvalues 1 and -1 respectively.*

Lemma 4.1.22. *If x, an involution from $SL_n(K)$, preserves a non-degenerate symplectic form up to similarity, with multiplier $\lambda(x)$, then at least one of the following holds:*

1. $\lambda(x) = 1$;

2. $\dim(V^+(x)) = \dim(V^-(x))$.

Proof. Since x is an involution, we have $\lambda(x) = \pm 1$. Suppose that $\lambda(x) = -1$. Then for any $u, v \in V^\epsilon(x)$, for $\epsilon = \pm 1$, we have $\langle u, v\rangle = \langle xu, xv\rangle = -\langle u, v\rangle$. This gives $\langle u, v\rangle = 0$ for any $u, v \in V^\epsilon(x)$, for $\epsilon = \pm 1$. Hence we have that $V^+(x)$ and $V^-(x)$ are totally isotropic. If then $\dim(V^+(x)) \neq \dim(V^-(x))$ the form must be degenerate. □

To show that $H := \langle g \rangle^G = \langle R \rangle^G$ is not conjugate to $Sp_n(q)$ (and hence must be isomorphic to $SL_n(q)$), we will be using the explicit generators of G to show that G does not preserve a non-degenerate symplectic form up to similarity (possibly with some restrictions on α). We will show that any form that is preserved by G up to similarity must be degenerate, i.e. $\langle u, v \rangle = 0 \ \forall u, v \in V$. For $g \in G$, $u_1, u_2, v_1, v_2 \in V$, if $gu_1 = u_2$ and $gv_1 = v_2$, as a shorthand, we will replace

$$\langle gu_1, gv_1 \rangle \quad = \quad \langle u_2, v_2 \rangle$$

with

$$\langle u_1, v_1 \rangle \quad =_g \quad \langle u_2, v_2 \rangle$$

4.1.4 Equations

There will be several conditions for the value $\alpha \in \mathbb{F}_q$ to satisfy. As such, the following result will be very useful:

Lemma 4.1.23. *Let $\mathbb{F}_q$ for $q = p^m$ p prime, be a finite field and let $f(\alpha) \in \mathbb{F}_q[\alpha]$ be a polynomial over $\mathbb{F}_q$ of degree $d > 0$. Let $X \subseteq \mathbb{F}_q$ be a subset of the field with $|X| = s$. Suppose one of the following holds:*

- *$m = 1$ and $p > d + s$;*
- *$m = 2$ and $p > \max\{d, s\}$;*
- *$m = 3$ and $p > \sqrt{d + s}$;*
- *$m \geqslant 4$ and $p > \max\left\{\sqrt{d}, \ \sqrt[m-2]{s}\right\}$*

Then at least one value of $f(\alpha)$ on $\mathbb{F}_q \backslash X$ is a defining element of $\mathbb{F}_q$.

Proof. For a constant $\mu \in \mathbb{F}_q$, the polynomial $f(\alpha) - \mu$, has at most d distinct roots. Therefore there are at most d distinct elements, $\lambda \in \mathbb{F}_q$, s.t. $f(\lambda) = \mu$.

Hence we must have that $f(\alpha)$ assumes at least $(p^m - s)/d$ distinct values on $\mathbb{F}_q \backslash X$. If the number of values that $f(\alpha)$ assumes on $\mathbb{F}_q \backslash X$ is greater than the number of non-defining elements of $\mathbb{F}_q$, then at least one of the values of $f(\alpha)$ on $\mathbb{F}_q \backslash X$ must be a defining element of $\mathbb{F}_q$.

- If $m = 1$, then any non-zero element of $\mathbb{F}_q$ is a defining element of K, and the zero element is the only non-defining element of $\mathbb{F}_q$. Thus if $(p - s)/d > 1$ then at least one value of $f(\alpha)$ on $\mathbb{F}_q \backslash X$ is a defining element of $\mathbb{F}_q$. This holds if $p > d + s$.

- If $m = 2$, then there are p elements of $\mathbb{F}_q$ which are not defining elements of $\mathbb{F}_q$. Thus if $(p^2 - s)/d > p$ then at least one value of $f(\alpha)$ on $\mathbb{F}_q \backslash X$ is a defining element of $\mathbb{F}_q$. This holds if $p > d, s$.

- If $m = 3$, then there are p elements of $\mathbb{F}_q$ which are not defining elements of $\mathbb{F}_q$. Thus if $(p^3 - s)/d > p$ then at least one value of $f(\alpha)$ on $\mathbb{F}_q \backslash X$ is a defining element of $\mathbb{F}_q$. This holds if $p > \sqrt{d + s}$.

- If $m = 4$, then there are p^2 elements of $\mathbb{F}_q$ which are not defining elements of $\mathbb{F}_q$. Thus if $(p^4 - s)/d > p^2$ then at least one value of $f(\alpha)$ on $\mathbb{F}_q \backslash X$ is a defining element of $\mathbb{F}_q$. This holds if $p > \sqrt{d}, \sqrt{s}$.
  If $m \geqslant 5$, then there are no subfields of orders p^{m-1} and p^{m-2} in $\mathbb{F}_q$. An estimate shows us that there are at most $p^{m-3} + p^{m-4} + \ldots + p = \frac{p^{m-2} - p}{p-1} \leqslant p^{m-2}$ elements which are not defining. Thus if $(p^m - s)/d > p^{m-2}$ then at least one value of $f(\alpha)$ on $\mathbb{F}_q \backslash X$ is a defining element of $\mathbb{F}_q$. This holds if $p > \sqrt{d}, \sqrt[m-2]{s}$.

□

4.2 Dimension $n = 2$, $q \geqslant 5$

In this section we consider the groups $L_2(q)$ for $q \geqslant 5$. We show that the group $L_2(q)$ for $q \geqslant 5$ has Property 2 if and only if $q \neq 7, 9$, and has Property

1 if and only $q \neq 7$. It may be noted that, since there is only one conjugacy class of involutions in $L_2(q)$, Property 1 and Property 2 are equivalent to:

Property 3. *G can be generated by 5 involutions whose product is the identity.*

and

Property 4. *G can be generated by 3 involutions a, b and c, 2 of which, a and b, commute.*

respectively. Now the question of whether or not $L_2(q)$ has Property 4 was proved by Nuzhin in [Nuz97]. We include those results below with rewritten proofs for completeness.

It may be noted at this stage that the conjugacy class of involutions in $L_2(q)$ is the image, under the natural homomorphism $SL_2(q) \longrightarrow L_2(q)$, of the conjugacy class of $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(q)$ (i.e. the elements in $SL_2(q)$ that square to $-I_2$). Thus we will work often in $SL_2(q)$ with generators from this conjugacy class. We work in the standard representation of $SL_2(q)$, i.e. 2×2 matrices acting on the space of column vectors of length 2.

4.2.1 $q = 7$

Consider the ordinary irreducible module, V, of dimension 6 and use Theorem 1.2.4. In the terminology of Theorem 1.2.4, $n = 6$, $m = 5$ and $d_i = 2$ for $i = 1, 2, 3, 4, 5$, as the x_i are all conjugate. Then we have

$$d_1 + d_2 + d_3 + d_4 + d_5 = 10 < 12 = 2n.$$

So, by Theorem 1.2.4, $L_2(7)$ does not have Property 1 (and so does not have Property 2).

We do note however that $L_2(7)$ can be generated by 6 conjugate involutions whose product is 1. To prove this it is enough to show that $SL_2(q)$ can be

generated by an element that squares to $-I_2$ and an element of order 3. This is because then $L_2(7)$ will be $(2,3)$-generated, and by the discussion in chapter 1 will then be generated by 3 conjugate involutions.

We define:

$$\begin{aligned} a &:= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ b &:= \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \end{aligned}$$

Then, a, and b have the desired properties, and we define $G := \langle a, b \rangle$. Now,

$$\begin{aligned} (ab)^2 &= \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \\ (ba)^2 &= \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \end{aligned}$$

These elements are simultaneously conjugate in $GL_2(q)$ to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 3 & 1 \end{pmatrix}$ respectively, and so by Lemma 4.1.2 (Dickson's Lemma), if 3 is a defining element of $\mathbb{F}_7$, $\langle a, b \rangle \cong SL_2(7)$. Now, as $3 \neq 0$, 3 is a defining element of $\mathbb{F}_7$, and so we conclude that $L_2(7)$ can be generated by 6 conjugate involutions whose product is 1.

4.2.2 $q = 9$

The linear group $L_2(9)$ is isomorphic to the alternating group A_6. Hence from chapter 2, we have that $L_2(9)$ has Property 1, but not Property 2.

4.2.3 $q = 11$

For $q = 11$ we define:

$$\begin{aligned} a &:= \begin{pmatrix} 3 & 1 \\ 1 & -3 \end{pmatrix} \\ b &:= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ c &:= \begin{pmatrix} 2 & 5 \\ -1 & -2 \end{pmatrix} \end{aligned}$$

Then, a, b and c map, to involutions a', b' and $c' \in L_2(11)$, under the natural homomorphism $SL_2(11) \longrightarrow L_2(11)$, with $a'b' = b'a'$. We define $H := \langle a', c' \rangle \leqslant L_2(11)$. Then H is a dihedral group of order 12. Thus, from information in the Web-ATLAS, [WNB+05], H is a maximal subgroup of $L_2(11)$. Now $b' \notin H$, and so $\langle a', b', c' \rangle \cong L_2(11)$. Hence the group $L_2(11)$ has Property 4, and so has Property 2.

4.2.4 $q \equiv 1 \mod 4$, $q \geqslant 5$ and $q \neq 9$

For $q \equiv 1 \mod 4$, $q \geqslant 5$ and $q \neq 9$ then we take i as a square root of -1 (which exists since $q \equiv 1 \mod 4$), and we define:

$$\begin{aligned} a &:= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \\ b &:= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ c &:= \begin{pmatrix} i & 0 \\ i\alpha & -i \end{pmatrix} \end{aligned}$$

Then, a, b and c map, to involutions a', b' and $c' \in L_2(q)$, under the natural homomorphism $SL_2(q) \longrightarrow L_2(q)$, with $a'b' = b'a'$. Then,

$$\begin{aligned} cabb &= \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} \\ bcab &= \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix} \end{aligned}$$

These elements are simultaneously conjugate in $GL_2(q)$ to $\begin{pmatrix} 1 & 0 \\ -\alpha^2 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ respectively, and so by Lemma 4.1.2 (Dickson's Lemma), if $-\alpha^2$ is a defining element of $\mathbb{F}_q$, $\langle a, b, c \rangle \cong SL_2(q)$. Hence for $q \geqslant 5, q \neq 9$, if $\exists \alpha \in \mathbb{F}_q$ s.t. $-\alpha^2$ is a defining element of $\mathbb{F}_q$, $L_2(q)$ has Property 4, and so has Property 2 (which of course means $L_2(q)$ has Property 3 and Property 1 as well).

The only restrictions we have are that $q \equiv 1 \mod 4$, $q \geqslant 5$ and $q \neq 9$ and $-\alpha^2 \neq 0$ and is a defining element of $\mathbb{F}_q$. Taking α to be any primitive element of $\mathbb{F}_q$ will satisfy these restrictions on α. Hence for $q \equiv 1 \mod 4$, $q \geqslant 5$ and $q \neq 9$, there exists an element $\alpha \in \mathbb{F}_q$ that satisfies these restrictions.

4.2.5 $q \equiv 3 \mod 4$ and $q > 11$

When $q \equiv 3 \mod 4$ and $q > 11$, we define:

$$\begin{aligned} a &:= \begin{pmatrix} \gamma & \delta \\ \delta & -\gamma \end{pmatrix} \\ b &:= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ c &:= \begin{pmatrix} 0 & \alpha \\ -\alpha^{-1} & 0 \end{pmatrix} \end{aligned}$$

where $\gamma^2 + \delta^2 = -1$ and α is a primitive element of $\mathbb{F}_q$.

Then, a, b and c map, to involutions a', b' and $c' \in L_2(q)$, under the natural homomorphism $SL_2(q) \longrightarrow L_2(q)$, with $a'b' = b'a'$. We define $H := \langle b', c' \rangle \leqslant L_2(q)$. Then H is a dihedral group of order $q-1$. Now, the subgroups of $L_2(q)$ were determined by Dickson (see [Dic01]), and we have that H is a maximal subgroup of $L_2(q)$. Now $a' \notin H$, and so $\langle a', b', c' \rangle \cong L_2(q)$. Hence, for $q \equiv 3 \mod 4$ and $q > 11$, the group $L_2(q)$ has Property 4, and so has Property 2.

4.3 Dimension $n = 3$, $q \equiv 1 \mod 3$

In this section, we show that, for q odd, $q \equiv 1 \mod 3$, $L_3(q)$ has Property 1. We do so by showing that $SL_3(q)$ can be generated by suitable elements by following the method outlined in section 4.1. We work in the standard representation of $SL_3(q)$, i.e. 3×3 matrices acting on the space of column vectors of length 3. We call this vector space V. Note that in this case $SL_3(q)$ is not isomorphic to $L_3(q)$.

4.3.1 Generators

For $0 \neq \alpha \in \mathbb{F}_q$ and $\beta \in \mathbb{F}_q$, s.t. β is a primitive element (note that $\beta^{q-1} = 1$), we define:

$$a := \begin{pmatrix} \cdot & 1 & \cdot \\ 1 & \cdot & \cdot \\ \cdot & \cdot & -1 \end{pmatrix}$$

$$
\begin{aligned}
b &:= \begin{pmatrix} -1 & \cdot & \cdot \\ \cdot & -1 & \cdot \\ \alpha & \alpha\beta^{\frac{q-1}{6}} & 1 \end{pmatrix} \\
c &:= \begin{pmatrix} -1 & \cdot & \cdot \\ \cdot & \cdot & 1 \\ \cdot & 1 & \cdot \end{pmatrix} \\
d &:= \begin{pmatrix} -1 & \cdot & \cdot \\ \cdot & \cdot & \beta^{\frac{q-1}{3}} \\ \cdot & \beta^{2\frac{q-1}{3}} & \cdot \end{pmatrix} \\
e &:= \begin{pmatrix} \cdot & \beta^{5\frac{q-1}{6}} & \cdot \\ \beta^{\frac{q-1}{6}} & \cdot & \cdot \\ \alpha\beta^{\frac{q-1}{6}} & \alpha & -1 \end{pmatrix}
\end{aligned}
$$

Hence

$$
abcde = \begin{pmatrix} \beta^{\frac{q-1}{3}} & \cdot & \cdot \\ \cdot & \beta^{\frac{q-1}{3}} & \cdot \\ \cdot & \cdot & \beta^{\frac{q-1}{3}} \end{pmatrix}
$$

As a, b, c, d and e are involutions and there is only one conjugacy class of involutions in $SL_3(q)$, they are all conjugate. Also, under the natural homomorphism $SL_3(q) \longrightarrow L_3(q)$, $abcde$ maps to 1. We take $G := \langle a, b, c, d, e \rangle$.

4.3.2 Transvections and Root Subgroups

In this section, we show that the group G defined above contains two opposite transvections, and so from Lemma 4.1.11, G contains a root subgroup.

We have:

$$
\begin{aligned}
g &:= (ab)^2 \\
&= \begin{pmatrix} 1 & \cdot & \cdot \\ \cdot & 1 & \cdot \\ \alpha + \alpha\beta^{\frac{q-1}{6}} & \alpha + \alpha\beta^{\frac{q-1}{6}} & 1 \end{pmatrix} \\
&= I_3 + \begin{pmatrix} 0 \\ 0 \\ \alpha + \alpha\beta^{\frac{q-1}{6}} \end{pmatrix} \times 1 \times \begin{pmatrix} 1 & 1 & 0 \end{pmatrix}
\end{aligned}
$$

Hence we have, g, a one-dimensional transformation the values $a(g)$ and $c(g)$ given by:

$$
a(g) = \begin{pmatrix} 1 & 1 & 0 \end{pmatrix}
$$

$$c(g) = \begin{pmatrix} 0 \\ 0 \\ \alpha + \alpha\beta^{\frac{q-1}{6}} \end{pmatrix}$$

Now, by Lemma 4.1.6, g is a transvection as

$$a(g)\,c(g) = \begin{pmatrix} 1 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ \alpha + \alpha\beta^{\frac{q-1}{6}} \end{pmatrix} = 0$$

Now we want another transvection, h, such that h is opposite to g. From Lemma 4.1.10 g and h are opposite if, for $\gamma := a(g)\,c(h)$, and $\delta := a(h)\,c(g)$, we have $\gamma\delta \neq 0$. We also want $\gamma\delta$ to be a defining element of $\mathbb{F}_q$.

We take $h := g^c$. Since h is conjugate to g, h is a transvection. Now

$$\begin{aligned} h &= g^c \\ &= \begin{pmatrix} 1 & \cdot & \cdot \\ -\alpha - \alpha\beta^{\frac{q-1}{6}} & 1 & \alpha + \alpha\beta^{\frac{q-1}{6}} \\ \cdot & \cdot & 1 \end{pmatrix} \\ &= I_3 + \begin{pmatrix} 0 \\ -\alpha - \alpha\beta^{\frac{q-1}{6}} \\ 0 \end{pmatrix} \times 1 \times \begin{pmatrix} 1 & 0 & -1 \end{pmatrix} \end{aligned}$$

Hence h has values $a(h)$ and $c(h)$ given by:

$$\begin{aligned} a(h) &= \begin{pmatrix} 1 & 0 & -1 \end{pmatrix} \\ c(h) &= \begin{pmatrix} 0 \\ -\alpha - \alpha\beta^{\frac{q-1}{6}} \\ 0 \end{pmatrix} \end{aligned}$$

Now

$$\begin{aligned} \gamma\delta &= a(g)\,c(h)\,a(h)\,c(g) \\ &= \begin{pmatrix} 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ -\alpha - \alpha\beta^{\frac{q-1}{6}} \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ \alpha + \alpha\beta^{\frac{q-1}{6}} \end{pmatrix} \\ &= \left(-\alpha - \alpha\beta^{\frac{q-1}{6}}\right)\left(-\alpha - \alpha\beta^{\frac{q-1}{6}}\right) \\ &= \alpha^2\left(1 + \beta^{\frac{q-1}{6}}\right)^2 \end{aligned}$$

So if α is chosen such that $\alpha^2\left(1 + \beta^{\frac{q-1}{6}}\right)^2$ is a defining element of $\mathbb{F}_q$, we have, by Lemma 4.1.11, that $\langle g, h\rangle \leqslant G$ contains a root subgroup R.

4.3.3 Irreducibility

In this section we show that $H := \langle g \rangle^G = \langle R \rangle^G$ acts irreducibly on the vector space V. First we define the group $G_1 := \langle a, b, c \rangle$.

Lemma 4.3.1. *The group G_1 acts irreducibly on the vector space V if $\alpha\beta^{\frac{q-1}{6}} - \alpha \neq 2$.*

Proof. Let U be a G_1-invariant subspace. Let g be the transvection in G calculated in the last section, with values $a(g)$ and $c(g)$, defined as above.

So we have:

$a(g) = (1, 1, 0)$

$c(g) = \left(0, 0, \alpha + \alpha\beta^{\frac{q-1}{6}}\right)^T$

If there exists a vector $u \in U$ which does not lie on the axis of g, then by Lemma 4.1.18 we have that $c(g) \in U$, and since $\alpha \neq 0$ and $\beta^{\frac{q-1}{6}} \neq -1$, we have $u := (0, 0, 1)^T \in U$. Then we have:

$$\begin{aligned} w_1 &:= cu \\ &= (0, 1, 0)^T \in U \\ w_2 &:= aw_1 \\ &= (1, 0, 0)^T \in U \end{aligned}$$

The vectors u, w_1 and w_2 form a basis of V. Hence $U = V$.

So, we may assume that U is contained in the axis of g, i.e. if $u = (u_1, u_2, u_3)^T \in U$, then $u_1 + u_2 = 0$. We look at this dually, i.e. the homogeneous linear equations satisfied by all vectors of U are represented by rows of length 3, on which G_1 acts on the right. All such equations form a subspace, X, of ${}^3\mathbb{F}_q$. Since U is G_1-invariant, X is also.

We have $x := (1, 1, 0) \in X$. Then we have:

$$\begin{aligned} y_1 &:= xc \\ &= (-1, 0, 1) \in X \end{aligned}$$

$$\begin{aligned} y_2 &:= y_1 b \\ &= \left(1+\alpha, \alpha\beta^{\frac{q-1}{6}}, 1\right) \in X \end{aligned}$$

The vectors x, y_1 and y_2 form a basis of ${}^3\mathbb{F}_q$, as long as $\alpha\beta^{\frac{q-1}{6}} - \alpha \neq 2$. So, with these restrictions we have $X = {}^3\mathbb{F}_q$, and so $U = 0$.

Hence G_1 is irreducible if $\alpha\beta^{\frac{q-1}{6}} - \alpha \neq 2$. □

Then, as the group $G_1 = \langle a, b, c\rangle$ satisfies the conditions of Proposition 4.1.17, if $\alpha\beta^{\frac{q-1}{6}} - \alpha \neq 2$, the group $H_1 := \langle g\rangle^{G_1} = \langle R\rangle^{G_1}$ is irreducible, and so the group $H \geqslant H_1$ is also. Now, by the choice of H it is easy to see that it contains the group R defined in the last section. Thus, if the restrictions on α (from this section and from the previous section) are satisfied, we have that H is an irreducible group generated by Root subgroups.

4.3.4 Invariant Forms

There are no non-degenerate symplectic forms in dimension 3.

4.3.5 Equations

The only restrictions we have are that $q \equiv 1 \mod 3$, $\alpha^2\left(1+\beta^{\frac{q-1}{6}}\right)^2 \neq 0$ and is a defining element of $\mathbb{F}_q$ and $\alpha\beta^{\frac{q-1}{6}} - \alpha \neq 2$. Thus we have a polynomial, $\alpha^2\left(1+\beta^{\frac{q-1}{6}}\right)^2 \in \mathbb{F}_q[\alpha]$ of degree 2 over $\mathbb{F}_q$, for $q = p^k$ and $q \equiv 1 \mod 3$. We take the subset of $\mathbb{F}_q$, $X := \left\{\alpha \ : \ \alpha\beta^{\frac{q-1}{6}} - \alpha = 2\right\}$. Thus $|X| = 1$. From Lemma 4.1.23, one of values that $f(\alpha)$ assumes on $\mathbb{F}_q \backslash X$ is a defining element of $\mathbb{F}_q$ if one of the following hold:

1. $k = 1$ and $p > 3$;
2. $k = 2$ and $p > 2$;
3. $k = 3$ and $p \geqslant 2$;
4. $k \geqslant 4$ and $p \geqslant 2$;

These clearly hold for all q, $q = p^k$ and $q \equiv 1 \mod 3$. Hence for $q \equiv 1 \mod 3$, there exists an element $\alpha \in \mathbb{F}_q$ that satisfies the restrictions above.

4.3.6 Conclusion

We conclude this section by summarising the above.

Lemma 4.3.2. *For q odd and $q \equiv 1 \mod 3$, $\exists\ \alpha \in \mathbb{F}_q$ s.t. the elements a, b, c, d and e generate $SL_3(q)$, and so $L_3(q)$ has Property 1.*

Proof.

1. In section 4.3.1 we exhibited elements in $SL_3(q)$, a, b, c, d and e such that a, b, c, d and e are conjugate involutions in $SL_3(q)$. Under the natural homomorphism $SL_3(q) \longrightarrow L_3(q)$ they map to involutions a', b', c', d' and e' such that $a'b'c'd'e' = 1$. The elements are defined in terms of a variable $\alpha \in \mathbb{F}_q$. We called the group generated by these elements G.

2. In section 4.3.2 we demonstrated that there is a non-trivial transvection, in G, $g := (ab)^2$. We also demonstrated that the transvection $h := g^c \in G$ is opposite to g. Dickson's Lemma (Lemma 4.1.2) then gives us that G contains the whole root subgroup R, consisting of all transvections with the same centre and the same axis as g, subject to $\alpha^2 \left(1 + \beta^{\frac{q-1}{6}}\right)^2$ being a defining element of $\mathbb{F}_q$.

3. In section 4.3.3 we then considered a subgroup $G_1 := \langle a, b, c \rangle \leqslant G$, containing R, and the normal closure $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1} \trianglelefteq G_1$ of the root subgroup R in G_1. We have shown that the group G_1 is irreducible and so the group H_1 is also irreducible. Thus $H := \langle g \rangle^G = \langle R \rangle^G$ is irreducible, and so is an irreducible group generated by root subgroups. Thus from Lemma 4.1.1, H must coincide with $SL_3(q)$.

4. There are no non-degenerate symplectic forms in dimension 3. This implies that, when α satisfies the imposed restrictions, we have that

$G \trianglerighteq H = SL_3(q)$and hence, $G \cong SL_3(q)$.

5. Finally, in section 4.3.5 it was shown that there exists an α such that the restrictions on it can be satisfied.

□

4.4 Dimension $n = 3$, $q \equiv 0$ or $2 \mod 3$

In this section, we show that for $q \equiv 0$ or $2 \mod 3$, $L_3(q)$ does not have property 1, (and hence also does not have Property 2). Note that, in this case, $SL_3(q) \cong L_3(q)$, and so it is sufficient to show that for general q odd, $SL_3(q)$ does not have Property 1. We use Theorem 1.2.4.

Lemma 4.4.1. *When q is odd, the group $SL_3(q)$ does not have Property 1.*

Proof. Consider the Symmetric Square representation of the natural representation of $SL_3(q)$ over $\mathbb{F}_q$. This is an irreducible representation of $SL_3(q)$ of dimension 6. As we only have one conjugacy class of involutions to consider, an involution in this representation will be conjugate in $GL_6(q)$ to:

$$\begin{pmatrix} -1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & -1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix}$$

Thus in the language of Theorem 1.2.4, $n = 6$ and $d_i = 2$, $i = 1, 2, 3, 4, 5$. So we have:

$$d_1 + d_2 + d_3 + d_4 + d_5 = 10 < 12 = 2n.$$

Hence, we have that $SL_3(q)$ does not have Property 1. □

Hence, when $q \equiv 0$ or $2 \mod 3$ (and thus $L_3(q) \equiv SL_3(q)$), we have that $L_3(q)$ does not have Property 1.

We do note, however that for q odd and $q \equiv 0$ or $2 \mod 3$, $L_3(q) \equiv SL_3(q)$ can be generated by 6 conjugate involutions whose product is 1. From the discussion in chapter 1, it suffices to show that $SL_3(q)$ is $(2,3)$-generated, and it has been shown in [Gar78] and [Coh81] that $L_3(q)$ is $(2,3)$-generated for all odd q.

4.5 Dimension $n = 3$, Additional Notes

It is interesting to note at this stage that the following result holds:

Lemma 4.5.1. *For q odd, the groups $L_3(q)$ do not have Property 2.*

This was originally proved by Nuzhin in [Nuz97]. This was done by showing that any triple of elements in $SL_3(q)$, with the desired properties, either generate a reducible subgroup of $SL_3(q)$ or generate a subgroup of $SL_3(q)$ conjugate in $GL_3(q^4)$ to a subgroup of $\langle SO_3(q^4), \lambda I_3 \rangle$ with $\lambda^3 = 1$.

