Maximal cocliques and cohomology in rank one linear groups

by

Jack Phillip Saunders

A thesis submitted to The University of Birmingham for the degree of Doctor of Philosophy

School of Mathematics
College of Engineering and Physical Sciences
University of Birmingham

April 2020

UNIVERSITY OF
BIRMINGHAM

University of Birmingham Research Archive

e-theses repository

This unpublished thesis/dissertation is copyright of the author and/or third parties. The intellectual property rights of the author or third parties in respect of this work are as defined by The Copyright Designs and Patents Act 1988 or as modified by any successor legislation.

Any use made of information contained in this thesis/dissertation must be in accordance with that legislation and must be properly acknowledged. Further distribution or reproduction in any format is prohibited without the permission of the copyright holder.

Abstract

In this thesis, we investigate certain aspects of $\mathrm{PSL}_2(q)$. We begin by looking at the generating graph of $\mathrm{PSL}_2(q)$, a structure which may be used to encode certain information about the group, which was first introduced by Liebeck and Shalev and further investigated by many others. We provide a classification of maximal cocliques (independent sets) in the generating graph of $\mathrm{PSL}_2(q)$ when q is a prime and provide a family of examples to show that this result does not directly extend to the prime-power case. After this, we instead investigate the cohomology of finite groups and prove a general result relating the first cohomology of any module to the structure of some fixed module and a generalisation of this result to higher cohomology. We then completely determine the cohomology $\mathrm{H}^n(G, V)$ and its generalisation, $\mathrm{Ext}^n_G(V, W)$, for irreducible modules V, W for $G = \mathrm{PSL}_2(q)$ for all q in all non-defining characteristics before doing the same for the Suzuki groups.

ACKNOWLEDGEMENTS

Naturally, there are many people I would like to thank as I come to the end of my time here in Birmingham. The best years of my life so far have been spent working towards my PhD, and this is almost entirely due to the people here in Birmingham. At no time has this been more apparent than sitting here during the Covid-19 lockdown thinking about the past 3 and a half years or so.

First off, of course, I would like to thank my supervisors, Hoff and Chris, for putting up with my stupid questions and helping me somehow get this far, and of course so much more. I would also like to thank Michael Grove and John Meyer for a variety of things. Additional thanks go to all of the other staff in the algebra group, past and present. The post-seminar pub will certainly be missed. A bonus thanks to Penny and Paula, too, for all of their help in the organisation of PGTC and otherwise. I also thank The University of Birmingham for funding this work.

I would also like to thank everyone else from down in The Dungeon, even those that defected to the second and third floors. I could try to list notable names and reasons, but then I think this'll end up being the largest chapter in this thesis. Thus, in no particular order (I applied a random permutation to them, just to be sure), I'd like to thank James, Raúl, Clare, Ryan, Matt, Alberto, Matt, Alex, Rachel, Martin, Andy, Jordan, Nan, Joel, Andrea, Tyrrell, Yixin, Mark and Arthur. Finally, I'd like to thank Jerry, Calum and Zia from the pub quiz team, Melissa and Mun See for keeping conferences fun, Ruth for putting up with my general nonsense, Doug for existing sometimes and of course my dad for continuing to check that I am indeed still alive. I gave myself a one page limit, so by necessity many people have been missed. You likely know who you are, so thank you, too.

CONTENTS

CHAPTER 1

INTRODUCTION

This thesis consists of two projects, one in finite group theory and the other dealing with cohomology of finite groups. There are five chapters. The first is this one, and in here one may find a brief overview of the thesis as a whole, a brief note on notation and an introduction to each of the two projects in the thesis. For a proper introduction to these projects the reader should consult the introduction in their respective chapters. Chapter 2 gives a brief background on some topics in group theory.; the first half of this chapter discusses topics required to understand Chapter 3 while the latter half gives an introduction to finite groups of Lie type and some less elementary results in group theory that are needed for Chapter 5.

In Chapter 3 we give the first of the main projects, adapted from a paper published in Communications in Algebra [65]. This paper concerns the classification of maximal cocliques (independent sets) in the generating graph of $\mathrm{PSL}_2(q)$. The generating graph is a structure that was introduced in 1996 by Liebeck and Shalev in [54] and is a graph whose vertices are the non-identity elements of a finite group G, joined whenever this pair of elements generates the group. Of course, if G is not 2-generated then this graph will tell us nothing. However, due to work of Steinberg and later others, we know that all of the finite simple groups are 2-generated and as such there are many important, interesting examples to investigate.

The generating graph was initially introduced as a tool in a proof about ‘large’ subsets of finite simple groups such that all pairs of elements in this subset generate the whole group — this is simply a clique in the group's generating graph — but has since been found to determine certain information about the group as well. Indeed, it is interesting to consider the generating graph as a means of encoding information about a group: if one was given the graph in isolation, what would it tell us? We see one example in [60], where it was shown that the generating graph in fact determines symmetric groups and 'large' finite simple groups up to isomorphism. It has also been conjectured in [12] that the generating graph of G contains a Hamiltonian cycle if and only if G/N is cyclic for all $1 \neq N \trianglelefteq G$. Various graph-theoretic properties of the generating graph have also been investigated by other people, including its clique number, chromatic number and the relationship between them [58, 59].

Returning to an earlier point: all finite simple groups can be generated by just 2 elements, but the result is much stronger than this. In fact, as $|G| \to \infty$, the probability of a pair of elements chosen uniformly at random from G generating the group tends to 1, and the least such a probability may be is $57/90$ for A_6 [27, 48, 55, 62]. In particular, this means that the generating graph of finite simple groups is incredibly dense, and in a dense graph it is natural to wonder what happens where it is at its least dense. To this end, we investigate the maximal (with respect to inclusion) independent sets or *cocliques* in this graph and show that the only maximal cocliques in $\mathrm{PSL}_2(p)$ for p prime are maximal subgroups, the conjugacy class of all involutions or have order at most linear in p. We then give a family of examples stemming from the isomorphism $\mathrm{PSL}_2(q^2) \cong \mathrm{P}\Omega_4^-(q)$ for $\mathrm{PSL}_2(p^n)$ for even $n > 1$ which indicates that this result does not hold in the more general setting.

After this, in Chapter 4 we give more background for Chapter 5; this time concerning representation theory of finite groups. In this chapter, we give a brief introduction to representation theory in general before defining group cohomology and its generalisation, Ext, and giving some useful results for calculating cohomology in a great many cases. Next, we introduce the notion of blocks of a group algebra and give some results from modular representation theory dealing with the structure of modules in characteristic $p > 0$. We finish this chapter with an introduction to Brauer graphs, as these play a vital role in some of the later material in Chapter 5.

Finally, in Chapter 5 we present the second project. One may find this chapter formatted as an article on arXiv [64]. We begin with some motivation. Let H and N be finite groups with some action of H as automorphisms of N. Then one may form the semidirect product $E = N \rtimes H$, which is a group with normal subgroup N such that $HN = E$ and $H \cap N = 1$. One natural question to ask here is, given $N \trianglelefteq E$, how many choices do we have for a *complement* H? When N is abelian, this question is answered by the first cohomology group $\mathrm{H}^1(H, N)$, which corresponds precisely to conjugacy classes of complements to N in E. For nonabelian N, the complements are still parameterised by the first cohomology $\mathrm{H}^1(H, N)$, but it is only a pointed set rather than a group. Another natural situation to investigate is what happens when such a complement H does not exist. Then we instead have a *group extension* of H by N. This is a group E such that $N \trianglelefteq E$ and $E/N \cong H$. One can check that a semidirect product is in fact a special case of this. Then given N and H one naturally asks how many such extensions we can find (with a prescribed action of H on N) — this is known as the extension problem and is a very difficult and important problem in group theory. The answer is again given to us by cohomology, but this time the second cohomology group $\mathrm{H}^2(H, Z(N))$ is in 1–1 correspondence with the equivalence classes of such extensions (in most cases, but certainly when N is abelian — see [31, Theorem 11.1]).

As all finite groups may be constructed through a series of extensions of finite simple groups, these make a logical starting point. Further, a lot is known about the representation theory of finite simple groups and there are a great many tools available to us when working in this area. Thus, it is natural to begin by investigating extensions of finite simple groups by their irreducible representations. However, even in this very well-studied case, remarkably little is known about the cohomology outside of the simplest examples, and what we do know amounts to some very large bounds for H^1 in most cases and even less for H^2.

To give an idea of the current situation in this area, Guralnick conjectured in 1986 [37] that if G was a finite group and V a faithful, absolutely irreducible kG-module, then $\dim \mathrm{H}^1(G,V) \leq c$ for some absolute constant c. In fact, the original conjecture was with $c = 2$. However, Scott, Bray, Wilson and others found multiple examples with $\dim \mathrm{H}^1(G,V) = 3$ [11, 66]. More recently, Lübeck [56, Theorem 4.7] found a module for $\mathrm{E}_6(q)$, where $q = p^a$ is a prime power, in defining characteristic with $\dim \mathrm{H}^1(G,V) = 3537142$. This suggests that Guralnick's conjecture is likely false, though it has not yet been disproven. Some results are known though, and we go into more detail on these in the introduction to Chapter 5. If G is a finite group of Lie type in cross characteristic, then Guralnick and Tiep showed that $\dim \mathrm{H}^1(G,V)$ is bounded by roughly the order of the Weyl group of G [40, 42]. If G is an arbitrary finite group then Guralnick, Kantor, Kassabov and Lubotzky [39, Theorem C] showed that $\dim \mathrm{H}^2(G,V) \leq \frac{37}{2} \dim V$ for any faithful irreducible kG-module V.

In Chapter 5, we first prove that, given a finite group G, a subgroup $H \leq G$ such that $O_{r'}(H) = O^r(H)$ and a kG-module V defined in characteristic r such that $V^H = 0$, the cohomology $\mathrm{H}^n(G,V) \cong \mathrm{Ext}_G^{n-1}(V^*, \mathcal{L}/k)$ where $\mathcal{L}$ is the permutation module over k of G acting on cosets of H. This gives as a corollary that, under the above hypotheses and the further assumption that V is irreducible, $\mathrm{H}^1(G,V)$ is simply the multiplicity of V in the head of $\mathcal{L}$. One may use this as a simple criterion to check whether the first cohomology of an irreducible module vanishes based entirely on whether it can be found as a composition factor of $\mathcal{L}$. We then discuss a few corollaries of this result and some applications in various situations before moving on to completely determine the cohomology of $G = \mathrm{PSL}_2(q)$ for all prime powers q and all irreducible kG-modules in cross characteristic. Once this is done, we go further and determine $\mathrm{Ext}_G^n(V,W)$ for all irreducible modules V, W in cross characteristic for $\mathrm{PSL}_2(q)$ (all q) and $\mathrm{Sz}(2^{2m+1}$ for all m.

There will be *italicised* terms throughout this thesis which we use to refer to certain objects that have not yet been defined here and maybe never will be. An understanding of these terms is not required for an understanding of this thesis and such terms are included to allow the interested reader to research these objects themselves whilst simultaneously telling more familiar readers what we are actually referring to in a more concrete sense.

We include on the next few pages a table of notation for the thesis and while we have tried to be as complete as possible there are some pieces of standard notation which we have left out for brevity. For example, the various different families of classical groups would take up a full page and the reader unfamiliar with the notation for these groups may wish to learn about these first before reading this thesis. The notation used here for classical groups is completely standard, with the possible exception of our use of $\mathrm{O}_n^\varepsilon(q)$ to denote the *general orthogonal group* and not its simple subquotient $\mathrm{P}\Omega_n^\varepsilon(q)$ as in the ATLAS [20].

There are also some abuses of notation that we shall use which are not worth a place in the table, and would only add confusion if they were included. In particular, when we refer to $\{0\}$ or $\{1\}$, we will just say 0 or 1, respectively.

Table of notation

Notation	Definition/Name
p	A prime number
q	A prime power, p^n unless otherwise specified
$\mathbb{F}_q$	Finite field of order q
$\operatorname{char} k$	Characteristic of a field k
R^*	Multiplicative group of units of a ring R
$\overline{k}$	Algebraic closure of a field k
kv	k-span of a vector v in a k–vector space
$\dim V$	Dimension of the vector space V over its base field
$\operatorname{Hom}(V, W)$	Space of linear maps $\varphi\colon V \to W$
$V \oplus W$	Direct sum of V and W
$V \otimes W$	Tensor product of vector spaces V and W over their base field
V^*	Dual space of V
$U^\perp$	Orthogonal complement in V of a subspace $U \subseteq V$
$\operatorname{rad} U$	Radical $U \cap U^\perp$ of U
C_n	Cyclic group of order n
E_q	Elementary abelian group of order q, namely $\prod_{i=1}^n C_p$
D_{2n}	Dihedral group of order $2n$
S_n	Symmetric group on n elements
A_n	Alternating group on n elements
$H \leq G$	H is a subgroup of G
$[G : H]$	Index in G of a subgroup H
$N \trianglelefteq G$	N is a normal subgroup of G
$C_G(H)$	Centraliser in G of a subgroup H
$Z(G)$	Centre of a group G, $C_G(G)$
$N_G(H)$	Normaliser in G of a subgroup H

G/H	Set of left cosets of H in G
$H\backslash G/K$	Set of (H,K)–double cosets in G
$\operatorname{Inv} G$	Set of involutions in G
$\operatorname{Aut} G$	Automorphism group of G
$\operatorname{Syl}_p G$	Set of Sylow p-subgroups of G
$N \rtimes_\varphi H$	Semidirect product of N and H with respect to φ
$G.N$	Extension of a group G by N with N normal
$O_p(G)$	p-core of G
$O^p(G)$	p-residual subgroup of G
$M \hookrightarrow N$	There exists an injective homomorphism $M \to N$
$M \twoheadrightarrow N$	There exists a surjective homomorphism $M \to N$
$\operatorname{Hom}_R(V,W)$	Space of R-module homomorphisms $\varphi\colon V \to W$
$V \otimes_R W$	Tensor product of modules V and W over R
$\operatorname{soc} M$	Socle of a module M
$\operatorname{rad} M$	Radical of a module M
$\mathcal{H} M$	Heart of a module M, given by $\operatorname{rad} M/(\operatorname{rad} M \cap \operatorname{soc} M)$
$\operatorname{Irr}_k G$	Set of irreducible kG-modules
V^G	Fixed point space of a G-module V
$\operatorname{Res}^G_H V$, V_H	Restriction of a kG-module V from G to H
$\operatorname{Ind}^G_H V$	Induction of a kG-module V from H to G
$\mathcal{P}(V)$	Projective cover of a kG-module V
ΩV	Heller translate or syzygy of a kG-module V
$\mathrm{H}^n(G,V)$	n^{th} cohomology group of G with coefficients in V
$M \sim N$	The modules M and N have the same radical series
$[N_1 \mid \ldots \mid N_l]$	A module whose i^{th} radical factor is N_i

CHAPTER 2

BACKGROUND ON GROUP THEORY

In this chapter we introduce the main group-theoretic concepts which will be used throughout the thesis. The reader that is familiar with graduate-level group theory may skip this chapter entirely. We have tried to assume only undergraduate-level results when writing this chapter, so all one needs to be able to read it is a good understanding of undergraduate group theory, knowledge of the notions of rings and fields and a little bit of linear algebra. At the beginning of each section, we outline the general direction in which it will be heading and provide the main references for that section. Where results are neither cited nor proven they are assumed to be taken from one of the references given at the start of the corresponding section or the proof of the result is immediate and thus omitted.

This chapter is by no means a complete collection of useful results in group theory; by necessity it can only attempt to scratch the surface of a variety of topics. In any case, the reader interested in learning more about any of this background is directed to the references given at the start of each section as these will usually be thorough introductory texts on the relevant subject matters.