Now, for $q \equiv 0$ or $2 \mod 3$, this result is a corollary of Lemma 4.4.1. However, this result along with the results in section 4.3 gives us that $L_3(q)$ has Property 1, but not Property 2 for $q \equiv 1 \mod 3$.

4.6 Dimension $n = 4$

In this section, we show that, for q odd and $q \neq 9$, $L_4(q)$ has Property 2, and hence Property 1. We do so by showing that $SL_4(q)$ can be generated by suitable elements by following the method outlined in section 4.1. We work in the standard representation of $SL_4(q)$, i.e. 4×4 matrices acting on the space of column vectors of length 4. We call this vector space V.

4.6.1 Generators

We define:

$$
\begin{aligned}
a &:= \begin{pmatrix} \cdot & 1 & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \end{pmatrix} \\
b &:= \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & -1 & \cdot \\ \cdot & \cdot & \cdot & -1 \end{pmatrix} \\
c &:= \begin{pmatrix} \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot \\ 1 & \alpha & 1 & -1 \end{pmatrix} \text{ for some } 0 \neq \alpha \in \mathbb{F}_q \\
&\text{Hence} \\
ab &= \begin{pmatrix} \cdot & 1 & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & -1 \\ \cdot & \cdot & -1 & \cdot \end{pmatrix}
\end{aligned}
$$

As a, b, c and ab are all involutions with eigenvalues $\left\{(1)^2, (-1)^2\right\}$, from the properties of involutions, we can see that they are conjugate in $SL_4(q)$, and a and b commute. We take $G := \langle a, b, c \rangle$.

4.6.2 Transvections and Root Subgroups

In this section, we show that the group G defined above, contains two opposite transvections, and so from Lemma 4.1.11, G contains a root subgroup.

We have:

$$
\begin{aligned}
g &:= (bc)^4 \\
&= \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & -4\alpha & \cdot & 1 \end{pmatrix} \\
&= I_4 + \begin{pmatrix} 0 \\ 0 \\ 0 \\ -4\alpha \end{pmatrix} \times 1 \times \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix}
\end{aligned}
$$

Hence, g is a one-dimensional transformation, and has values $a(g)$ and $c(g)$ given by:

$$\begin{aligned} a(g) &= \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix} \\ c(g) &= \begin{pmatrix} 0 \\ 0 \\ 0 \\ -4\alpha \end{pmatrix} \end{aligned}$$

Thus, by Lemma 4.1.6, g is a transvection as

$$a(g)\,c(g) = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ 0 \\ -4\alpha \end{pmatrix} = 0$$

Now we want another transvection, h, such that h is opposite to g. From Lemma 4.1.10 g and h are opposite if, for $\gamma := a(g)\,c(h)$, and $\delta := a(h)\,c(g)$, we have $\gamma\delta \neq 0$. We also want $\gamma\delta$ to be a defining element of $\mathbb{F}_q$.

We take $h := g^k = k^{-1}gk$, where $k := (ac)^2$. Since h is conjugate to g, h is a transvection. Now

$$(ac)^2 = \begin{pmatrix} \cdot & \cdot & 1 & \cdot \\ 1 & \alpha & 1 & -1 \\ \cdot & 1+\alpha & 1+\alpha & -1 \\ \cdot & 1 & \cdot & \cdot \end{pmatrix} \text{ and}$$

$$(ca)^2 = \begin{pmatrix} \alpha & 1 & -1 & 1 \\ \cdot & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & \cdot \\ 1+\alpha & \cdot & -1 & 1+\alpha \end{pmatrix}.$$

Hence

$$\begin{aligned} h &:= k^{-1}gk \\ &= (ca)^2\, g\, (ac)^2 \\ &= \begin{pmatrix} 1-4\alpha & -4\alpha^2 & -4\alpha & 4\alpha \\ -4\alpha & 1-4\alpha^2 & -4\alpha & 4\alpha \\ \cdot & \cdot & 1 & \cdot \\ -4\alpha(1+\alpha) & -4\alpha^2(1+\alpha) & -4\alpha(1+\alpha) & 1+4\alpha(1+\alpha) \end{pmatrix} \\ &= I_4 + \begin{pmatrix} -4\alpha \\ -4\alpha \\ 0 \\ -4\alpha(1+\alpha) \end{pmatrix} \times 1 \times \begin{pmatrix} 1 & \alpha & 1 & -1 \end{pmatrix} \end{aligned}$$

Hence h has values $a(h)$ and $c(h)$ given by:

$$\begin{aligned} a(h) &= \begin{pmatrix} 1 & \alpha & 1 & -1 \end{pmatrix} \\ c(h) &= \begin{pmatrix} -4\alpha \\ -4\alpha \\ 0 \\ -4\alpha(1+\alpha) \end{pmatrix} \end{aligned}$$

Now

$$\begin{aligned} \gamma\delta &= a(g)\,c(h)\,a(h)\,c(g) \\ &= \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} -4\alpha \\ -4\alpha \\ 0 \\ -4\alpha(1+\alpha) \end{pmatrix} \begin{pmatrix} 1 & \alpha & 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ -4\alpha \end{pmatrix} \\ &= (-4\alpha) \times (4\alpha) \\ &= -16\alpha^2 \end{aligned}$$

So if α is chosen such that $-16\alpha^2$ is a defining element of $\mathbb{F}_q$, we have, by Lemma 4.1.11, that $\langle g, h \rangle \leqslant G$ contains a root subgroup R.

4.6.3 Irreducibility

In this section we show that $H := \langle g \rangle^G = \langle R \rangle^G$ acts irreducibly on the vector space V. First we define the group $G_1 := \langle b, c, (ac)^2 \rangle$.

Lemma 4.6.1. *The group G_1 acts irreducibly on the vector space V if $\alpha \neq -2$.*

Proof. Let U be a G_1-invariant subspace. Let g be the transvection in G calculated in the last section, with values $a(g)$ and $c(g)$, defined as above.

So we have:

$a(g) = (0, 1, 0, 0)$

$c(g) = (0, 0, 0, -4\alpha)^T$

If there exists a vector $u \in U$ which does not lie on the axis of g, then by Lemma 4.1.18 we have that $c(g) \in U$, and since $\alpha \neq 0$, we have $u := (0, 0, 0, 1)^T \in U$. Then we have:

$$w_1 := (ac)^2 u$$

$$
\begin{aligned}
&= (1,-1,-1,0)^T \in U \\
w_2 &:= cw_1 \\
&= (-1,-1,0,0)^T \in U \\
w_3 &:= (ac)^2 w_2 \\
&= (0,-1,0,0)^T \in U
\end{aligned}
$$

The vectors u, w_1, w_2 and w_3 form a basis of V. Hence $U = V$.

So, we may assume that U is contained in the axis of g, i.e. if $u = (u_1, u_2, u_3, u_4)^T \in U$, then $u_2 = 0$. We look at this dually, i.e. the homogeneous linear equations satisfied by all vectors of U are represented by rows of length 4, on which G_1 acts on the right. All such equations form a subspace, X, of ${}^4\mathbb{F}_q$. Since U is G_1-invariant, X is also.

We have $x := (0,1,0,0) \in X$. Then we have:

$$
\begin{aligned}
y_1 &:= x\,(ac)^2 \\
&= (1,\alpha,1,-1) \in X \\
y_2 &:= x\,(ca)^2 \\
&= (0,0,0,1) \in X \\
y_3 &:= x\,(ca)^4 \\
&= (1+\alpha,0,-1,1+\alpha) \in X
\end{aligned}
$$

The vectors x, y_1, y_2 and y_3 form a basis of ${}^4\mathbb{F}_q$, as long as $\alpha \neq -2$. So, with these restrictions we have $X = {}^4\mathbb{F}_q$, and so $U = 0$.

Hence G_1 is irreducible if $\alpha \neq -2$. □

Then, as the group $G_1 = \langle b, c, (ac)^2 \rangle$ satisfies the conditions of Proposition 4.1.17, if $\alpha \neq -2$, the group $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1}$ is irreducible, and so the group $H \geqslant H_1$ is also. Now, by the choice of H it is easy to see that it contains the group R defined in the last section. Thus, if the restrictions on α (from

this section and from the previous section) are satisfied, we have that H is an irreducible group generated by Root subgroups.

4.6.4 Invariant Forms

Lemma 4.6.2. *H does not preserve a non-degenerate symplectic form.*

Proof. We need to prove that there exists no non-degenerate symplectic form on V which is invariant under the action of G up to similarity. Let $\langle\ ,\ \rangle$ be a symplectic form on V that is preserved by G up to similarity. Then a,b and $c \in G$ preserve $\langle\ ,\ \rangle$ up to similarity with multipliers $\lambda(a)$, $\lambda(b)$ and $\lambda(c)$ respectively. Then, as a, b and c are involutions we have, from Lemma 4.1.20, $\lambda(a) = \pm 1$, $\lambda(b) = \pm 1$ and $\lambda(c) = \pm 1$.

Now we know that a, b, c and ab are conjugate in $SL_4(q)$, and from information in table 4.5.1 in [GLS98], we have that a, b, c and ab are conjugate in $GSp_4(q)$. Thus from Lemma 4.1.20, we have $\lambda(a) = \lambda(b) = \lambda(c) = \lambda(ab) = \lambda(a)\lambda(b)$, and so $\lambda(a) = \lambda(b) = \lambda(c) = 1$. Thus, as a, b and c generate G, for all $x \in G$, the multiplier for x, $\lambda(x)$ must be equal to 1, i.e. for all $x \in G$ and all u,$v \in V$, $\langle xu, xv\rangle = \langle u, v\rangle$.

So we have:

$$\begin{aligned}
\langle v_1, v_2\rangle &=_a \langle v_2, v_1\rangle \\
&= -\langle v_1, v_2\rangle, \text{ and so} \\
\langle v_1, v_2\rangle &= 0. \\
\langle v_1, v_3\rangle &=_b \langle v_1, -v_3\rangle \\
&= -\langle v_1, v_3\rangle, \text{ and so} \\
\langle v_1, v_3\rangle &= 0. \\
\langle v_1, v_4\rangle &=_b \langle v_1, -v_4\rangle \\
&= -\langle v_1, v_4\rangle, \text{ and so} \\
\langle v_1, v_4\rangle &= 0.
\end{aligned}$$

(4.6.1)

Hence we have $\langle v_1, v_i \rangle = 0 \forall i,\ 1 \leqslant i \leqslant n$. Thus, $v_1 \in V_\perp$ and so the form $\langle\ ,\ \rangle$ is degenerate.

Hence there is no non-degenerate symplectic form on V which is invariant under the action of G up to similarity, and so H does not preserve a non-degenerate symplectic form. □

Hence H cannot be conjugate to $Sp_4(q)$.

4.6.5 Equations

The only restrictions we have are that $q \neq 9$, $-16\alpha^2 \neq 0$ and is a defining element of $\mathbb{F}_q$ and $\alpha \neq -2$. Taking α to be any primitive element of $\mathbb{F}_q$ will satisfy these restrictions on α, since for $q > 3$ there is more than one primitive element in $\mathbb{F}_q$ and so we can take $\alpha \neq -2$, and for $q = 3$ we have $-2 = 1$ which is not a primitive element of $\mathbb{F}_3$.

1. $k = 1$ and $p > 3$;
2. $k = 2$ and $p > 2$;
3. $k = 3$ and $p \geqslant 2$;
4. $k \geqslant 4$ and $p \geqslant 2$;

Hence for $q \neq 9$, there exists an element $\alpha \in \mathbb{F}_q$ that satisfies these restrictions.

4.6.6 Conclusion

We conclude this section by summarising the above.

Lemma 4.6.3. *For q odd and $q \neq 9$, $\exists\ \alpha \in \mathbb{F}_q$ s.t. the elements a, b and c generate $SL_4(q)$, and so $L_4(q)$ has Property 2 and hence also has Property 1.*

Proof. 1. In section 4.6.1 we exhibited elements in $SL_4(q)$, a, b and c such that a and b commute and a, b, c and ab are conjugate involutions in $SL_4(q)$. Under the natural homomorphism $SL_4(q) \longrightarrow L_4(q)$ they map to involutions a', b' and c' such that a' and b' commute and a', b', c' and $a'b'$ are conjugate in $L_4(q)$. The elements are defined in terms of a variable $\alpha \in \mathbb{F}_q$. We called the group generated by these elements G.

2. In section 4.6.2 we demonstrated that there is a non-trivial transvection, in G, $g := (bc)^4$. We also demonstrated that the transvection $h := g^{(ac)^2} \in G$ is opposite to g. Dickson's Lemma (Lemma 4.1.2) then gives us that G contains the whole root subgroup R, consisting of all transvections with the same centre and the same axis as g, subject to $-16\alpha^2$ being a defining element of $\mathbb{F}_q$.

3. In section 4.6.3 we then considered a subgroup $G_1 := \left\langle b, c, (ac)^2 \right\rangle \leqslant G$, containing R, and the normal closure $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1} \trianglelefteq G_1$ of the root subgroup R in G_1. We have shown that the group G_1 is irreducible and so the group H_1 is also irreducible. Thus $H := \langle g \rangle^G = \langle R \rangle^G$ is irreducible, and so is an irreducible group generated by root subgroups. Thus from Lemma 4.1.1, H either coincides with $SL_4(q)$, or H is conjugate to $Sp_4(q)$.

4. In section 4.6.4 we excluded the symplectic case by showing that G does not preserve a non-degenerate symplectic form up to similarity. This implies that, when α satisfies the imposed restrictions, we have that $G \trianglerighteq H = SL_4(q)$and hence, $G \cong SL_4(q)$.

5. Finally, in section 4.6.5 it was shown that the there exists an α such that the restrictions on it can be satisfied.

□

4.7 Dimension $n = 5$

In this section, we show that, for q odd and $q \neq 9$, $L_5(q)$ has Property 2, and hence Property 1. We do so by showing that $SL_5(q)$ can be generated by suitable elements by following the method outlined in section 4.1. We work in the standard representation of $SL_5(q)$, i.e. 5×5 matrices acting on the space of column vectors of length 5. We call this vector space V.

4.7.1 Generators

We define:

$$a := \begin{pmatrix} \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & 1 & \cdot \end{pmatrix}$$

$$b := \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & -1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & -1 \end{pmatrix}$$

$$c := \begin{pmatrix} \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \alpha & -\alpha & \cdot & 1 \end{pmatrix} \text{ for some } 0 \neq \alpha \in \mathbb{F}_q$$

Hence

$$ab = \begin{pmatrix} \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & -1 \\ \cdot & \cdot & \cdot & -1 & \cdot \end{pmatrix}$$

As a, b, c and ab are all involutions with eigenvalues $\left\{(1)^3, (-1)^2\right\}$, from the properties of involutions, we can see that they are conjugate in $SL_5(q)$, and a and b commute. We take $G := \langle a, b, c \rangle$.

4.7.2 Transvections and Root Subgroups

In this section, we show that the group G defined above, contains two opposite transvections, and so from Lemma 4.1.11, G contains a root subgroup.

We have:

$$\begin{aligned} g &:= (bc)^4 \\ &= \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & 4\alpha & -4\alpha & \cdot & 1 \end{pmatrix} \\ &= I_5 + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 4\alpha \end{pmatrix} \times 1 \times \begin{pmatrix} 0 & 1 & -1 & 0 & 0 \end{pmatrix} \end{aligned}$$

Hence, g is a one-dimensional transformation, and has values $a(g)$ and $c(g)$ given by:

$$\begin{aligned} a(g) &= \begin{pmatrix} 0 & 1 & -1 & 0 & 0 \end{pmatrix} \\ c(g) &= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 4\alpha \end{pmatrix} \end{aligned}$$

Thus, by Lemma 4.1.6, g is a transvection as

$$a(g)\,c(g) = \begin{pmatrix} 0 & 1 & -1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 4\alpha \end{pmatrix} = 0$$

Now we want another transvection, h, such that h is opposite to g. From Lemma 4.1.10 g and h are opposite if, for $\gamma := a(g)\,c(h)$, and $\delta := a(h)\,c(g)$, we have $\gamma\delta \neq 0$. We also want $\gamma\delta$ to be a defining element of $\mathbb{F}_q$.

We take $h := g^k = k^{-1}gk$, where $k := (ac)^2$. Since h is conjugate to g, h is a transvection. Now

$$(ac)^2 = \begin{pmatrix} \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \alpha & -\alpha & \cdot & 1 \\ 1 & \cdot & \alpha & -\alpha & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot \end{pmatrix} \text{ and}$$

$$(ca)^2 = \begin{pmatrix} -\alpha & \alpha & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot \\ \alpha & \cdot & 1 & \cdot & -\alpha \end{pmatrix}.$$

Hence

$$\begin{aligned} h &:= k^{-1}gk \\ &= (ca)^2 g (ac)^2 \\ &= \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1-4\alpha^2 & 4\alpha^2 & 4\alpha & -4\alpha \\ \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & 4\alpha^3 & -4\alpha^3 & -4\alpha^2 & 1+4\alpha^2 \end{pmatrix} \\ &= I_5 + \begin{pmatrix} 0 \\ -4\alpha^2 \\ 0 \\ 0 \\ 4\alpha^3 \end{pmatrix} \times 1 \times \begin{pmatrix} 0 & 1 & -1 & -\frac{1}{\alpha} & \frac{1}{\alpha} \end{pmatrix} \end{aligned}$$

Hence h has values $a(h)$ and $c(h)$ given by:

$$\begin{aligned} a(h) &= \begin{pmatrix} 0 & 1 & -1 & -\frac{1}{\alpha} & \frac{1}{\alpha} \end{pmatrix} \\ c(h) &= \begin{pmatrix} 0 \\ -4\alpha^2 \\ 0 \\ 0 \\ 4\alpha^3 \end{pmatrix} \end{aligned}$$

Now

$$\gamma\delta = a(g)\, c(h)\, a(h)\, c(g)$$

$$
\begin{aligned}
&= \begin{pmatrix} 0 & 1 & -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ -4\alpha^2 \\ 0 \\ 0 \\ 4\alpha^3 \end{pmatrix} \begin{pmatrix} 0 & 1 & -1 & -\frac{1}{\alpha} & \frac{1}{\alpha} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 4\alpha \end{pmatrix} \\
&= \left(-4\alpha^2\right) \times (4) \\
&= -16\alpha^2
\end{aligned}
$$

So if α is chosen such that $-16\alpha^2$ is a defining element of $\mathbb{F}_q$, we have, by Lemma 4.1.11, that $\langle g, h \rangle \leqslant G$ contains a root subgroup R.

4.7.3 Irreducibility

In this section we show that $H := \langle g \rangle^G = \langle R \rangle^G$ acts irreducibly on the vector space V. First we define the group $G_1 := \langle b, c, (ac)^2 \rangle$.

Lemma 4.7.1. *The group G_1 acts irreducibly on the vector space V.*

Proof. Let U be a G_1-invariant subspace. Let g be the transvection in G calculated in the last section, with values $a(g)$ and $c(g)$, defined as above.

So we have:

$a(g) = (0, 1, -1, 0, 0)$

$c(g) = (0, 0, 0, 0, 4\alpha)^T$

If there exists a vector $u \in U$ which does not lie on the axis of g, then by Lemma 4.1.18 we have that $c(g) \in U$, and since $\alpha \neq 0$, we have $u := (0, 0, 0, 0, 1)^T \in U$. Then we have:

$$
\begin{aligned}
w_1 &:= (ac)^2 u \\
&= (0, 0, 1, 0, 0)^T \in U \\
w_2 &:= cw_1 + \alpha u \\
&= (0, 1, 0, 0, 0)^T \in U \\
w_3 &:= (ca)^2 w_2 \\
&= (\alpha, 0, 0, 1, 0)^T \in U
\end{aligned}
$$

$$\begin{aligned} w_4 &:= bw_3 \\ &= (\alpha, 0, 0, -1, 0)^T \in U \end{aligned}$$

The vectors u, w_1, w_2, w_3 and w_4 form a basis of V. Hence $U = V$.

So, we may assume that U is contained in the axis of g, i.e. if $u = (u_1, u_2, u_3, u_4, u_5)^T \in U$, then $u_2 - u_3 = 0$. We look at this dually, i.e. the homogeneous linear equations satisfied by all vectors of U are represented by rows of length 5, on which G_1 acts on the right. All such equations form a subspace, X, of ${}^5\mathbb{F}_q$. Since U is G_1-invariant, X is also.

We have $x := (0, 1, -1, 0, 0) \in X$. Then we have:

$$\begin{aligned} y_1 &:= x\,(ca)^2 \\ &= (-1, 0, 0, 0, 1) \in X \\ y_2 &:= y_1 b \\ &= (-1, 0, 0, 0, -1) \in X \\ y_3 &:= y_2\,(ac)^2 \\ &= (0, -1, -1, 0, 0) \in X \\ y_4 &:= x\,(ac)^2 \\ &= (0, -\alpha, \alpha, 1, -1) \in X \end{aligned}$$

The vectors x, y_1, y_2, y_3 and y_4 form a basis of ${}^5\mathbb{F}_q$, as long as $\alpha \neq 0$. So, with these restrictions we have $X = {}^5\mathbb{F}_q$, and so $U = 0$.

Hence G_1 is irreducible. □

Then, as the group $G_1 = \langle b, c, (ac)^2 \rangle$ satisfies the conditions of Proposition 4.1.17, and as $\alpha \neq 0$, the group $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1}$ is irreducible, and so the group $H \geqslant H_1$ is also. Now, by the choice of H it is easy to see that it contains the group R defined in the last section. Thus, if the restrictions on α from the previous section are satisfied, we have that H is an irreducible group generated by Root subgroups.

4.7.4 Invariant Forms

There are no non-degenerate symplectic forms in dimension 5.

4.7.5 Equations

The only restrictions we have are that $q \neq 9$ and $-16\alpha^2 \neq 0$ and is a defining element of $\mathbb{F}_q$. Taking α to be any primitive element of $\mathbb{F}_q$ will satisfy these restrictions on α. Hence for $q \neq 9$, there exists an element $\alpha \in \mathbb{F}_q$ that satisfies these restrictions.

4.7.6 Conclusion

We conclude this section by summarising the above.

Lemma 4.7.2. *For q odd and $q \neq 9$, $\exists\ \alpha \in \mathbb{F}_q$ s.t. the elements a, b and c generate $SL_5(q)$, and so $L_5(q)$ has Property 2 and hence also has Property 1.*

Proof.

1. In section 4.7.1 we exhibited elements in $SL_5(q)$, a, b and c such that a and b commute and a, b, c and ab are conjugate involutions in $SL_5(q)$. Under the natural homomorphism $SL_5(q) \longrightarrow L_5(q)$ they map to involutions a', b' and c' such that a' and b' commute and a', b', c' and $a'b'$ are conjugate in $L_5(q)$. The elements are defined in terms of a variable $\alpha \in \mathbb{F}_q$. We called the group generated by these elements G.

2. In section 4.7.2 we demonstrated that there is a non-trivial transvection, in G, $g := (bc)^4$. We also demonstrated that the transvection $h := g^{(ac)^2} \in G$ is opposite to g. Dickson's Lemma (Lemma 4.1.2) then gives us that G contains the whole root subgroup R, consisting of all transvections with the same center and the same axis as g, subject to $-16\alpha^2$ being a defining element of $\mathbb{F}_q$.

3. In section 4.7.3 we then considered a subgroup $G_1 := \left\langle b, c, (ac)^2 \right\rangle \leqslant G$, containing R, and the normal closure $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1} \trianglelefteq G_1$ of the

root subgroup R in G_1. We have shown that the group G_1 is irreducible and so the group H_1 is also irreducible. Thus $H := \langle g \rangle^G = \langle R \rangle^G$ is irreducible, and so is an irreducible group generated by root subgroups. Thus from Lemma 4.1.1, H must coincide with $SL_5(q)$.

4. There are no non-degenerate symplectic forms in dimension 5. This implies that, when α satisfies the imposed restrictions, we have that $G \trianglerighteq H = SL_5(q)$and hence, $G \cong SL_5(q)$.

5. Finally, in section 4.7.5 it was shown that the there exists an α such that the restrictions on it can be satisfied.

□

4.8 Dimension $n = 6$, $q \equiv 1 \mod 4$

In this section, we show that, for $q \equiv 1 \mod 4$ and $q \neq 9$, $L_6(q)$ has Property 2, and hence Property 1. We do so by showing that $SL_6(q)$ can be generated by suitable elements by following the method outlined in section 4.1. We work in the standard representation of $SL_6(q)$, i.e. 6×6 matrices acting on the space of column vectors of length 6. We call this vector space V. The question for other values of q are not dealt with in this Thesis.

4.8.1 Generators

We take $q \equiv 1 \mod 4$ and $q \neq 9$, and so $\exists\, i \in \mathbb{F}_q \; s.t. \; i^2 = -1$. The we define:

$$a := \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ -1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & -1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & -1 & \cdot \end{pmatrix}$$

$$b := \begin{pmatrix} \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & -1 & \cdot & \cdot & \cdot & \cdot \\ -1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & i & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & -i \end{pmatrix}$$

$$c := \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ -1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & -i & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & -1 & \cdot & \cdot \\ \alpha & i\alpha & \cdot & \alpha & i\alpha & i \end{pmatrix} \text{ for some } 0 \neq \alpha \in \mathbb{F}_q$$

Hence

$$ab = \begin{pmatrix} \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & -1 & \cdot & \cdot \\ -1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & -i \\ \cdot & \cdot & \cdot & \cdot & -i & \cdot \end{pmatrix}$$

As a, b, c and ab are conjugate in $SL_6(q)$, and map to involutions, a', b', c' and $a'b'$ in $L_6(q)$, we can see that a', b', c' and $a'b'$ are conjugate involutions in $L_6(q)$, and a' and b' commute. We take $G := \langle a, b, c \rangle$.

4.8.2 Transvections and Root Subgroups

In this section, we show that the group G defined above, contains two opposite transvections, and so from Lemma 4.1.11, G contains a root subgroup.

We have:

$$g := (bc)^5$$

$$= \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ 2\alpha - 2i\alpha & 2\alpha + 2i\alpha & 2\alpha - 2i\alpha & -2\alpha - 2i\alpha & 2\alpha - 2i\alpha & 1 \end{pmatrix}$$

$$= I_6 + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 2\alpha - 2i\alpha \end{pmatrix} \times 1 \times \begin{pmatrix} 1 & i & 1 & -i & 1 & 0 \end{pmatrix}$$

Hence, g is a one-dimensional transformation, and has values $a(g)$ and $c(g)$ given by:

$$a(g) = \begin{pmatrix} 1 & i & 1 & -i & 1 & 0 \end{pmatrix}$$

$$c(g) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 2\alpha - 2i\alpha \end{pmatrix}$$

Thus, by Lemma 4.1.6, g is a transvection as

$$a(g)\,c(g) = \begin{pmatrix} 1 & i & 1 & -i & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 2\alpha - 2i\alpha \end{pmatrix} = 0$$

Now we want another transvection, h, such that h is opposite to g. From Lemma 4.1.10 g and h are opposite if, for $\gamma := a(g)\,c(h)$, and $\delta := a(h)\,c(g)$, we have $\gamma\delta \neq 0$. We also want $\gamma\delta$ to be a defining element of $\mathbb{F}_q$.

We take $h := g^a = a^{-1}ga$. Since h is conjugate to g, h is a transvection. Now

$$h := g^a$$

$$= \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ 2\alpha + 2i\alpha & -2\alpha + 2i\alpha & -2\alpha - 2i\alpha & -2\alpha + 2i\alpha & 1 & -2\alpha + 2i\alpha \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix}$$

$$= I_6 + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2\alpha + 2i\alpha \\ 0 \end{pmatrix} \times 1 \times \begin{pmatrix} 1 & i & -1 & i & 0 & i \end{pmatrix}$$

Hence h has values $a(h)$ and $c(h)$ given by:

$$\begin{aligned} a(h) &= \begin{pmatrix} 1 & i & -1 & i & 0 & i \end{pmatrix} \\ c(h) &= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2\alpha + 2i\alpha \\ 0 \end{pmatrix} \end{aligned}$$

Now

$$\begin{aligned} \gamma\delta &= a(g)\, c(h)\, a(h)\, c(g) \\ &= \begin{pmatrix} 1 & i & 1 & -i & 1 & 0 \end{pmatrix} \cdots \\ &\quad \cdots \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 2\alpha + 2i\alpha \\ 0 \end{pmatrix} \begin{pmatrix} 1 & i & -1 & i & 0 & i \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 2\alpha - 2i\alpha \end{pmatrix} \\ &= 1 \times (2\alpha + 2i\alpha) \times i \times (2\alpha - 2i\alpha) \\ &= (2\alpha + 2i\alpha) \times (2\alpha + 2i\alpha) \\ &= 8i\alpha^2 \end{aligned}$$

So if α is chosen such that $8i\alpha^2$ is a defining element of $\mathbb{F}_q$, we have, by Lemma 4.1.11, that $\langle g, h \rangle \leqslant G$ contains a root subgroup R.

4.8.3 Irreducibility

In this section we show that $H := \langle g \rangle^G = \langle R \rangle^G$ acts irreducibly on the vector space V.

Lemma 4.8.1. *The group G acts irreducibly on the vector space V if $\alpha \neq i, -i$.*

Proof. Let U be a G-invariant subspace. Let g be the transvection in G calculated in the last section, with values $a(g)$ and $c(g)$, defined as above. Let us also assume that $\alpha \neq 0$ and $\alpha \neq i, -i$.

So we have:

$a(g) = (1, i, 1, -i, 1, 0)$

$c(g) = (0, 0, 0, 0, 0, 2\alpha + 2i\alpha)^T$

If there exists a vector $u \in U$ which does not lie on the axis of g, then by Lemma 4.1.18 we have that $c(g) \in U$, and since $\alpha \neq 0$ and $\alpha \neq i, -i$, we have $u := (0, 0, 0, 0, 0, 1)^T \in U$. Then we have:

$$\begin{aligned}
w_1 &:= au \\
&= (0, 0, 0, 0, 1, 0)^T \in U \\
w_2 &:= cw_1 \\
&= (0, 0, 0, 1, 0, i\alpha)^T \in U \\
w_3 &:= a(w_2 - i\alpha u) \\
&= (0, 0, 1, 0, 0, 0)^T \in U \\
w_4 &:= bw_3 \\
&= (0, 1, 0, 0, 0, 0)^T \in U \\
w_5 &:= aw_4 \\
&= (1, 0, 0, 0, 0, 0) \in U
\end{aligned}$$

The vectors u, w_1, w_2, w_3, w_4 and w_5 form a basis of V. Hence $U = V$.

So, we may assume that U is contained in the axis of g, i.e. if $u = (u_1, u_2, u_3, u_4, u_5, u_6)^T \in U$, then $u_1 + iu_2 + u_3 - iu_4 + u_5 = 0$. We look at this dually, i.e. the homogeneous linear equations satisfied by all vectors of U are represented by rows of length 6, on which G acts on the right. All such equations form a subspace, X, of ${}^6\mathbb{F}_q$. Since U is G-invariant, X is also.

We have $x := (1, i, 1, -i, 1, 0)^T \in X$. Then we have:

$$\begin{aligned}
y_1 &:= xac - (1 + i\alpha)\, x \\
&= (-2 + \alpha - i\alpha, -2i + i\alpha + \alpha, -i\alpha, i, 0, i) \in X \\
y_2 &:= ixa - y_1 \\
&= (3 - \alpha + i\alpha, 3i - i\alpha - \alpha, -1 + i\alpha, 0, 0, 0) \in X \\
y_3 &:= y_2 a + i y_2 \\
&= (0, 0, -i - \alpha, -1 + i\alpha, 0, 0) \in X \\
y_4 &:= (3i - i\alpha - \alpha)\, y_3 + (i + \alpha)\, y_2 b \\
&= (0, (1 - i\alpha)\,(i + \alpha)\,, 0, 0, 0, 0) \in X \\
y_5 &:= y_4 a \\
&= (-(1 - i\alpha)\,(i + \alpha)\,, 0, 0, 0, 0, 0) \in X
\end{aligned}$$

The vectors x, y_1, y_2, y_3, y_4 and y_5, form a basis of ${}^6\mathbb{F}_q$, as long as $\alpha \neq i, -i$. To see this is in fact a basis of ${}^6\mathbb{F}_q$ under these restrictions, we show here how to obtain the standard basis from these vectors:

$$\begin{aligned}
\frac{-1}{(1 - i\alpha)\,(i + \alpha)} y_5 &= (1, 0, 0, 0, 0, 0) = e_1^T \\
\frac{1}{(1 - i\alpha)\,(i + \alpha)} y_4 &= (0, 1, 0, 0, 0, 0) = e_2^T \\
\frac{1}{-1 + i\alpha}\left(y_2 - (3 - \alpha + i\alpha)\, e_1^T\right. & \\
\left. - (3i - i\alpha - \alpha)\, e_2^T\right) &= (0, 0, 1, 0, 0, 0) = e_3^T \\
\frac{1}{-1 + i\alpha}\left(y_3 + (i + \alpha)\, e_3^T\right) &= (0, 0, 0, 1, 0, 0) = e_4^T \\
x - e_1^T - i e_2^T - e_3^T + i e_4^T &= (0, 0, 0, 0, 1, 0) = e_5^T \\
-i\left(y_1 - (-2 + \alpha - i\alpha)\, e_1^T\right. & \\
\left. - (-2i + i\alpha + \alpha)\, e_2^T + i\alpha e_3^T - i e_4^T\right) &= (0, 0, 0, 0, 0, 1) = e_6^T
\end{aligned}$$

So, with these restrictions we have $X = {}^6\mathbb{F}_q$, and so $U = 0$.

Hence G_1 is irreducible if $\alpha \neq i, -i$. □

Then, as the group $G = \langle a, b, c \rangle$ satisfies the conditions of Proposition 4.1.17, if $\alpha \neq i, -i$, the group $H := \langle g \rangle = \langle R \rangle^G$ is irreducible. Now, by the choice of H it is easy to see that it contains the group R defined in the last section. Thus, if the restrictions on α (from this section and from the previous section) are satisfied, we have that H is an irreducible group generated by Root subgroups.

4.8.4 Invariant Forms

Lemma 4.8.2. *H does not preserve a non-degenerate symplectic form if either $1 + i\alpha - \alpha = 0$ or $-2i + 2\alpha + i\alpha \neq 0$.*

Proof. We need to prove that there exists no non-degenerate symplectic form on V which is invariant under the action of G up to similarity. Let $\langle\ ,\ \rangle$ be a symplectic form on V that is preserved by G up to similarity. Then a,b and $c \in G$ preserve $\langle\ ,\ \rangle$ up to similarity with multipliers $\lambda(a)$, $\lambda(b)$ and $\lambda(c)$ respectively. Then, as a, b and c are elements of order 4 we have, from Lemma 4.1.20, $\lambda(a)^4 = 1$, $\lambda(b)^4 = 1$ and $\lambda(c)^4 = 1$.

Now we know that a, b, c and ab are conjugate in $SL_6(q)$, and from information in table 4.5.1 in [GLS98], we have that a, b, c and ab are conjugate in $GSp_6(q)$. Thus from Lemma 4.1.20, we have $\lambda(a) = \lambda(b) = \lambda(c) = \lambda(ab) = \lambda(a)\lambda(b)$, and so $\lambda(a) = \lambda(b) = \lambda(c) = 1$. Thus, as a, b and c generate G, for all $x \in G$, the multiplier for x, $\lambda(x)$ must be equal to 1, i.e. for all $x \in G$ and all u,$v \in V$, $\langle xu, xv \rangle = \langle u, v \rangle$.

Now,

$$\begin{aligned}
\langle v_2, v_5 \rangle &=_c \langle v_1 + i\alpha v_6, v_4 + i\alpha v_6 \rangle \\
&= \langle v_1, v_4 \rangle + \langle v_1, i\alpha v_6 \rangle + \langle i\alpha v_6, v_4 \rangle + \langle i\alpha v_6, i\alpha v_6 \rangle \\
&= \langle v_1, v_4 \rangle + i\alpha \langle v_1, v_6 \rangle - i\alpha \langle v_4, v_6 \rangle \\
&=_a \langle v_1, v_4 \rangle + i\alpha \langle -v_2, v_5 \rangle - i\alpha \langle v_3, v_5 \rangle \\
&= \langle v_1, v_4 \rangle - i\alpha \langle v_2, v_5 \rangle - i\alpha \langle v_3, v_5 \rangle
\end{aligned}$$

$$
\begin{aligned}
=_b \quad & \langle v_1, v_4 \rangle - i\alpha \langle v_2, v_5 \rangle - i\alpha \langle v_2, iv_5 \rangle \\
= \quad & \langle v_1, v_4 \rangle - i\alpha \langle v_2, v_5 \rangle + \alpha \langle v_2, v_5 \rangle
\end{aligned}
$$

Hence

$$
\begin{aligned}
\langle v_1, v_4 \rangle &= \langle v_2, v_5 \rangle + i\alpha \langle v_2, v_5 \rangle - \alpha \langle v_2, v_5 \rangle \\
&= (1 - \alpha + i\alpha) \langle v_2, v_5 \rangle
\end{aligned}
$$

Now if $1 - \alpha + i\alpha = 0$, then,

$$
\langle v_1, v_4 \rangle = 0
$$

and so,

$$
\begin{aligned}
\langle v_2, v_3 \rangle &=_a \langle v_1, -v_4 \rangle \\
&= - \langle v_1, v_4 \rangle \\
&= 0
\end{aligned}
$$

Now,

$$
\begin{aligned}
0 &= \langle v_2, v_3 \rangle \\
&=_c \langle v_1 + i\alpha v_6, -iv_3 \rangle \\
&= -i \langle v_1, v_3 \rangle - \alpha \langle v_3, v_6 \rangle
\end{aligned}
$$

Hence,

$$
-i \langle v_1, v_3 \rangle = \alpha \langle v_3, v_6 \rangle
$$

Now,

$$
\begin{aligned}
\langle v_1, v_5 \rangle &=_c \langle -v_2 + \alpha v_6, v_4 + i\alpha v_6 \rangle \\
&= - \langle v_2, v_4 \rangle - i\alpha \langle v_2, v_6 \rangle - \alpha \langle v_4, v_6 \rangle
\end{aligned}
$$

and so,

$$
\langle v_2, v_4 \rangle = - \langle v_1, v_5 \rangle - i\alpha \langle v_2, v_6 \rangle - \alpha \langle v_4, v_6 \rangle
$$

$$
\begin{aligned}
=_a \quad & -\langle v_1, v_5\rangle - i\alpha\langle v_1, v_5\rangle - \alpha\langle v_4, v_6\rangle \\
=_b \quad & -\langle v_1, v_5\rangle - i\alpha\langle v_1, v_5\rangle - \alpha\langle v_1, -iv_6\rangle \\
= \quad & -\langle v_1, v_5\rangle - i\alpha\langle v_1, v_5\rangle + i\alpha\langle v_1, v_6\rangle \\
=_c \quad & -\langle v_1, v_5\rangle - i\alpha\langle v_1, v_5\rangle + i\alpha\langle -v_2 + \alpha v_6, iv_6\rangle \\
= \quad & -\langle v_1, v_5\rangle - i\alpha\langle v_1, v_5\rangle + \alpha\langle v_2, v_6\rangle \\
=_a \quad & -\langle v_1, v_5\rangle - i\alpha\langle v_1, v_5\rangle + \alpha\langle v_1, v_5\rangle \\
= \quad & (-1 - i\alpha + \alpha)\langle v_1, v_5\rangle \\
= \quad & 0
\end{aligned}
$$

Hence,

$$
\begin{aligned}
\langle v_1, v_3\rangle \quad =_a \quad & \langle v_2, v_4\rangle \\
= \quad & 0
\end{aligned}
$$

Now,

$$
\begin{aligned}
\langle v_5, v_6\rangle \quad =_c \quad & \langle v_4 + i\alpha v_6, iv_6\rangle \\
= \quad & i\langle v_4, v_6\rangle \\
=_a \quad & i\langle v_3, v_5\rangle \\
=_b \quad & i\langle v_2, iv_5\rangle \\
= \quad & -\langle v_2, v_5\rangle \\
=_a \quad & -\langle v_1, -v_6\rangle \\
= \quad & \langle v_1, v_6\rangle \\
=_c \quad & \langle -v_2 + \alpha v_6, iv_6\rangle \\
= \quad & -i\langle v_2, v_6\rangle \\
=_b \quad & -i\langle -v_3, -iv_6\rangle \\
= \quad & \langle v_3, v_6\rangle \\
= \quad & -\frac{i}{\alpha}\langle v_1, v_3\rangle
\end{aligned}
$$

$$= \quad 0$$

and

$$\begin{aligned}
\langle v_1, v_5 \rangle &=_b \langle -v_4, iv_5 \rangle \\
&= -i \langle v_4, v_5 \rangle \\
&=_a -i \langle v_3, -v_6 \rangle \\
&= i \langle v_3, v_6 \rangle \\
&= \frac{1}{\alpha} \langle v_1, v_3 \rangle \\
&= 0
\end{aligned}$$

Hence

$$\begin{aligned}
\langle v_1, v_2 \rangle &=_b \langle -v_4, v_3 \rangle \\
&= \langle v_3, v_4 \rangle \\
&=_c \langle -iv_3, -v_5 + \alpha v6 \rangle \\
&= i \langle v_3, v_5 \rangle - i\alpha \langle v_3, v_6 \rangle \\
&= 0
\end{aligned}$$

Hence, $\langle v_i, v_j \rangle = 0 \; \forall \; 1 \leqslant i, j \leqslant 6$.

Now assume that $1 + i\alpha - \alpha \neq 0$.

Then we have

$$\begin{aligned}
\langle v_1, v_5 \rangle &=_c \langle -v_2 + \alpha v_6, v_4 + i\alpha v_6 \rangle \\
&= -\langle v_2, v_4 \rangle - i\alpha \langle v_2, v_6 \rangle - \alpha \langle v_4, v_6 \rangle \\
&=_a -\langle v_2, v_4 \rangle - i\alpha \langle v_1, v_5 \rangle - \alpha \langle v_4, v_6 \rangle \\
&=_b -\langle v_2, v_4 \rangle - i\alpha \langle v_1, v_5 \rangle - \alpha \langle v_1, -iv_6 \rangle \\
&= -\langle v_2, v_4 \rangle - i\alpha \langle v_1, v_5 \rangle + i\alpha \langle v_1, v_6 \rangle \\
&=_c -\langle v_2, v_4 \rangle - i\alpha \langle v_1, v_5 \rangle + i\alpha \langle -v_2 + \alpha v_6, iv_6 \rangle \\
&= -\langle v_2, v_4 \rangle - i\alpha \langle v_1, v_5 \rangle + \alpha \langle v_2, v_6 \rangle
\end{aligned}$$

$$
\begin{aligned}
&=_a && -\langle v_2, v_4\rangle - i\alpha \langle v_1, v_5\rangle + \alpha \langle v_1, v_5\rangle \\
(1 + i\alpha - \alpha)\langle v_1, v_5\rangle &= && -\langle v_2, v_4\rangle \\
\langle v_1, v_5\rangle &= && \frac{-1}{1 + i\alpha - \alpha}\langle v_2, v_4\rangle
\end{aligned}
$$

and

$$
\begin{aligned}
\langle v_1, v_3\rangle &=_c && \langle -v_2 + \alpha v_6, -iv_3\rangle \\
&= && i\langle v_2, v_3\rangle + i\alpha \langle v_3, v_6\rangle \\
&=_a && i\langle v_1, -v_4\rangle + i\alpha \langle v_3, v_6\rangle \\
&= && -i\langle v_1, v_4\rangle + i\alpha \langle v_3, v_6\rangle \\
&= && -i(1 + i\alpha - \alpha)\langle v_2, v_5\rangle + i\alpha \langle v_3, v_6\rangle \\
&=_a && -i(1 + i\alpha - \alpha)\langle v_1, -v_6\rangle + i\alpha \langle v_3, v_6\rangle \\
&= && i(1 + i\alpha - \alpha)\langle v_1, v_6\rangle + i\alpha \langle v_3, v_6\rangle \\
&=_c && i(1 + i\alpha - \alpha)\langle -v_2 + \alpha v_6, iv_6\rangle + i\alpha \langle v_3, v_6\rangle \\
&= && (1 + i\alpha - \alpha)\langle v_2, v_6\rangle + i\alpha \langle v_3, v_6\rangle \\
&=_b && (1 + i\alpha - \alpha)\langle -v_3, -iv_6\rangle + i\alpha \langle v_3, v_6\rangle \\
&= && i(1 + i\alpha - \alpha)\langle v_3, v_6\rangle + i\alpha \langle v_3, v_6\rangle \\
&= && (i - \alpha)\langle v_3, v_6\rangle
\end{aligned}
$$

Also we have

$$
\begin{aligned}
\langle v_1, v_3\rangle &=_a && \langle -v_2, -v_4\rangle \\
&= && \langle v_2, v_4\rangle \\
&= && (-1 - i\alpha + \alpha)\langle v_1, v_5\rangle \\
&=_b && (-1 - i\alpha + \alpha)\langle -v_4, iv_5\rangle \\
&= && i(1 + i\alpha - \alpha)\langle v_4, v_5\rangle \\
&=_a && i(1 + i\alpha - \alpha)\langle v_3, -v_6\rangle \\
&= && -i(1 + i\alpha - \alpha)\langle v_3, v_6\rangle
\end{aligned}
$$

Hence we have $(i-\alpha)\langle v_3, v_6\rangle = \langle v_1, v_3\rangle = -i(1+i\alpha-\alpha)\langle v_3, v_6\rangle$.

Hence if $\langle v_3, v_6\rangle \neq 0$ then, $(i-\alpha) = -i(1+i\alpha-\alpha)$ which implies that $-2i+2\alpha+i\alpha = 0$.

Hence if $-2i+2\alpha+i\alpha \neq 0$ then $\langle v_3, v_6\rangle = 0$.

Now if $\langle v_3, v_6\rangle = 0$, we have, similar to the above, $\langle v_i, v_j\rangle = 0 \forall 1 \leqslant i, j \leqslant 6$.

Hence under the restrictions above, there is no non-degenerate symplectic form on V which is invariant under the action of G up to similarity, and so H does not preserve a non-degenerate symplectic form. □

Hence if the restrictions in the above lemma hold, then H cannot be conjugate to $Sp_6(q)$.

4.8.5 Equations

The only restrictions we have are that $q \neq 9$, $q \equiv 1 \mod 4$, $8i\alpha^2 \neq 0$ and is a defining element of $\mathbb{F}_q$, $\alpha \neq i, -i$ and that either $1+i\alpha-\alpha = 0$ or $-2i+2\alpha+i\alpha \neq 0$. Thus we have a polynomial, $8i\alpha^2 \in \mathbb{F}_q[\alpha]$ of degree 2 over $\mathbb{F}_q$, for $q = p^k$, $q \equiv 1 \mod 4$ and $q \neq 9$. Also, we require that $\alpha \neq i, -i$ and that either $1+i\alpha-\alpha = 0$ or $-2i+2\alpha+i\alpha \neq 0$, so we take X to be the subset of $\mathbb{F}_q$ that contains the elements, α, s.t. $\alpha = i, -i$ or $-2i+2\alpha+i\alpha = 0$. Thus $|X| \leqslant 3$. From Lemma 4.1.23, one of values that $f(\alpha)$ assumes on $\mathbb{F}_q \backslash X$ is a defining element of $\mathbb{F}_q$ if one of the following hold:

1. $k = 1$ and $p > 5$;
2. $k = 2$ and $p > 3$;
3. $k = 3$ and $p \geqslant 3$;
4. $k \geqslant 4$ and $p \geqslant 2$;

These clearly hold for all $q \equiv 1 \mod 4$, $q = p^k$ and $q \neq 5, 9$. Now for $q = 5$, if we take $\alpha = -1$, then $8i\alpha^2 \neq 0$ and so is a defining element of $\mathbb{F}_q$. Also

$\alpha \neq i, -i$ and $1 + i\alpha - \alpha = 0$. Hence for $q \equiv 1 \mod 4$, $q \neq 9$, there exists an element $\alpha \in \mathbb{F}_q$ that satisfies the restrictions above.

4.8.6 Conclusion

We conclude this section by summarising the above.

Lemma 4.8.3. *For $q \equiv 1 \mod 4$ and $q \neq 9$, $\exists\ \alpha \in \mathbb{F}_q$ s.t. the elements a, b and c generate $SL_6(q)$, and so $L_6(q)$ has Property 2 and hence also has Property 1.*

Proof.

1. In section 4.8.1 we exhibited elements in $SL_6(q)$, a, b and c. Under the natural homomorphism $SL_6(q) \longrightarrow L_6(q)$ they map to involutions a', b' and c' such that a' and b' commute and a', b', c' and $a'b'$ are conjugate in $L_6(q)$. The elements are defined in terms of a variable $\alpha \in \mathbb{F}_q$. We called the group generated by these elements G.

2. In section 4.8.2 we demonstrated that there is a non-trivial transvection, in G, $g := (bc)^5$. We also demonstrated that the transvection $h := g^a \in G$ is opposite to g. Dickson's Lemma (Lemma 4.1.2) then gives us that G contains the whole root subgroup R, consisting of all transvections with the same center and the same axis as g, subject to $8i\alpha^2$ being a defining element of $\mathbb{F}_q$.

3. In section 4.8.3 we then considered the normal closure $H := \langle g \rangle^G = \langle R \rangle^G \trianglelefteq G$ of the root subgroup R in G. We have shown that the group G is irreducible and so the group H is also irreducible, under the restriction that $\alpha \neq 0, i, -i$. Thus $H := \langle g \rangle^G = \langle R \rangle^G$ is irreducible, and so is an irreducible group generated by root subgroups. Thus from Lemma 4.1.1, H either coincides with $SL_6(q)$, or H is conjugate to $Sp_6(q)$.

4. In section 4.8.4 we excluded the symplectic case by showing that G does not preserve a non-degenerate symplectic form up to similarity. This

implies that, when α satisfies the imposed restrictions, we have that $G \trianglerighteq H = SL_6(q)$and hence, $G \cong SL_6(q)$.

5. Finally, in section 4.8.5 it was shown that the there exists an α such that the restrictions on it can be satisfied.

□

4.9 Dimension $n = 7$

In this section, we show that, for q odd and $q \neq 9$, $L_7(q)$ has Property 2, and hence Property 1. We do so by showing that $SL_7(q)$ can be generated by suitable elements by following the method outlined in section 4.1. We work in the standard representation of $SL_7(q)$, i.e. 7×7 matrices acting on the space of column vectors of length 7. We call this vector space V.

4.9.1 Generators

We define:

$$a := \begin{pmatrix} \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & -1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \end{pmatrix}$$

$$b := \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & -1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 \end{pmatrix}$$

$$c := \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \alpha & \alpha & \cdot & \cdot & -1 \end{pmatrix} \text{ for some } 0 \neq \alpha \in \mathbb{F}_q$$

Hence

$$ab = \begin{pmatrix} \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & -1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & -1 & \cdot \end{pmatrix}$$

As a, b, c and ab are all involutions with eigenvalues $\left\{(1)^3, (-1)^4\right\}$, from the properties of involutions, we can see that they are conjugate in $SL_7(q)$, and a and b commute. We take $G := \langle a, b, c \rangle$.

4.9.2 Transvections and Root Subgroups

In this section, we show that the group G defined above, contains two opposite transvections, and so from Lemma 4.1.11, G contains a root subgroup.

We have:

$$g := (bc)^8$$

$$= \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & -8\alpha & -8\alpha & \cdot & \cdot & 1 \end{pmatrix}$$

$$= I_7 + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -8\alpha \end{pmatrix} \times 1 \times \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Hence, g is a one-dimensional transformation, and has values $a(g)$ and $c(g)$ given by:

$$\begin{aligned} a(g) &= \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \\ c(g) &= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -8\alpha \end{pmatrix} \end{aligned}$$

Thus, by Lemma 4.1.6, g is a transvection as

$$\begin{aligned} a(g)\,c(g) &= \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -8\alpha \end{pmatrix} \\ &= 0 \end{aligned}$$

Now we want another transvection, h, such that h is opposite to g. From Lemma 4.1.10 g and h are opposite if, for $\gamma := a(g)\,c(h)$, and $\delta := a(h)\,c(g)$, we have $\gamma\delta \neq 0$. We also want $\gamma\delta$ to be a defining element of $\mathbb{F}_q$.

We take $h := g^k = k^{-1}gk$, where $k := (ac)^2$. Since h is conjugate to g, h is a transvection. Now

$$(ac)^2 = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & -1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \alpha & \alpha & \cdot & \cdot & -1 \\ \cdot & \cdot & \cdot & -1 & \cdot & \cdot & \cdot \\ -1 & \cdot & \cdot & \cdot & \alpha & \alpha & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \end{pmatrix} \text{ and}$$

$$(ca)^2 = \begin{pmatrix} \alpha & \alpha & \cdot & \cdot & \cdot & -1 & \cdot \\ \cdot & \cdot & -1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & -1 & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & -1 & -\alpha & \cdot & \alpha \end{pmatrix}.$$

Hence

$$\begin{aligned} h &:= k^{-1}gk \\ &= (ca)^2 g (ac)^2 \\ &= \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 8\alpha & 1-8\alpha^2 & -8\alpha^2 & \cdot & \cdot & 8\alpha \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & 8\alpha^2 & -8\alpha^3 & -8\alpha^3 & \cdot & \cdot & 1+8\alpha^2 \end{pmatrix} \\ &= I_7 + \begin{pmatrix} 0 \\ 0 \\ 8\alpha \\ 0 \\ 0 \\ 0 \\ 8\alpha^2 \end{pmatrix} \times 1 \times \begin{pmatrix} 0 & 1 & -\alpha & -\alpha & 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

Hence h has values $a(h)$ and $c(h)$ given by:

$$\begin{aligned} a(h) &= \begin{pmatrix} 0 & 1 & -\alpha & -\alpha & 0 & 0 & 1 \end{pmatrix} \\ c(h) &= \begin{pmatrix} 0 \\ 0 \\ 8\alpha \\ 0 \\ 0 \\ 0 \\ 8\alpha^2 \end{pmatrix} \end{aligned}$$

Now

$$\begin{aligned} \gamma\delta &= a(g)\, c(h)\, a(h)\, c(g) \\ &= \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \cdots \end{aligned}$$

$$
\begin{aligned}
& \cdots \begin{pmatrix} 0 \\ 0 \\ 8\alpha \\ 0 \\ 0 \\ 0 \\ 8\alpha^2 \end{pmatrix} \begin{pmatrix} 0 & 1 & -\alpha & -\alpha & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -8\alpha \end{pmatrix} \\
= \; & (8\alpha) \times (-8\alpha) \\
= \; & -64\alpha^2
\end{aligned}
$$

So if α is chosen such that $-64\alpha^2$ is a defining element of $\mathbb{F}_q$, we have, by Lemma 4.1.11, that $\langle g, h \rangle \leqslant G$ contains a root subgroup R.