In this first background chapter we introduce any results that may be required to understand the material in Chapter 3, along with a few definitions for objects which will be present in Chapter 5. In particular, we very briefly introduce the linear and orthogonal groups and then state Aschbacher's theorem on the classification of maximal subgroups of classical groups in the context of these particular groups. Next, in order to understand parts of Chapter 5, we very quickly introduce the finite groups of Lie type and their classification before finishing with a few group-theoretic results which are used in passing later on and are included primarily for completeness.

The reader looking for background on representation theory is referred to Chapter 4.

2.1 Fields and linear algebra

When talking about classical groups, we often talk a lot about how they act on their natural vector spaces and how parts of the group may preserve various decompositions or structures associated to this space. As such, in order to understand the definition of certain classical groups and to be able to talk about them in as understandable a way as possible, we will introduce here some of the linear algebra required for Section 2.2. In this chapter, and indeed for the rest of the thesis, we denote by $\mathbb{F}_q$ the finite field of order q. Any material in this section may be found in one of [51, 52].

We first include the following basic definitions for completeness as they will be used throughout the thesis.

Definition 2.1.1

A *field extension* $k : k'$ is a pair of fields $k' \subseteq k$ and the *degree* or *index* $(k : k')$ of this extension is the dimension of k as a k'–vector space.

Definition 2.1.2

Given two k–vector spaces V and W, we define the *direct sum* $V \oplus W$ of V and W to be the space $\{(v, w) \mid v \in V, w \in W\}$. One may also think of this as the space spanned by the concatenation of the bases for V and W, so if V has basis $\mathcal{B}$ and W has basis $\mathcal{C}$, then $V \oplus W$ has basis $\mathcal{B} \cup \mathcal{C}$. We also define $V^{\oplus n}$ to be the n-fold direct sum of V with itself, so $V^{\oplus n} := \bigoplus_{i=1}^{n} V$.

It is easy to check that this is equivalent to the notion of *internal* direct sum, where we have subspaces V, $W \subseteq U$ such that $U = V + W$ and $V \cap W = 0$.

Definition 2.1.3

Given k–vector spaces U, V and W, we say that a map $f\colon U \times V \to W$ is *bilinear* if for all u_1, $u_2 \in U$, v_1, $v_2 \in V$ and $\lambda \in k$ we have that

$$f(u_1 + \lambda u_2, v_1) = f(u_1, v_1) + \lambda f(u_2, v_1)$$

and

$$f(u_1, v_1 + \lambda v_2) = f(u_1, v_1) + \lambda f(u_1, v_2).$$

A function $f\colon U \times V \to W$ being bilinear is equivalent to being linear in each coordinate. Formally, this means that for all $u_1 \in U$, $v_1 \in V$, the functions $f_{u_1}\colon V \to W$ and $f_{v_1}\colon U \to W$ given respectively by $f_{u_1}(v) = f(u_1, v)$ and $f_{v_1}(u) = f(u, v_1)$ are both linear.

Definition 2.1.4

Given two k–vector spaces V and W, we define the *tensor product* $V \otimes W$ to be the space generated by the elements $v \otimes w$ for $v \in V$ and $w \in W$ under the assumption that the operation $\otimes$ is bilinear (that is, the map $(v, w) \mapsto v \otimes w$ is bilinear). As with direct sums, we also define the n-fold tensor product of V with itself to be $V^{\otimes n} := \bigotimes_{i=1}^{n} V$.

One may also think of $V \otimes W$ as the k–vector space with basis $\{v \otimes w \mid v \in \mathcal{B},\ w \in \mathcal{C}\}$ where $\mathcal{B}$ is a basis for V and $\mathcal{C}$ is a basis for W.

We now introduce the notion of a formed vector space, as all of the classical groups are the collection of linear transformations of a vector space which preserve some form on it. Such linear transformations are called *isometries*.

Definition 2.1.5

Let V be a vector space over a field k. A *bilinear form* on V is a bilinear map $f\colon V \times V \to k$. We say that two forms on V are *equivalent* if they are equal up to a change of basis. Furthermore, we say that f is *symmetric* if $f(u, v) = f(v, u)$, *skew-symmetric* or *anti-symmetric* if $f(u, v) = -f(v, u)$ and *alternating* if $f(v, v) = 0$ for all u, $v \in V$. Skew-symmetric and alternating mean the same thing provided $\operatorname{char} k \neq 2$. If we wish to only consider one bilinear form on V then we often drop the f and simply define the *inner product* of two vectors to be $(u, v) \coloneqq f(u, v)$ and (although it may not be a norm in the usual sense), we call (v, v) the *norm* of v. We shall refer to a vector space V with a nondegenerate symmetric bilinear form as an *orthogonal space.*

Definition 2.1.6

Let V be a k–vector space. A *quadratic form* on V is a map $Q\colon V \to k$ such that $Q(\lambda u + v) = \lambda^2 Q(u) + \lambda f(u, v) + Q(v)$ for all u, $v \in V$, $\lambda \in k$ and some symmetric bilinear form f on V.

When $\operatorname{char} k \neq 2$ then every quadratic form defines a bilinear form from this definition and vice versa via $Q(v) \coloneqq \frac{1}{2} f(v, v)$. Given some nontrivial form on V, it is natural to want to use this to compare vectors and divide V into subspaces in a way that respects the form or is somehow 'natural.' The main way of doing this is via *orthogonality.*

Definition 2.1.7

Given a vector space V with an inner product $(\cdot, \cdot)$ (or symmetric bilinear form f), we say that two vectors u, $v \in V$ are *orthogonal* or *perpendicular* if $(u, v) = 0$ and we define the *orthogonal complement* of a subspace $U \subseteq V$ to be $U^\perp \coloneqq \{v \in V \mid (v, u) = 0 \ \forall u \in U\}$. Further, we define the *radical* of a subspace U of V to be $\operatorname{rad} U \coloneqq U \cap U^\perp$. If $\operatorname{rad} f \coloneqq \operatorname{rad} V = V^\perp$ is nonzero then we say that f is *singular* and that V is a *degenerate* space. Otherwise f is nonsingular and V is nondegenerate. If instead the form on V is zero then we say that V is *totally isotropic.*

Lemma 2.1.8

If V is a vector space over a field k with a nonsingular inner product and $U \subseteq V$ a subspace, then $\dim V = \dim U + \dim U^\perp$, $(U^\perp)^\perp = U$ and if U is nondegenerate then $V = U \oplus U^\perp$.

Proof: For $u \in U$, define $\varphi_u\colon V \to k$ by $\varphi_u(v) \coloneqq (u, v)$. Then $U^\perp = \bigcap_{u \in \mathcal{B}} \ker \varphi_u$ for some basis $\mathcal{B} = \{u_1, \ldots, u_n\}$ of U. Note that $\{\varphi_{u_i} \mid 1 \leq i \leq n\}$ is linearly independent since

$\sum_{i=1}^n \lambda_i\varphi_{u_i} = 0$ only when $\sum_{i=1}^n \lambda_i\varphi_{u_i}(v) = 0$ for all $v \in V$. But then

$$\sum_{i=1}^n \lambda_i\varphi_{u_i}(v) = \sum_{i=1}^n \lambda_i(u_i, v) = \left(\sum_{i=1}^n \lambda_i u_i, v\right) = 0$$

for all $v \in V$ and so $\sum_{i=1}^n \lambda_i u_i \in \operatorname{rad} V = 0$. Now, let $\varphi\colon V \to k^{\oplus n}$ be given by $\varphi = (\varphi_{u_i})_{i=1}^n$. By linear independence of the φ_{u_i}, $\dim \operatorname{Im}\varphi = n = \dim U$.

Then using the rank-nullity theorem we see that $\dim U^\perp = \dim V - n$ and so $\dim V = \dim U + \dim U^\perp$ (in particular if $\operatorname{rad} U = U \cap U^\perp = 0$ then $V = U \oplus U^\perp$). Using this one notes that $\dim(U^\perp)^\perp = \dim U$, but we also have that $U \subseteq (U^\perp)^\perp$ and so $U = (U^\perp)^\perp$ and we are done. ■

Note that if U is degenerate then of course $\operatorname{rad} U = U \cap U^\perp \neq 0$ and thus $U + U^\perp$ cannot be a direct sum.

Definition 2.1.9

Given a formed vector space V, an *isometry* of V is a linear map $g\colon V \to V$ such that $(g(u), g(v)) = (u, v)\ \forall u, v \in V$.

Definition 2.1.10

Suppose that V is a vector space of dimension n over $\mathbb{F}_q$ with a nonsingular symmetric bilinear form. We define the *Witt index* of V to be the maximal dimension of a totally isotropic subspace of V. If n is odd then all such V have the same Witt index, but when $n = 2m$ is even it may be either m or $m - 1$. Spaces of Witt index m are said to be of *plus type* while the rest are of *minus type.*

2.2 Linear and orthogonal groups

Here we begin by defining the orthogonal groups and then give some results on linear groups which will be useful in Chapter 3. The goal of this section is to give Aschbacher's Theorem in the case of 'small' linear and orthogonal groups and thus give a description of their maximal subgroups. A good reference for this section, as with the previous one, is [51].

We assume the reader is already familiar with the definition of linear groups, and thus begin by defining the orthogonal groups. We will only give the definition for the orthogonal groups in odd characteristic because, as is often the case, when the characteristic is 2 things end up getting rather complicated. Everything we need still holds in characteristic 2, it's just a lot harder to prove. The even case is treated in [51, 69] for the curious reader.

Definition 2.2.1

Given a vector space V over a finite field $\mathbb{F}_q$ of odd order with a nonsingular symmetric bilinear form, we define the *orthogonal group* on V to be the isometry group $\mathrm{O}(V)$ of V. When n is odd we have that the isometry groups of any two such vector spaces are isomorphic, thus we may denote such a group by $\mathrm{O}_n(q)$. Otherwise when n is even there are two isomorphism classes of such groups, denoted $\mathrm{O}_n^+(q)$ and $\mathrm{O}_n^-(q)$, dependent on whether V is of plus type or minus type. When referring to a finite orthogonal group in a general context, we tend to denote it by $\mathrm{O}_n^\varepsilon(q)$, where ε is either 1, -1 or 0 (for when n is odd).

Now that we have the definition of these groups, it is important to know to what extent we may use it to move subspaces of V around. The below results tell us that the answer is as much as one could reasonably expect, since of course an isometry can't map a space onto one that is not isometric to it.

Theorem 2.2.2 (Witt's Lemma, [69, Theorem 3.3])

Any isometry between two subspaces of a nondegenerate quadratic space (space with associated quadratic form) may be extended to an isometry of the whole space.

Corollary 2.2.3

Given any two isometric subspaces U, W of an orthogonal space V, there exists $g \in \mathrm{O}_n^\varepsilon(q) = \mathrm{O}(V)$ such that $gU = W$.

Like with all other classical groups (with few exceptions), somewhere buried inside of the finite orthogonal groups there is a finite simple group. Usually, one just takes the elements of determinant 1 and quotients out by the centre like with $\mathrm{PSL}_n(q)$, $\mathrm{PSp}_{2n}(q)$ and $\mathrm{PSU}_n(q)$. However, the orthogonal groups decided to be awkward, so to find the simple group buried within we (usually) have to find an additional subgroup of index 2 in $\mathrm{SO}(V)$ before taking the quotient by the centre to obtain the simple group. In order to find this subgroup of index 2, we use the spinor norm.

Definition 2.2.4 [51, p. 29]

Given an orthogonal vector space V of dimension at least 3 in odd characteristic and an element $A = r_{v_1} \dots r_{v_k} \in \mathrm{SO}(V)$ written as a product of reflections, where for $(v, v) \neq 0$ we define

$$r_v(x) \coloneqq x - 2\frac{(x, v)}{(v, v)}v,$$

the *spinor norm* $\theta\colon\ \mathrm{SO}_n^{\varepsilon}(q) \to \mathbb{F}_q^*/(\mathbb{F}_q^*)^2$ is defined by

$$\theta(A) \coloneqq \prod_{i=1}^{k}(v_i, v_i) \mod (\mathbb{F}_q^*)^2.$$

Then there is a subgroup of $\mathrm{SO}(V)$ of index 2 given by $\Omega(V) \coloneqq \ker\theta$ whose quotient $\mathrm{P}\Omega(V) \coloneqq \Omega(V)/Z(\Omega(V))$ is simple except for $(\dim V, q) = (3, 2)$, $(3, 3)$, $(5, 2)$ or when V is a 4-dimensional space of plus type. Note that when $\dim V = 2m$ and V is of type ε such that $q^m \equiv \varepsilon \mod 4$ then $\Omega(V) \cong \mathrm{P}\Omega(V)$ and in these cases we shall use the notation for each interchangeably.

Definition 2.2.5

Given a vector space V, a *flag* of (totally isotropic) subspaces of V is a chain of proper containments of (totally isotropic) subspaces $0 \eqqcolon V_0 \subsetneq V_1 \subsetneq \dots \subsetneq V_n$ where $V_n = V$ (or $\dim V_n$ is the Witt index of V for a totally isotropic flag). We say that such a flag is *maximal* if $\dim V_i = i$ for each i.

If G is a *classical group* acting on a vector space V (for example, $\mathrm{SL}(V)$, $\mathrm{Sp}(V)$, $\mathrm{SO}(V)$

or $\mathrm{SU}(V)$), then we define a *Borel subgroup* of G to be the stabiliser of a maximal flag of totally isotropic subspaces of V. In general, up to conjugacy this is simply the upper triangular subgroup of G.

Further, we define a *maximal torus* of G to be a subgroup of G which is maximal with respect to being isomorphic to a direct product of copies of the multiplicative group of the field over which G is defined. In general, up to conjugacy this is the set of diagonal matrices in G.

We shall see a much more general definition of these subgroups in Section 2.3, but this more friendly geometric version is sufficient for Chapter 3 and the remainder of this section.

For the linear groups, we view the vector space on which they naturally act as being equipped with the zero form so that all subspaces are totally isotropic.

We now provide a classification theorem for the maximal subgroups of $\mathrm{SL}_2(q)$ and $\Omega_4^-(q)$, for more information on this one should consult [10, Chapter 2] and [51, Chapter 3] which cover it in far greater detail. In particular, a vastly more general version of this result appears as Theorem 2.2.19 in [10]. Some of the terms in the below table remain undefined in this thesis, but these properties will not be used here and so the reader is referred to one of the previous references should they wish to learn more.

Theorem 2.2.6 (Aschbacher's Theorem for $\mathrm{SL}_2(q)$ and $\Omega_4^-(q)$)
The maximal subgroups of $\mathrm{SL}_2(q)$ $(q > 3)$ and $\Omega_4^-(q)$ (acting naturally on $V = \mathbb{F}_q^n$, $n = 2$ for $\mathrm{SL}_2(q)$ and $n = 4$ for $\Omega_4^-(q)$) lie in one of the following classes:

Class	Description
$\mathcal{C}_1$	Stabilisers of totally singular or non-singular subspaces.
$\mathcal{C}_2$	Stabilisers of direct sum decompositions $V = \bigoplus_{i=1}^{t} V_i$ where $\dim V_i = n/t$ for some t.
$\mathcal{C}_3$	Stabilisers of extension fields of $\mathbb{F}_q$ of index 2.
$\mathcal{C}_5$	Stabilisers of subfields of $\mathbb{F}_q$ of prime index.
$\mathcal{C}_6$	Normalisers of symplectic-type or extraspecial groups in absolutely irreducible representations.
$\mathcal{S}$	See [10, Definition 2.1.3], the specifics of this will not be used here.

We also provide below a more specific version of the above theorem, full tables for which may be found in [26, §260 (p286)] for just the linear groups and [10, Tables 8.1, 8.2, 8.17] for $\mathrm{SL}_2(p)$ and the orthogonal groups. One may obtain the maximal subgroups for $\mathrm{PSL}_2(p)$ by simply taking the quotient by the centre of G when it lies inside the subgroup.

Theorem 2.2.7 (Maximal subgroups of $\mathrm{PSL}_2(p)$)
The conjugacy classes of maximal subgroups of $\mathrm{PSL}_2(p)$ for $p > 3$ prime are as follows:

i) The Borel subgroups $C_p \rtimes C_{\frac{1}{2}(p-1)}$ for all p.

ii) D_{p-1} for all $p > 11$.

iii) D_{p+1} for all $p > 7$.

iv) A_4 when $p \equiv \pm 3, \pm 13 \mod 40$.

v) S_4 when $p \equiv \pm 1 \mod 8$, two conjugacy classes.

vi) A_5 when $p \equiv \pm 1 \mod 10$, two conjugacy classes.

In the linear case, the Borel subgroups are the stabilisers of lines (*i.e.* the maximal flag $0 \subseteq \mathbb{F}_q v \subseteq V$ for some $v \in V$) and the dihedral maximal subgroups of order $p-1$ are the stabilisers of pairs of lines (in this case, stabilising the direct sum decomposition $V = \mathbb{F}_q v \oplus \mathbb{F}_q u$ for $u \notin \mathbb{F}_q v$).

Next, we give the specific version of Aschbacher's Theorem for $\Omega_4^-(q)$, since this group is isomorphic to $\mathrm{PSL}_2(q^2)$ we still attribute the maximal subgroups themselves to [26, §260]. This is also given as [10, Table 8.17].

Theorem 2.2.8 (Maximal Subgroups of $\Omega_4^-(q)$)
The conjugacy classes of maximal subgroups of $\Omega_4^-(q)$ are as follows:

i) The Borel subgroups, $E_{q^2} \rtimes C_{\frac{1}{2}(q^2-1)}$ for all q.

ii) $2.\,\mathrm{PSL}_2(q)$ for $q > 2$, which splits into two conjugacy classes.

iii) D_{q^2-1} for $q \neq 3$.

iv) D_{q^2+1} for $q \neq 3$.

v) $\mathrm{PSL}_2(q_1^2) \cong \Omega_4^-(q_1)$ where $q = q_1^r$ for an odd prime r.

vi) Two conjugacy classes of A_5 for $q = p$, $p \equiv \pm 3 \mod 10$ prime.

In the orthogonal case, the Borel subgroups are the stabilisers of isotropic 1-spaces and $2.\,\mathrm{PSL}_2(q)$ stabilises a non-isotropic 1-space. The dihedral maximal subgroup of order q^2-1 stabilises a non-degenerate 2-space and each copy of $\mathrm{PSL}_2(q_1)$ stabilises some subfield of $\mathbb{F}_q$ of index r. The other dihedral maximal subgroups stabilise extension fields and A_5 lies in class $\mathcal{S}$, but we do not need to use these facts here.

2.3 Groups of Lie type

The finite simple groups have been studied extensively over the years and are known to fall into four distinct categories (with very little overlap): there are the cyclic groups of prime order, the 26 sporadic groups, the alternating groups (A_n for $n \geq 5$) and the finite simple groups of Lie type. The finite groups of Lie type are divided further into classical, exceptional and twisted groups (though some of the twisted groups are in fact classical).

We assume some familiarity with the classical groups $\mathrm{SL}_n(q)$, $\mathrm{SO}_n^{\varepsilon}(q)$, $\mathrm{Sp}_{2n}(q)$, $\mathrm{SU}_n(q)$ and their quotients, central extensions and combinations thereof.

In this section, we provide a very fast introduction to the groups of Lie type and outline their classification and a few important parts of their structure. This is mainly included for completeness to allow for a better understanding of the implications of Chapter 5 and will not be required before then. The groups of Lie type are very closely linked to Lie groups, hence the name, which are in turn linked to reductive linear algebraic groups. Much of the terminology used to talk about groups of Lie type comes from the theory of linear algebraic groups, and many of their properties are inherited from their infinite analogues. We will avoid going into much detail on linear algebraic groups, but the interested reader is referred to [61] for a good introduction which also discusses the finite groups of Lie type or [46] for just the linear algebraic groups. For this section, it can be assumed that any result that is not specifically cited is found in one of [17, 18].

We begin with the definition of a linear algebraic group, though we will completely avoid talking about any form of algebraic geometry. The reader that does not know what an affine variety is should therefore consider reading one of the above references.

Definition 2.3.1

Let $k = \overline{k}$ be a field. A *linear algebraic group* over k is a group which is also an affine variety over k such that the maps $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are morphisms of varieties.

Many structures for linear algebraic groups behave just as they do in the theory of groups, except that whenever we have a homomorphism we must also require that it is a morphism of varieties and whenever we have a subgroup we usually require that it be closed with respect to the *Zariski topology* (*i.e.* it must also be a variety). For example, a closed subgroup of a linear algebraic group is itself a linear algebraic group.

The typical first example anyone ever sees of a linear algebraic group is $\mathrm{GL}_n(k)$, and in fact it turns out that linear algebraic groups are precisely the closed subgroups of $\mathrm{GL}_n(k)$ for some n and k. For brevity, we shall drop the 'linear' from linear algebraic groups, as we shall not be talking about any other kind.

Definition 2.3.2

Let G be an algebraic group over k and let G_m denote the multiplicative group of k. Then any subgroup of G of the form $G_m \times G_m \times \cdots \times G_m$ is called a *torus* of G. We call T a *maximal torus* of G if it is not contained in any strictly larger torus.

In $\mathrm{GL}_n(k)$, the diagonal subgroup forms a maximal torus and in an arbitrary connected algebraic group we have that any two maximal tori are conjugate. Here, and indeed in future, we mean connected in a topological sense.

Definition 2.3.3

Let G be a connected algebraic group. Then a *Borel subgroup* of G is a maximal closed connected solvable subgroup of G.

Lemma 2.3.4

Let G be a connected algebraic group. Then every element of G lies in some Borel subgroup of G, and a maximal torus of a Borel subgroup of G is a maximal torus of G.

Definition 2.3.5

An element g in an algebraic group G viewed as a subgroup of $\mathrm{GL}_n(k)$ is said to be *unipotent* if $g - I_n$ is nilpotent, where I_n is the $n \times n$ identity matrix. A group G is said to be unipotent if all of its elements are unipotent. The *unipotent radical* of an algebraic group G is a maximal connected normal unipotent subgroup of G. We say that an algebraic group G is *reductive* if its unipotent radical is trivial.

Again in $\mathrm{GL}_n(k)$, the upper triangular matrices form a Borel subgroup B and the upper unitriangular matrices form a maximal unipotent subgroup of G which is also the unipotent radical of B. As with maximal tori, we have that any two Borel subgroups are conjugate in an arbitrary connected algebraic group.

The following lemma is an important property of Borel subgroups which we do not prove here, and an analogous result holds in the finite case.

Lemma 2.3.6

Let G be a connected algebraic group with $B \leq G$ a Borel subgroup. Then $B = U \rtimes T$ where U is the unipotent radical of B and T is any maximal torus of B.

Definition 2.3.7

Let G be a connected algebraic group and let T be a maximal torus of G. We define the *Weyl group* W of G to be $W \coloneqq N_G(T)/C_G(T)$. Note that the choice of maximal torus does not matter as all such tori are conjugate and so the Weyl group is well-defined for G.

The Weyl group is a particularly important (and finite!) group when dealing with algebraic groups and their analogues. To formalise this importance, we need to introduce the root system of G as follows. Fix a maximal torus T of an algebraic group G. The following is adapted from the discussion on [17, pp. 17–20] and the reader should refer to this discussion if more detail is required.

Definition 2.3.8

Let $X \coloneqq \operatorname{Hom}(T, G_m)$ be the set of algebraic group homomorphisms from T into G_m. Then X is an abelian group under multiplication, and we call X the *character group* of T.

Let $Y \coloneqq \operatorname{Hom}(G_m, T)$. We call Y the *cocharacter group* of T. Given $\chi \in X$, $\gamma \in Y$, their composition $\chi \circ \gamma \colon G_m \to G_m$ will act on G_m so that $(\chi \circ \gamma)(\lambda) = \lambda^n$ for some $n \in \mathbb{Z}$ and any $\lambda \in G_m$. We define $\langle \chi, \gamma \rangle = n$.

Now, let B be some Borel subgroup containing T. We have that $B = UT$ where U is the unipotent radical of B. Then there is a unique *opposite* Borel subgroup B^- such that $B \cap B^- = T$ with unipotent radical U^- so that $U \cap U^- = 1$. The minimal nontrivial subgroups of U and U^- normalised by T are all isomorphic to the additive group of k, denoted G_a, and T acts on each such subgroup as automorphisms. This gives us a homomorphism from T into $\operatorname{Aut} G_a \cong G_m$ and thus determines a nonzero element of X.

Definition 2.3.9

The elements of X given by the above process are called *roots* of G. The roots form a finite subset Φ of X. For each $\alpha \in \Phi$, the unipotent subgroup from which it was obtained is denoted X_α.

The roots coming from the subgroups in U^- are the negatives of the roots coming from the subgroups in U. Let α and $-\alpha$ be a pair of opposite roots corresponding to subgroups X_α and $X_{-\alpha}$. Then there is a homomorphism $\psi\colon \mathrm{SL}_2(k) \to \langle X_\alpha, X_{-\alpha}\rangle$ such that the image under ψ of the upper unitriangular matrices is X_α and the lower unitriangular matrices are mapped onto $X_{-\alpha}$. The diagonal matrices in $\mathrm{SL}_2(k)$ are thus mapped onto a subgroup of T. Let $\alpha^\vee \in Y$ be given by $\alpha^\vee(\lambda) = \psi(\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1}\end{smallmatrix}\right))$. This $\alpha^\vee$ is called a *coroot* of G and is related to α by $\langle \alpha, \alpha^\vee\rangle = 2$. Similarly to the roots, the coroots form a finite subset of Y denoted $\Phi^\vee$.

The Weyl group W acts on Φ, and for each $\alpha \in \Phi$ we have a map $w_\alpha\colon \chi \mapsto \chi - \langle \chi, \alpha^\vee\rangle\alpha$. The map w_α is an involution such that $w_\alpha(\alpha) = -\alpha$. We call the roots coming from U the *positive roots*, and those from U^- the *negative roots*. Let $\Delta \subseteq \Phi$ be the set of positive roots which cannot be written as the sum of two other positive roots. These are called the *simple roots*, and in fact we have that $W = \langle w_\alpha \mid \alpha \in \Delta\rangle$. If we label the simple roots α_1, $\dots$, α_l and let $s_i \coloneqq w_{\alpha_i}$, $m_{ij} \coloneqq |s_i s_j|$ for $i \neq j$, then in fact W has a *Coxeter presentation*

$$W = \langle s_1, \dots, s_l \mid s_i^2 = 1,\ (s_i s_j)^{m_{ij}} = 1 \text{ for } i \neq j\rangle.$$

As an example, if we let $G = \mathrm{SL}_n(k)$ and take B to be the upper triangular matrices, the simple roots $\{\alpha_1, \dots, \alpha_{n-1}\}$ correspond to the upper unitriangular subgroups generated by matrices with nonzero entries in position $(i, i+1)$. If we let T denote the diagonal subgroup of G, then T is a maximal torus whose normaliser is the set of matrices which permute the entries of T. From this it is easy to check that the Weyl group W of G is isomorphic to S_n.

The next definition and corresponding result give us an important structural property of algebraic groups.

Definition 2.3.10

Let G be a group and B, $N \leq G$. These subgroups form a BN*-pair* in G if the following statements hold.

i) $G = \langle B, N \rangle$,

ii) $B \cap N \trianglelefteq N$,

iii) $N/(B \cap N) =: W$ is generated by a set $S = \{s_i \mid i \in I\}$ of involutions,

iv) Let $n_i \in N$ map to $s_i \in W$. Then $n_i B n_i \neq B$,

v) $n_i B n \subseteq B n_i n B \cup B n B$ for any $n \in N$.

We say that a BN-pair is *split* for an algebraic group G if $B = U \rtimes (B \cap N)$ for U unipotent, $B \cap N$ abelian and semisimple (consisting entirely of diagonalisable elements), and $\bigcap_{n \in N} B^n = B \cap N$.

Theorem 2.3.11
Let G be a connected reductive algebraic group. Then G has a split BN-pair, where $B \leq G$ is a Borel subgroup and $N = N_G(T)$ is the normaliser of some maximal torus T contained in B.

We now have all of the structural information that we will need for later on, so we move to the classification of the connected simple algebraic groups. First, of course, we require some definitions.

Definition 2.3.12
A nontrivial algebraic group G is said to be *simple* if it contains no proper nontrivial normal subgroups, and *semisimple* if it contains no proper nontrivial closed connected solvable normal subgroups.

The following two definitions and theorem may be found in [17, 1.11].

Definition 2.3.13
Let G be a connected semisimple algebraic group with simple roots $\{\alpha_i, \dots, \alpha_n\}$. Let

$A_{ij} = \langle \alpha_j, \alpha_i^\vee \rangle$. These integers A_{ij} are called the *Cartan integers*, and the matrix $A = (A_{ij})$ the *Cartan matrix*.

We have $A_{ii} = 2$ for any i, and $A_{ij} \leq 0$ for $i \neq j$. If $i \neq j$, then $A_{ij} \in \{0, -1, -2, -3\}$ and $A_{ij} = 0 \iff A_{ji} = 0$. If $A_{ij} = -2$ or -3 then $A_{ji} = -1$. Using these Cartan integers, we define an integer $n_{ij} = A_{ij}A_{ji} \in \{0, 1, 2, 3\}$, connected to m_{ij}. The integer n_{ij} is 0, 1, 2 or 3 precisely when m_{ij} is 2, 3, 4 or 6, respectively.