4.9.3 Irreducibility

In this section we show that $H := \langle g \rangle^G = \langle R \rangle^G$ acts irreducibly on the vector space V. First we define the group $G_1 := \langle b, c, (ac)^2 \rangle$.

Lemma 4.9.1. *The group G_1 acts irreducibly on the vector space V.*

Proof. Let U be a G_1-invariant subspace. Let g be the transvection in G calculated in the last section, with values $a(g)$ and $c(g)$, defined as above.

So we have:

$a(g) = (0, 0, 1, 1, 0, 0, 0)$

$c(g) = (0, 0, 0, 0, 0, 0, -8\alpha)^T$

If there exists a vector $u \in U$ which does not lie on the axis of g, then by Lemma 4.1.18 we have that $c(g) \in U$, and since $\alpha \neq 0$, we have $u := (0, 0, 0, 0, 0, 0, 1)^T \in U$. Then we have:

$$
\begin{aligned}
w_1 &:= (ac)^2 u \\
&= (0, 0, 0, -1, 0, 0, 0)^T \in U \\
w_2 &:= bw_1 \\
&= (0, 0, -1, 0, 0, 0, 0)^T \in U \\
w_3 &:= (ca)^2 u_2
\end{aligned}
$$

$$
\begin{aligned}
&= (0,1,0,0,0,0,0)^T \in U \\
w_4 &:= bw_3 \\
&= (1,0,0,0,0,0,0)^T \in U \\
w_5 &:= cw_3 \\
&= (0,0,0,0,1,0,0)^T \in U \\
w_6 &:= cw_4 \\
&= (0,0,0,0,0,1,0)^T \in U
\end{aligned}
$$

The vectors u, w_1, w_2, w_3, w_4, w_5 and w_6 form a basis of V. Hence $U = V$.

So, we may assume that U is contained in the axis of g, i.e. if $u = (u_1, u_2, u_3, u_4, u_5, u_6, u_7)^T \in U$, then $u_3 + u_4 = 0$. We look at this dually, i.e. the homogeneous linear equations satisfied by all vectors of U are represented by rows of length 5, on which G_1 acts on the right. All such equations form a subspace, X, of ${}^7\mathbb{F}_q$. Since U is G_1-invariant, X is also.

We have $x := (0,0,1,1,0,0,0) \in X$. Then we have:

$$
\begin{aligned}
y_1 &:= x\,(ca)^2 \\
&= (0,0,0,0,-1,0,1) \in X \\
y_2 &:= y_1 b \\
&= (0,0,0,0,-1,0,-1) \in X \\
y_3 &:= y_1 c - \alpha x \\
&= (0,-1,0,0,0,0,-1) \in X \\
y_4 &:= y_3 b \\
&= (-1,0,0,0,0,0,1) \in X \\
y_5 &:= y_4 c - \alpha x \\
&= (0,0,0,0,0,-1,-1) \in X \\
y_6 &:= y_2\,(ac)^2 \\
&= (0,0,-1,1,0,0,0) \in X
\end{aligned}
$$

The vectors x, y_1, y_2, y_3, y_4, y_5 and y_6 form a basis of ${}^7\mathbb{F}_q$, as long as $\alpha \neq 0$. So, with these restrictions we have $X = {}^7\mathbb{F}_q$, and so $U = 0$.

Hence G_1 is irreducible. □

Then, as the group $G_1 = \langle b, c, (ac)^2 \rangle$ satisfies the conditions of Proposition 4.1.17, an as $\alpha \neq 0$, the group $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1}$ is irreducible, and so the group $H \geqslant H_1$ is also. Now, by the choice of H it is easy to see that it contains the group R defined in the last section. Thus, if the restrictions on α from the previous section are satisfied, we have that H is an irreducible group generated by Root subgroups.

4.9.4 Invariant Forms

There are no non-degenerate symplectic forms in dimension 7.

4.9.5 Equations

The only restrictions we have are that $q \neq 9$ and $-64\alpha^2 \neq 0$ and is a defining element of $\mathbb{F}_q$. Taking α to be any primitive element of $\mathbb{F}_q$ will satisfy these restrictions on α. Hence for $q \neq 9$, there exists an element $\alpha \in \mathbb{F}_q$ that satisfies these restrictions.

4.9.6 Conclusion

We conclude this section by summarising the above.

Lemma 4.9.2. *For q odd and $q \neq 9$, $\exists\ \alpha \in \mathbb{F}_q$ s.t. the elements a, b and c generate $SL_7(q)$, and so $L_7(q)$ has Property 2 and hence also has Property 1.*

Proof. 1. In section 4.9.1 we exhibited elements in $SL_7(q)$, a, b and c such that a and b commute and a, b, c and ab are conjugate involutions in $SL_7(q)$. Under the natural homomorphism $SL_7(q) \longrightarrow L_7(q)$ they map to involutions a', b' and c' such that a' and b' commute and a', b', c'

and $a'b'$ are conjugate in $L_7(q)$. The elements are defined in terms of a variable $\alpha \in \mathbb{F}_q$. We called the group generated by these elements G.

2. In section 4.9.2 we demonstrated that there is a non-trivial transvection, in G, $g := (bc)^4$. We also demonstrated that the transvection $h := g^{(ac)^2} \in G$ is opposite to g. Dickson's Lemma (Lemma 4.1.2) then gives us that G contains the whole root subgroup R, consisting of all transvections with the same centre and the same axis as g, subject to $-64\alpha^2$ being a defining element of $\mathbb{F}_q$.

3. In section 4.9.3 we then considered a subgroup $G_1 := \left\langle b, c, (ac)^2 \right\rangle \leqslant G$, containing R, and the normal closure $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1} \trianglelefteq G_1$ of the root subgroup R in G_1. We have shown that the group G_1 is irreducible and so the group H_1 is also irreducible. Thus $H := \langle g \rangle^G = \langle R \rangle^G$ is irreducible, and so is an irreducible group generated by root subgroups. Thus from Lemma 4.1.1, H must coincide with $SL_7(q)$.

4. There are no non-degenerate symplectic forms in dimension 7. This implies that, when α satisfies the imposed restrictions, we have that $G \trianglerighteq H = SL_7(q)$and hence, $G \cong SL_7(q)$.

5. Finally, in section 4.9.5 it was shown that the there exists an α such that the restrictions on it can be satisfied.

□

4.10 Dimension $n = 8$

In this section, we show that, for q odd and $q \neq 9$, $L_8(q)$ has Property 2, and hence Property 1. We do so by showing that $SL_8(q)$ can be generated by suitable elements by following the method outlined in section 4.1. We work in the standard representation of $SL_8(q)$, i.e. 8×8 matrices acting on the space of column vectors of length 8. We call this vector space V.

4.10.1 Generators

We define:

$$a := \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \end{pmatrix}$$

$$b := \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & -1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & -1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 \end{pmatrix}$$

$$c := \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \alpha & 1 & \cdot & \cdot & -1 \end{pmatrix} \text{ for some } 0 \neq \alpha \in \mathbb{F}_q$$

Hence

$$ab = \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & -1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & -1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & -1 & \cdot \end{pmatrix}$$

As a, b, c and ab are all involutions with eigenvalues $\left\{(1)^4, (-1)^4\right\}$, from the properties of involutions, we can see that they are conjugate in $SL_8(q)$, and a and b commute. We take $G := \langle a, b, c \rangle$.

4.10.2 Transvections and Root Subgroups

In this section, we show that the group G defined above, contains two opposite transvections, and so from Lemma 4.1.11, G contains a root subgroup.

We have:

$$\begin{aligned} g &:= (bc)^4 \\ &= \begin{pmatrix} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & -4\alpha & \cdot & \cdot & \cdot & 1 \end{pmatrix} \\ &= I_8 + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -4\alpha \end{pmatrix} \times 1 \times \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

Hence, g is a one-dimensional transformation, and has values $a(g)$ and $c(g)$ given by:

$$\begin{aligned} a(g) &= \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \\ c(g) &= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -4\alpha \end{pmatrix} \end{aligned}$$

Thus, by Lemma 4.1.6, g is a transvection as

$$a(g)\,c(g) \;=\; \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -4\alpha \end{pmatrix} \;=\; 0$$

Now we want another transvection, h, such that h is opposite to g. From Lemma 4.1.10 g and h are opposite if, for $\gamma := a(g)\,c(h)$, and $\delta := a(h)\,c(g)$, we have $\gamma\delta \neq 0$. We also want $\gamma\delta$ to be a defining element of $\mathbb{F}_q$.

We take $h := g^k = k^{-1}gk$, where $k := (ac)^4$. Since h is conjugate to g, h is a transvection. Now

$$(ac)^4 \;=\; \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \alpha & \cdot & \cdot & 1 & -1 & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & 1 & \alpha & 1 & \cdot & \cdot & -1 \\ -1 & 1 & \cdot & 1 & \alpha & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \alpha & 1 & \cdot & \alpha & -1 \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \end{pmatrix} \text{ and}$$

$$(ca)^4 \;=\; \begin{pmatrix} \alpha & \cdot & \cdot & \cdot & -1 & 1 & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \alpha & 1 & \cdot & 1 & -1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & -1 & 1 & \cdot & \cdot & \alpha & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \alpha & \cdot & \cdot & 1 & -1 & \alpha \end{pmatrix}$$

Hence

$$\begin{aligned} h \;&:=\; k^{-1}gk \\ &=\; (ca)^4\, g\, (ac)^4 \end{aligned}$$

$$
\begin{aligned}
&= \begin{pmatrix}
1 & \cdot & -4\alpha & -4\alpha^2 & -4\alpha & \cdot & \cdot & 4\alpha \\
\cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & -4\alpha & 1-4\alpha^2 & -4\alpha & \cdot & \cdot & 4\alpha \\
\cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\
\cdot & \cdot & -4\alpha^2 & -4\alpha^3 & -4\alpha^2 & \cdot & \cdot & 1+4\alpha^2
\end{pmatrix} \\
&= I_8 + \begin{pmatrix} -4\alpha \\ 0 \\ 0 \\ -4\alpha \\ 0 \\ 0 \\ 0 \\ -4\alpha^2 \end{pmatrix} \times 1 \times \begin{pmatrix} 0 & 0 & 1 & \alpha & 1 & 0 & 0 & -1 \end{pmatrix}
\end{aligned}
$$

Hence h has values $a(h)$ and $c(h)$ given by:

$$
\begin{aligned}
a(h) &= \begin{pmatrix} 0 & 0 & 1 & \alpha & 1 & 0 & 0 & -1 \end{pmatrix} \\
c(h) &= \begin{pmatrix} -4\alpha \\ 0 \\ 0 \\ -4\alpha \\ 0 \\ 0 \\ 0 \\ -4\alpha^2 \end{pmatrix}
\end{aligned}
$$

Now

$$
\begin{aligned}
\gamma\delta &= a(g)\,c(h)\,a(h)\,c(g) \\
&= \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \cdots \\
&\quad \cdots \begin{pmatrix} -4\alpha \\ 0 \\ 0 \\ -4\alpha \\ 0 \\ 0 \\ 0 \\ -4\alpha^2 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & \alpha & 1 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -4\alpha \end{pmatrix} \\
&= (-4\alpha) \times (4\alpha)
\end{aligned}
$$

$$= \quad -16\alpha^2$$

So if α is chosen such that $-16\alpha^2$ is a defining element of $\mathbb{F}_q$, we have, by Lemma 4.1.11, that $\langle g, h\rangle \leqslant G$ contains a root subgroup R.

4.10.3 Irreducibility

In this section we show that $H := \langle g\rangle^G = \langle R\rangle^G$ acts irreducibly on the vector space V. First we define the group $G_1 := \langle b, c, (ac)^4\rangle$.

Lemma 4.10.1. *The group G_1 acts irreducibly on the vector space V.*

Proof. Let U be a G_1-invariant subspace. Let g be the transvection in G calculated in the last section, with values $a(g)$ and $c(g)$, defined as above.

So we have:

$a(g) = (0, 0, 0, 1, 0, 0, 0, 0)$

$c(g) = (0, 0, 0, 0, 0, 0, 0, -4\alpha)^T$

If there exists a vector $u \in U$ which does not lie on the axis of g, then by Lemma 4.1.18 we have that $c(g) \in U$, and since $\alpha \neq 0$, we have $u := (0, 0, 0, 0, 0, 0, 0, 1)^T \in U$. Then we have:

$$\begin{aligned}
w_1 &:= (ac)^4 u \\
&= (0, 0, 0, -1, 0, 0, -1, 0)^T \in U \\
w_2 &:= bw_1 \\
&= (0, 0, 0, -1, 0, 0, 1, 0)^T \in U \\
w_3 &:= (ac)^4 w_1 \\
&= (0, -1, -1, -\alpha, -1, 0, -2\alpha, -1)^T \in U \\
w_4 &:= (ca)^4 u \\
&= (1, 0, 0, 1, 0, 0, 0, \alpha)^T \in U \\
w_5 &:= (ca)^4 w_4 \\
&= \left(2\alpha, 0, 1, \alpha, 1, 1, 0, 1 + \alpha^2\right)^T \in U
\end{aligned}$$

$$\begin{aligned} w_6 &:= (ac)^4 w_2 - w_3 \\ &= (0,2,2,0,0,0,2\alpha,0)^T \in U \\ w_7 &:= (ca)^4 w_2 - u \\ &= (0,0,-1,0,0,0,0,-1)^T \in U \end{aligned}$$

The vectors u, w_1, w_2, w_3, w_4, w_5, w_6 and w_7 form a basis of V. To see this is in fact a basis of $\mathbb{F}_q^8$, we show here how to obtain the standard basis from these vectors:

$$\begin{aligned} u &= (0,0,0,0,0,0,0,1)^T = e_8 \\ \frac{1}{-2}(w_1 + w_2) &= (0,0,0,1,0,0,0,0)^T = e_4 \\ \frac{1}{2}(w_2 - w_1) &= (0,0,0,0,0,0,1,0)^T = e_7 \\ -w_7 - u &= (0,0,1,0,0,0,0,0)^T = e_3 \\ w_4 - e_4 - \alpha e_8 &= (1,0,0,0,0,0,0,0)^T = e_1 \\ \frac{1}{2}(w_6 - 2e_3 - 2\alpha e_7) &= (0,1,0,0,0,0,0,0)^T = e_2 \\ -w_3 - e_2 - e_3 - \alpha e_4 - 2\alpha e_7 - e_8 &= (0,0,0,0,1,0,0,0)^T = e_5 \\ w_5 - 2\alpha e_1 - e_3 - \alpha e_4 - e_5 - \left(1+\alpha^2\right) e_8 &= (0,0,0,0,0,1,0,0)^T = e_6 \end{aligned}$$

Hence $U = V$.

So, we may assume that U is contained in the axis of g, i.e. if $u = (u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8)^T \in U$, then $u_4 = 0$. We look at this dually, i.e. the homogeneous linear equations satisfied by all vectors of U are represented by rows of length 8, on which G_1 acts on the right. All such equations form a subspace, X, of ${}^8\mathbb{F}_q$. Since U is G_1-invariant, X is also.

We have $x := (0,0,0,1,0,0,0,0)^T \in X$. Then we have:

$$\begin{aligned} y_1 &:= x(ca)^4 \\ &= (0,0,0,0,0,0,0,1) \in X \\ y_2 &:= x(ac)^4 - \alpha x + y_1 \end{aligned}$$

$$
\begin{aligned}
&= (0,0,1,0,1,0,0,0) \in X \\
y_3 &:= y_2 b \\
&= (0,0,1,0,-1,0,0,0) \in X \\
y_4 &:= y_2 \left(I_8 - b\right) (ca)^4 \\
&= (2,0,0,0,0,0,0,0) \in X \\
y_5 &:= y_2 \left(I_8 + b\right) (ac)^4 \\
&= (0,0,0,0,0,0,2,0) \in X \\
y_6 &:= y_5 (ac)^4 \\
&= (0,1,0,\alpha,1,0,\alpha,-1) \in X \\
y_7 &:= y_2 \left(I_8 + b\right) (ca)^4 \\
&= (0,0,\alpha,1,0,1,-1,0) \in X
\end{aligned}
$$

The vectors x, y_1, y_2, y_3, y_4, y_5, y_6 and y_7 form a basis of ${}^8\mathbb{F}_q$, as long as $\alpha \neq 0$. To see this is in fact a basis of ${}^8\mathbb{F}_q$ with these restrictions, we show here how to obtain the standard basis from these vectors:

$$
\begin{aligned}
x &= (0,0,0,1,0,0,0,0) = e_4^T \\
y_1 &= (0,0,0,0,0,0,0,1) = e_8^T \\
\frac{1}{2}\left(y_2 + y_3\right) &= (0,0,1,0,0,0,0,0) = e_3^T \\
\frac{1}{2}\left(y_2 - y_3\right) &= (0,0,0,0,1,0,0,0) = e_5^T \\
\frac{1}{2} y_4 &= (1,0,0,0,0,0,0,0) = e_1^T \\
\frac{1}{2} y_5 &= (0,0,0,0,0,0,1,0) = e_7^T \\
y_6 - \alpha e_4^T - e_5^T - \alpha e_7^T + e_8^T &= (0,1,0,0,0,0,0,0) = e_2^T \\
y_7 - \alpha e_3^T - e_4^T + e_7^T &= (0,0,0,0,0,1,0,0) = e_6^T
\end{aligned}
$$

So, with these restrictions we have $X = {}^8\mathbb{F}_q$, and so $U = 0$.

Hence G_1 is irreducible. □

Then, as the group $G_1 = \langle b, c, (ac)^4 \rangle$ satisfies the conditions of Proposition

4.1.17, and as $\alpha \neq 0$, the group $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1}$ is irreducible, and so the group $H \geqslant H_1$ is also. Now, by the choice of H it is easy to see that it contains the group R defined in the last section. Thus, if the restrictions on α from the previous section are satisfied, we have that H is an irreducible group generated by Root subgroups.

4.10.4 Invariant Forms

Lemma 4.10.2. *H does not preserve a non-degenerate symplectic form.*

Proof. We need to prove that there exists no non-degenerate symplectic form on V which is invariant under the action of G up to similarity. Let $\langle\ ,\ \rangle$ be a symplectic form on V that is preserved by G up to similarity. Then a,b and $c \in G$ preserve $\langle\ ,\ \rangle$ up to similarity with multipliers $\lambda(a)$, $\lambda(b)$ and $\lambda(c)$ respectively. Then, as a, b and c are involutions we have, from Lemma 4.1.20, $\lambda(a) = \pm 1$, $\lambda(b) = \pm 1$ and $\lambda(c) = \pm 1$.

Now we know that a, b, c and ab are conjugate in $SL_8(q)$, and from information in table 4.5.1 in [GLS98], we have that a, b, c and ab are conjugate in $GSp_8(q)$. Thus from Lemma 4.1.20, we have $\lambda(a) = \lambda(b) = \lambda(c) = \lambda(ab) = \lambda(a)\lambda(b)$, and so $\lambda(a) = \lambda(b) = \lambda(c) = 1$. Thus, as a, b and c generate G, for all $x \in G$, the multiplier for x, $\lambda(x)$ must be equal to 1, i.e. for all $x \in G$ and all u,$v \in V$, $\langle xu, xv \rangle = \langle u, v \rangle$.

So for $1 \leqslant i \leqslant 4$ and $5 \leqslant j \leqslant 8$, we have:

$$\begin{aligned} \langle v_i, v_j \rangle &=_b \langle v_i, -v_j \rangle \\ &= -\langle v_i, v_j \rangle, \text{ and so} \\ \langle v_i, v_j \rangle &= 0 \text{ for } 1 \leqslant i \leqslant 4 \text{ and } 5 \leqslant j \leqslant 8. \end{aligned}$$

Also, for $i = 1, 3, 5, 7$ and $j = i + 1$, we have:

$$\begin{aligned} \langle v_i, v_j \rangle &=_a \langle v_j, v_i \rangle \\ &= -\langle v_i, v_j \rangle, \text{ and so} \end{aligned}$$

$$\langle v_i, v_j \rangle \quad = \quad 0 \text{ for } i = 1, 3, 5, 7 \text{ and } j = i + 1.$$

Thus, we have:

$$\begin{aligned}
\langle v_6, v_8 \rangle &=_c \langle v_2, -v_8 \rangle \\
&= -\langle v_2, v_8 \rangle \\
&= 0, \\
\langle v_5, v_7 \rangle &=_a \langle v_6, v_8 \rangle \\
&= 0, \\
\langle v_1, v_3 \rangle &=_c \langle v_7, v_5 + v_8 \rangle \\
&= \langle v_7, v_5 \rangle + \langle v_7, v_8 \rangle \\
&= -\langle v_5, v_7 \rangle + \langle v_7, v_8 \rangle \\
&= 0, \\
\langle v_2, v_4 \rangle &=_a \langle v_1, v_3 \rangle \\
&= 0, \\
\langle v_2, v_3 \rangle &=_c \langle v_6, v_5 + v_8 \rangle \\
&= \langle v_6, v_5 \rangle + \langle v_6, v_8 \rangle \\
&= -\langle v_5, v_6 \rangle + \langle v_6, v_8 \rangle \\
&= 0, \\
\langle v_1, v_4 \rangle &=_a \langle v_2, v_3 \rangle \\
&= 0, \\
\langle v_5, v_8 \rangle &=_c \langle v_3 + v_8, -v_8 \rangle \\
&= \langle v_3, -v_8 \rangle + \langle v_8, -v_8 \rangle \\
&= -\langle v_3, v_8 \rangle - \langle v_8, v_8 \rangle \\
&= 0, \\
\langle v_6, v_7 \rangle &=_c \langle v_2, v_1 \rangle \\
&= -\langle v_1, v_2 \rangle
\end{aligned}$$

$$= \quad 0.$$

Hence we have $\langle v_i, v_j \rangle = 0 \forall i, j,\ 1 \leqslant i, j \leqslant n$.

Hence there is no non-degenerate symplectic form on V which is invariant under the action of G up to similarity, and so H does not preserve a non-degenerate symplectic form. □

Hence H cannot be conjugate to $Sp_8(q)$.

4.10.5 Equations

The only restrictions we have are that $q \neq 9$ and $-16\alpha^2 \neq 0$ and is a defining element of $\mathbb{F}_q$. Taking α to be any primitive element of $\mathbb{F}_q$ will satisfy these restrictions on α. Hence for $q \neq 9$, there exists an element $\alpha \in \mathbb{F}_q$ that satisfies these restrictions.

4.10.6 Conclusion

We conclude this section by summarising the above.

Lemma 4.10.3. *For q odd and $q \neq 9$, $\exists\ \alpha \in \mathbb{F}_q$ s.t. the elements a, b and c generate $SL_4(q)$, and so $L_4(q)$ has Property 2 and hence also has Property 1.*

Proof.

1. In section 4.10.1 we exhibited elements in $SL_8(q)$, a, b and c such that a and b commute and a, b, c and ab are conjugate involutions in $SL_8(q)$. Under the natural homomorphism $SL_8(q) \longrightarrow L_8(q)$ they map to involutions a', b' and c' such that a' and b' commute and a', b', c' and $a'b'$ are conjugate in $L_8(q)$. The elements are defined in terms of a variable $\alpha \in \mathbb{F}_q$. We called the group generated by these elements G.

2. In section 4.10.2 we demonstrated that there is a non-trivial transvection, in G, $g := (bc)^4$. We also demonstrated that the transvection $h := g^{(ac)^4} \in G$ is opposite to g. Dickson's Lemma (Lemma 4.1.2) then gives us that G contains the whole root subgroup R, consisting of all

transvections with the same centre and the same axis as g, subject to $-16\alpha^2$ being a defining element of $\mathbb{F}_q$.

3. In section 4.10.3 we then considered a subgroup $G_1 := \left\langle b, c, (ac)^2 \right\rangle \leqslant G$, containing R, and the normal closure $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1} \trianglelefteq G_1$ of the root subgroup R in G_1. We have shown that the group G_1 is irreducible and so the group H_1 is also irreducible. Thus $H := \langle g \rangle^G = \langle R \rangle^G$ is irreducible, and so is an irreducible group generated by root subgroups. Thus from Lemma 4.1.1, H either coincides with $SL_8(q)$, or H is conjugate to $Sp_8(q)$.

4. In section 4.10.4 we excluded the symplectic case by showing that G does not preserve a non-degenerate symplectic form up to similarity. This implies that, when α satisfies the imposed restrictions, we have that $G \trianglerighteq H = SL_8(q)$and hence, $G \cong SL_8(q)$.

5. Finally, in section 4.10.5 it was shown that the there exists an α such that the restrictions on it can be satisfied.

□

4.11 Dimension $n = 4m + 1$, $m \geqslant 2$

In this section, we show that, for q odd, $q \neq 9$ and $m \geqslant 2$, $L_{4m+1}(q)$ has Property 2, and hence Property 1. We do so by showing that $SL_{4m+1}(q)$ can be generated by suitable elements by following the method outlined in section 4.1. We work in the standard representation of $SL_{4m+1}(q)$, i.e. $(4m+1)\times(4m+1)$ matrices acting on the space of column vectors of length $4m+1$. We call this vector space V.