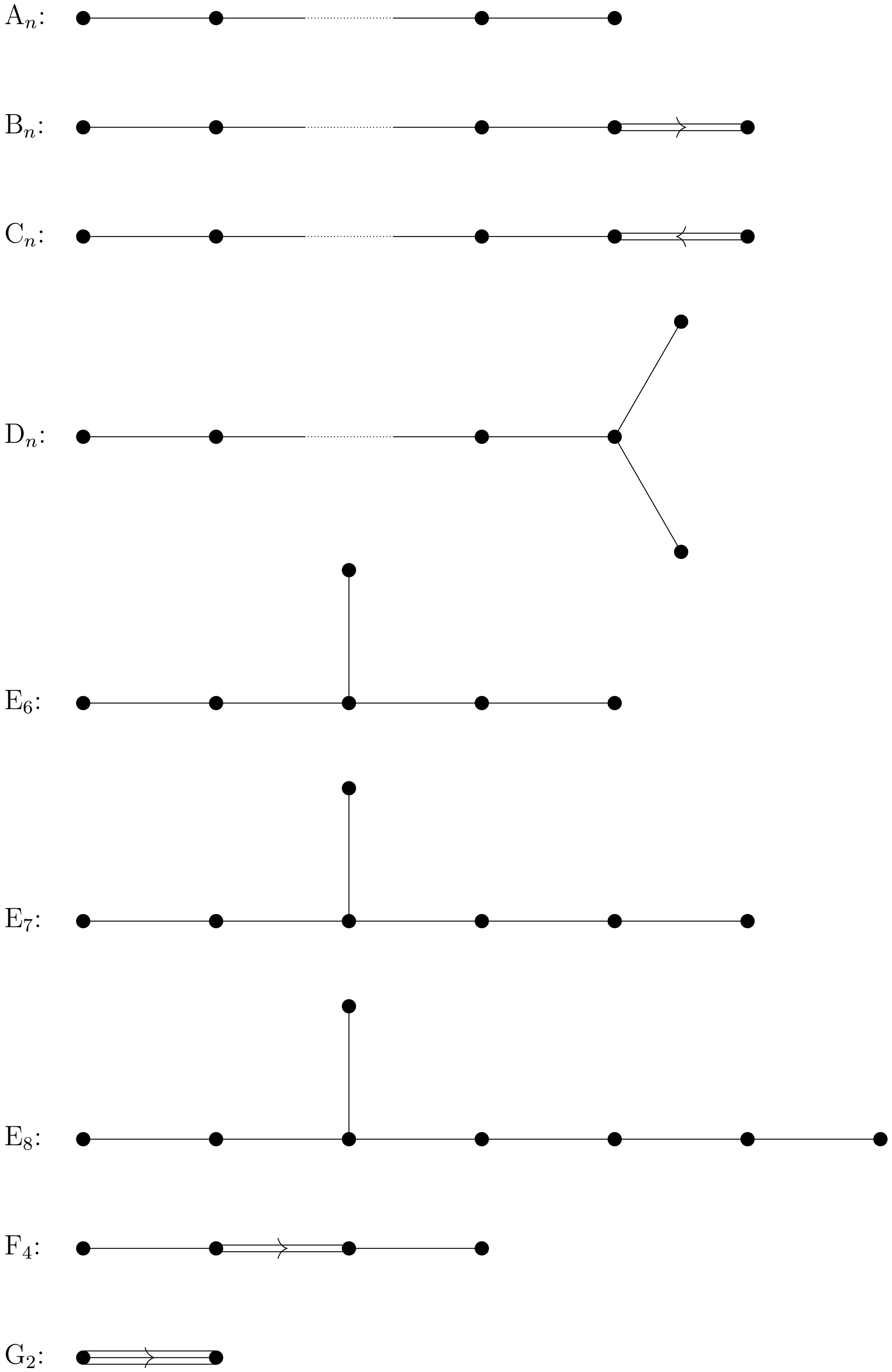
Definition 2.3.14

Retain notation as in Definition 2.3.13 and the discussion which follows. The *Dynkin diagram* of G is a graph with n nodes labelled by the simple roots, and we connect α_i and α_j with n_{ij} arcs. When $A_{ji} \neq -1$, draw an arrow from α_i to α_j.

The connected components of a group's Dynkin diagram correspond to simple components of the group. A connected semisimple algebraic group thus has a connected Dynkin diagram if and only if it is simple as an algebraic group.

Theorem 2.3.15

Let G be a connected simple algebraic group. Then its Dynkin diagram is one of the following.



The types A_n through to D_n give us the classical groups: $\mathrm{SL}_{n+1}(k)$ is of type A_n, $\mathrm{SO}_{2n+1}(k)$ is of type B_n, $\mathrm{Sp}_{2n}(k)$ is of type C_n and $\mathrm{SO}_{2n}(k)$ is of type D_n. These are not the only simple algebraic groups of these types though. For example, $\mathrm{PGL}_{n+1}(k)$ is also of type A_n. If G is of one of the other types, then G is said to be an *exceptional group* or of *exceptional type*. The subscript n (number of nodes) in the above diagrams is called the *rank* of G, and can be seen to be equal to the number of generators in the Coxeter presentation of the Weyl group of G.

We now know enough about simple algebraic groups to be able to discuss their finite counterparts in sufficient detail. We obtain these finite groups using something known as a Frobenius map. The simplest example of such a map is, again in $\mathrm{GL}_n(k)$ but now for $\operatorname{char} k = p > 0$, the map $F_q \colon \mathrm{GL}_n(k) \to \mathrm{GL}_n(k)$ such that $F_q((a_{ij})) = (a_{ij}^q)$ for $q = p^n$.

Definition 2.3.16

Let G be an algebraic group. A homomorphism $F \colon G \to G$ is called a *standard Frobenius map* if there exists $i \colon G \hookrightarrow \mathrm{GL}_n(k)$ for some n and k such that $i \circ F = F_q \circ i$ for some $q = p^m$. A *Frobenius map* is then any homomorphism F such that some power of F is a standard Frobenius map.

Definition 2.3.17

Let G be an algebraic group and $F \colon G \to G$ a Frobenius map. Then $G^F \coloneqq \{g \in G \mid F(g) = g\}$ is a finite subgroup of G. A finite group of this form where G is a connected reductive algebraic group is called a *finite group of Lie type*.

Most of the finite groups of Lie type are then obtained in the way one may expect. For example, $\mathrm{GL}_n(q) = \mathrm{GL}_n(\overline{\mathbb{F}_q})^{F_q}$ and similarly for the other (non-orthogonal) classical groups. Also, many of the structural properties of algebraic groups are preserved upon taking F-fixed points, which we shall now highlight.

We denote a finite group of Lie type by its type and the order of the field over which it is defined. For example, $\mathrm{SL}_n(q)$ is of type A_{n-1} and defined over the field of order q, so we may denote it by $\mathrm{A}_{n-1}(q)$.

The remainder of this section is based on the discussion in [17, 1.18].

Definition 2.3.18

Let G be a connected reductive algebraic group with Frobenius map F. We say that

$H \leq G$ is *F-stable* if $F(H) = H$. We define a *maximal torus* of G^F to be T^F for an F-stable maximal torus of G. Similarly, a Borel subgroup of G^F is B^F where B is an F-stable Borel subgroup of G. We call a maximal torus of G^F *maximally split* if it lies in a Borel subgroup of G^F — this need not always be the case, as a maximal torus of G could lie only in Borel subgroups which are not F-stable and thus the Borel subgroups containing it may fail to be in G^F.

As in the algebraic group case, all Borel subgroups of G^F are conjugate, and so are all maximally split tori.

Theorem 2.3.19

Let G be a connected reductive algebraic group with Frobenius map F. Then G^F has a split BN-pair with B a Borel subgroup of G^F and N the normaliser of a maximal torus of G^F contained in B.

Let G be a connected reductive algebraic group. Take an F-stable Borel subgroup B of G. Then since B is F-stable, so is its unipotent radical U. The root subgroups $X_\alpha \leq U$ are minimal (nontrivial) subgroups and normalised by T, so will be permuted by F (the specifics of this action are given in [17, 1.18]). This will therefore give rise to a permutation of the positive roots lying in B, which in fact preserves the set of simple roots. As such, this gives rise to a permutation of the simple roots of G and in turn a permutation of its Dynkin diagram. When F is a standard Frobenius map, the permutation induced by F on the simple roots of G is trivial and so F preserves the Dynkin diagram (and thus Weyl group) of G entirely. In this case, the Weyl group of G is isomorphic to the Weyl group of G^F.

When F is not a standard Frobenius map, however, it will induce a nontrivial permutation of the simple roots (thus automorphism of the Dynkin diagram). In fact, given a simple algebraic group G with automorphism ρ of the Dynkin diagram, there is only one possible type for G^F [17, p. 37]. Thus to determine the possible types one may obtain, it is sufficient to determine the possible automorphisms of the Dynkin diagrams. Of course, taking the identity automorphism will give rise to a family of finite groups and these are known as the *Chevalley groups* or *untwisted* groups of Lie type. Allowing nontrivial automorphisms then gives us some extra families of finite groups which do not have obvious equivalents in the algebraic group case. These extra groups are known as *twisted* groups of Lie type, and are denoted by adding a superscript before the type of Dynkin diagram which gives the order of the twist. For example, there is an automorphism of A_n corresponding to the permutation swapping α_i and α_{n-i} and this gives rise to the twisted groups of type ${}^2\mathrm{A}_n$. The groups ${}^2\mathrm{A}_n(q)$ may then be defined for all q and are the finite unitary groups.

With one exception, all of these twists are involutions. The first such twist is that of A_n seen above. Another gives rise to ${}^2\mathrm{D}_n(q)$, obtained by swapping the two vertices on the far right. This twist of $\mathrm{D}_n(q)$ gives rise to finite orthogonal groups of minus type and can be defined for all q. Next, we have ${}^2\mathrm{B}_2(q)$ by swapping the vertices in the diagram. This may only be done for $q = 2^{2m+1}$ (see [18, 14.1] for why) and gives rise to the Suzuki groups $\mathrm{Sz}(q)$. Similarly, we have ${}^2\mathrm{G}_2(q)$, the small Ree groups, which are defined only for $q = 3^{2m+1}$ and ${}^2\mathrm{F}_4(q)$ gives us the large Ree groups for $q = 2^{2m+1}$. Then a reflection about the central column of the diagram yields ${}^2\mathrm{E}_6(q)$ for all q. Finally, there is an automorphism of order three of the Dynkin diagram of type D_4 given by a 120 degree rotation. This automorphism, commonly referred to as *triality*, gives rise to the groups ${}^3\mathrm{D}_4(q)$ for all q.

These extra groups are called the *twisted groups of Lie type* or *Steinberg groups*.

Definition 2.3.20

Let G be a finite group of Lie type. Then we define the *rank* of G to be the number of generators in the Coxeter presentation of its Weyl group.

When G is not twisted then the rank of G is still the subscript n seen in its Dynkin diagram, but for twisted groups it is more complicated. A treatment of this may be found in [18, Chapter 13]. In short, the ranks of the twisted groups of Lie type are as in the below table. In fact, the Weyl groups of all of these groups except for ${}^2\mathrm{F}_4$ are Weyl groups of existing groups of Lie type, and the Weyl group of ${}^2\mathrm{F}_4$ is dihedral of order 16.

Type	${}^2\mathrm{A}_{2l-1}$	${}^2\mathrm{A}_{2l}$	${}^2\mathrm{D}_l$	${}^2\mathrm{E}_6$	${}^3\mathrm{D}_4$	${}^2\mathrm{B}_2$	${}^2\mathrm{G}_2$	${}^2\mathrm{F}_4$
Rank	l	l	$l-1$	4	2	1	1	2

2.4 Some results from group theory

In this section, we will provide some general results and definitions from finite group theory that we will make use of later. Any expert in finite group theory may very safely skip this section, and those in need of more detail can find most of the material in this section in either of [3, 35].

We begin by looking at semidirect products. Given a pair of groups, a semidirect product is a means of combining them to form a larger group. In general, not all groups can be made as semidirect products but rather as a more general construction known as a *group extension.* Extensions of or by nontrivial groups always have normal subgroups and thus a means to break them down into smaller groups. This, in short, is why we care so much about the finite simple groups — using the finite simple groups it is possible, through a series of extensions, to construct any other finite group. We will discuss extensions in more detail in Chapters 4 and 5, but for now we investigate their slightly friendlier examples.

Definition 2.4.1

Let N, H be groups and $\varphi\colon H \to \operatorname{Aut} N$ a homomorphism. Then we define the (external) *semidirect product* $N \rtimes_\varphi H$, identified with the set $N \times H$ with multiplication given by

$$(n_1, h_1)(n_2, h_2) \coloneqq (n_1 n_2^{h_1^{-1}}, h_1 h_2).$$

This is a group in which N is normal such that $(N \rtimes_\varphi H)/N \cong H$.

There is also a notion of *internal semidirect product* where we say $G = N \rtimes H$ if $N \trianglelefteq G$, $G = NH$ and $N \cap H$ is trivial. In both of these cases, we call H a *complement* to N in G.

Lemma 2.4.2

The notions of internal and external semidirect product are equivalent.

Proof: That an external semidirect product then gives rise to an internal one in the resulting group is clear from the definition. To see the converse, take a group $G = NH$ such that $N \trianglelefteq G$ and $N \cap H = 1$ and define $\varphi\colon H \to \operatorname{Aut} N$ by $\varphi(n)\colon h \mapsto h^n$. It now suffices to check that $G \cong N \rtimes_\varphi H$. Let $\psi\colon N \rtimes_\varphi H \to G$ be defined by $\psi((n,h)) = nh$, then $\psi((n_1 n_2^{h_1^{-1}}, h_1 h_2)) = n_1 n_2^{h_1^{-1}} h_1 h_2 = n_1 h_1 n_2 h_2$ and so ψ is a homomorphism. Clearly ψ is an injection and $\operatorname{Im}\psi$ contains $\{\psi(1,h) \mid h \in H\}$ and $\{\psi(n,1) \mid n \in N\}$ which may be identified with H and N, respectively. Thus $\operatorname{Im}\psi$ contains $NH = G$ and so ψ is an isomorphism. ■

In future, when the map φ can be easily understood, we usually omit it from the notation.

Semidirect products appear very frequently in finite groups and there are many important examples, including as subgroups of finite simple groups. One such example is the Borel subgroup for general linear groups, seen below.

Lemma 2.4.3

Let $G := \mathrm{GL}_n(p^k)$ with $B \leq G$ a Borel subgroup. Then $B = Q \rtimes_\varphi T$ where $Q \in \mathrm{Syl}_p G$, T is a maximal torus lying in B, and $\varphi(t)(x) = x^t$ for $t \in T$, $x \in Q$.

Proof: For this we recall from the previous section that, up to conjugacy, we may choose B to be the upper triangular matrices, Q may be chosen to be the set of upper unitriangular matrices and T the set of diagonal matrices in G. One may verify that $Q \in \mathrm{Syl}_p G$ by just checking its order, and then the result follows from the definition since $B = QT$ and $Q \cap T = 1$. ■

The above result holds for Borel subgroups of all groups of Lie type. This is because, as mentioned in Section 2.3, all finite groups of Lie type have a split BN-pair where B is a Borel subgroup and $N = N_G(T)$ for T a maximal torus contained in B.

Before moving away from semidirect products, we also give the Schur–Zassenhaus Theorem. This gives us a nice easy way to prove that certain groups may be expressed as semidirect products.

Theorem 2.4.4 (Schur–Zassenhaus)
Let G be a finite group with normal subgroup N. If $|N|$ and $[G : N]$ are coprime then $G \cong N \rtimes_\varphi G/N$. Moreover, all such complements of N in G are conjugate.

It is clear from the definition that semidirect products of H by N correspond to homomorphisms $\varphi\colon H \to \operatorname{Aut} N$, but what can we say about the structure of $N \rtimes H$? One natural question towards this would be to ask, given $N \trianglelefteq G$, how many complements H can we find? At least when N is abelian, the answer to this question is given by the first *cohomology group* $\mathrm{H}^1(H, N)$ which will be defined in Section 4.2. In fact, there are precisely $|\mathrm{H}^1(H, N)|$ conjugacy classes of complements to N in $N \rtimes_\varphi H$ where φ gives the action of H on N. So by the Schur–Zassenhaus Theorem we have that $\mathrm{H}^1(H, N) = 0$ when $|N|$ and $|H|$ are coprime. One should also note that the action φ is implicit in the definition of $\mathrm{H}^1(H, N)$, and one may wish to denote it by $\mathrm{H}^1_\varphi(H, N)$ for clarity.

Another natural question one may ask is what happens when we have $N \trianglelefteq G$ but cannot find a complement H? This gives rise to a *group extension* of $H \coloneqq G/N$ by N, which are simply defined to be groups G such that $N \trianglelefteq G$ and $G/N \cong H$. These, too, will be formalised in Section 4.2. Semidirect products as seen above are special cases of group extensions known as *split extensions* and we shall see more about these later, too.