4.11.1 Generators

We define:

$$a := \left(\begin{array}{c|c} \begin{array}{ccc} & & 1 \\ & \iddots & \\ 1 & & \end{array} & \overbrace{\begin{array}{cccc} & & & \\ & & & \\ & & & \end{array}}^{2m} \\ \underbrace{\begin{array}{ccc} & & \\ & & \\ & & \end{array}}_{2m+1} & \begin{array}{cccc} 0 & 1 & & \\ 1 & 0 & & \\ & & \ddots & \\ & & & \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \end{array} \end{array}\right)$$

which can be thought of as permuting the

standard basis as the permutation

$$a' = \underbrace{(1, 2m+1) \dots (m, m+2)}_{(l, 2m+1-l)\ 1 \leqslant l \leqslant m} (m+1) \underbrace{(2m+2, 2m+3) \dots (n-1, n)}_{(2l, 2l+1)\ m+1 \leqslant l \leqslant 2m}$$

$$b := \left(\begin{array}{c|c} \begin{array}{ccc} 1 & & \\ & \ddots & \\ & & 1 \end{array} & \overbrace{\begin{array}{ccc} & & \\ & & \\ & & \end{array}}^{2m} \\ \underbrace{\begin{array}{ccc} & & \\ & & \\ & & \end{array}}_{2m+1} & \begin{array}{ccc} -1 & & \\ & \ddots & \\ & & -1 \end{array} \end{array}\right)$$

$$c := \left(\begin{array}{ccc|cc|ccc|c} & & & & & & & 1 & \\ & & & & & & \iddots & & \\ & & & & & 1 & & & \\ & & & & 1 & & & & \\ & & & 1 & & & & & \\ & & \iddots & & & & & & \\ 1 & & & & & & & & \\ 0 & \cdots & 0 & \alpha & -\alpha & 0 & \cdots & 0 & 1 \end{array}\right) \text{ for some } 0 \neq \alpha \in \mathbb{F}_q$$

$$\underbrace{}_{2m-1} \qquad\qquad \underbrace{}_{2m-1}$$

which is close to permuting the standard basis as the permutation

$$c' = \underbrace{(1, n-1) \dots (2m, 2m+1)}_{(l, n-l)\ 1 \leqslant l \leqslant 2m} (n)$$

Hence

$$ab = \left(\begin{array}{ccc|cccc} & & 1 & & & & \\ & \iddots & & & & & \\ 1 & & & & & & \\ & & & 0 & -1 & & \\ & & & -1 & 0 & & \\ & & & & & \ddots & \\ \underbrace{\qquad}_{2m+1} & & & & & & \\ & & & & & 0 & -1 \\ & & & & & -1 & 0 \end{array}\right) \quad \overbrace{\qquad}^{2m}$$

As a, b, c and ab are all involutions with eigenvalues $\left\{(1)^{2m+1}, (-1)^{2m}\right\}$, from the properties of involutions, we can see that they are conjugate in $SL_{4m+1}(q)$, and a and b commute. We take $G := \langle a, b, c\rangle$.

4.11.2 Transvections and Root Subgroups

In this section, we show that the group G defined above, contains two opposite transvections, and so from Lemma 4.1.11, G contains a root subgroup.

We have:

$$\begin{aligned} g &:= (bc)^4 \\ &= \left(\begin{array}{ccc|ccc|ccc|c} 1 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & 1 & & & & & & & \\ & & & 1 & & & & & & \\ & & & & & 1 & & & & \\ & & & & & & 1 & & & \\ & & & & & & & \ddots & & \\ & & & & & & & & 1 & \\ \underbrace{0 \quad \cdots \quad 0}_{2m-1} & & & 4\alpha & & -4\alpha & \underbrace{0 \quad \cdots \quad 0}_{2m-1} & & & 1 \end{array}\right) \\ &= I_n + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 4\alpha \end{pmatrix} \times 1 \times \underbrace{(0 \quad \cdots \quad 0|}_{2m-1} \quad 1 \quad -1 \quad \underbrace{|0 \quad \cdots \quad 0)}_{2m} \end{aligned}$$

Hence, g is a one-dimensional transformation, and has values $a(g)$ and

$c(g)$ given by:

$$a(g) = (\underbrace{0 \cdots 0|}_{2m-1} \; 1 \; -1 \; \underbrace{|0 \cdots 0)}_{2m}$$

$$c(g) = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 4\alpha \end{pmatrix}$$

Thus, by Lemma 4.1.6, g is a transvection as

$$a(g)\,c(g) = \underbrace{(0 \cdots 0|}_{2m-1} \; 1 \; -1 \; \underbrace{|0 \cdots 0)}_{2m} \times \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 4\alpha \end{pmatrix} = 0$$

Now we want another transvection, h, such that h is opposite to g. From Lemma 4.1.10 g and h are opposite if, for $\gamma := a(g)\,c(h)$, and $\delta := a(h)\,c(g)$, we have $\gamma\delta \neq 0$. We also want $\gamma\delta$ to be a defining element of $\mathbb{F}_q$.

We take $h := g^k = k^{-1}gk$, where $k := (ac)^2$. Since h is conjugate to g, h is a transvection. Now, since we only want to know the value of $\gamma\delta$, we do not need to calculate h explicitly. We use the fact that the generators we have chosen are very close to being permutation matrices to do a much easier calculation.

Now

$$ac = \left(\begin{array}{c|cccccc|cc|ccc|c} & & & & & & & 1 & & & & & \\ & & & & & & & & 1 & & & & \\ & & & & & & & & & 1 & & & \\ & & & & & & & & & & \ddots & & \\ & & & & & & & & & & & 1 & \\ & & & & & 1 & & & & & & & \\ & & & & & & 1 & & & & & & \\ & & & & \iddots & & & & & & & & \\ & & 1 & & & & & & & & & & \\ & & & 1 & & & & & & & & & \\ 0 & 0 & \cdots & \cdots & \cdots & 0 & & \alpha & -\alpha & 0 & \cdots & 0 & 1 \\ 1 & & & & & & & & & & & & \end{array}\right) \text{ and}$$

$$\underbrace{\qquad\qquad}_{2m-2} \qquad\qquad \underbrace{\qquad\qquad}_{2m-1}$$

$$ca = (ac)^{-1}$$

$$= \left(\begin{array}{ccc|ccc|ccccc|cc} & & & & & & & & & & 1 & & \\ & & & & & & & & & 1 & & & \\ & & & & & & & & & & 1 & & \\ & & & & & & & & \iddots & & & & \\ & & & & & & & 1 & & & & & \\ & & & & & & & & 1 & & & & \\ 1 & & & & & & & & & & & & \\ & \ddots & & & & & & & & & & & \\ & & 1 & & & & & & & & & & \\ & & & 1 & & & & & & & & & \\ & & & & 1 & & & & & & & & \\ & & & & & 1 & & & & & & & \\ & & & & & & 1 & & & & & & \\ 0 & \cdots & 0 & \alpha & 0 & -\alpha & 0 & \cdots & \cdots & \cdots & 0 & 1 & 0 \end{array}\right)$$

$$\underbrace{\qquad\qquad}_{2m-2} \qquad\qquad \underbrace{\qquad\qquad}_{2m-2}$$

i.e. ac is very close to being the permutation matrix representing the permutation

$$a'c' = (1, 2m, n-2, 3, \ldots 2, 2m+1, n-1, n)\,,$$

(a cycle of length $4m+1$). Using this we can easily calculate $(ac)^2$ and $(ca)^2$.

Note that $(a'c')^2 : 2m \longmapsto n \longmapsto 2m+1$.

In calculating $\gamma\delta$, we will need the $(2m)^{th}$ and the $(2m+1)^{th}$ rows of k^{-1}, and the entries $(k)_{2m,n}$, $(k)_{2m+1,n}$, $(k)_{n-3,n}$ and $(k)_{n,n}$ from k. This will be made clear below. Since ca is very close to being a permutation matrix, it is easy to see that the $(2m)^{th}$ row of $k^{-1} = (ca)^2$ is in fact equal to $\begin{pmatrix} 0 & \cdots & 0 & 1 \end{pmatrix}$, The $(2m+1)^{th}$ row of k^{-1} is equal to $\begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$ Similarly, since ac is very close to being a permutation matrix, it is easy to see that $(k)_{2m,n} = 0$, $(k)_{2m+1,n} = 1$, $(k)_{n-3,n} = 0$ and $(k)_{n,n} = 0$.

Now

$$\begin{aligned}
\gamma\delta &= a(g)\,c(h)\,a(h)\,c(g) \\
&= (\underbrace{0 \quad \cdots \quad 0}_{2m-1}|\ 1\ \ -1\ \ |\underbrace{0 \quad \cdots \quad 0}_{2m})\ (c(h)\,a(h)) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 4\alpha \end{pmatrix} \\
&= (\underbrace{0 \quad \cdots \quad 0}_{2m-1}|\ 1\ \ -1\ \ |\underbrace{0 \quad \cdots \quad 0}_{2m})\ (h - I_n) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 4\alpha \end{pmatrix} \\
&= \Big(1 \times \Big((2m)^{th}\ row\ of\ (h - I_n)\Big) \cdots \\
&\qquad \cdots - 1 \times \Big((2m+1)^{th}\ row\ of\ (h - I_n)\Big)\Big) \times \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 4\alpha \end{pmatrix} \\
&= \Big(1 \times \Big((h - I_n)_{2m,n}\Big) - 1 \times \Big((h - I_n)_{2m+1,n}\Big)\Big) \times (4\alpha) \\
&= (4\alpha) \times \Big((h)_{2m,n} - (h)_{2m+1,n}\Big) \\
&= (4\alpha) \times \Big(\big(k^{-1}gk\big)_{2m,n} - \big(k^{-1}gk\big)_{2m+1,n}\Big) \\
&= (4\alpha) \times \Big(\Big((2m)^{th}\ row\ of\ k^{-1}\Big) \times \big(n^{th}\ column\ of\ gk\big) \cdots \\
&\qquad \cdots - \Big((2m+1)^{th}\ row\ of\ k^{-1}\Big) \times \big(n^{th}\ column\ of\ gk\big)\Big) \\
&= (4\alpha) \times \big(\begin{pmatrix} 0 & \cdots & 0 & 1 \end{pmatrix} \times \big(n^{th}\ column\ of\ gk\big) - \cdots \\
&\qquad \cdots \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \times \big(n^{th}\ column\ of\ gk\big)\big)
\end{aligned}$$

$$
\begin{aligned}
&= (4\alpha) \times \left(1 \times (gk)_{n,n} - 1 \times (gk)_{n-3,n}\right) \\
&= (4\alpha) \times \left(\left(n^{th}\ row\ of\ g\right) \times \left(n^{th}\ column\ of\ k\right) \cdots \right. \\
&\quad \left. \cdots - \left((n-3)^{th}\ row\ of\ g\right) \times \left(n^{th}\ column\ of\ k\right)\right) \\
&= (4\alpha) \times \cdots \\
&\quad \cdots \times \left(\left(\begin{array}{ccc|cc|ccc|c} 0 & \cdots & 0 & 4\alpha & -4\alpha & 0 & \cdots & 0 & 1 \end{array}\right) \times \left(n^{th}\ column\ of\ k\right) \cdots \right. \\
&\quad \left. \cdots - \left(\begin{array}{ccccccc} 0 & \cdots & 0 & 1 & 0 & 0 & 0 \end{array}\right) \times \left(n^{th}\ column\ of\ k\right)\right) \\
&= (4\alpha) \times \cdots \\
&\quad \cdots \times \left(\left(4\alpha \times (k)_{2m,n} - 4\alpha \times (k)_{2m+1,n} + 1 \times (k)_{n,n}\right) - 1 \times (k)_{n-3,n}\right) \\
&= (4\alpha) \times (4\alpha \times 0 - 4\alpha \times 1 + 1 \times 0 - 1 \times 0) \\
&= (4\alpha) \times (-4\alpha) \\
&= -16\alpha^2
\end{aligned}
$$

So if α is chosen such that $-16\alpha^2$ is a defining element of $\mathbb{F}_q$, we have, by Lemma 4.1.11, that $\langle g, h\rangle \leqslant G$ contains a root subgroup R.

4.11.3 Irreducibility

In this section we show that $H := \langle g\rangle^G = \langle R\rangle^G$ acts irreducibly on the vector space V. First we define the group $G_1 := \langle b, c, (ac)^2\rangle$.

Lemma 4.11.1. *The group G_1 acts irreducibly on the vector space V.*

Proof. Let U be a G_1-invariant subspace. Let g be the transvection in G calculated in the last section, with values $a(g)$ and $c(g)$, defined as above.

So we have:

$$
a(g) = (\underbrace{0 \quad \cdots \quad 0}_{2m-1} | \quad 1 \quad -1 \quad | \underbrace{0 \quad \cdots \quad 0}_{2m})
$$

$$
c(g) = (0, \ldots, 0, 4\alpha)^T
$$

If there exists a vector $u \in U$ which does not lie on the axis of g, then by Lemma 4.1.18 we have that $c(g) \in U$, and since $\alpha \neq 0$, we have $u :=$

$(0,\ldots,0,1)^T \in U$. In fact, u is the standard basis vector e_n. Now since the matrix ac is close to being a permutation matrix, it is relatively simple to see how $(ac)^2$ acts on standard basis vectors. For $i \neq 2m, 2m+1, n-2, n-1$ we have:

$(ac)^2 e_i = \pm e_j$, where $j = i^{(c'a')^2}$.

Thus, for $i \neq 2m, 2m+1, n-2, n-1$, if $e_i \in U$ then $e_{i^{(c'a')^2}} \in U$. Also:

$$\begin{aligned}
(ac)^2 e_{2m} &= e_n + \alpha e_{2m+1} \\
&= e_{(2m)^{(c'a')^2}} + \alpha e_{2m+1} \\
(ac)^2 e_{2m+1} &= e_{n-3} - \alpha e_{2m+1} \\
&= e_{(2m+1)^{(c'a')^2}} + \alpha e_{2m+1} \\
(ac)^2 e_{n-2} &= e_1 + \alpha e_{n-1} \\
&= e_{(n-2)^{(c'a')^2}} + \alpha e_{n-1} \\
(ac)^2 e_{n-1} &= e_2 - \alpha e_{n-1} \\
&= e_{(n-1)^{(c'a')^2}} - \alpha e_{n-1}
\end{aligned}$$

Thus, for $i = 2m, 2m+1$, if $e_i \in U$ and $e_{2m+1} \in U$, then $e_{i^{(c'a')^2}} \in U$. Also, for $i = n-2, n-1$, if $e_i \in U$ then $(b + I_{4m+1})\left(e_{i^{(c'a')^2}} \pm \alpha e_{n-1}\right) = 2e_{i^{(c'a')^2}} \in U$ and so $e_{i^{(c'a')^2}} \in U$.

Now, from above, we have $e_n \in U$. Also, $(ac)^2 e_n = e_{2m+1} \in U$. And so, as $e_n \in U$, $e_{2m+1} \in U$, $e_{n-2} \in U$, $e_{n-1} \in U$ and the permutation $(c'a')^2$ is a cycle of length $4m+1$, we have $e_i \in U$ for all i, $1 \leqslant i \leqslant 4m+1$. Hence, since U is G_1-invariant, we have $U = V$.

So, we may assume that U is contained in the axis of g, i.e. if $u = (u_1,\ldots,u_n)^T \in U$, then $u_{2m} - u_{2m+1} = 0$. We look at this dually, i.e. the homogeneous linear equations satisfied by all vectors of U are represented by rows of length $4m+1$, on which G_1 acts on the right. All such equations form a subspace, X, of ${}^{4m+1}\mathbb{F}_q$. Since U is G_1-invariant, X is also.

So, we have $x := (\underbrace{0 \quad \cdots \quad 0}_{2m-1}| \quad 1 \quad -1 \quad |\underbrace{0 \quad \cdots \quad 0}_{2m}) \in X$.

Then $\left(x\left(ca\right)^2\right)\left(I_{4m+1} - b\right) = (0, \ldots, 0, 2, 0) \in X$. So we have the standard basis vector $e_{n-1}^T \in X$. Now since ca is close to being a permutation matrix, it is relatively simple to see how $\left(ca\right)^2$ acts on standard basis vectors. For $i \neq 1, n$ we have:

$e_i^T \left(ac\right)^2 = \pm e_j^T$, where $j = i^{(c'a')^2}$.

Thus, for $i \neq 1, n$, if $e_i^T \in X$ then $e_{i^{(c'a')^2}}^T \in X$. Also:

$$\begin{aligned} e_n^T \left(ca\right)^2 &= e_{2m+1}^T + \alpha e_{2m+3}^T - \alpha e_2^T \\ &= e_{(n)^{(c'a')^2}}^T + \alpha e_{2m+3}^T - \alpha e_2^T \end{aligned}$$

and, if $e_n^T \in X$, then $\left(e_{2m+1}^T + \alpha e_{2m+3}^T - \alpha e_2^T\right)(1 - b) = 2\alpha e_{2m+3}^T \in X$, and so we have $e_{2m+3} \in X$. Thus, if $e_n \in X$, and $e_2^T \in X$, then $e_{(n)^{(c'a')^2}}^T \in X$.

Now, from above, we have $e_{n-1}^T \in X$. Also, since the permutation $\left(c'a'\right)^2$ is a cycle of length $4m+1$ and we have $(n-1)^{(c'a')^{4m}} = n$, $(n-1)^{(c'a')^{8m+2}} = 1$ and $(n-1)^{(c'a')^2} = 2$ then we can see that $e_{n-1}^T \left(ca\right)^2 = e_2^T \in X$. From this it can be seen that for all i, $1 \leqslant i \leqslant 4m+1$, $e_i^T \in X$. Since X is G_1-invariant, we have $X = {}^{4m+3}\mathbb{F}_q$, and so $U = 0$.

Hence G_1 is irreducible. □

Then, as the group $G_1 = \langle b, c, (ac)^2 \rangle$ satisfies the conditions of Proposition 4.1.17, and as $\alpha \neq 0$, the group $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1}$ is irreducible, and so the group $H \geqslant H_1$ is also. Now, by the choice of H it is easy to see that it contains the group R defined in the last section. Thus, if the restrictions on α from the previous section are satisfied, we have that H is an irreducible group generated by Root subgroups.

4.11.4 Invariant Forms

There are no non-degenerate symplectic forms in dimension $4m+1$.

4.11.5 Equations

The only restrictions we have are that $q \neq 9$ and $-16\alpha^2 \neq 0$ and is a defining element of $\mathbb{F}_q$. Taking α to be any primitive element of $\mathbb{F}_q$ will satisfy these restrictions on α. Hence for $q \neq 9$, there exists an element $\alpha \in \mathbb{F}_q$ that satisfies these restrictions.

4.11.6 Conclusion

We conclude this section by summarising the above.

Lemma 4.11.2. *For q odd, $q \neq 9$ and $m \geqslant 2$, $\exists\ \alpha \in \mathbb{F}_q$ s.t. the elements a, b and c generate $SL_{4m+1}(q)$, and so $L_{4m+1}(q)$ has Property 2 and hence also has Property 1.*

Proof.

1. In section 4.11.1 we exhibited elements in $SL_{4m+1}(q)$, a, b and c such that a and b commute and a, b, c and ab are conjugate involutions in $SL_{4m+1}(q)$. Under the natural homomorphism $SL_{4m+1}(q) \longrightarrow L_{4m+1}(q)$ they map to involutions a', b' and c' such that a' and b' commute and a', b', c' and $a'b'$ are conjugate in $L_{4m+1}(q)$. The elements are defined in terms of a variable $\alpha \in \mathbb{F}_q$. We called the group generated by these elements G.

2. In section 4.11.2 we demonstrated that there is a non-trivial transvection, in G, $g := (bc)^4$. We also demonstrated that the transvection $h := g^{(ac)^2} \in G$ is opposite to g. Dickson's Lemma (Lemma 4.1.2) then gives us that G contains the whole root subgroup R, consisting of all transvections with the same centre and the same axis as g, subject to $-16\alpha^2$ being a defining element of $\mathbb{F}_q$.

3. In section 4.11.3 we then considered a subgroup $G_1 := \left\langle b, c, (ac)^2 \right\rangle \leqslant G$, containing R, and the normal closure $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1} \trianglelefteq G_1$ of the root subgroup R in G_1. We have shown that the group G_1 is irreducible

and so the group H_1 is also irreducible. Thus $H := \langle g \rangle^G = \langle R \rangle^G$ is irreducible, and so is an irreducible group generated by root subgroups. Thus from Lemma 4.1.1, H must coincide with $SL_{4m+1}(q)$.

4. There are no non-degenerate symplectic forms in dimension $4m+1$. This implies that, when α satisfies the imposed restrictions, we have that $G \trianglerighteq H = SL_{4m+1}(q)$ and hence, $G \cong SL_{4m+1}(q)$.

5. Finally, in section 4.11.5 it was shown that the there exists an α such that the restrictions on it can be satisfied.

□

4.12 Dimension $n = 4m+2$, $m \geqslant 2$

In this section, we show that, for q odd, $q \neq 9$ and $m \geqslant 2$, $L_{4m+2}(q)$ has Property 2, and hence Property 1. We do so by showing that $SL_{4m+2}(q)$ can be generated by suitable elements by following the method outlined in section 4.1. We work in the standard representation of $SL_{4m+2}(q)$, i.e. $(4m+2)\times(4m+2)$ matrices acting on the space of column vectors of length $4m+2$. We call this vector space V.

4.12.1 Generators

We define:

$$a := \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \end{pmatrix}$$

which can be thought of as permuting the

standard basis as the permutation

$$a' = \underbrace{(1,2)\dots(n-5,n-4)}_{(2l-1,2l)\ 1\leqslant l\leqslant 2m-1}(n-1,n)\,,$$

$$b := \left(\begin{array}{c|c|c|c} \begin{matrix} & & & & 1 \\ & & & 1 & \\ & & 1 & & \\ & 1 & & & \\ 1 & & & & \end{matrix} & \begin{matrix} & \overbrace{\quad}^{2m-4} & \\ & & \\ -1 & & \\ & \ddots & \\ & & -1 \end{matrix} & \begin{matrix} \overbrace{\quad}^{2m} \\ \\ 1 & \\ & \ddots \\ & & 1 \end{matrix} & \begin{matrix} \\ \\ \\ \\ -1 & \\ & -1 \end{matrix} \end{array}\right)$$

which is close to permuting the standard basis as the permutation

$$b' = (1,4)\,(2,3)$$

$$c := \left(\begin{array}{cccccccccc} & & & & & & & & & 1 \\ & & & & & & & & 1 & \\ & & & & & & & 1 & & \\ & & & & & & 1 & & & \\ & & & & & \iddots & & & & \\ & & & & 1 & & & & & \\ & & & 1 & & & & & & \\ & & 1 & & & & & & & \\ & 1 & & & & & & & & \\ 1 & & & & & & & & & \\ 0 & \alpha & \alpha & 0 & \cdots & 0 & -\alpha & -\alpha & 0 & 1 \end{array}\right) \text{ for some } 0 \neq \alpha \in \mathbb{F}_q$$

which is close to permuting the standard basis as the permutation

$$c' = \underbrace{(1,n-1)\dots(2m,2m+2)}_{(l,n-l)\ 1\leqslant l\leqslant 2m}(2m+1)\,(n)$$

Hence

$$ab = \left(\begin{array}{ccc|c|c|c}
 & 1 & & & & \\
 & & 1 & & & \\
1 & & & & & \\
 & 1 & & & & \\
\hline
 & & & \overbrace{\begin{array}{ccccc} -1 & & & & \\ & \ddots & & & \\ & & & -1 & \\ & & & & -1 \end{array}}^{2m-4} & & \\
\hline
 & & & & \overbrace{\begin{array}{ccccc} 1 & & & & \\ & \ddots & & & \\ & & & 1 & \\ & & & & 1 \end{array}}^{2m-2} & \\
\hline
 & & & & & \begin{array}{cccc} 1 & & & \\ & 1 & & \\ & & & -1 \\ & & -1 & \end{array}
\end{array}\right)$$

As a, b, c and ab are all involutions with eigenvalues $\left\{(1)^{2m+2}, (-1)^{2m}\right\}$, from the properties of involutions, we can see that they are conjugate in $SL_{4m+2}(q)$, and a and b commute. We take $G := \langle a, b, c\rangle$.

4.12.2 Transvections and Root Subgroups

In this section, we show that the group G defined above, contains two opposite transvections, and so from Lemma 4.1.11, G contains a root subgroup.

We have:

$$\begin{aligned} g &:= (bc)^8 \\ &= \begin{pmatrix} 1 & & & & & & & & & \\ & 1 & & & & & & & & \\ & & 1 & & & & & & & \\ & & & 1 & & & & & & \\ & & & & \ddots & & & & & \\ & & & & & 1 & & & & \\ & & & & & & 1 & & & \\ & & & & & & & 1 & & \\ & & & & & & & & 1 & \\ 0 & 8\alpha & 8\alpha & 0 & \cdots & 0 & -8\alpha & -8\alpha & 0 & 1 \end{pmatrix} \end{aligned}$$

$$= I_n + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 8\alpha \end{pmatrix} \times 1 \times \begin{pmatrix} 0 & 1 & 1 & 0 & \cdots & 0 & -1 & -1 & 0 & 0 \end{pmatrix}$$

Hence, g is a one-dimensional transformation, and has values $a(g)$ and $c(g)$ given by:

$$a(g) = \begin{pmatrix} 0 & 1 & 1 & 0 & \cdots & 0 & -1 & -1 & 0 & 0 \end{pmatrix}$$
$$c(g) = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 8\alpha \end{pmatrix}$$

Thus, by Lemma 4.1.6, g is a transvection as

$$a(g)\,c(g) = \begin{pmatrix} 0 & 1 & 1 & 0 & \cdots & 0 & -1 & -1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 8\alpha \end{pmatrix} = 0$$

Now we want another transvection, h, such that h is opposite to g. From Lemma 4.1.10 g and h are opposite if, for $\gamma := a(g)\,c(h)$, and $\delta := a(h)\,c(g)$, we have $\gamma\delta \neq 0$. We also want $\gamma\delta$ to be a defining element of $\mathbb{F}_q$.

We take $h := g^k = k^{-1}gk$, where $k := (ac)^2$. Since h is conjugate to g, h is a transvection. Now, since we only want to know the value of $\gamma\delta$, we do not need to calculate h explicitly. We use the fact that the generators we have chosen are very close to being permutation matrices to do a much easier calculation.

Now

$$ac = \begin{pmatrix} & & & & & & & & & 1 & & \\ & & & & & & & & & & 1 & \\ & & & & & & & 1 & & & & \\ & & & & & & & & 1 & & & \\ & & & & & & \iddots & & & & & \\ & & & & & \iddots & & & & & & \\ & & & & 1 & & & & & & & \\ & & & & & 1 & & & & & & \\ & & & 1 & & & & & & & & \\ & & 1 & & & & & & & & & \\ 0 & \alpha & \alpha & 0 & 0 & \cdots & \cdots & 0 & -\alpha & -\alpha & 0 & 1 \\ 1 & & & & & & & & & & & \end{pmatrix} \text{ and}$$

$$ca = \begin{pmatrix} & & & & & & & & & & & 1 \\ & & & & & & & & & 1 & & \\ & & & & & & & & 1 & & & \\ & & & & & & & 1 & & & & \\ & & & & & & 1 & & & & & \\ & & & & & \iddots & & & & & & \\ & & & & \iddots & & & & & & & \\ & & & 1 & & & & & & & & \\ & & & & 1 & & & & & & & \\ & & 1 & & & & & & & & & \\ & 1 & & & & & & & & & & \\ \alpha & 0 & 0 & \alpha & 0 & \cdots & 0 & 0 & -\alpha & -\alpha & 1 & 0 \end{pmatrix}$$

i.e. ac is very close to being the permutation matrix representing the permutation

$$a'c' = (1, n-2, 2, n-1, n)\,(3, n-4, 5, n-6, \ldots, 6, n-5, 4, n-3)\,.$$

(a product of two distinct cycles, one of length 5, one of length $4m-3$). Using this we can easily calculate $(ac)^2$ and $(ca)^2$.