In the meantime, there are a few structures we will need to use in Chapter 5 so we give below the definitions of double cosets, the p-core and p-residual subgroup along with a few of their properties to close out the chapter.

Definition 2.4.5
Let H, $K \leq G$ be groups. For $g \in G$, we define the set of elements $HgK \coloneqq \{hgk \mid h \in H,\ k \in K\}$ to be the (H, K)*–double coset* of g and denote by $H\backslash G/K$ the set of such double cosets.

Lemma 2.4.6

Let H, $K \leq G$ and $g \in G$. Then

$$HgK = \bigcup_{h \in K \cap H^g} hgK = \bigcup_{k \in H \cap K^g} Hgk.$$

Proof: We can write $HgK = \bigcup_{h \in H} hgK$. Now, note that $hgK = h'gK$ precisely when $g^{-1}h'^{-1}hg \in K$, or $(h'^{-1})^g h^g \in K$. Thus we see that double cosets HgK correspond to left cosets of $K \cap H^g$ in K. The case for writing this as right cosets of H is similar. ■

Lemma 2.4.7

Let H, $K \leq G$ be groups. Then G is the disjoint union of its (H, K)–double cosets.

Proof: The easiest way to see this is to show that the relation on G defined by $x \sim y \iff y = hxk$ for some $h \in H$, $k \in K$, is an equivalence relation. This is trivial to check. ■

Definition 2.4.8

Let G be a group and p a prime. We define the *p-core* $O_p(G)$ to be the largest normal p-subgroup of G. Similarly we define the p'-core $O_{p'}(G)$ to be the largest normal subgroup of G whose order is not divisible by p, *i.e.* the largest normal p'-subgroup.

Lemma 2.4.9

Let G be a finite group and p a prime. Then $O_p(G) = \bigcap_{P \in \mathrm{Syl}_p G} P$.

Proof: We have that $\bigcap_{P \in \mathrm{Syl}_p G} P = \bigcap_{g \in G} Q^g$ for some fixed $Q \in \mathrm{Syl}_p G$, thus clearly this is a normal p-subgroup of G and is contained in $O_p(G)$. To see the reverse containment, note that any normal p-subgroup of G must lie in some Sylow p-subgroup P of G, and by normality must lie in $\bigcap_{g \in G} P^g$. ■

While the p-core above gives us a large normal p-subgroup, we also care about the dual notion and wish to look at the largest p-quotient. To this end, we introduce the following subgroup.

Definition 2.4.10

Let G be a group and p a prime. We define the *p-residual subgroup* $O^p(G)$ to be the smallest normal subgroup N of G such that G/N is a p-group. As before, we also have $O^{p'}(G)$ as the smallest normal subgroup such that the quotient is a p'-group.

Lemma 2.4.11

Let G be a finite group and p a prime. Then $O^{p'}(G) = \langle P \mid P \in \operatorname{Syl}_p G\rangle$.

Proof: That $\langle P \mid P \in \operatorname{Syl}_p G\rangle \trianglelefteq G$ is clear as it is generated by a conjugacy class of subgroups, and since it contains a Sylow p-subgroup of G then the quotient by this subgroup must have order not divisible by p. It remains only to check that this is the minimal such subgroup of G, but this is clear since any $N \trianglelefteq G$ such that G/N has order not divisible by p must contain a Sylow p-subgroup P of G lest there be p-elements left in the quotient. So N must contain the normal closure of P. That is, N must contain $\langle P^g \mid g \in G\rangle = \langle P \mid P \in \operatorname{Syl}_p G\rangle$ as required. ■

CHAPTER 3

MAXIMAL COCLIQUES IN PSL_2

This chapter is adapted from a paper published in Communications in Algebra [65]. The material has been slightly reorganised. Some parts of the original paper have been shifted back into the background material and some points have been expanded upon in the name of clarity. Otherwise, the paper is more or less presented as it was submitted.

It is a well-known result of Steinberg (and later others) that every finite simple group may be generated by just 2 elements, and from [48, 55] we know that if we pick two elements of the group at random then the chance that they will generate the group is high. This then motivated the definition of the generating graph by [54], a graph whose vertex set consists of the non-identity elements of the group G and we draw an edge between two elements precisely when they generate G.

It is then interesting to look at what information the generating graph alone can tell us about the group. For example, in [60], Lucchini, Maróti and Roney-Dougal showed that the generating graph determines the group up to isomorphism for sufficiently large simple groups and for symmetric groups. The structure of the graph itself has also been investigated, such as the clique number, the presence of Hamiltonian cycles and many other things (some examples: [12, 58, 59]).

In this case, we will be looking at what we may be able to identify in the group simply by looking at maximal cocliques (totally disconnected induced subgraphs) of the generating graph for $\mathrm{PSL}_2(q)$ for q a prime power, and we show that when q is prime the largest maximal cocliques are either entirely made up of involutions or are maximal subgroups. In particular, we prove the following theorem:

Theorem 1

Let $G = \mathrm{PSL}_2(p)$ for some prime $p > 2$ and let A be a maximal coclique in G. Then A is either a maximal subgroup, the conjugacy class of all involutions or $|A| \leq \frac{129}{2}(p-1)+2$.

Further, when q is no longer prime there is an interesting geometric example which crops up due to the isomorphism $\mathrm{PSL}_2(q^2) \cong \mathrm{P}\Omega_4^-(q)$ which we illustrate and show to be a maximal coclique which prevents the extension of the previous theorem to the non-prime case. More formally, we have the following:

Theorem 2

Let V be a 4-dimensional orthogonal space of $-$ type over $\mathbb{F}_q$ and fix some non-isotropic vector $v \in V$. Then the set of all elements of $G := \mathrm{P}\Omega_4^-(q)$ with 2-dimensional eigenspaces lying in $v^\perp$ is a maximal coclique of G of order $q^3 + q$.

We currently believe that, in the prime power case, the example we have found and its conjugates are the only sufficiently large exceptions and that otherwise a similar result to the prime case should hold. The prime result tells us that, in particular, given the generating graph for $\mathrm{PSL}_2(p)$ we can identify and distinguish the conjugacy class of all involutions and the Borel subgroups by size alone. In the prime power case, it should be possible to identify and distinguish the Borel subgroups, $2.\,\mathrm{PSL}_2(q) \leq \mathrm{PSL}_2(q^2)$ and the geometric example.

We proceed by examining the maximal subgroups of $\mathrm{PSL}_2(p)$ and their intersections in order to provide a linear bound (in p) on those maximal cocliques which contain at least one element of order greater than 2 and are not maximal subgroups. After this, we provide an example in the case of $\mathrm{PSL}_2(q^2)$ which does not fit in with the result for $\mathrm{PSL}_2(p)$ to show that the result does not generalise as-is and provide some evidence to suggest why using the same approach as in the prime case is likely to be either very complicated or impossible.

3.1 The prime case

Definition 3.1.1

Let G be a group. Then $A \subseteq G$ is a *coclique* if for all $g, h \in A$ we have that $\langle g, h\rangle \neq G$. We say that a coclique A is maximal if whenever B is a coclique we have that $A \subseteq B \implies A = B$.

Lemma 3.1.2

If G is a group and $A \subseteq G$ is a maximal coclique then $\langle A\rangle \neq G \implies \langle A\rangle = A$ and A is a maximal subgroup of G.

Proof: Suppose $\langle A\rangle \neq G$. If $g \in \langle A\rangle \setminus A$ then $\langle A \cup \{g\}\rangle \subseteq \langle A\rangle \neq G$. But then this contradicts the maximality of A and so $\langle A\rangle = A$. Also, if $A \subseteq H \lneq G$ and we assume $A \neq H$ then we may pick $g \in H \setminus A$ and again note that $\langle A \cup \{g\}\rangle \subseteq \langle H\rangle = H \neq G$. In particular, $\langle g, h\rangle \neq G$ for all $h \in A$ but this again contradicts the maximality of A and so $A = H$ is a maximal subgroup. ■

Lemma 3.1.3

If $g \in G$ lies in a unique maximal subgroup M of G then any maximal coclique A containing g must be equal to M.

Proof: Let $h \notin M$ and consider $\langle g, h\rangle$. Since every proper subgroup is contained in a maximal subgroup, we have that $\langle g, h\rangle$ lies in a maximal subgroup containing g. But M is the only such subgroup. Thus we must have that $\langle g, h\rangle \subseteq M$ or $\langle g, h\rangle = G$. But $h \notin M$ and so $\langle g, h\rangle = G$. Thus $A \subseteq M$ and the maximality of A gives us that $A = M$. ■

Throughout this section, one should be aware of the result stated in Theorem 2.2.7 as it may be used without explicit reference.

Theorem 3.1.4

Let $G = \mathrm{PSL}_2(p)$ for some prime $p > 2$ and let A be a maximal coclique in G. Then A is either a maximal subgroup, the conjugacy class of all involutions or $|A| \leq \frac{129}{2}(p-1)+2$.

In fact, this result splits into two bounds — we have that $|A| \leq \frac{93}{2}(p+1)$ when $p < 7$ and $|A| \leq \frac{129}{2}(p-1)+2$ otherwise, though in either case for $p < 11$ both bounds are larger than $|G|$ so we may take the latter. Further, the above bounds are not tight, there is definitely room for improvement in the case where we allow for multiple elements of large order lying in distinct cyclic subgroups. However, we can at least show that there exists a maximal coclique of order linear in p which is not a maximal subgroup or the conjugacy class of all involutions.

Indeed, in the case where G contains A_4 as a maximal subgroup, we may fix an element x of order 3 in A_4 and suppose that $3 \mid p+1$. Acting by $N_G(x)$ we see that x lies in $\frac{1}{3}(p+1)$ copies of A_4 and so we may include all of the involutions from these subgroups to form a coclique, along with the involutions from $N_G(x)$. Note that there is no multiple counting here since $\langle x \rangle$ is already a maximal subgroup of A_4. We hence obtain a coclique of order $\frac{3}{2}(p+1)+3$ (or one higher, if $N_G(x)$ contains a central involution) which one can check is maximal.

This is the smallest example we obtain in this way out of all of the cases; the others give larger examples since either we also include contributions from the Borel subgroups or there are more conjugacy classes of these small maximal subgroups in G.

We will prove Theorem 3.1.4 further on in this thesis. First, though, we will highlight a case which arose very frequently in computer-generated examples. Note that if we take two elements x, $y \in G$ of order 2, the group $\langle x, y \rangle$ will be dihedral. In particular, provided $p \neq 2$, $\mathrm{PSL}_2(p)$ cannot be generated by two involutions. So, if we take an element x with $|x| > 2$ and take all involutions from all maximal subgroups which contain x then we will obtain a coclique. This is because these involutions were chosen so that they do not generate G with x (indeed, the group they generate must lie inside the maximal subgroup from which the involution was taken) and there is no danger of the involutions pairwise generating G either.

In particular, if we pick x such that $|x| > 5$, then x cannot lie in any maximal subgroups in class $\mathcal{S}$ (A_4, S_4 or A_5). This leaves very few choices if we wish to form a maximal coclique containing x which is not a maximal subgroup, as any element y of order greater than 2 cannot share a maximal subgroup with x unless $\langle x, y\rangle$ is cyclic or x and y lie in a common Borel subgroup. Thus, on the path to proving the main theorem we decided to investigate this case through the following four lemmas. The proofs of these lemmas give a feel for how the proof of the main theorem works when we release the restriction that x is essentially the only non-involution in the maximal coclique A. For example, the main method used is to let $x \in A$ with $|x| > 2$ and pick a maximal subgroup M whose order may be divisible by $|x|$. Then we show that $N_G(x)$ acts transitively on the set of conjugates of M which contain x and use this to bound the size of the contribution that M may make to A.

In the following, G and A are taken to be as in the statement of the theorem; A is not a maximal subgroup and contains some x ($|x| > 2$) such that $A \setminus \langle x\rangle$ consists entirely of involutions.

Lemma 3.1.5

If G and A are as above with $|x|$ dividing $p+1$ and G contains A_4 as a maximal subgroup then $|A| \leq \frac{3}{2}(p+1)+4$.

Proof: Here x may lie in D_{p+1} or A_4. If $|x| > 3$ then x may only lie in D_{p+1} and thus lies in a unique maximal subgroup since the intersection of conjugate dihedral groups in $\mathrm{PSL}_2(p)$ consists only of involutions. Then by Lemma 3.1.3 we have that A must be a maximal subgroup.

Otherwise $|x| = 3$ and we must count all of the involutions present in all subgroups in which x appears. We start off by noting that A_4 contains 3 involutions and a dihedral group D_{p+1} contains at most $\frac{p+3}{2}$ involutions (it contains one fewer if $p \equiv 3 \mod 4$). In order to figure out how many copies of A_4 can contain x, we note that D_{p+1} acts on the set of copies of A_4 which contain x with stabiliser $N_G(x) \cap A_4 = N_{A_4}(x) = \langle x\rangle$. This action is transitive since if $x \in H_1 \cap H_2$ where $H_1 \cong H_2 \cong A_4$ and $H_2 = H_1^g$ then there exists $h \in H_2$ such that $(x^h)^g = x$ and so $gh \in N_G(x)$ and $H_1^{gh} = H_2$.

Thus the orbit of any copy of A_4 containing x under this action will have length $\frac{p+1}{3}$.

Therefore from the entire conjugacy class of A_4 in G we shall get a contribution of at most $3\frac{p+1}{3}$ involutions. Adding this up, we see that

$$A \subseteq \langle x \rangle \cup \operatorname{Inv} D_{p+1} \cup \frac{p+1}{3} \operatorname{Inv} A_4$$

where $\operatorname{Inv} H$ denotes the set of involutions in H, and we abuse notation so that $k \operatorname{Inv} A_4 := \bigcup_{i=1}^{k} \operatorname{Inv} G_i$ where $G_i \cong A_4$ for all i. This gives

$$|A| \leq 3 + \frac{p+3}{2} + p + 1 = \frac{3(p+1)}{2} + 4. \qquad \blacksquare$$

Lemma 3.1.6

If G and A are as above with $|x|$ dividing $p+1$ and G contains A_5 or S_4 as maximal subgroups then $|A| \leq \frac{17}{2}(p+1) + 4$.

Proof: Since we are only dealing with upper bounds, we shall combine the cases where either A_5, S_4 or both appear as maximal subgroups of G as this encompasses the arguments used for each individual case. Our worst case bound occurs when $|x| = 3$ and both A_5 and S_4 are maximal in G, so we shall only consider this situation. There will be two conjugacy classes of both A_5 and S_4, so we must double the contribution we get from each type of subgroup. We act by D_{p+1} as in the previous lemma, noting that normalisers in A_5 and S_4 are dihedral rather than cyclic as in A_4, to see that

$$A \subseteq \langle x \rangle \cup \operatorname{Inv} D_{p+1} \cup \frac{2(p+1)}{6} \operatorname{Inv} S_4 \cup \frac{2(p+1)}{6} \operatorname{Inv} A_5$$

and so

$$|A| \leq 3 + \frac{p+3}{2} + 3(p+1) + 5(p+1) = \frac{17(p+1)}{2} + 4. \qquad \blacksquare$$

Lemma 3.1.7

If G and A are as above with $|x|$ dividing $p-1$ and G contains A_4 as a maximal subgroup then $|A| \leq \frac{7}{2}(p-1) + 5$.

Proof: In this case, we have the most subgroups to consider as x may lie in a Borel subgroup, D_{p-1} or A_4.