Note that $(a'c')^2 : 2 \longmapsto n \longmapsto n-2$.

In calculating $\gamma\delta$, we will only need the 2^{nd}, the 3^{rd}, the $(n-3)^{rd}$ and the $(n-2)^{nd}$ rows of k^{-1} and the entries $(k)_{1,n}$, $(k)_{2,n}$, $(k)_{3,n}$, $(k)_{4,n}$, $(k)_{n-5,n}$, $(k)_{n-3,n}$, $(k)_{n-2,n}$ and $(k)_{n,n}$ from k, as will be made clear below. Since

ca is very close to being a permutation matrix, it is easy to see that the 2^{nd} row of $k^{-1} = (ca)^2$ is in fact equal to $\begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$, the 3^{rd} row of k^{-1} is equal to $\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$, the $(n-3)^{rd}$ row of k^{-1} is equal to $\begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$, and the $(n-2)^{nd}$ row of k^{-1} is equal to $\begin{pmatrix} 0 & \cdots & 0 & 1 \end{pmatrix}$. Similarly, since ac is very close to being a permutation matrix, it is easy to see that $(k)_{1,n} = 0$, $(k)_{2,n} = 1$, $(k)_{3,n} = 0$, $(k)_{4,n} = 0$, $(k)_{n-5,n} = 0$, $(k)_{n-3,n} = 0$, $(k)_{n-2,n} = 0$ and $(k)_{n,n} = 0$.

Now

$$\begin{aligned}
\gamma\delta &= a(g)\,c(h)\,a(h)\,c(g) \\
&= \begin{pmatrix} 0 & 1 & 1 & 0 & \cdots & 0 & -1 & -1 & 0 & 0 \end{pmatrix} (c(h)\,a(h)) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 8\alpha \end{pmatrix} \\
&= \begin{pmatrix} 0 & 1 & 1 & 0 & \cdots & 0 & -1 & -1 & 0 & 0 \end{pmatrix} (h - I_n) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 8\alpha \end{pmatrix} \\
&= \left(1 \times \left(2^{nd}\ row\ of\ (h - I_n)\right) \cdots \right. \\
&\quad \cdots + 1 \times \left(3^{rd}\ row\ of\ (h - I_n)\right) \cdots \\
&\quad \cdots - 1 \times \left((n-3)^{rd}\ row\ of\ (h - I_n)\right) \cdots \\
&\quad \left. \cdots - 1 \times \left((n-2)^{nd}\ row\ of\ (h - I_n)\right)\right) \times \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 8\alpha \end{pmatrix} \\
&= \left(1 \times \left((h - I_n)_{2,n}\right) + 1 \times \left((h - I_n)_{3,n}\right) \cdots \right. \\
&\quad \left. \cdots - 1 \times \left((h - I_n)_{n-3,n}\right) - 1 \times \left((h - I_n)_{n-2,n}\right)\right) \times (8\alpha) \\
&= (8\alpha) \times \left((h)_{2,n} + (h)_{3,n} - (h)_{n-3,n} - (h)_{n-2,n}\right) \\
&= (8\alpha) \times \left(\left(k^{-1}gk\right)_{2,n} + \left(k^{-1}gk\right)_{3,n} - \left(k^{-1}gk\right)_{n-3,n} - \left(k^{-1}gk\right)_{n-2,n}\right) \\
&= (8\alpha) \times \left(\left(2^{nd}\ row\ of\ k^{-1}\right) \times \left(n^{th}\ column\ of\ gk\right) \cdots \right. \\
&\quad \left. \cdots + \left(3^{rd}\ row\ of\ k^{-1}\right) \times \left(n^{th}\ column\ of\ gk\right)\right.
\end{aligned}$$

$$
\begin{aligned}
& -\Big((n-3)^{rd}\ row\ of\ k^{-1}\Big) \times \big(n^{th}\ column\ of\ gk\big) \cdots \\
& \cdots - \Big((n-2)^{nd}\ row\ of\ k^{-1}\Big) \times \big(n^{th}\ column\ of\ gk\big)\Big) \\
= \ & (8\alpha) \times \big(\begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix} \times \big(n^{th}\ column\ of\ gk\big) \cdots \\
& \cdots + \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & \cdots & 0 \end{pmatrix} \times \big(n^{th}\ column\ of\ gk\big) \cdots \\
& \cdots - \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \times \big(n^{th}\ column\ of\ gk\big) \cdots \\
& \cdots - \begin{pmatrix} 0 & \cdots & 0 & 1 \end{pmatrix} \times \big(n^{th}\ column\ of\ gk\big)\big) \\
= \ & (8\alpha) \times \Big(1 \times (gk)_{1,n} + 1 \times (gk)_{4,n} - 1 \times (gk)_{n-5,n} - 1 \times (gk)_{n,n}\Big) \\
= \ & (8\alpha) \times \big(\big(1^{st}\ row\ of\ g\big) \times \big(n^{th}\ column\ of\ k\big) \cdots \\
& \cdots + \big(4^{th}\ row\ of\ g\big) \times \big(n^{th}\ column\ of\ k\big) \cdots \\
& \cdots - \Big((n-5)^{th}\ row\ of\ g\Big) \times \big(n^{th}\ column\ of\ k\big) \cdots \\
& \cdots - \big(n^{th}\ row\ of\ g\big) \times \big(n^{th}\ column\ of\ k\big)\big) \\
= \ & (8\alpha) \times \big(\begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix} \times \big(n^{th}\ column\ of\ k\big) \cdots \\
& \cdots + \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & \cdots & 0 \end{pmatrix} \times \big(n^{th}\ column\ of\ k\big) \cdots \\
& \cdots - \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \times \big(n^{th}\ column\ of\ k\big) \cdots \\
& \cdots - \begin{pmatrix} 0 & 8\alpha & 8\alpha & 0 & \cdots & 0 & -8\alpha & -8\alpha & 0 & 1 \end{pmatrix} \times \cdots \\
& \cdots \times \big(n^{th}\ column\ of\ k\big)\big) \\
= \ & (8\alpha) \times \Big(\Big(1 \times (k)_{1,n} + 1 \times (k)_{4,n} - 1 \times (k)_{n-5,n} - 8\alpha \times (k)_{2,n} \cdots \\
& \cdots - 8\alpha \times (k)_{3,n}\Big) + 8\alpha \times (k)_{n-3,n} + 8\alpha \times (k)_{n-2,n} - 1 \times (k)_{n,n}\Big) \\
= \ & (8\alpha) \times (1 \times 0 + 1 \times 0 - 1 \times 0 - 8\alpha \times 1 - 8\alpha \times 0 + 8\alpha \times 0 \cdots \\
& \cdots + 8\alpha \times 0 - 1 \times 0) \\
= \ & (8\alpha) \times (-8\alpha) \\
= \ & -64\alpha^2
\end{aligned}
$$

So if α is chosen such that $-64\alpha^2$ is a defining element of $\mathbb{F}_q$, we have, by Lemma 4.1.11, that $\langle g, h\rangle \leqslant G$ contains a root subgroup R.

4.12.3 Irreducibility

In this section we show that $H := \langle g \rangle^G = \langle R \rangle^G$ acts irreducibly on the vector space V. First we define the group $G_1 := \langle b, c, (ac)^2 \rangle$.

Lemma 4.12.1. *The group G_1 acts irreducibly on the vector space V.*

Proof. Let U be a G_1-invariant subspace. Let g be the transvection in G calculated in the last section, with values $a(g)$ and $c(g)$, defined as above.

So we have:

$a(g) = (0, 1, 1, 0 \ldots, 0, -1, -1, 0, 0)$

$c(g) = (0, \ldots, 0, 8\alpha)^T$

If there exists a vector $u \in U$ which does not lie on the axis of g, then by Lemma 4.1.18 we have that $c(g) \in U$, and since $\alpha \neq 0$, we have $u := (0, \ldots, 0, 1)^T \in U$. In fact, u is the standard basis vector e_n. Now since the matrices ac and ca are close to being a permutation matrices, it is relatively simple to see how $(ac)^2$ and $(ca)^2$ act on standard basis vectors. For $i \neq 2, 3, n-4, n-3, n-2, n-1$ we have:

$(ac)^2 e_i = e_j$, where $j = i^{(c'a')^2}$.

Thus, for $i \neq 2, 3, n-4, n-3, n-2, n-1$, if $e_i \in U$ then $e_{i^{(c'a')^2}} \in U$. Also:

$$\begin{aligned}
(ac)^2 e_2 &= e_1 + \alpha e_2 - \alpha e_{n-1} \\
&= e_{2^{(c'a')^2}} + \alpha e_2 - \alpha e_{n-1} \\
(ac)^2 e_3 &= e_4 + \alpha e_2 - \alpha e_{n-1} \\
&= e_{3^{(c'a')^2}} + \alpha e_2 - \alpha e_{n-1} \\
(ac)^2 e_{n-4} &= e_{n-3} + \alpha e_{n-1} \\
&= e_{(n-4)^{(c'a')^2}} + \alpha e_{n-1} \\
(ac)^2 e_{n-3} &= e_{n-5} - \alpha e_2 \\
&= e_{(n-3)^{(c'a')^2}} - \alpha e_2 \\
(ac)^2 e_{n-2} &= e_n - \alpha e_2
\end{aligned}$$

$$
\begin{aligned}
&= e_{(n-2)^{(c'a')^2}} - \alpha e_2 \\
(ac)^2 e_{n-1} &= e_{n-2} + \alpha e_{n-1} \\
&= e_{(n-1)^{(c'a')^2}} + \alpha e_{n-1}
\end{aligned}
$$

Thus, for any i, $1 \leqslant i \leqslant 4m+2$, if $e_i \in U$, $e_2 \in U$ and $e_{n-1} \in U$ then $e_{i^{(c'a')^2}} \in U$.

Now from above, we have $e_n \in U$. Hence we have $(ac)^2 e_n = e_2 \in U$. Also we have $(ca)^2 e_n = e_{n-2} + \alpha e_n \in U$ giving us $e_{n-2} \in U$. Thus, we have $(ca)^2 e_{n-2} = -\alpha e_2 + e_{n-1} \in U$ giving us $e_{n-1} \in U$.

So, for any i, $1 \leqslant i \leqslant 4m+2$, if $e_i \in U$ then $e_{i^{(c'a')^2}} \in U$. Now, we also have $be_2 = e_3 \in U$. And so, as $e_n \in U$, $e_3 \in U$ and the permutation $(c'a')^2$ is a product of a cycle of length 5 containing n and a cycle of length $4m-3$ containing 3, we have $e_i \in U$ for all i, $1 \leqslant i \leqslant 4m+2$. Hence, since U is G_1-invariant, we have $U = V$.

So, we may assume that U is contained in the axis of g, i.e. if $u = (u_1, \ldots, u_n)^T \in U$, then $u_2 + u_3 - u_{n-3} - u_{n-2} = 0$. We look at this dually, i.e. the homogeneous linear equations satisfied by all vectors of U are represented by rows of length $4m+2$, on which G_1 acts on the right. All such equations form a subspace, X, of ${}^{4m+2}\mathbb{F}_q$. Since U is G_1-invariant, X is also.

So, we have $x := (0, 1, 1, 0 \ldots, 0, -1, -1, 0, 0) \in X$.

Then $(b + I_{4m+2}) \left(x\,(ac)^2 - \alpha x\right) = (0, \ldots 0, -2, 0, 0, 0, 0) \in X$. So we have the standard basis vector $e_{n-4}^T \in X$. Now since ac is close to being a permutation matrix, it is relatively simple to see how $(ac)^2$ acts on standard basis vectors. For $i \neq 2, n-1$ we have:

$e_i^T (ac)^2 = e_j^T$, where $j = i^{(a'c')^2}$.

Thus, for $i \neq 2, n-1$, if $e_i^T \in X$ then $e^T_{i^{(a'c')^2}} \in X$.

Now, from above, we have $e_{n-4}^T \in X$. Also, since the permutation $(a'c')^2$ is the product of a cycle of length 5 containing 1, 2, $n-2$, $n-1$ and n, and a cycle of length $4m-3$ containing $n-4$, then we can see that for

$i \neq 1, 2, n-2, n-1, n$, $e_i^T \in X$. Moreover, $e_4^T b = e_1^T \in X$, $e_3^T b = e_2^T \in X$, $e_2^T c = e_{n-2}^T \in X$, $e_1^T c = e_{n-1}^T \in X$ and $e_{n-2}^T (ca)^2 = e_n^T \in X$. Therefore,for all i, $1 \leqslant i \leqslant 4m+2$, $e_i^T \in X$. Since X is G_1-invariant, we have $X = {}^{4m+2}\mathbb{F}_q$, and so $U = 0$.

Hence G_1 is irreducible. □

Then, as the group $G_1 = \langle b, c, (ac)^2 \rangle$ satisfies the conditions of Proposition 4.1.17, and as $\alpha \neq 0$, the group $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1}$ is irreducible, and so the group $H \geqslant H_1$ is also. Now, by the choice of H it is easy to see that it contains the group R defined in the last section. Thus, if the restrictions on α from the previous section are satisfied, we have that H is an irreducible group generated by Root subgroups.

4.12.4 Invariant Forms

Lemma 4.12.2. *H does not preserve a non-degenerate symplectic form.*

Proof. We need to prove that there exists no non-degenerate symplectic form on V which is invariant under the action of G up to similarity. Let $\langle\ ,\ \rangle$ be a symplectic form on V that is preserved by G up to similarity. Then a,b and $c \in G$ preserve $\langle\ ,\ \rangle$ up to similarity with multipliers $\lambda(a)$, $\lambda(b)$ and $\lambda(c)$ respectively. Then, as a, b and c are involutions we have, from Lemma 4.1.20, $\lambda(a) = \pm 1$, $\lambda(b) = \pm 1$ and $\lambda(c) = \pm 1$.

Now as $\dim(V^+(x)) = 2m+2 \neq 2m = \dim(V^-(x))$ for all $x \in \{a, b, c\}$, by Lemma 4.1.22, $\lambda(a) = \lambda(b) = \lambda(c) = 1$. Thus, as a, b and c generate G, for all $x \in G$, the multiplier for x, $\lambda(x)$ must be equal to 1, i.e. for all $x \in G$ and all u,$v \in V$, $\langle xu, xv \rangle = \langle u, v \rangle$.

So, for $i \neq 2, 3, n-3, n-2$ we have:

$$\begin{aligned} \langle v_i, v_2 \rangle &=_g \langle v_i, v_2 - 8\alpha v_n \rangle \\ &= \langle v_i, v_2 \rangle - 8\alpha \langle v_i, v_n \rangle \end{aligned}$$

and so

$$\langle v_i, v_n \rangle = 0.$$

Also, we have:

$$\begin{aligned}
\langle v_2, v_3 \rangle &=_g \langle v_2 + 8\alpha v_n, v_3 + 8\alpha v_n \rangle \\
&= \langle v_2, v_3 \rangle + 8\alpha \langle v_2, v_n \rangle + 8\alpha \langle v_n, v_3 \rangle + 64\alpha^2 \langle v_n, v_n \rangle \\
&= \langle v_2, v_3 \rangle + 8\alpha \langle v_2, v_n \rangle - 8\alpha \langle v_3, v_n \rangle + 0, \\
\langle v_2, v_{n-3} \rangle &=_g \langle v_2 + 8\alpha v_n, v_{n-3} - 8\alpha v_n \rangle \\
&= \langle v_2, v_{n-3} \rangle - 8\alpha \langle v_2, v_n \rangle + 8\alpha \langle v_n, v_{n-3} \rangle - 64\alpha^2 \langle v_n, v_n \rangle \\
&= \langle v_2, v_{n-3} \rangle - 8\alpha \langle v_2, v_n \rangle - 8\alpha \langle v_{n-3}, v_n \rangle + 0, \\
\langle v_2, v_{n-2} \rangle &=_g \langle v_2 + 8\alpha v_n, v_{n-2} - 8\alpha v_n \rangle \\
&= \langle v_2, v_{n-2} \rangle - 8\alpha \langle v_2, v_n \rangle + 8\alpha \langle v_n, v_{n-2} \rangle - 64\alpha^2 \langle v_n, v_n \rangle \\
&= \langle v_2, v_{n-2} \rangle - 8\alpha \langle v_2, v_n \rangle - 8\alpha \langle v_{n-2}, v_n \rangle + 0
\end{aligned}$$

and so

$$\begin{aligned}
\langle v_2, v_n \rangle &= \langle v_3, v_n \rangle \\
&= -\langle v_{n-3}, v_n \rangle \\
&= -\langle v_{n-2}, v_n \rangle
\end{aligned}$$

Now since we also have:

$$\begin{aligned}
\langle v_2, v_n \rangle &=_b \langle v_3, -v_n \rangle \\
&= -\langle v_3, v_n \rangle,
\end{aligned}$$

we have, for all i, $1 \leqslant i \leqslant n$, $\langle v_i, v_n \rangle = 0$. Thus, $v_n \in V_\perp$ and so the form $\langle\ ,\ \rangle$ is degenerate.

Hence there is no non-degenerate symplectic form on V which is invariant under the action of G up to similarity, and so H does not preserve a non-degenerate symplectic form. □

Hence H cannot be conjugate to $Sp_{4m+2}(q)$.

4.12.5 Equations

The only restrictions we have are that $q \neq 9$ and $-64\alpha^2 \neq 0$ and is a defining element of $\mathbb{F}_q$. Taking α to be any primitive element of $\mathbb{F}_q$ will satisfy these restrictions on α. Hence for $q \neq 9$, there exists an element $\alpha \in \mathbb{F}_q$ that satisfies these restrictions.

4.12.6 Conclusion

We conclude this section by summarising the above.

Lemma 4.12.3. *For q odd, $q \neq 9$ and $m \geqslant 2$, $\exists\ \alpha \in \mathbb{F}_q$ s.t. the elements a, b and c generate $SL_{4m}(q)$, and so $L_{4m}(q)$ has Property 2 and hence also has Property 1.*

Proof.

1. In section 4.12.1 we exhibited elements in $SL_{4m+2}(q)$, a, b and c such that a and b commute and a, b, c and ab are conjugate involutions in $SL_{4m+2}(q)$. Under the natural homomorphism $SL_{4m+2}(q) \longrightarrow L_{4m+2}(q)$ they map to involutions a', b' and c' such that a' and b' commute and a', b', c' and $a'b'$ are conjugate in $L_{4m+2}(q)$. The elements are defined in terms of a variable $\alpha \in \mathbb{F}_q$. We called the group generated by these elements G.

2. In section 4.12.2 we demonstrated that there is a non-trivial transvection, in G, $g := (bc)^8$. We also demonstrated that the transvection $h := g^{(ac)^2} \in G$ is opposite to g. Dickson's Lemma (Lemma 4.1.2) then gives us that G contains the whole root subgroup R, consisting of all transvections with the same centre and the same axis as g, subject to $-64\alpha^2$ being a defining element of $\mathbb{F}_q$.

3. In section 4.12.3 we then considered a subgroup $G_1 := \left\langle b, c, (ac)^2 \right\rangle \leqslant G$, containing R, and the normal closure $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1} \trianglelefteq G_1$ of the root subgroup R in G_1. We have shown that the group G_1 is irreducible

and so the group H_1 is also irreducible. Thus $H := \langle g \rangle^G = \langle R \rangle^G$ is irreducible, and so is an irreducible group generated by root subgroups. Thus from Lemma 4.1.1, H either coincides with $SL_{4m+2}(q)$, or H is conjugate to $Sp_{4m+2}(q)$.

4. In section 4.12.4 we excluded the symplectic case by showing that G does not preserve a non-degenerate symplectic form up to similarity. This implies that, when α satisfies the imposed restrictions, we have that $G \trianglerighteq H = SL_{4m+2}(q)$ and hence, $G \cong SL_{4m+2}(q)$.

5. Finally, in section 4.12.5 it was shown that the there exists an α such that the restrictions on it can be satisfied.

□

4.13 Dimension $n = 4m + 3$, $m \geqslant 2$

In this section, we show that, for q odd, $q \neq 9$ and $m \geqslant 2$, $L_{4m+3}(q)$ has Property 2, and hence Property 1. We do so by showing that $SL_{4m+3}(q)$ can be generated by suitable elements by following the method outlined in section 4.1. We work in the standard representation of $SL_{4m+3}(q)$, i.e. $(4m+3)\times(4m+3)$ matrices acting on the space of column vectors of length $4m+3$. We call this vector space V.

4.13.1 Generators

We define:

$$a := \begin{pmatrix} & & 1 & & & \\ & \iddots & & & & \\ 1 & & & & & \\ & & & -1 & & \\ & & & & 0 & 1 \\ & & & & 1 & 0 \end{pmatrix}$$

which is close to permuting the standard basis as the permutation

$$a' = \underbrace{(1,n-3)\dots(2m,2m+1)}_{(l,n-2-l)\ 1\leqslant l\leqslant 2m}(n-2)\,(n-1,n)$$

$$b := \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & 1 & & \\ & & & & & & -1 & \\ & & & & & & & -1 \end{pmatrix}$$

which is close to permuting the standard basis as the permutation

$$b' = \underbrace{(1,2)\dots(n-4,n-3)}_{(2l-1,2l)\ 1\leqslant l\leqslant 2m}$$

$$c := \begin{pmatrix} & & & & & & & & & & 1 & \\ & & & & & & & & & 1 & & \\ & & & & & & & & 1 & & & \\ & & & & & & & 1 & & & & \\ & & & & & & 1 & & & & & \\ & & & & & \iddots & & & & & & \\ & & & & 1 & & & & & & & \\ & & & 1 & & & & & & & & \\ & & 1 & & & & & & & & & \\ & 1 & & & & & & & & & & \\ 1 & & & & & & & & & & & \\ 0 & 0 & \alpha & \alpha & 0 & \cdots & 0 & \alpha & \alpha & 0 & 0 & -1 \end{pmatrix} \text{ for some } 0 \neq \alpha \in \mathbb{F}_q$$

which is close to permuting the standard basis as the permutation

$$c' = \underbrace{(1,n-1)\dots(2m+1,2m+2)}_{(l,n-l)\ 1\leqslant l\leqslant 2m+1}(n)$$

Hence

$$ab = \begin{pmatrix} & & 1 & & & & & \\ & & & 1 & & & & \\ & \iddots & & & & & & \\ 1 & & & & & & & \\ & 1 & & & & & & \\ & & & & -1 & & & \\ & & & & & 0 & -1 & \\ & & & & & -1 & 0 & \end{pmatrix}$$

As a, b, c and ab are all involutions with eigenvalues $\left\{(1)^{2m+1},(-1)^{2m+2}\right\}$,

from the properties of involutions, we can see that they are conjugate in $SL_{4m+3}(q)$, and a and b commute. We take $G := \langle a, b, c \rangle$.

4.13.2 Transvections and Root Subgroups

In this section, we show that the group G defined above, contains two opposite transvections, and so from Lemma 4.1.11, G contains a root subgroup.

We have:

$$
\begin{aligned}
g &:= (bc)^8 \\
&= \begin{pmatrix}
1 & & & & & & & & & & & \\
& 1 & & & & & & & & & & \\
& & 1 & & & & & & & & & \\
& & & 1 & & & & & & & & \\
& & & & 1 & & & & & & & \\
& & & & & \ddots & & & & & & \\
& & & & & & 1 & & & & & \\
& & & & & & & 1 & & & & \\
& & & & & & & & 1 & & & \\
& & & & & & & & & 1 & & \\
& & & & & & & & & & 1 & \\
0 & 0 & -8\alpha & -8\alpha & 0 & \cdots & 0 & -8\alpha & -8\alpha & 0 & 0 & -1
\end{pmatrix} \\
&= I_n + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -8\alpha \end{pmatrix} \times 1 \times \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}
\end{aligned}
$$

Hence, g is a one-dimensional transformation, and has values $a(g)$ and $c(g)$ given by:

$$
\begin{aligned}
a(g) &= \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \\
c(g) &= \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -8\alpha \end{pmatrix}
\end{aligned}
$$

Thus, by Lemma 4.1.6, g is a transvection as

$$a(g)\,c(g) \;=\; \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -8\alpha \end{pmatrix} \;=\; 0$$

Now we want another transvection, h, such that h is opposite to g. From Lemma 4.1.10 g and h are opposite if, for $\gamma := a(g)\,c(h)$, and $\delta := a(h)\,c(g)$, we have $\gamma\delta \neq 0$. We also want $\gamma\delta$ to be a defining element of $\mathbb{F}_q$.

We take $h := g^k = k^{-1}gk$, where $k := (ac)^2$. Since h is conjugate to g, h is a transvection. Now, since we only want to know the value of $\gamma\delta$, we do not need to calculate h explicitly. We use the fact that the generators we have chosen are very close to being permutation matrices to do a much easier calculation.

Now

$$ac \;=\; \begin{pmatrix} & & 1 & & & & & & & & & \\ & & & 1 & & & & & & & & \\ & & & & 1 & & & & & & & \\ & & & & & \ddots & & & & & & \\ & & & & & & 1 & & & & & \\ & & & & & & & 1 & & & & \\ & & & & & & & & 1 & & & \\ & & & & & & & & & 1 & & \\ & & & & & & & & & & 1 & \\ & -1 & & & & & & & & & & \\ 0 & 0 & \alpha & \alpha & 0 & \cdots & 0 & \alpha & \alpha & 0 & 0 & -1 \\ 1 & & & & & & & & & & & \end{pmatrix} \text{ and}$$

$$ca = \begin{pmatrix} & & & & & & & & & & & 1 \\ & & & & & & & & & -1 & & \\ 1 & & & & & & & & & & & \\ & 1 & & & & & & & & & & \\ & & 1 & & & & & & & & & \\ & & & \ddots & & & & & & & & \\ & & & & 1 & & & & & & & \\ & & & & & 1 & & & & & & \\ & & & & & & 1 & & & & & \\ & & & & & & & 1 & & & & \\ & & & & & & & & 1 & & & \\ \alpha & \alpha & 0 & \cdots & 0 & \alpha & \alpha & 0 & 0 & 0 & -1 & 0 \end{pmatrix}$$

i.e. ac is very close to being the permutation matrix representing the permutation

$$a'c' = (1, 3, 5, \ldots, n-2, 2, 4, 6, \ldots, n-1, n).$$

(a cycle of length $4m+3$). Using this we can easily calculate $(ac)^2$ and $(ca)^2$.

Note that $(a'c')^2 : n-3 \longmapsto n \longmapsto 3$.