We again start by considering the case where $|x| > 5$. Such an x will lie in one copy of D_{p-1} and two distinct Borel subgroups which will consist of the upper and lower triangular matrices with respect to a basis in which x is diagonal. We need only count the involutions in these subgroups, noting that a Borel subgroup contains at most p involutions. In this case we get

$$A \subseteq \langle x \rangle \cup \operatorname{Inv} \mathcal{B}_1 \cup \operatorname{Inv} \mathcal{B}_2 \cup \operatorname{Inv} D_{p-1}$$

where $\mathcal{B}_1$ and $\mathcal{B}_2$ are the Borel subgroups in which x lies. This then gives us

$$|A| \leq |x| + 2p + \frac{p+1}{2} = \frac{5(p+1)}{2} + |x| - 2.$$

When $|x| \leq 5$ we must split this into several subcases as before.

Since G contains A_4 as a maximal subgroup we need only concern ourselves with the case where $|x| = 3$ and we count involutions as before. We may find out how many copies of A_4 contain x by using the action of D_{p-1} on the set of A_4s containing x in a very similar way to previous cases. So we have

$$A \subseteq \langle x \rangle \cup \operatorname{Inv} \mathcal{B}_1 \cup \operatorname{Inv} \mathcal{B}_2 \cup \operatorname{Inv} D_{p-1} \cup \frac{p-1}{3} \operatorname{Inv} A_4$$

which then gives

$$|A| \leq 3 + 2p + \frac{p-1}{2} + p - 1 = \frac{7(p-1)}{2} + 5. \qquad \blacksquare$$

Lemma 3.1.8

If G and A are as above with $|x|$ dividing $p-1$ and G contains A_5 and S_4 as maximal subgroups then $|A| \leq \frac{21}{2}(p-1) + 5$.

Proof: As with the last time, we shall merge all of the cases where A_5, S_4 or both appear as maximal subgroups of G. Acting with D_{p-1} we see that

$$A \subseteq \langle x \rangle \cup \operatorname{Inv} \mathcal{B}_1 \cup \operatorname{Inv} \mathcal{B}_2 \cup \operatorname{Inv} D_{p-1} \cup \frac{2(p-1)}{6} \operatorname{Inv} A_5 \cup \frac{2(p-1)}{6} \operatorname{Inv} S_4$$

and so, noting that if D_{p-1} contains a central involution it will also lie in a Borel subgroup,

$$|A| \leq 3 + 2p + \frac{p-1}{2} + 5(p-1) + 3(p-1) = \frac{21(p-1)}{2} + 5. \qquad \blacksquare$$

This completes the examination of the case where our maximal coclique A contains only one non-involution (and its powers). We will now use some of the techniques applied above in the more general case. Thus, let A be a maximal coclique of G which is not a maximal subgroup and suppose that A contains some element of order greater than two. The key observation in this next case is that the maximal subgroups which cause the most difficulty are those in class $\mathcal{S}$, but are also very small relative to the order of G (the order of a class $\mathcal{S}$ subgroup here is at most 60, while $|G|$ is cubic in p). As such, we do not lose too much if we simply take the union of all class $\mathcal{S}$ subgroups containing fixed elements of A and then treat the much larger subgroups with more care.

The following five results, Lemmas 3.1.9 to 3.1.13, make up the bulk of the proof of Theorem 3.1.4.

Lemma 3.1.9

Choose some $x \in A$ with $|x| > 2$. If $|x|$ divides $p+1$ and G contains A_4 as a maximal subgroup then $|A| \leq \frac{9}{2}(p+1) + 1$.

Proof: If $|x| > 3$ then x may only lie in D_{p+1} and thus by Lemma 3.1.3 we are done. Otherwise, we need only concern ourselves with $|x| = 3$. We note again that D_{p+1} contains a unique cyclic subgroup of order 3. As usual, $N_G(x)$ acts on the set of A_4s containing x by conjugation with orbit length at most $\frac{1}{|x|}(p-1) =: k_x$.

Now, we note that any involutions which lie outside of D_{p+1} must lie in some shared maximal subgroup with every element of A of order 3. Thus we have that any such involutions must lie in

$$\bigcap_{\substack{|x|=3\\ x\in A}} \bigcup_{i=1}^{k_x} A_4 \subseteq \bigcup_{i=1}^{k_x} A_4.$$

We therefore see that

$$|A| \leq \frac{p+1}{3}|A_4| + |\mathrm{Inv}\, D_{p+1}| \leq 4(p+1) + \frac{p+1}{2} + 1 = \frac{9(p+1)}{2} + 1. \qquad \blacksquare$$

Lemma 3.1.10

Choose some $x \in A$ with $|x| > 2$. If $|x|$ divides $p+1$ and G contains A_5 and S_4 as maximal subgroups then $|A| \leq \frac{93}{2}(p+1)$.

Proof: Again, we merge the cases where any of these maximal subgroups appear. As before, if $|x| > 5$ then we are done by Lemma 3.1.3. Our worst case of course is when both A_5 and S_4 appear as maximal subgroups of G, so this is the one we shall deal with. Here we fix up to three elements, x, y and z of respective orders 3, 4 and 5, lying in a single copy of D_{p+1}. Then any element of A will lie in one of the copies of S_4 or A_5 containing any of x, y or z or be an involution in D_{p+1} since D_{p+1} has a unique cyclic subgroup of any given order greater than 2. Thus,

$$A \subseteq \mathrm{Inv}\, D_{p+1} \cup 2\left(\bigcup_{x\in S_4} S_4 \cup \bigcup_{y\in S_4} S_4\right) \cup 2\left(\bigcup_{x\in A_5} A_5 \cup \bigcup_{z\in A_5} A_5\right).$$

Using our normal approach to determine how many copies of S_4 or A_5 may contain a given element, noting that their normalisers in these groups are dihedral, we obtain

$$|A| \leq \frac{p+1}{2} + 120\left(\frac{p+1}{6} + \frac{p+1}{10}\right) + 48\left(\frac{p+1}{6} + \frac{p+1}{8}\right) = \frac{93(p+1)}{2}. \qquad \blacksquare$$

Lemma 3.1.11

Choose some $x \in A$ with $|x| > 2$. If $|x|$ divides $p-1$ and G contains A_4 as a maximal subgroup then $|A| \leq \frac{17}{2}(p-1) + 6$ (and the +6 may be dropped for $p > 5$).

Proof: Here we need to consider contributions from two Borel subgroups, a copy of D_{p-1}

and several copies of A_4. If $|x| > 3$ then x may lie in D_{p-1} or two Borel subgroups, $\mathcal{B}_1$ and $\mathcal{B}_2$. If A is not one of these subgroups then A either consists of a few larger order elements along with all of the involutions from the subgroups in which they lie or A is simply made up of the intersections of these groups. In either case,

$$A \subseteq (D_{p-1} \cap \mathcal{B}_1) \cup (D_{p-1} \cap \mathcal{B}_2) \cup (\mathcal{B}_1 \cap \mathcal{B}_2) \cup \operatorname{Inv} D_{p-1} \cup \operatorname{Inv} \mathcal{B}_1 \cup \operatorname{Inv} \mathcal{B}_2.$$

But then

$$|A| \leq |D_{p-1} \cap \mathcal{B}_1| + |\operatorname{Inv} D_{p-1}| + 2|\operatorname{Inv} \mathcal{B}_1| \leq 3p$$

since D_{p-1} has at most $\frac{1}{2}(p+1)$ involutions and the intersection of the Borel subgroups and D_{p-1} is the cyclic group of order $\frac{1}{2}(p-1)$ consisting of those matrices which are diagonal with respect to the basis given by the eigenvectors of the two Borel subgroups.

Otherwise, we need only concern ourselves with $|x| = 3$. We note again that D_{p-1} contains a unique cyclic subgroup of order 3 and also that the Borel subgroups each contain p distinct cyclic subgroups of order 3. As usual, $N_G(x)$ acts on the set of A_4s containing x by conjugation with orbit length $\frac{1}{3}(p-1)$.

If we allow nH for $H \leq G$ to denote the union of n copies of H, we then get

$$A \subseteq 2p\langle x\rangle \cup \operatorname{Inv} \mathcal{B}_1 \cup \operatorname{Inv} \mathcal{B}_2 \cup \operatorname{Inv} D_{p-1} \cup \frac{p-1}{|x|} \operatorname{Inv} A_4$$

and so, accounting for some double counting,

$$|A| \leq 4(p-1) + 2p + \frac{p-1}{2} + 3\frac{p-1}{|x|} \leq 4(p-1) + 2p + \frac{p-1}{2} + 3\frac{p-1}{3} = 15\frac{p-1}{2} + 2$$

where we have taken $\frac{1}{2}(p-1)$ in place of $|\operatorname{Inv} D_{p-1}|$ since the additional involution will be contained in the Borel subgroups if it exists. Alternatively, we have

$$A \subseteq (\mathcal{B}_1 \cap \mathcal{B}_2 \cap D_{p-1}) \cup 2p\langle x\rangle \cup \bigcap_{\substack{|x|=3 \\ x \in A}} \bigcup_{i=1}^{k_x} A_4$$

and from the above we may tidy up the final term to get

$$|A| \leq \frac{p-1}{2} + 4(p-1) + 12\frac{p-1}{|x|} \leq \frac{p-1}{2} + 4(p-1) + 12\frac{p-1}{3} = 17\frac{p-1}{2}. \qquad \blacksquare$$

Lemma 3.1.12

Choose some $x \in A$ with $|x| > 2$. If $|x|$ divides $p-1$ and G contains A_5 or S_4 as maximal subgroups then $|A| \leq \frac{129}{2}(p-1)+2$.

Proof: As with the above cases, if $|x| > 5$ then we are done by Lemma 3.1.3. Otherwise our worst bound comes from when both A_5 and S_4 are present so we consider only this case and proceed in exactly the same way as before. Let k_x here be $2|x|$, *i.e.* the order of the normaliser of x in either A_5 or S_4. Then we have

$$A \subseteq \mathrm{Inv}(\mathcal{B}_1 \cup \mathcal{B}_2 \cup D_{p-1}) \cup 2p\langle x\rangle \cup 2p\langle y\rangle \cup 2p\langle z\rangle \cup 2 \bigcap_{\substack{|x|\in\{3,4\}\\ x\in A}} \bigcup_{i=1}^{k_x} S_4 \cup 2 \bigcap_{\substack{|x|\in\{3,5\}\\ x\in A}} \bigcup_{i=1}^{k_x} A_5.$$

Bounding this as usual, and accounting for some obvious multiple counting of $\langle x\rangle$, $\langle y\rangle$ and $\langle z\rangle$, we have

$$\begin{aligned} |A| &\leq \frac{p-1}{2} + 2p + 4(p-1) + 4(p-1) + 8(p-1) + \left(\frac{24}{3} + \frac{60}{3} + \frac{24}{4} + \frac{60}{5}\right)(p-1) \\ &= \frac{p-1}{2} + 2p + 16(p-1) + 46(p-1) \\ &= \frac{129}{2}(p-1) + 2, \end{aligned}$$

as required. $\blacksquare$

Lemma 3.1.13

Let A be a maximal coclique in G containing some element x of order p. Then A is a Borel subgroup.

Proof: If $|x| = p > 5$ then this is clear since the Borel subgroups are the only subgroups of order divisible by p. If $|x| = p = 5$ then the only subgroup which could also contain x is A_5, but A_5 is not a maximal subgroup of $\mathrm{PSL}_2(5)$. If $|x| = p = 3$ then $G = \mathrm{PSL}_2(3) \cong A_4$

and all elements of order 3 lie in unique maximal subgroups. In all cases, we are done by Lemma 3.1.3. ■

We are now ready to combine all of the above results to prove the main theorem.

Proof of Theorem 3.1.4. First we note that if $\langle A \rangle \neq G$ then A is a maximal subgroup by Lemma 3.1.2. Otherwise, if $\langle A \rangle = G$ then we have several cases to consider. In the first case, A may consist entirely of involutions since the group generated by two involutions will always be dihedral and thus is never equal to G for $p > 2$.

The structure of A is determined by the orders of its elements. If we fix some element $x \in A$ of order at least 3, then $|x|$ must divide precisely one of $p-1$, p or $p+1$. If $|x|$ divides $p-1$, we refer to Lemmas 3.1.11 and 3.1.12. If $|x|$ divides $p+1$ then we refer to Lemmas 3.1.9 and 3.1.10. Otherwise $|x|$ divides p, so $|x| = p$ and we refer to Lemma 3.1.13. In any case, we are done. ■

3.2 The prime-power case

We now consider the case of $G := \mathrm{PSL}_2(q_0)$ for $q_0 = p^n$ a prime power. We have little hope of achieving the same result as before due to the existence of copies of $\mathrm{PSL}_2(r)$ for $q_0 = r^s$, s prime, as a maximal subgroup of G. Indeed, simply trying to use the same methods as before would give us bounds to the order of $q_0^{\frac{3}{2}}$ for all even n in the case where the coclique was mostly involutions with a single large order element. We also have an interesting geometry which crops up for even n due to the fact that $\mathrm{PSL}_2(q^2) \cong \mathrm{P}\Omega_4^-(q)$ which we will investigate in this section.

At various points throughout this section, the maximal subgroups of G may be required, so we refer the reader to Theorem 2.2.8.

In terms of their classes in Aschbacher's Theorem (Theorem 2.2.6), we recall that a Borel subgroup is the stabiliser of an isotropic 1-space; $2.\mathrm{PSL}_2(q)$ is the stabiliser of a non-isotropic 1-space; D_{q_0-1} is the stabiliser of a non-degenerate 2-space and the copies of $\mathrm{PSL}_2(q)$ are stabilisers of subfields of prime index. We will not need to consider the classes of the other types of maximal subgroup.

3.2.1 Other cocliques of large order

We will now calculate explicitly the bound of order $q_0^{\frac{3}{2}}$ given above, which is evidence as to why the previous method may not work as well for this situation. We suppose that q is large enough that all of the necessary maximal subgroups exist.

As before, we assume that A is a maximal coclique which contains an element x with $|x| > 2$ such that $A \setminus \langle x \rangle$ consists entirely of involutions. If we suppose that x lies in $H \cong \mathrm{PSL}_2(q)$ and $|x|$ divides $q_0 - 1$ for $q_0 = q^r$, r an odd prime, then at the very least we may include all of the involutions from this subgroup. We then also note that $N_G(x)$ acts on the set of copies of $\mathrm{PSL}_2(q)$ containing x with orbit length

$$\frac{|N_G(x)|}{|N_H(x)|} = \frac{q_0 - 1}{q \pm 1}.$$

Including all of the involutions from these other subgroups too, we count

$$\frac{q_0 - 1}{q \pm 1} |\mathrm{Inv}\,\mathrm{PSL}_2(q)| = \frac{(q_0 - 1)|\mathrm{PSL}_2(q)|}{(q \pm 1)(q \pm 1)} = \frac{q_0 - 1}{q \pm 1} q(q \mp 1)$$

involutions. There is still some multiple-counting which we must account for.

We now suppose that $|x| = \frac{1}{2}(q-1)$, so $x \in D_{q_0-1}$. We then note that x lies in the intersection of all copies of $\mathrm{PSL}_2(q)$ above and since x must lie in some maximal subgroup of $\mathrm{PSL}_2(q)$, we know it must lie in a unique copy of D_{q-1}. Then we have that the intersection of any two copies of $\mathrm{PSL}_2(q)$ containing x must be either $\langle x \rangle$ or D_{q-1}, but since D_{q-1} normalises x we must also have that $D_{q-1} \subseteq D_{q_0-1}$. In fact, any such D_{q-1} must lie in $N_{D_{q_0-1}}(N_H(x)) \le D_{2(q-1)}$ (any proper non-cyclic normal subgroup of a dihedral group must have index 2) where $H \cong \mathrm{PSL}_2(q)$. If we assume the worst possible overcounting we see that our coclique must contain at least

$$2\frac{q_0-1}{q-1}q(q+1) - 2\frac{q_0-1}{q-1}(q+1) = 2\frac{q_0-1}{q-1}(q^2-1)$$

involutions. We don't know if the coclique this gives us is necessarily maximal, but we at least have a lower bound on its order.

So we obtain a bound of order $q_0^{1+\frac{1}{r}}$ where $q_0 = q^r$ and r is the least odd prime such that this happens. The least bound is obtained when we suppose that $|x| = \frac{1}{2}(q \pm 1)$. It's possible that one could improve this with a good understanding of how these subfield stabilisers intersect, but the smallest case in which this occurs is $\mathrm{PSL}_2(3^6)$ and is not easy to compute such things in. Doing the same with $2.\,\mathrm{PSL}_2(q)$ for $q_0 = q^2$ gives us the bound of order $q_0^{\frac{3}{2}}$ mentioned above.

We suspect that a similar result to Theorem 3.1.4 will hold in the prime-power case and that the geometric anomaly described below is the only exception to what we had before, but the existence of this example makes trying to use the previous methods very complicated. We think that if a maximal coclique A is such that $|A| > O(\sqrt{|G|})$ then it either consists of involutions or is a Borel subgroup; if $|A| = O(\sqrt{|G|})$ then it should be one of the subfield stabiliser maximal subgroups; and if it is smaller we can't really say much.

3.2.2 Construction

We first let $q_0 = q^2$ and consider the action of G on $\mathbb{F}_q^4$ as $\mathrm{P}\Omega_4^-(q)$. Fix some non-isotropic vector v. To ease notation, we let v denote the $\mathbb{F}_q$-span of v as well as the vector itself since the distinction is not overly important here. Then $\mathbb{F}_q^4 = v \oplus v^\perp$. We wish to consider the elements of G which have 2-dimensional eigenspaces lying in $v^\perp$, so we must start by determining how many such subspaces one may have.

We wish to collect all of these elements in order to obtain a large coclique with order cubic in q since if one takes any two elements g, h with 2 dimensional eigenspaces V_g,

$V_h \subseteq v^\perp$ then since $\dim v^\perp = 3$ the intersection of any two 2-dimensional subspaces must be nontrivial. Thus $\langle g, h\rangle$ must be contained in the stabiliser of $V_g \cap V_h \neq 0$ and so $\langle g, h\rangle \neq G$.

A subspace of dimension 3 over $\mathbb{F}_q$ has $\frac{q^3-1}{q-1} = q^2+q+1$ subspaces of dimension 2, and as seen in [51, Propositions 2.5.10, 2.5.12] we have that if such a subspace (with symmetric bilinear form having gram matrix g) has an orthonormal basis ($\det g$ a square) then it is of $-$ type for $q \equiv 3 \mod 4$ and if such a basis does not exist ($\det g$ is a non-square) then it is of $+$ type. If a space is of neither $+$ nor $-$ type then it is degenerate ($\det g = 0$). For $q \equiv 1 \mod 4$, the 2-spaces with orthonormal bases are of $+$ type and to obtain a $-$ type space we must instead consider a space with basis $\{e, f\}$ where $(e, e) = 1$ and $(f, f) = \alpha$ for some non-square $\alpha \in \mathbb{F}_q^*$.

Using the fact that the orthogonal group acts transitively on isometric subspaces (Corollary 2.2.3) one sees that a 3-dimensional orthogonal $\mathbb{F}_q$-space contains $q\frac{q-1}{2}$ 2-spaces of $-$ type, $q\frac{q+1}{2}$ 2-spaces of $+$ type and $q+1$ degenerate 2-spaces. We wish to construct a coclique by taking the elements of G which have any of these 2-spaces as eigenspaces. The only possible eigenvalues for elements of G are ± 1.

Lemma 3.2.3

Let $U \subseteq V$ be a degenerate 2-space. Then its pointwise stabiliser in G is isomorphic to $(\mathbb{F}_q, +)$.

Proof: For this, we refer to [51, Proposition 2.9.1 (v)] for an explicit isomorphism between $\mathrm{PSL}_2(q^2)$ and $\Omega_4^-(q)$, along with the form stabilised by G under this map. Using the basis $\{u_1 \coloneqq v_1 \otimes v_1, u_2 \coloneqq v_2 \otimes v_2, w_1 \coloneqq v_1 \otimes v_2 + v_2 \otimes v_2, w_2 \coloneqq \lambda v_1 \otimes v_2 + \bar{\lambda} v_2 \otimes v_1\}$ for $\bar{\cdot}$ an involutory automorphism of $\mathbb{F}_{q^2}$ and $\lambda \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ we may now also consider this action from a linear point of view. For one of the w_i, we have that $\mathrm{span}_{\mathbb{F}_q}\{u_1, u_2, w_i\}$ is a 3-space of $-$ type and contains the degenerate subspace $W \coloneqq \mathrm{span}_{\mathbb{F}_q}\{u_1, w_i\}$. The pointwise stabiliser of W is contained in the stabiliser of its radical, $\mathbb{F}_q u_1$, and thus lies in a (linear) Borel subgroup. It is then a straightforward calculation using the aforementioned isomorphism to confirm that the pointwise stabiliser of this space is isomorphic to E_q. ■

We next wish to determine the subgroups which have given nondegenerate 2-dimensional eigenspaces $U \subseteq v^{\perp}$. Such an element must act as ± 1 on U and as an element of $\mathrm{SO}(U^{\perp})$ on $U^{\perp}$. A direct calculation using the spinor norm (Definition 2.2.4) or similar to that above shows that the set of elements with U as an eigenspace is cyclic of order $|\mathrm{SO}(U^{\perp})|$. In particular, if $\mathrm{SO}(U^{\perp}) = \langle h \rangle$ then for $q \equiv 1 \mod 4$ the sets we are looking for are subgroups generated by $h^2 \oplus -I_2$ and $h \oplus -I_2$ for $U^{\perp}$ of $+$ type and $-$ type, respectively. For $q \equiv 3 \mod 4$ then we instead have $h \oplus -I_2$ and $h^2 \oplus -I_2$ (where $A \oplus B$ is the block-diagonal matrix with A in the top left and B in the bottom right).

Lemma 3.2.4

The set of all elements with 2-dimensional eigenspaces in $v^{\perp}$ is a coclique of order $q^3 + q$.

Proof: To see that such elements form a coclique, note that if g, h have 2-dimensional eigenspaces V_g, $V_h \subseteq v^{\perp}$, then $V_g \cap V_h \neq 0$ and thus $\langle g, h \rangle \leq \mathrm{Stab}_G(V_g \cap V_h) \neq G$. We also have a description of the elements with 2-dimensional eigenspaces in $v^{\perp}$ in the lemmas above, so it is sufficient to check that there is no overlap.

Suppose that some element g has two distinct 2-dimensional eigenspaces inside of $v^{\perp}$. Then clearly g must have a 3-dimensional 1-eigenspace (namely $v^{\perp}$) and so g must also stabilise v and since we require $\det g = 1$ we must have that $gv = v$ and $g = I_4$. Thus the intersection of any pair of groups generated by the elements of the coclique of maximal order is trivial. Collecting all of these groups together, we see that we obtain a set of size

$$(q-2)\frac{q(q-1)}{2} + \frac{q^2(q+1)}{2} + (q-1)(q+1) + 1 = q^3 + q$$

and so, as claimed, we obtain a coclique of order cubic in q. ■

Theorem 3.2.5

The coclique A obtained above is maximal.

We first state a lemma to clean up the end of the proof of this theorem.

Lemma 3.2.6

Suppose V has a decomposition $V = V_\lambda \oplus V_\mu \oplus V_\nu \oplus V_\kappa$ into distinct (or zero) eigenspaces of $g \in G$ such that no eigenspace has at least 2-dimensional intersection with $v^\perp$. Then there exists some $h \in A$ such that $\langle g, h \rangle$ stabilises no proper nontrivial subspace of V.

Proof: Without loss of generality, we may say that $V_\kappa \cap v^\perp = 0$ and the other three eigenspaces have at most 1-dimensional intersection with $v^\perp$. Since an element $h \in A$ of maximal order fixes some point if and only if it lies in its eigenspace U (or is one of two isotropic vectors when $|h| = q - 1$), we may choose any $h \in A$ of maximal order such that none of the eigenspaces with nontrivial intersection with $v^\perp$ intersect with U and U is non-degenerate. We may do this since even in the worst case where $v^\perp$ has a basis of eigenvectors for distinct eigenvalues, there are at most $3(q+1)$ 2-spaces containing any of these three points. However, there are q^2 non-degenerate 2-spaces in $v^\perp$ and since we chose $q > 3$ earlier, $q^2 > 3(q+1)$. Then $\langle g, h \rangle$ cannot stabilise any proper, nontrivial subspaces of V. ■

Proof of Theorem 3.2.5. We now show that the coclique obtained above is indeed maximal by considering the maximal subgroups of $\mathrm{P}\Omega_4^-(q)$. In what follows, the term 'point' refers to a 1-space.

This time around, we may ignore D_{q^2+1} since for $q > 3$ we have $q \pm 1 > 2$ and if r divides both $q - 1$ and $q^2 + 1$ then $r \mid (q-1)(q+1) = q^2 - 1$, thus $r \mid q^2 + 1 - (q^2 - 1) = 2$. A similar argument holds for $q + 1$, and clearly the only natural number dividing both p and $q^2 + 1$ is 1. Then we may ignore A_5 and the subfield stabilisers $\mathrm{PSL}_2(q)$ by simply choosing the stabilisers of non-degenerate 2-spaces in the argument that follows since these are generated by elements of order $q \pm 1$ which are not found in A_5 or $\mathrm{PSL}_2(q)$ for $q > 3$. If we take an element h of maximal order in the stabiliser of some non-degenerate subspace and some other $g \in G$ then we have that $\langle g, h \rangle$ cannot be contained in either A_5 or $\mathrm{PSL}_2(q)$ as these groups do not have elements of sufficiently large orders.

We note that the remaining three maximal subgroups are all of class $\mathcal{C}_1$ and so represent the stabilisers of singular or non-singular subspaces. We thus look at how the stabilisers of various subspaces of $\mathbb{F}_q^4$ interact with A. We first note that the dihedral subgroups D_{q^2-1} represent the stabilisers of non-degenerate 2-dimensional subspaces (as the stabiliser of a degenerate one lies in the point stabiliser of its radical) and recall that the Borel subgroups and $2.\operatorname{PSL}_2(q)$ are the stabilisers of isotropic and non-isotropic 1-spaces, respectively.

We also note that an element $h \in A$ of maximal order stabilising a non-degenerate 2-space $U \subseteq v^\perp$ will stabilise some point if and only if this point lies inside U or $|h| = q-1$ and this point is one of two isotropic points in $U^\perp$. We first consider the case where $g \in G$ stabilises some non-degenerate 2-space. If g stabilises $V \subseteq v^\perp$ either V is an eigenspace of g or there is some 1-space $\mathbb{F}_q u \subseteq V$ not fixed by g. If there is one such point then there are many others, since if g fixes more than 2 non-isotropic points in the same 2-space then this space would have to be an eigenspace for g. We may therefore choose some $u \in V$ not fixed by g and a corresponding $x \in V^\perp$, also not fixed by g, such that $\operatorname{span}_{\mathbb{F}_q}\{u, x\}$ is non-degenerate. Then the element of A of maximal order with eigenspace $(\operatorname{span}_{\mathbb{F}_q}\{u, x\})^\perp$ will be such that $\langle g, h\rangle$ stabilises no proper nontrivial subspace of $\mathbb{F}_q^4$ and so must be equal to G.

Next, we consider the case where g stabilises some degenerate 2-space $V \subseteq v^\perp$. Either V is an eigenspace for g or there is a (non-isotropic) 1-space $\mathbb{F}_q u \subseteq V$ not fixed by g. Then, as in the non-degenerate case, we may pick some non-isotropic vector $x \in V^\perp$ such that $\operatorname{span}_{\mathbb{F}_q}\{u, x\}$ is non-degenerate and an element $h \in A$ of maximal order with eigenspace $(\operatorname{span}_{\mathbb{F}_q}\{u, x\})^\perp$ such that $\langle g, h\rangle = G$.

Otherwise, if g has a 2-dimensional degenerate eigenspace inside of $v^\perp$ then either the corresponding eigenvalue is 1 and so $g \in A$ or it is -1 and a direct computation shows us that some power of such an element would be $-I_4 \notin G$, thus no such element exists.

We are now left with a number of simpler cases corresponding to the possible eigenspaces of a general element $g \in G$. If g has an eigenspace of dimension at least 3 then its intersection with $v^\perp$ must be at least 2-dimensional and so $g \in A$. Otherwise, g must have eigenspaces of dimension at most 2 and so we know that either it lies in A or, by Lemma 3.2.6, there will exist some $h \in A$ such that $\langle g, h\rangle$ does not stabilise any proper nontrivial subspaces of V and thus g and h will generate G. Maximality of A follows. ■

CHAPTER 4

BACKGROUND ON MODULAR REPRESENTATION THEORY

In this chapter, we present all of the results from representation theory which will be required for Chapter 5. We have not assumed any prior knowledge of representation theory for this chapter, but to properly present some of the results contained herein would require an entire (rather large) book and as such this chapter will necessarily be light on detail in some areas. For a thorough treatment of more advanced results, almost all of the material in this chapter can be found somewhere in the books by Curtis and Reiner [22, 23, 24], with some notable (and thus noted) exceptions. For an introduction that doesn't require three entire books, consider [21] instead.

Many objects in algebra are often best understood or explained not by working axiomatically or staying entirely within this object, but by investigating what it actually does to other well-understood objects. For example, we most frequently understand symmetric and alternating groups through their natural actions on sets of subsets of $\{1, \ldots, n\}$; we would explain dihedral groups by realising them as automorphism groups of n-gons; and we best understand matrix groups such as $\mathrm{SL}_n(q)$ through their natural actions on vector spaces. This last example is the core idea behind representation theory — realise some abstract algebraic object as a set of linear transformations of a vector space in order to use properties of this action to understand more about our original object.

The natural action of $\mathrm{SL}_n(q)$ on the vector space $\mathbb{F}_q^n$ is an example of a linear representation of $\mathrm{SL}_n(q)$ and, in general, a representation of a finite group G is a map from G into $\mathrm{GL}_n(k)$ for some $n \in \mathbb{N}$ and some field k. Matrix groups acting on their natural vector spaces are great examples of the power of representation theory in general, as we can use properties of these actions to give us lots of information about the group. For example, most of the classes in Theorem 2.2.6 (and its more general version — Aschbacher's Theorem [10, Theorem 2.2.19]) correspond to certain decompositions or properties of the natural vector space preserved by subgroups in the class. Another important example of this classifies the maximal subgroups of S_n in a similar way — the O'Nan–Scott Theorem [16, Theorem 4.8], which has even gone so far as to classify all primitive permutation groups.

The following assumption is vital for several results in this chapter. Throughout this section we shall assume that all groups are finite and **all modules are finitely generated**. Many of the results here are true in greater generality, but we will not need anything more than what we have assumed for this thesis.

4.1 Introductory representation theory

In this section we briefly introduce representations of finite groups and outline some of the key results required to understand group cohomology and several that we will use to help out in Chapter 5. The main references for this section are [29] and [53], but [1] makes for a nice quick introduction to modular representation theory and any of [22, 23, 24] are good for a thorough approach with a lot of machinery.