In calculating $\gamma\delta$, we will only need the 1^{st} and the $(2m+1)^{th}$ rows of k^{-1} and the entries $(k)_{1,n}$, $(k)_{2m+1,n}$, $(k)_{n-2,n}$ and $(k)_{n,n}$ from k, as will be made clear below. Since ca is very close to being a permutation matrix, it is easy to see that the 1^{st} row of $k^{-1} = (ca)^2$ is in fact equal to $\begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & 0 \end{pmatrix}$, and the $(2m+1)^{th}$ row of k^{-1} is equal to $\begin{pmatrix} 0 & \cdots & 0 & 1 \end{pmatrix}$. Similarly, since ac is very close to being a permutation matrix, it is easy to see that $(k)_{1,n} = -1$, $(k)_{2m+1,n} = 0$, $(k)_{n-2,n} = 0$ and $(k)_{n,n} = 0$.

Now

$$\begin{aligned} \gamma\delta &= a(g)\, c(h)\, a(h)\, c(g) \\ &= \left(\begin{array}{cccc|c|cccc} 0 & 0 & 1 & 1 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 & 0 \end{array}\right) (c(h)\, a(h)) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -8\alpha \end{pmatrix} \end{aligned}$$

$$
\begin{aligned}
&= \left(\begin{array}{cccc|c|cccc} 0 & 0 & 1 & 1 & 0 \cdots 0 & 1 & 1 & 0 & 0 & 0 \end{array}\right)(h - I_n)\begin{pmatrix} 0 \\ \vdots \\ 0 \\ -8\alpha \end{pmatrix} \\
&= \left(1 \times \left(3^{rd}\ row\ of\ \ (h - I_n)\right) + 1 \times \left(4^{th}\ row\ of\ \ (h - I_n)\right) \cdots\right. \\
&\quad \cdots + 1 \times \left((n-4)^{th}\ \ row\ of\ \ (h - I_n)\right) \cdots \\
&\quad \left. \cdots + 1 \times \left((n-3)^{th}\ \ row\ of\ \ (h - I_n)\right)\right) \times \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -8\alpha \end{pmatrix} \\
&= \left(1 \times \left((h - I_n)_{3,n}\right) + 1 \times \left((h - I_n)_{4,n}\right) \cdots\right. \\
&\quad \left. \cdots + 1 \times \left((h - I_n)_{n-4,n}\right) + 1 \times \left((h - I_n)_{n-3,n}\right)\right) \times (-8\alpha) \\
&= (-8\alpha) \times \left((h)_{3,n} + (h)_{4,n} + (h)_{n-4,n} + (h)_{n-3,n}\right) \\
&= (-8\alpha) \times \left(\left(k^{-1}gk\right)_{3,n} + \left(k^{-1}gk\right)_{4,n} + \left(k^{-1}gk\right)_{n-4,n} + \left(k^{-1}gk\right)_{n-3,n}\right) \\
&= (-8\alpha) \times \left(\left(3^{rd}\ row\ of\ k^{-1}\right) \times \left(n^{th}\ column\ of\ gk\right) \cdots\right. \\
&\quad \cdots + \left(4^{th}\ row\ of\ k^{-1}\right) \times \left(n^{th}\ column\ of\ gk\right) \cdots \\
&\quad \cdots + \left((n-4)^{th}\ \ row\ of\ k^{-1}\right) \times \left(n^{th}\ column\ of\ gk\right) \cdots \\
&\quad \left. \cdots + \left((n-3)^{rd}\ \ row\ of\ k^{-1}\right) \times \left(n^{th}\ column\ of\ gk\right)\right) \\
&= (-8\alpha) \times \left(\left(\begin{array}{cccc} 0 & \cdots & 0 & 1 \end{array}\right) \times \left(n^{th}\ column\ of\ gk\right) \cdots\right. \\
&\quad \cdots + \left(\begin{array}{cccccc} 0 & \cdots & 0 & -1 & 0 & 0 \end{array}\right) \times \left(n^{th}\ column\ of\ gk\right) \cdots \\
&\quad \cdots + \left(\begin{array}{cccccccccc} 0 & \cdots & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \times \cdots \\
&\quad \cdots \times \left(n^{th}\ column\ of\ gk\right) + \cdots \\
&\quad \left. \cdots + \left(\begin{array}{cccccccccc} 0 & \cdots & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \times \left(n^{th}\ column\ of\ gk\right)\right) \\
&= (-8\alpha) \times \cdots \\
&\quad \cdots \times \left(1 \times (gk)_{n,n} - 1 \times (gk)_{n-2,n} + 1 \times (gk)_{n-8,n} + 1 \times (gk)_{n-7,n}\right) \\
&= (-8\alpha) \times \left(\left(n^{th}\ row\ of\ g\right) \times \left(n^{th}\ column\ of\ k\right) \cdots\right. \\
&\quad \cdots - \left((n-2)^{th}\ \ row\ of\ g\right) \times \left(n^{th}\ column\ of\ k\right) \cdots \\
&\quad \left. \cdots + \left((n-8)^{th}\ \ row\ of\ g\right) \times \left(n^{th}\ column\ of\ k\right) \cdots\right.
\end{aligned}
$$

$$
\begin{aligned}
&\cdots + \Big((n-7)^{th} \ row\ of\ g \Big) \times \big(n^{th}\ column\ of\ k \big) \Big) \\
= \ & (-8\alpha) \times \big((\ 0 \ \ 0 \ \ -8\alpha \ \ -8\alpha \ \ 0 \ \cdots \ 0 \ \ -8\alpha \ \ -8\alpha \ \ 0 \ \ 0 \ \ 1\ ) \cdots \\
& \cdots \times \big(n^{th}\ column\ of\ k \big) \cdots \\
& \cdots - (\ 0 \ \ \cdots \ \ 0 \ \ 1 \ \ 0 \ \ 0\ ) \times \big(n^{th}\ column\ of\ k \big) \cdots \\
& \cdots + (\ 0 \ \ \cdots \ \ 0 \ \ 1 \ \ 0 \ \ 0 \ \ 0 \ \ 0 \ \ 0 \ \ 0 \ \ 0 \ \ 0\ ) \times \cdots \\
& \cdots \times \big(n^{th}\ column\ of\ k \big) + \cdots \\
& \cdots + (\ 0 \ \ \cdots \ \ 0 \ \ 1 \ \ 0 \ \ 0 \ \ 0 \ \ 0 \ \ 0 \ \ 0 \ \ 0\ ) \times \big(n^{th}\ column\ of\ k \big) \big) \\
= \ & (-8\alpha) \times \Big(\Big(-8\alpha \times (k)_{3,n} - 8\alpha \times (k)_{4,n} - 8\alpha \times (k)_{n-4,n} \ \cdots \\
& \cdots - 8\alpha \times (k)_{n-3,n} + 1 \times (k)_{n,n} \Big) \cdots \\
& \cdots - 1 \times (k)_{n-2,n} + 1 \times (k)_{n-8,n} + 1 \times (k)_{n-7,n} \Big) \\
= \ & (-8\alpha) \times ((-8\alpha \times 0 - 8\alpha \times 0 - 8\alpha \times 0 - 8\alpha \times (-1) + 1 \times 0) \cdots \\
& \cdots - 1 \times 0 + 1 \times 0 + 1 \times 0) \\
= \ & (-8\alpha) \times (8\alpha) \\
= \ & -64\alpha^2
\end{aligned}
$$

So if α is chosen such that $-64\alpha^2$ is a defining element of $\mathbb{F}_q$, we have, by Lemma 4.1.11, that $\langle g, h \rangle \leqslant G$ contains a root subgroup R.

4.13.3 Irreducibility

In this section we show that $H := \langle g \rangle^G = \langle R \rangle^G$ acts irreducibly on the vector space V. First we define the group $G_1 := \langle b, c, (ac)^2 \rangle$.

Lemma 4.13.1. *The group G_1 acts irreducibly on the vector space V.*

Proof. Let U be a G_1-invariant subspace. Let g be the transvection in G calculated in the last section, with values $a(g)$ and $c(g)$, defined as above.

So we have:

$a(g) = (0, 0, 1, 1, 0, \ldots, 0, 1, 1, 0, 0, 0)$

$c(g) = (0, \ldots, 0, -8\alpha)^T$

If there exists a vector $u \in U$ which does not lie on the axis of g, then by Lemma 4.1.18 we have that $c(g) \in U$, and since $\alpha \neq 0$, we have $u := (0, \ldots, 0, 1)^T \in U$. In fact, u is the standard basis vector e_n. Now since the matrix ca is close to being a permutation matrix, it is relatively simple to see how $(ca)^2$ acts on standard basis vectors. For $i \neq 1, 2, n-8, n-7, n-6, n-5, n-2, n$ we have:

$(ca)^2 e_i = \pm e_j$, where $j = i^{(a'c')^2}$.

Thus, for $i \neq 1, 2, n-8, n-7, n-6, n-5, n-2, n$, if $e_i \in U$ then $e_{i^{(a'c')^2}} \in U$. Also:

$$\begin{aligned}
(ca)^2 e_1 &= e_5 + \alpha e_1 \\
&= e_{1^{(a'c')^2}} + \alpha e_1 \\
(ca)^2 e_2 &= e_6 + \alpha e_1 \\
&= e_{2^{(a'c')^2}} + \alpha e_1 \\
(ca)^2 e_{n-8} &= e_{n-4} + \alpha e_n \\
&= e_{(n-8)^{(a'c')^2}} + \alpha e_n \\
(ca)^2 e_{n-7} &= e_{n-3} + \alpha e_n \\
&= e_{(n-7)^{(a'c')^2}} + \alpha e_n \\
(ca)^2 e_{n-6} &= e_{n-2} + \alpha e_1 \\
&= e_{(n-6)^{(a'c')^2}} + \alpha e_1 \\
(ca)^2 e_{n-5} &= e_{n-1} + \alpha e_1 \\
&= e_{(n-5)^{(a'c')^2}} + \alpha e_1 \\
(ca)^2 e_{n-2} &= e_4 + \alpha e_n \\
&= e_{(n-5)^{(a'c')^2}} + \alpha e_n \\
(ca)^2 e_n &= e_3 + \alpha e_n \\
&= e_{n^{(a'c')^2}} + \alpha e_n
\end{aligned}$$

Thus, for $i = 1, 2, n-6, n-5$, if $e_i \in U$ and $e_1 \in U$, then $e_{i^{(a'c')^2}} \in U$. Also,

for $i = n-8, n-7, n-2, n$, if $e_i \in U$ and $e_n \in U$, then $e_{i^{(a'c')^2}} \in U$.

Now, from above, we have $e_n \in U$. Also, $n^{(a'c')^{2m+2}} = 2$, and as $n^{(a'c')^{2i}} \neq 1, n-6, n-5$ for $1 \leqslant i \leqslant m+1$, we have $e_2 \in U$. Thus, we have $be_2 = e_1 \in U$. And so, as $e_1 \in U$, $e_n \in U$ and the permutation $(a'c')^2$ is a cycle of length $4m+3$, we have $e_i \in U$ for all i, $1 \leqslant i \leqslant 4m+3$. Hence, since U is G_1-invariant, we have $U = V$.

So, we may assume that U is contained in the axis of g, i.e. if $u = (u_1, \ldots, u_n)^T \in U$, then $u_3 + u_4 + u_{n-4} + u_{n-3} = 0$. We look at this dually, i.e. the homogeneous linear equations satisfied by all vectors of U are represented by rows of length $4m+3$, on which G_1 acts on the right. All such equations form a subspace, X, of ${}^{4m+3}\mathbb{F}_q$. Since U is G_1-invariant, X is also.

So, we have $x := (0, 0, 1, 1, 0, \ldots, 0, 1, 1, 0, 0, 0) \in X$.

Then $x(ac)^2 (I_{4m+3} - b) = (0, \ldots, 0, 2) \in X$. So we have the standard basis vector $e_n^T \in X$. Now since ac is close to being a permutation matrix, it is relatively simple to see how $(ac)^2$ acts on standard basis vectors. For $i \neq n-1, n-3$ we have:

$e_i^T (ac)^2 = \pm e_j^T$, where $j = i^{(a'c')^2}$.

Thus, for $i \neq n-1, n-3$, if $e_i^T \in X$ then $e^T_{i^{(a'c')^2}} \in X$.

Now, from above, we have $e_n^T \in X$. Also, since the permutation $(a'c')^2$ is a cycle of length $4m+3$ and we have $n^{(a'c')^{2m+2}} = 2$, $n^{(a'c')^{4m+2}} = n-1$ and $n^{(a'c')^{8m+4}} = n-3$, then we can see that $e_n^T (ac)^{2m+2} = e_2^T \in X$. Thus $e_2^T b = e_1^T \in X$. From this it can be seen that the set $\left\{ e_n^T (ac)^{2k}, e_1^T (ac)^{2l} \,|\, 0 \leqslant k \leqslant 2m+1, 0 \leqslant l \leqslant 2m \right\} \subset X$ must be a set of standard basis vectors of size $4m+3$. Therefore, for all i, $1 \leqslant i \leqslant 4m+3$, $e_i^T \in X$. Since X is G_1-invariant, we have $X = {}^{4m+3}\mathbb{F}_q$, and so $U = 0$.

Hence G_1 is irreducible. □

Then, as the group $G_1 = \langle b, c, (ac)^2 \rangle$ satisfies the conditions of Proposition 4.1.17, and as $\alpha \neq 0$, the group $H_1 = \langle g \rangle^{G_1} = \langle R \rangle^{G_1}$ is irreducible, and so

the group $H \geqslant H_1$ is also. Now, by the choice of H it is easy to see that it contains the group R defined in the last section. Thus, if the restrictions on α from the previous section are satisfied, we have that H is an irreducible group generated by Root subgroups.

4.13.4 Invariant Forms

There are no non-degenerate symplectic forms in dimension $4m + 3$.

4.13.5 Equations

The only restrictions we have are that $q \neq 9$ and $-64\alpha^2 \neq 0$ and is a defining element of $\mathbb{F}_q$. Taking α to be any primitive element of $\mathbb{F}_q$ will satisfy these restrictions on α. Hence for $q \neq 9$, there exists an element $\alpha \in \mathbb{F}_q$ that satisfies these restrictions.

4.13.6 Conclusion

We conclude this section by summarising the above.

Lemma 4.13.2. *For q odd, $q \neq 9$ and $m \geqslant 2$, $\exists\ \alpha \in \mathbb{F}_q$ s.t. the elements a, b and c generate $SL_{4m+3}(q)$, and so $L_{4m+3}(q)$ has Property 2 and hence also has Property 1.*

Proof.

1. In section 4.13.1 we exhibited elements in $SL_{4m+3}(q)$, a, b and c such that a and b commute and a, b, c and ab are conjugate involutions in $SL_{4m+3}(q)$. Under the natural homomorphism $SL_{4m+3}(q) \longrightarrow L_{4m+3}(q)$ they map to involutions a', b' and c' such that a' and b' commute and a', b', c' and $a'b'$ are conjugate in $L_{4m+3}(q)$. The elements are defined in terms of a variable $\alpha \in \mathbb{F}_q$. We called the group generated by these elements G.

2. In section 4.13.2 we demonstrated that there is a non-trivial transvection, in G, $g := (bc)^8$. We also demonstrated that the transvection

$h := g^{(ac)^2} \in G$ is opposite to g. Dickson's Lemma (Lemma 4.1.2) then gives us that G contains the whole root subgroup R, consisting of all transvections with the same centre and the same axis as g, subject to $-16\alpha^2$ being a defining element of $\mathbb{F}_q$.

3. In section 4.13.3 we then considered a subgroup $G_1 := \left\langle b, c, (ac)^2 \right\rangle \leqslant G$, containing R, and the normal closure $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1} \trianglelefteq G_1$ of the root subgroup R in G_1. We have shown that the group G_1 is irreducible and so the group H_1 is also irreducible. Thus $H := \langle g \rangle^G = \langle R \rangle^G$ is irreducible, and so is an irreducible group generated by root subgroups. Thus from Lemma 4.1.1, H must coincide with $SL_{4m+3}(q)$.

4. There are no non-degenerate symplectic forms in dimension $4m + 1$. This implies that, when α satisfies the imposed restrictions, we have that $G \trianglerighteq H = SL_{4m+3}(q)$ and hence, $G \cong SL_{4m+3}(q)$.

5. Finally, in section 4.13.5 it was shown that the there exists an α such that the restrictions on it can be satisfied.

□

4.14 Dimension $n = 4m$, $m \geqslant 3$

In this section, we show that, for q odd, $q \neq 9$ and $m \geqslant 3$, $L_{4m}(q)$ has Property 2, and hence Property 1. We do so by showing that $SL_{4m}(q)$ can be generated by suitable elements by following the method outlined in section 4.1. We work in the standard representation of $SL_{4m}(q)$, i.e. $(4m) \times (4m)$ matrices acting on the space of column vectors of length $4m$. We call this vector space V.

4.14.1 Generators

We define:

$$a := \begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & 1 \\ & & & 1 & 0 \end{pmatrix}$$

which can be thought of as permuting the

standard basis as the permutation

$$a' = \underbrace{(1,2)\dots(n-1,n)}_{(2l-1,2l)\ 1\leqslant l\leqslant 2m},$$

$$b := \left(\begin{array}{ccc|c|c|cc} & & 1 & & & & \\ & 1 & & & & & \\ 1 & & & & & & \\ & & & -1 & & & \\ & & & & \ddots & & \\ & & & & & -1 & \\ \hline & & & & & & \\ \hline & & & & & & \\ \hline & & & & & & \end{array}\right.$$

$$\left.\begin{array}{c|c|cc} & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ \hline 1 & & & \\ \hline & \ddots & & \\ & & 1 & \\ \hline & & -1 & \\ & & & -1 \end{array}\right)$$

which is close to permuting the standard basis as the permutation

$$b' = (1,4)\,(2,3)$$

$$c := \begin{pmatrix} & & & & & & & & 1 & \\ & & & & & & & 1 & & \\ & & & & & & 1 & & & \\ & & & & & 1 & & & & \\ & & & & \iddots & & & & & \\ & & & 1 & & & & & & \\ & & 1 & & & & & & & \\ & 1 & & & & & & & & \\ 1 & & & & & & & & & \\ 0 & \alpha & \alpha & 0 & \cdots & 0 & \alpha & \alpha & 0 & -1 \end{pmatrix} \text{ for some } 0 \neq \alpha \in \mathbb{F}_q$$

which is close to permuting the standard basis as the permutation

$$c' = \underbrace{(1, n-1) \dots (2m-1, 2m+1)}_{(l,n-l)\ 1 \leqslant l \leqslant 2m-1} (2m)\,(n)$$

Hence

$$ab = \left(\begin{array}{cccc|c|c|cc}
 & & 1 & & & & & \\
 & & & 1 & & & & \\
1 & & & & & & & \\
 & 1 & & & & & & \\
\hline
 & & & & \overbrace{\begin{matrix} & -1 \\ -1 & \\ & & \ddots \\ & & & & -1 \\ & & & -1 & \end{matrix}}^{2m-4} & & & \\
\hline
 & & & & & \overbrace{\begin{matrix} & 1 \\ 1 & \\ & & \ddots \\ & & & & 1 \\ & & & 1 & \end{matrix}}^{2m-2} & & \\
\hline
 & & & & & & & -1 \\
 & & & & & & -1 &
\end{array}\right)$$

As a, b, c and ab are all involutions with eigenvalues $\left\{(1)^{2m}, (-1)^{2m}\right\}$, from the properties of involutions, we can see that they are conjugate in $SL_{4m}(q)$, and a and b commute. We take $G := \langle a, b, c \rangle$.

4.14.2 Transvections and Root Subgroups

In this section, we show that the group G defined above, contains two opposite transvections, and so from Lemma 4.1.11, G contains a root subgroup.

We have:

$$\begin{aligned} g &:= (bc)^8 \\ &= \begin{pmatrix} 1 & & & & & & & & & \\ & 1 & & & & & & & & \\ & & 1 & & & & & & & \\ & & & 1 & & & & & & \\ & & & & \ddots & & & & & \\ & & & & & 1 & & & & \\ & & & & & & 1 & & & \\ & & & & & & & 1 & & \\ & & & & & & & & 1 & \\ 0 & -8\alpha & -8\alpha & 0 & \cdots & 0 & -8\alpha & -8\alpha & 0 & 1 \end{pmatrix} \end{aligned}$$

$$= I_n + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -8\alpha \end{pmatrix} \times 1 \times \begin{pmatrix} 0 & 1 & 1 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Hence, g is a one-dimensional transformation, and has values $a(g)$ and $c(g)$ given by:

$$\begin{aligned} a(g) &= \begin{pmatrix} 0 & 1 & 1 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \\ c(g) &= \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -8\alpha \end{pmatrix} \end{aligned}$$

Thus, by Lemma 4.1.6, g is a transvection as

$$a(g)\,c(g) = \begin{pmatrix} 0 & 1 & 1 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -8\alpha \end{pmatrix} = 0$$

Now we want another transvection, h, such that h is opposite to g. From Lemma 4.1.10 g and h are opposite if, for $\gamma := a(g)\,c(h)$, and $\delta := a(h)\,c(g)$, we have $\gamma\delta \neq 0$. We also want $\gamma\delta$ to be a defining element of $\mathbb{F}_q$.

We take $h := g^k = k^{-1}gk$, where $k := (ac)^2$. Since h is conjugate to g, h is a transvection. Now, since we only want to know the value of $\gamma\delta$, we do not need to calculate h explicitly. We use the fact that the generators we have chosen are very close to being permutation matrices to do a much easier calculation.

Now

$$ac = \begin{pmatrix} & & & & & & & & 1 & \\ & & & & & & & & & 1 \\ & & & & & & & \iddots & & \\ & & & & & & \iddots & & & \\ & & & & & \iddots & & & & \\ & & & & \iddots & & & & & \\ & & 1 & & & & & & & \\ & & & 1 & & & & & & \\ 0 & \alpha & \alpha & 0 & \cdots & 0 & \alpha & \alpha & 0 & -1 \\ 1 & & & & & & & & & \end{pmatrix} \text{ and}$$

$$ca = \begin{pmatrix} & & & & & & & & & 1 \\ & & & & & & & & 1 & \\ & & & & & & & \iddots & & \\ & & & & & & \iddots & & & \\ & & & & & \iddots & & & & \\ & & & & \iddots & & & & & \\ & & & 1 & & & & & & \\ & & & & 1 & & & & & \\ 1 & & & & & & & & & \\ & 1 & & & & & & & & \\ \alpha & 0 & 0 & \alpha & 0 & \cdots & 0 & \alpha & \alpha & -1 & 0 \end{pmatrix}$$

i.e. ac is very close to being the permutation matrix representing the permutation

$$a'c' = (1, n-2, 3, n-4, \ldots, 2, n-1, n),$$

(a cycle of length $4m$). Using this we can easily calculate $(ac)^2$ and $(ca)^2$.

Note that $(a'c')^2 : 2 \longmapsto n \longmapsto n-2$.

In calculating $\gamma\delta$, we will only need the 2^{nd}, 3^{rd}, $(n-3)^{rd}$ and $(n-2)^{nd}$ rows of k^{-1} and the entries $(k)_{1,n}$, $(k)_{2,n}$, $(k)_{3,n}$, $(k)_{4,n}$, $(k)_{n-5,n}$, $(k)_{n-3,n}$, $(k)_{n-2,n}$ and $(k)_{n,n}$ from k, as will be made clear below. Since ca is very close to being a permutation matrix, it is easy to see that the 2^{nd} row of $k^{-1} = (ca)^2$ is in fact equal to $\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$, the 3^{rd} row of k^{-1} is equal to

$\begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$, the $(n-3)^{rd}$ row of k^{-1} is equal to
$\begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$, and the $(n-2)^{nd}$ row of k^{-1} is equal to
$\begin{pmatrix} 0 & \cdots & 0 & 1 \end{pmatrix}$ Similarly, since ac is very close to being a permutation matrix, it is easy to see that $(k)_{1,n} = 0$, $(k)_{2,n} = -1$, $(k)_{3,n} = 0$, $(k)_{4,n} = 0$, $(k)_{n-5,n} = 0$, $(k)_{n-3,n} = 0$, $(k)_{n-2,n} = 0$ and $(k)_{n,n} = 0$.

Now

$$\begin{aligned}
\gamma\delta &= a(g)\,c(h)\,a(h)\,c(g) \\
&= \begin{pmatrix} 0 & 1 & 1 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 \end{pmatrix} (c(h)\,a(h)) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -8\alpha \end{pmatrix} \\
&= \begin{pmatrix} 0 & 1 & 1 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 \end{pmatrix} (h - I_n) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -8\alpha \end{pmatrix} \\
&= \left(1 \times \left(2^{nd}\ row\ of\ h - I_n\right) + 1 \times \left(3^{rd}\ row\ of\ h - I_n\right) \cdots \right. \\
&\quad \cdots + 1 \times \left((n-3)^{rd}\ row\ of\ h - I_n\right) + \cdots \\
&\quad \left. \cdots + 1 \times \left((n-2)^{nd}\ row\ of\ h - I_n\right)\right) \times \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -8\alpha \end{pmatrix} \\
&= \left(1 \times \left((h - I_n)_{2,n}\right) + 1 \times \left((h - I_n)_{3,n}\right) \cdots \right. \\
&\quad \left. \cdots + 1 \times \left((h - I_n)_{n-3,n}\right) + 1 \times \left((h - I_n)_{n-2,n}\right)\right) \times (-8\alpha) \\
&= (-8\alpha) \times \left((h)_{2,n} + (h)_{3,n} + (h)_{n-3,n} + (h)_{n-2,n}\right) \\
&= (-8\alpha) \times \left(\left(k^{-1}gk\right)_{2,n} + \left(k^{-1}gk\right)_{3,n} \left(k^{-1}gk\right)_{n-3,n} + \left(k^{-1}gk\right)_{n-2,n}\right) \\
&= (-8\alpha) \times \left(\left(2^{nd}\ row\ of\ k^{-1}\right) \times \left(n^{th}\ column\ of\ gk\right) \cdots \right. \\
&\quad \cdots + \left(3^{rd}\ row\ of\ k^{-1}\right) \times \left(n^{th}\ column\ of\ gk\right) \cdots \\
&\quad \cdots + \left((n-3)^{rd}\ row\ of\ k^{-1}\right) \times \left(n^{th}\ column\ of\ gk\right) \cdots \\
&\quad \left. \cdots + \left((n-2)^{nd}\ row\ of\ k^{-1}\right) \times \left(n^{th}\ column\ of\ gk\right)\right) \\
&= (-8\alpha) \times \left(\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 \end{pmatrix} \times \left(n^{th}\ column\ of\ gk\right) \cdots \right.
\end{aligned}$$

$$
\begin{aligned}
&\cdots + \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix} \times \left(n^{th}\ column\ of\ gk\right) \cdots \\
&\cdots + \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \times \left(n^{th}\ column\ of\ gk\right) \cdots \\
&\cdots + \begin{pmatrix} 0 & \cdots & 0 & 1 \end{pmatrix} \times \left(n^{th}\ column\ of\ gk\right) + \Big) \\
= \;& (-8\alpha) \times \Big(1 \times (gk)_{4,n} + 1 \times (gk)_{1,n} + 1 \times (gk)_{n-5,n} + 1 \times (gk)_{n,n}\Big) \\
= \;& (-8\alpha) \times \Big(\left(4^{th}\ row\ of\ g\right) \times \left(n^{th}\ column\ of\ k\right) \cdots \\
&\cdots + \left(1^{st}\ row\ of\ g\right) \times \left(n^{th}\ column\ of\ k\right) \cdots \\
&\cdots + \Big(\left(n-5\right)^{th}\ row\ of\ g\Big) \times \left(n^{th}\ column\ of\ k\right) \cdots \\
&\cdots + \left(n^{th}\ row\ of\ g\right) \times \left(n^{th}\ column\ of\ k\right)\Big) \\
= \;& (-8\alpha) \times \Big(\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & \cdots & 0 \end{pmatrix} \times \left(n^{th}\ column\ of\ k\right) \cdots \\
&\cdots + \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix} \times \left(n^{th}\ column\ of\ k\right) \cdots \\
&\cdots + \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \times \left(n^{th}\ column\ of\ k\right) \cdots \\
&\cdots + \begin{pmatrix} 0 & -8\alpha & -8\alpha & 0 & \cdots & 0 & -8\alpha & -8\alpha & 0 & 1 \end{pmatrix} \times \cdots \\
&\cdots \times \left(n^{th}\ column\ of\ k\right)\Big) \\
= \;& (-8\alpha) \times \Big(1 \times (k)_{4,n} + 1 \times (k)_{1,n} + 1 \times (k)_{n-5,n} \cdots \\
&\cdots + (-8\alpha \times k_{2,n} - 8\alpha \times k_{3,n} - 8\alpha \times k_{n-3,n} - 8\alpha \times k_{n-2,n} \cdots \\
&\cdots + 1 \times k_{n,n})) \\
= \;& (-8\alpha) \times (1 \times (0) + 1 \times (0) + 1 \times (0) - 8\alpha \times (-1) - 8\alpha \times (0) \cdots \\
&\cdots - 8\alpha \times (0) - 8\alpha \times (0) + 1 \times (0)) \\
= \;& (-8\alpha) \times (8\alpha) \\
= \;& -64\alpha^2
\end{aligned}
$$

So if α is chosen such that $-64\alpha^2$ is a defining element of $\mathbb{F}_q$, we have, by Lemma 4.1.11, that $\langle g, h\rangle \leqslant G$ contains a root subgroup R.

4.14.3 Irreducibility

In this section we show that $H := \langle g\rangle^G = \langle R\rangle^G$ acts irreducibly on the vector space V. First we define the group $G_1 := \langle b, c, (ac)^2\rangle$.

Lemma 4.14.1. *The group G_1 acts irreducibly on the vector space V.*

Proof. Let U be a G_1-invariant subspace. Let g be the transvection in G calculated in the last section, with values $a(g)$ and $c(g)$, defined as above.

So we have:

$a(g) = (0, 1, 1, 0 \ldots, 0, 1, 1, 0, 0)$

$c(g) = (0, \ldots, 0, -8\alpha)^T$

If there exists a vector $u \in U$ which does not lie on the axis of g, then by Lemma 4.1.18 we have that $c(g) \in U$, and since $\alpha \neq 0$, we have $u := (0, \ldots, 0, 1)^T \in U$. In fact, u is the standard basis vector e_n. Now since the matrix ac is close to being a permutation matrix, it is relatively simple to see how $(ac)^2$ acts on standard basis vectors. For $i \neq 2, 3, n-4, n-3, n-2, n-1$ we have:

$(ac)^2 e_i = \pm e_j$, where $j = i^{(c'a')^2}$. Thus, for $i \neq 2, 3, n-4, n-3, n-2, n-1$, if $e_i \in U$ then $e_{i^{(c'a')^2}} \in U$. Also:

$$\begin{aligned}
(ac)^2 e_2 &= e_4 + \alpha e_2 + \alpha e_{n-1} \\
&= e_{2^{(c'a')^2}} + \alpha e_2 + \alpha e_{n-1} \\
(ac)^2 e_3 &= e_1 + \alpha e_2 + \alpha e_{n-1} \\
&= e_{3^{(c'a')^2}} + \alpha e_2 + \alpha e_{n-1} \\
(ac)^2 e_{n-4} &= e_{n-2} + \alpha e_{n-1} \\
&= e_{(n-4)^{(c'a')^2}} + \alpha e_{n-1} \\
(ac)^2 e_{n-3} &= e_{n-5} + \alpha e_2 \\
&= e_{(n-3)^{(c'a')^2}} + \alpha e_2 \\
(ac)^2 e_{n-2} &= e_n + \alpha e_2 \\
&= e_{(n-2)^{(c'a')^2}} + \alpha e_2 \\
(ac)^2 e_{n-1} &= e_{n-3} + \alpha e_{n-1} \\
&= e_{(n-1)^{(c'a')^2}} + \alpha e_{n-1}
\end{aligned}$$

Thus, for $i = 2, 3, n-4, n-3, n-2, n-1$, if $e_i \in U$, $e_2 \in U$ and $e_{n-1} \in U$, then $e_{i^{(c'a')^2}} \in U$.

Now, from above, we have $e_n \in U$ and so we have $e_2 \in U$. Thus we have $(ac)^2 be_2 = e_1 + \alpha e_2 + \alpha e_{n-1} \in U$, and so $e_1 + \alpha e_{n-1} \in U$. Also, we have $(ac)^2 e_2 = e_4 + \alpha e_2 + \alpha e_{n-1} \in U$, and so $e_4 + \alpha e_{n-1} \in U$, which gives us $b(e_4 + \alpha e_{n-1}) = e_1 - \alpha e_{n-1} \in U$. Thus we must also have $e_{n-1} \in U$. And so, as $e_n \in U$, $e_{n-1} \in U$, $e_2 \in U$ and the permutation $(c'a')^2$ is a product of two cycles of length $2m$, one containing all odd numbers and the other all even, and $be_4 = e_1$, we have $e_i \in U$ for all i, $1 \leqslant i \leqslant 4m$. Hence, since U is G_1-invariant, we have $U = V$.

So, we may assume that U is contained in the axis of g, i.e. if $u = (u_1, \ldots, u_n)^T \in U$, then $u_2 + u_3 + u_{n-3} + u_{n-2} = 0$. We look at this dually, i.e. the homogeneous linear equations satisfied by all vectors of U are represented by rows of length $4m$, on which G_1 acts on the right. All such equations form a subspace, X, of ${}^{4m}\mathbb{F}_q$. Since U is G_1-invariant, X is also.

So, we have $x := (0, 1, 1, 0 \ldots, 0, 1, 1, 0, 0) \in X$.

Then $\left(x(ca)^2\right)(I_{4m} - b) = (0, \ldots, 0, 2, 0) \in X$. So we have the standard basis vector $e_{n-1}^T \in X$. Now since ca is close to being a permutation matrix, it is relatively simple to see how $(ca)^2$ acts on standard basis vectors. For $i \neq 1, n$ we have:

$e_i^T (ca)^2 = \pm e_j^T$, where $j = i^{(c'a')^2}$. Thus, for $i \neq 1, n$, if $e_i^T \in X$ then $e_{i^{(c'a')^2}}^T \in X$.

Now, from above, we have $e_{n-1}^T \in X$. Also, since the permutation $(c'a')^2$ is a prouct of two cycles of length $2m$, one containing all odd numbers and the other all even, and we have $n^{(c'a')^{4m-2}} = 1$ and $n^{(c'a')^{4m-2}} = 3$ then we have $e_i^T \in X$ for odd i, $1 \leqslant i \leqslant 4m-1$. Thus we also have $e_3^T b = e_2^T \in X$, and since $2^{(c'a')^{4m-2}} = n$, we have $e_i^T \in X$ for even i, $2 \leqslant i \leqslant 4m$. and $n^{(a'c')^{8m+4}} = n-3$, then we can see that $e_n^T (ac)^{2m+2} = e_2^T \in X$. Therefore,for all i, $1 \leqslant i \leqslant 4m$, $e_i^T \in X$. Since X is G_1-invariant, we have $X = {}^{4m}\mathbb{F}_q$, and so $U = 0$.

Hence G_1 is irreducible. □

Then, as the group $G_1 = \langle b, c, (ac)^2 \rangle$ satisfies the conditions of Proposition 4.1.17, and as $\alpha \neq 0$, the group $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1}$ is irreducible, and so the group $H \geqslant H_1$ is also. Now, by the choice of H it is easy to see that it contains the group R defined in the last section. Thus, if the restrictions on α from the previous section are satisfied, we have that H is an irreducible group generated by Root subgroups.

4.14.4 Invariant Forms

Lemma 4.14.2. *H does not preserve a non-degenerate symplectic form.*

Proof. We need to prove that there exists no non-degenerate symplectic form on V which is invariant under the action of G up to similarity. Let $\langle\ ,\ \rangle$ be a symplectic form on V that is preserved by G up to similarity. Then a,b and $c \in G$ preserve $\langle\ ,\ \rangle$ up to similarity with multipliers $\lambda(a)$, $\lambda(b)$ and $\lambda(c)$ respectively. Then, as a, b and c are involutions we have, from Lemma 4.1.20, $\lambda(a) = \pm 1$, $\lambda(b) = \pm 1$ and $\lambda(c) = \pm 1$.

Now we know that a, b, c and ab are conjugate in $SL_{4m}(q)$, and from information in table 4.5.1 in [GLS98], we have that a, b, c and ab are conjugate in $GSp_{4m}(q)$. Thus from Lemma 4.1.20, we have $\lambda(a) = \lambda(b) = \lambda(c) = \lambda(ab) = \lambda(a)\lambda(b)$, and so $\lambda(a) = \lambda(b) = \lambda(c) = 1$. Thus, as a, b and c generate G, for all $x \in G$, the multiplier for x, $\lambda(x)$ must be equal to 1, i.e. for all $x \in G$ and all u,$v \in V$, $\langle xu, xv \rangle = \langle u, v \rangle$.

So, for $i \neq 2, 3, n-3, n-2$ we have:

$$\begin{aligned} \langle v_i, v_2 \rangle &=_g \langle v_i, v_2 - 8\alpha v_n \rangle \\ &= \langle v_i, v_2 \rangle - 8\alpha \langle v_i, v_n \rangle \end{aligned}$$

and so

$$\langle v_i, v_n \rangle = 0.$$

Also, for $i, j \in \{2, 3, n-3, n-2\}$, we have:

$$\begin{aligned}\langle v_i, v_j \rangle &=_g \langle v_i - 8\alpha v_n, v_j - 8\alpha v_n \rangle \\ &= \langle v_i, v_j \rangle - 8\alpha \langle v_i, v_n \rangle - 8\alpha \langle v_n, v_j \rangle + 64\alpha^2 \langle v_n, v_n \rangle \\ &= \langle v_i, v_j \rangle - 8\alpha \langle v_i, v_n \rangle + 8\alpha \langle v_j, v_n \rangle + 0\end{aligned}$$

and so

$$\langle v_i, v_n \rangle = \langle v_j, v_n \rangle .$$

Now since we also have:

$$\begin{aligned}\langle v_2, v_n \rangle &=_b \langle v_2, -v_n \rangle \\ &= -\langle v_3, v_n \rangle ,\end{aligned}$$

we have, for all i, $1 \leqslant i \leqslant n$, $\langle v_i, v_n \rangle = 0$. Thus, $v_n \in V_\perp$ and so the form $\langle\ ,\ \rangle$ is degenerate.

Hence there is no non-degenerate symplectic form on V which is invariant under the action of G up to similarity, and so H does not preserve a non-degenerate symplectic form. □

Hence H cannot be conjugate to $Sp_{4m}(q)$.

4.14.5 Equations

The only restrictions we have are that $q \neq 9$, $-64\alpha^2 \neq 0$ and is a defining element of $\mathbb{F}_q$. Taking α to be any primitive element of $\mathbb{F}_q$ will satisfy these restrictions on α. Hence for $q \neq 9$, there exists an element $\alpha \in \mathbb{F}_q$ that satisfies these restrictions.

4.14.6 Conclusion

We conclude this section by summarising the above.

Lemma 4.14.3. *For q odd, $q \neq 9$ and $m \geqslant 3$, $\exists\ \alpha \in \mathbb{F}_q$ s.t. the elements a, b and c generate $SL_{4m}(q)$, and so $L_{4m}(q)$ has Property 2 and hence also has Property 1.*

Proof.

1. In section 4.14.1 we exhibited elements in $SL_{4m}(q)$, a, b and c such that a and b commute and a, b, c and ab are conjugate involutions in $SL_{4m}(q)$. Under the natural homomorphism $SL_{4m}(q) \longrightarrow L_{4m}(q)$ they map to involutions a', b' and c' such that a' and b' commute and a', b', c' and $a'b'$ are conjugate in $L_{4m}(q)$. The elements are defined in terms of a variable $\alpha \in \mathbb{F}_q$. We called the group generated by these elements G.

2. In section 4.14.2 we demonstrated that there is a non-trivial transvection, in G, $g := (bc)^8$. We also demonstrated that the transvection $h := g^{(ac)^2} \in G$ is opposite to g. Dickson's Lemma (Lemma 4.1.2) then gives us that G contains the whole root subgroup R, consisting of all transvections with the same centre and the same axis as g, subject to $-64\alpha^2$ being a defining element of $\mathbb{F}_q$.

3. In section 4.14.3 we then considered a subgroup $G_1 := \left\langle b, c, (ac)^2 \right\rangle \leqslant G$, containing R, and the normal closure $H_1 := \langle g \rangle^{G_1} = \langle R \rangle^{G_1} \trianglelefteq G_1$ of the root subgroup R in G_1. We have shown that the group G_1 is irreducible and so the group H_1 is also irreducible. Thus $H := \langle g \rangle^G = \langle R \rangle^G$ is irreducible, and so is an irreducible group generated by root subgroups. Thus from Lemma 4.1.1, H either coincides with $SL_{4m}(q)$, or H is conjugate to $Sp_{4m}(q)$.

4. In section 4.14.4 we excluded the symplectic case by showing that G does not preserve a non-degenerate symplectic form up to similarity. This implies that, when α satisfies the imposed restrictions, we have that $G \trianglerighteq H = SL_{4m}(q)$ and hence, $G \cong SL_{4m}(q)$.

5. Finally, in section 4.14.5 it was shown that the there exists an α such that the restrictions on it can be satisfied.

□

Chapter 5

Concluding Remarks

We conclude with a brief discussion about this Thesis. As we have seen, we have determined that the following simple groups have Property 1:

- The alternating groups, A_n for $n \geqslant 5$, $n \neq 7, 8, 12$;
- The sporadic groups except for M_{11}, M_{12}, M_{22}, M_{23} and McL;
- The projective linear groups, $L_n(q)$, over fields of odd order for $n = 2$ with $q \geqslant 5$ and $q \neq 7$; $n = 3$ with $q \equiv 1 \mod 3$; $n = 6$ with $q \equiv 1 \mod 4$ and $q \neq 9$; $n \geqslant 4$, $n \neq 6$ with $q \neq 9$,

and that the following simple groups have Property 2:

- The alternating groups, A_n for $n \geqslant 5$, $n \neq 6, 7, 8, 12$;
- The sporadic groups except for M_{11}, M_{12}, M_{22}, M_{23} and McL;
- The projective linear groups, $L_n(q)$, over fields of odd order for $n = 2$ with $q \geqslant 5$ and $q \neq 7, 9$; $n = 6$ with $q \equiv 1 \mod 4$ and $q \neq 9$; $n \geqslant 4$, $n \neq 6$ with $q \neq 9$,

Also, we have determined that the following simple groups do not have Property 1:

- The alternating groups, A_n for $n = 7, 8, 12$;

- The sporadic groups M_{11}, M_{12}, M_{22}, M_{23} and McL;
- The projective linear groups, $L_n(q)$, over fields of odd order for $n = 2$ with $q = 7$; $n = 3$ with $q \equiv 0$ or $2 \mod 3$,

and that the following simple groups do not have Property 2:

- The alternating groups, A_n for $n = 6, 7, 8, 12$;
- The sporadic groups M_{11}, M_{12}, M_{22}, M_{23} and McL;
- The projective linear groups, $L_n(q)$, over fields of odd order for $n = 2$ with $q = 7, 9$; $n = 3$ for all odd q^*,

(* Note that part of this proof is not included in this Thesis but can be found in [Nuz97]) Also we have also seen that the following simple groups can be generated by the following minimum number of conjugate involutions whose product is 1:

- A_7 and A_{12} - 6 involutions;
- A_8 - 7 involutions;
- M_{11}, M_{12}, M_{22}, M_{23} and McL - 6 involutions;
- $L_2(7)$ - 6 involutions;
- $L_3(q)$ with $q \equiv 0$ or $2 \mod 3$ - 6 involutions.

The above suggests several areas in which to continue this inquiry:

1. Determine whether the remaining simple Linear groups have Property 1 and/or Property 2;
2. Determine whether other simple groups, from the other families, have Property 1 and/or Property 2;

3. For those simple groups that do not have Property 1, determine the minimum number of conjugate involutions whose product is 1 which are required to generate the group.

We briefly discuss these areas below.

5.1 The Remaining Linear Groups

This thesis has not determined whether or not the following simple projective linear groups have Property 1 and/or Property 2:

1. $L_6(q)$ with $q \equiv 3 \mod 4$;
2. $L_n(q)$ with $n \geqslant 4$ and $q = 9$.

The following discussion of the methods used in chapter 4 will hopefully shed light on why I have not been able to answer these questions for these groups.

The method that was used in chapter 4 relies, first of all, on finding suitable generators in $SL_n(q)$. This, in many cases, was a matter of "educated guesswork".

First a 'likely' conjugacy class must be found. The non-generation results from chapter 1 (i.e. Theorems 1.2.3, 1.2.4 and 1.2.5) can be used to prove that a group does not have Property 1 and/or Property 2, and so a 'likely' conjugacy class is one whose elements fail to satisfy the conditions implied by these Theorems. The groups above contain such conjugacy classes, and so may have Property 1 and/or Property 2.

Next, we want elements in the conjugacy class that are easily manipulated. Generally this was obtained by using elements close to being permutation matrices. This then made the calculations to determine irreducibility easier.

Of course, suitable root subgroups must be obtained from the generators. As can be seen in the majority of cases, two opposite transvections are easily obtained. However, in the case of $q = 9$, the opposite transvections do not

always generate a group isomorphic to $SL_2(q)$. In fact the pairs of transvections obtained in each case do not generate such a group. This was the main barrier encountered in answering the questions for $q = 9$.

In the case of $L_6(q)$ with $q \equiv 3 \mod 4$, the main barrier encountered was finding elements that met the desired conditions, that clearly generated an irreducible group on $\mathbb{F}_q^6$ and that gave suitable transvections easily.

Now it may be noted that for the linear groups $L_6(q)$ with $q \equiv 1 \mod 4$, where suitable generators were found, this thesis did not prove that the corresponding special linear groups have Property 1 and/or Property 2 as it did with the other dimensions. Again, this was due to the difficulty in finding elements with the desired conditions that generated an irreducible group on $\mathbb{F}_q^6$ and that gave suitable transvections easily. Instead of involutions in $SL_6(q)$, elements that mapped to involutions under the natural homomorphism $SL_6(q) \longrightarrow L_6(q)$ were used. In this way the groups $L_6(q)$ could still be shown to have Property 1 and Property 2 even if the corresponding results for $SL_6(q)$ were not obtained.

In summary, I have no reason to believe that these groups do not have Property 1 and/or Property 2. However, due to the reasons outlined above, I have been unable to find suitable elements that generate these groups. Anecdotal evidence from similar problems to this suggest that as n increases, the group is more likely to contain suitable generators, and so given time and patience I do believe that these groups could be shown to have Property 1 and Property 2 (possibly with some exceptions).

5.2 The Other Simple Groups

The methods that have been used in this thesis rely on knowledge of the structure of the groups in question. Since an increasing amount is known about the simple groups, it is reasonable to approach this problem from a

similar angle for the remaining simple groups. A first step would be to consider the problem for the remaining simple classical groups over odd ordered fields. In [TZ97], [TWG94] and [TWG95] the authors consider matrix groups over commutative rings to simultaneously prove that groups from several different families can be generated in certain ways. It may be possible to use this method, along with information from this thesis, to obtain generators for these groups that satisfy our requirements.

Another direction that may be taken is to consider the classical groups over fields of even order. There are of course added complications with this problem, as the conjugacy classes of involutions behave differently when the field has even order.

5.3 Minimum Number of Involutions

We finish where we started - For each simple group, asking what is the minimum number of conjugate involutions, whose product is 1, that are needed to generate the group. Since a large number of simple groups are known to be generated by 3 conjugate involutions, then if it can be proved that you need more than 5 conjugate involutions whose product is 1, then it may be that only 6 involutions are needed. However, we have already seen that the alternating group A_8 needs 7 involutions with these properties to generate it, and so it is possible that more work may be required with other simple groups.

Bibliography

[AS76] M. Aschbacher and G. M. Seitz. Involutions in Chevalley groups over fields of even order. *Nagoya Math. J.*, 63:1–91, 1976.

[Cam99] P. J. Cameron. *Permutation Groups*. Cambridge University Press, Cambridge, 1999.

[CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of Finite Groups*. Clarendon Press, Oxford, 1985.

[CD93] M. Cazzola and L. Di Martino. $(2,3)$-generation of $PSp(4,q)$, $q = p^m$, $p \neq 2,3$. *Results in Mathematics*, 23:221–232, 1993.

[Coh81] J. Cohen. On non-Hurwitz groups and noncongruence subgroups of the modular groups. *Glasgow Math. J.*, 22(1):1–7, 1981.

[Coo79] B. Cooperstein. The geometry of root subgroups in exceptional groups. I. *Geom. Dedicata.*, 8(3):317–381, 1979.

[CR81] C. W. Curtis and I. Reiner. *Methods of Representation Theory with applications to finite groups and orders*, volume 1. John Wiley and Sons, Inc., New York, 1981.

[Dic01] L. E. Dickson. *Linear Groups, with an Exposition of the Galois Field Theory*. Teubner, Leipzig, 1901. Reprint by Dover, New York, 1958.

[DV94] L. Di Martino and N. Vavilov. $(2,3)-$generation of $SL(n,q)$. I. Cases $n = 5,6,7$. *Communications In Algebra*, 22(4):1321–1347, 1994.

[DV96] L. Di Martino and N. Vavilov. $(2,3)-$generation of $SL(n,q)$. II. Cases $n \geqslant 8$. *Communications In Algebra*, 24(2):487–515, 1996.

[Gar78] D. Garbe. Über eine Klasse von arithmetisch definierbaren Normal-teilern der Modulgruppe. *Math. Ann.*, 235:195–215, 1978.

[GLS98] D. Gorenstein, R. Lyons, and R. Solomon. *The classification of finite simple groups*, volume 3. American Mathematical Soceity, Providence, RI, 1998.

[Gor68] D. Gorenstein. *Finite Groups*. Harper and Row Publishers, New York-London, 1968.

[Gro08] The Gap Group. Gap - groups, algorithms and programming, version 4.4.12. `http://www.gap-systems.org`, 2008.

[Mac69] A. W. Macbeath. Generators of linear fractional groups. *Proc. Sympos. Pure Math.*, 12:14–32, 1969.

[Mal88] G. Malle. Exceptional groups of Lie type as Galois groups. *J. reine angew. Math.*, 392:70–109, 1988.

[Mal90] G. Malle. Hurwitz groups and G_2. *Canad. Math. Bull.*, 33(3):349–357, 1990.

[Maz03] V. D. Mazurov. On generation of sporadic simple groups by three involutions, two of which commute. *Siberian Mathematical Journal*, 44(1):160–164, 2003.

[McL67] J. E. McLaughlin. Some groups generated by transvections. *Arch. Math.*, 18:364–368, 1967.

[Mil01] G. A. Miller. On the groups generated by two operators. *Bull. Amer. Math. Soc.*, 7(10):424–426, 1901.

[MK02] V. D. Mazurov and E. I. Khukhro, editors. *The Kourovka Notebook. Unsolved problems in group theory. Fifteenth edition.* Inst. Mat. (Novosibirsk), Novosibirsk, 2002.

[MSW94] G. Malle, J. Saxl, and T. Weigel. Generation of classical groups. *Geometriae Dedicata*, 49(1):85–116, 1994.

[Nuz84] Ya. N. Nuzhin. The structure of groups of Lie type of rank 1. *Mat. Zametki*, 36(2):149–158, 1984.

[Nuz90] Ya. N. Nuzhin. Generating triples of involutions of Chevalley groups over a finite field of characteristic 2. *Algebra i Logika*, 29(2):192–206, 1990.

[Nuz92] Ya. N. Nuzhin. Generating triples of involutions of alternating groups. *Mat. Zametki*, 51(4):91–95, 1992.

[Nuz97] Ya. N. Nuzhin. Generating triples of involutions of Lie-type groups over a finite field of odd characteristic. II. *Algebra i Logika*, 36(4):442–440, 1997.

[NW02] S. P. Norton and R. A. Wilson. Anatomy of the Monster. II. *Proc. London Math. Soc. Ser. III*, 84(3):581–598, 2002.

[Pas68] D. Passman. *Permutation groups.* W. A. Benjamin, Inc., New York-Amsterdan, 1968.

[Ree71] R. Ree. A theorem on permutations. *J. Combinatorial Theory Ser. A*, 10:174–175, 1971.

[Sco77] L. L. Scott. Matrices and cohomology. *Ann. of Math. (2)*, 105(3):473–492, 1977.

[Tam88] M. C. Tamburini. Generation of certain simple groups by elements of small order. *Istit. Lombardo Accad. Sci. Lett. Rend. A*, 121:21–27, 1988.

[TV94] M. C. Tamburini and S. Vassallo. $(2,3)$-generation of $SL(4,q)$ in odd characteristic and associated problems. *Boll. Un. Mat. Ital. B (7)*, 8(1):121–134, 1994.

[TWG94] M. C. Tamburini, J. S. Wilson, and N. Gavioli. On the $(2,3)$-generation of some classical groups I. *Journal of Algebra*, 168(1):353–370, 1994.

[TWG95] M. C. Tamburini, J. S. Wilson, and N. Gavioli. On the $(2,3)$-generation of some classical groups II. *Journal of Algebra*, 176(2):667–680, 1995.

[TZ97] M. C. Tamburini and P. Zucca. Generation of certain matrix groups by three involutions, two of which commute. *Journal of Algebra*, 195(2):650–661, 1997.

[Vav88] N. A. Vavilov. The geometry of long root subgroups in Chevalley groups. *Vestnik Leningrad. Univ. Mat. Mekh. Astronom.*, 21(1):8–11, 1988.

[WNB+05] R. A. Wilson, S. J. Norton, J. N. Bray, R. W. Barraclough, et al. Atlas of finite group representations - version 3. `http://brauer.maths.qmul.ac.uk/Atlas/v3/`, 2005.

[Wol89] A. J. Woldar. On Hurwitz generation and genus actions of sporadic groups. *Illinois J. Math*, 33(3):416–437, 1989.