We begin with a basic introduction to modules, as working in the language of modules gives a nice way to think about representation theory and much of the machinery from this area is immensely useful for our purposes. The remainder of the section will then be devoted to various results and objects that we can use to investigate the structure of modules, how to take them apart and what happens when we move from one ring to another. We start, as one might expect, with the definition.

Definition 4.1.1

Given a ring R, we define a *left R-module* to be an additive abelian group M with an action by elements of R such that, for any r, $s \in R$, m, $n \in M$,

i) $r(m+n) = rm + rn$,

ii) $(r+s)m = rm + sm$,

iii) $r(sm) = (rs)m$,

iv) $1m = m$.

One equivalently defines a *right R-module* by using analogous properties with R acting on the right instead. If R is commutative then there is no real difference between left and right modules, and if R is a field then M is a vector space. In all the definitions for left modules that follow there will be a right module equivalent obtained in exactly the same way, we thus omit the left or right when referring to modules and treat all modules as though they were left modules unless explicitly stated.

The reader familiar with group actions should see that a module is essentially the equivalent structure except for a ring, though the structure of a module has to be much more rigid than for a set being acted upon by a group. Next, in the usual fashion, after having defined a 'thing,' we now define subthings, quotient things and thing homomorphisms. As is common in algebra, we also have all of the usual thing isomorphism theorems, too, proven in the same way as your favourite thing isomorphism theorem.

Definition 4.1.2

Given an R-module M, we say that $N \subseteq M$ is a *submodule* of M if $N \leq M$ as an abelian group and $RN := \{rn \mid r \in R,\ n \in N\} \subseteq N$. Given a submodule N of M we may form the *quotient module* by imposing the obvious R-module structure on the quotient group M/N.

Definition 4.1.3

Given two R-modules M and N, an *R-module homomorphism* is a map $\varphi\colon M \to N$ such that, for any $r \in R$, m, $n \in M$ we have that $\varphi(m+n) = \varphi(m) + \varphi(n)$ and $\varphi(rm) = r\varphi(m)$. We denote the set of all R-module homomorphisms $\varphi\colon M \to N$ by $\mathrm{Hom}(M, N)$, or $\mathrm{Hom}_R(M, N)$ if there is possible confusion about the underlying ring.

Definition 4.1.4

Given R-modules M and N with a homomorphism $\varphi\colon M \to N$, we use $\varphi\colon M \hookrightarrow N$ to say that φ is an injection or simply $M \hookrightarrow N$ to say that there exists such an injection. Similarly, we use $\varphi\colon M \twoheadrightarrow N$ to say that φ is a surjection or just $M \twoheadrightarrow N$ to say that such a surjection exists.

We have analogous definitions to Definitions 2.1.2 and 2.1.4 of direct sums and tensor products for general R-modules rather than simply vector spaces. However, a little more care is needed for the tensor products when R is not a commutative ring. Let M be a *right* R-module and N a left R-module. Then the tensor product $M \otimes_R N$ is defined as before, except that we require $\otimes$ to be R-bilinear so that $r(m \otimes n) = (mr) \otimes n = m \otimes (rn)$ for any $m \in M$, $n \in N$ and $r \in R$ along with the usual requirements of bilinearity. When tensoring modules together, we will always state the ring being used (*e.g.* we will use $M \otimes_R N$ rather than just $M \otimes N$) unless we are tensoring vector spaces together over their base field which will be true in the majority of cases.

We now define the dual space of a vector space before investigating some of the properties of Hom, tensor products and these dual spaces. These properties will come in very useful later when we start looking at Ext, which one can view as a generalisation of Hom. Recall that in this thesis we will only be dealing with modules which are finitely generated (and thus vector spaces which are finite-dimensional).

Definition 4.1.5

Let V be a k–vector space. Then we define the *dual* V^* of V to be $\mathrm{Hom}_k(V, k)$.

Usually, when working with vector spaces we omit the subscript k in Hom_k as this is generally well-understood. There is also a notion of duals for an arbitrary module, defined in exactly the same way, but we will only take vector space duals in this thesis and do not want there to be any possible confusion when taking the dual of a vector space that is also a module over a different ring.

Lemma 4.1.6

Let V be a k–vector space. Then there is a *natural isomorphism* $(V^*)^* \cong V$.

Proof: Let $\varphi\colon V \to (V^*)^*$ be the evaluation map $v \mapsto (\psi \mapsto \psi(v))$. It is easy to see that this is linear, and $\ker \varphi = \{v \in V \mid \psi(v) = 0 \ \forall \psi \in V^*\} = 0$. That φ is an isomorphism then follows from the fact that $\dim V = \dim V^* = \dim (V^*)^*$. ■

Lemma 4.1.7

Let R be a ring and A, B and C be R-modules. Then $\mathrm{Hom}_R(A, B \oplus C) \cong \mathrm{Hom}_R(A, B) \oplus \mathrm{Hom}_R(A, C)$ and $\mathrm{Hom}_R(A \oplus B, C) \cong \mathrm{Hom}_R(A, C) \oplus \mathrm{Hom}_R(B, C)$.

Proof: We prove the first isomorphism; the second is identical using inclusion maps rather than projections. Let $\pi_B\colon B \oplus C \to B$ be the projection onto the first coordinate and similarly $\pi_C\colon B \oplus C \to C$ onto the second. We show that $\varphi\colon \mathrm{Hom}_R(A, B \oplus C) \to \mathrm{Hom}_R(A, B) \oplus \mathrm{Hom}_R(A, C)$ given by $\varphi(\theta) = (\pi_B \circ \theta, \pi_C \circ \theta)$ is an isomorphism. That φ is a linear map is clear, as is injectivity since if $\pi_B \circ \theta = \pi_C \circ \theta = 0$ then θ has no nonzero image inside either B or C and is thus zero. Finally, to see surjectivity, let $(\theta_1, \theta_2) \in \mathrm{Hom}_R(A, B) \oplus \mathrm{Hom}_R(A, C)$. Then note that $(\theta_1, \theta_2) = \varphi(\theta)$ where $\theta(x) = (\theta_1(x), \theta_2(x))$ for any $x \in A$. ■

One well-known property of vector spaces is that for every subspace $U \subseteq V$ of V, there exists some *complement* W such that $V = U \oplus W$. This is quite a strong property and comes about because vector spaces are *free* (we will see what this means in Section 4.2), but for modules over arbitrary rings this is very much not the case. We will see an example of this when R is a group ring later on in this section, but here is another example outside of representation theory for groups. Let R be a ring and S be the subring

$$\begin{pmatrix} R & R \\ 0 & R \end{pmatrix} \subseteq \mathrm{M}_2(R)$$

of upper triangular 2×2 matrices over R. Now let M be the natural left S-module given by left multiplication on 2-dimensional column vectors over R. Then we see that

$$\begin{pmatrix} R & R \\ 0 & R \end{pmatrix} \begin{pmatrix} R \\ 0 \end{pmatrix} = \begin{pmatrix} R \\ 0 \end{pmatrix}$$

and thus $\left(\begin{smallmatrix} R \\ 0 \end{smallmatrix} \right)$ is a submodule of M. One would naturally expect that $\left(\begin{smallmatrix} 0 \\ R \end{smallmatrix} \right)$ would be a complement to this, but of course

$$\begin{pmatrix} R & R \\ 0 & R \end{pmatrix} \begin{pmatrix} 0 \\ R \end{pmatrix} = \begin{pmatrix} R \\ R \end{pmatrix}$$

and so this natural-looking complement is in fact not even a submodule. One can check that the submodules of M are of the form $\left(\begin{smallmatrix} I \\ J \end{smallmatrix} \right)$ where I, $J \trianglelefteq R$ and $J \subseteq I$. If such a module was a complement to $\left(\begin{smallmatrix} R \\ 0 \end{smallmatrix} \right)$, then we would need

$$\begin{pmatrix} R \\ 0 \end{pmatrix} + \begin{pmatrix} I \\ J \end{pmatrix} = \begin{pmatrix} R \\ J \end{pmatrix} = M$$

but also

$$\begin{pmatrix} R \\ 0 \end{pmatrix} \cap \begin{pmatrix} I \\ J \end{pmatrix} = 0.$$

The first condition tells us that we need $J = R$. Since $J \subseteq I$, this means $I = J = R$ and in fact we need all of M. Clearly, $M \cap \left(\begin{smallmatrix} R \\ 0 \end{smallmatrix} \right) \neq 0$ and so M is not a complement and indeed no such complement exists. Thus the module M as given is not *completely reducible*, a term which we shall see in the next definition.

Definition 4.1.8

We say that an R-module M is *decomposable* if we may decompose it into a direct sum $M = N \oplus N'$ of two proper nontrivial submodules N, N' of M and we call N' a *complement* to N in M. We call M *indecomposable* otherwise. Further, if M has no proper nontrivial submodules then M is said to be *irreducible* or *simple*. We say that a module M is *completely reducible* or *semisimple* if for every submodule $N \subseteq M$ there exists some complement N' such that $M = N \oplus N'$. We say that a ring R is *semisimple* if it is a completely reducible R-module.

One would expect that we would need definitions of left and right semisimple where R is semisimple as a left or right R-module, but in fact these conditions coincide and thus we need only speak of semisimple rings.

Lemma 4.1.9 [22, 3.12 and 3.15]
If R is a semisimple ring then every R-module is completely reducible.

There are wide classes of modules which are semisimple, but there are also a lot of natural structures that are actually not semisimple with one example seen above. Both of these cases occur in the representation theory of finite groups and we shall see examples of each later on in this thesis. To that end, we introduce the group algebra kG and start with the actual representation theory.

Definition 4.1.10
An *algebra* A over a field k is a k-module (thus vector space) which is also a ring with multiplication such that $\alpha rs = (\alpha r)s = r(\alpha s)$ for all r, $s \in A$, $\alpha \in k$. A *subalgebra* $B \subseteq A$ is both a subring and a vector subspace. Given a group G and a field k, we form the group ring kG which is defined to be the set of all sums $\sum_{g \in G} \alpha_g g$ where $\alpha_g \in k$ with the obvious notions of addition and multiplication. The group ring of any group over a field k is a k-algebra.

Definition 4.1.11
Given a group G, we define a *representation* of G to be a homomorphism $\varphi \colon G \to \mathrm{GL}(V)$ for some vector space V. We say that two representations $\varphi \colon G \to \mathrm{GL}(V)$ and $\psi \colon G \to \mathrm{GL}(W)$ of G are *isomorphic* if there exists a linear isomorphism $\theta \colon V \to W$ such that $\theta \circ \varphi(g) \circ \theta^{-1} = \psi(g)$ for all $g \in G$.

A representation $\varphi\colon G \to \mathrm{GL}(V)$ of a group G corresponds to imposing an action of G on V by linear maps. As such, one may also view representations of a group as modules over the ring kG (which we sometimes just call G-modules), where k is the underlying field of V. Similarly, isomorphisms of representations are equivalent to isomorphisms of kG-modules (so θ as seen above is a linear isomorphism which commutes with the G-action), and because of these properties we often abuse notation by referring to the kG-modules themselves as representations of G.

Definition 4.1.12

Given a group G, we say that a kG-module V is *absolutely irreducible* if $V \otimes_k k'$ is irreducible as a $k'G$-module for any extension field k' of k. In particular, it is sufficient to check that $V \otimes_k \overline{k}$ is irreducible as a $\overline{k}G$-module. We say that a field k is a *splitting field* for G if every irreducible kG-module is absolutely irreducible.

Definition 4.1.13

Let G be a group and k a field. We denote by $\mathrm{Irr}_k\, G$ the set of irreducible kG-modules.

Definition 4.1.14

Given a G-module V, we define the *G-fixed points* of V to be

$$V^G := \{v \in V \mid gv = v \ \forall g \in G\}.$$

Note that $V^G \cong \mathrm{Hom}_G(k, V)$, where k is regarded as the 1-dimensional trivial kG-module. We also define the *dual* representation to V to be the dual space $V^* := \mathrm{Hom}_k(V, k)$ with the G-action $g\varphi(v) := \varphi(g^{-1}v)$ and the *tensor product* representation of two G-modules V and W to be the usual tensor product $V \otimes_k W$ of the underlying vector spaces with the diagonal G-action $g(v \otimes w) = (gv) \otimes (gw)$.

It is important to note in the above definition that even when working with kG-modules, we still take duals and tensor products over k in most circumstances. As such, when dealing with kG-modules V and W the notation $V \otimes W$ will always mean a tensor product over k and tensor products over any other rings will always be explicitly stated when used.

Definition 4.1.15

Given a subgroup H of a group G we define the *permutation module* of G on H over k to be the k–vector space with basis G/H under the obvious G-action on cosets of H in G.

Lemma 4.1.16 (Schur's Lemma) [22, 3.17]

Let R be a ring and V, W be irreducible R-modules. Then $\mathrm{Hom}_R(V, W) = 0$ if V and W are not isomorphic and is otherwise a division ring.

Schur's Lemma above is often written in a variety of different forms, but in all cases the proof essentially says that any nonzero $\varphi\colon V \to W$ must have trivial kernel in V and its image must be all of W by irreducibility. All such maps are thus isomorphisms.

Definition 4.1.17

We say that a ring R is *simple* if it has no proper non-zero two-sided ideals.

This next theorem is a very important result in noncommutative algebra. We do not use it ourselves, but include it for context as it gives good insight into the structure of semisimple rings and their modules.

Theorem 4.1.18 (Artin–Wedderburn) [22, 3.22]

Let R be a semisimple ring. Then $R = R_1 \oplus \ldots \oplus R_n$, where each R_i is a simple ring such that $R_iR_j = 0$ whenever $i \neq j$. Moreover, each R_i is isomorphic to a matrix ring over a division ring (namely the endomorphism ring of some irreducible R-module V_i, by [22, 3.28]). Each irreducible R-module is isomorphic to precisely one such V_i and $R_iV_j = 0$ if $i \neq j$, while $R_iV_i = V_i$.

The next theorem we state is another very major result. This essentially says that in coprime characteristic, the representation theory of G is very nice indeed.

Theorem 4.1.19 (Maschke's Theorem) [22, 3.14]

Let G be a finite group and k a field with $\operatorname{char} k$ coprime to $|G|$. Then the group algebra kG is a semisimple ring.

Note that when $\operatorname{char} k \mid |G|$ then the conclusion of Maschke's Theorem is always false. For example, if $G = C_2$ and $k = \mathbb{F}_2$, then $\dim kG = |G| = 2$. If $G = \{1, g\}$ where $g^2 = 1$ then $kG = k1 \oplus kg$ as a vector space. Clearly then $(kG)^G = k(1+g)$ is 1-dimensional. If we assume that kG is semisimple, so $kG = (kG)^G \oplus V$ for some 1-dimensional (hence irreducible) module V, we must have that $V = k1$ or $V = kg$. However, in the first case we see that $1 \in GV \setminus V$ and in the second we see $g \in GV \setminus V$ so in both cases V is not a submodule. Thus no such complement V exists, and kG is not semisimple, but we can see that kG has a trivial submodule $(kG)^G$ and that $kG/(kG)^G$ is again trivial. So kG is somehow a pair of trivial modules 'stuck together,' but not as a direct sum. We say that kG is a *non-split extension* of the trivial module by itself and we shall see generalisations of this setting, along with definitions of these terms, in Section 4.2.

We now give names to some of the structures we quietly made use of in the previous argument, and put them into a more general setting. Even though modules need not be completely reducible, we can still break them down entirely in terms of simple modules. Formally, we have the following.

Definition 4.1.20

Given an R-module M, we define its *socle*, $\operatorname{soc} M$, to be the sum of its simple submodules (one may view this as the largest semisimple submodule of M). Dually, we define the *radical*, $\operatorname{rad} M$, of M to be the intersection of all of its maximal submodules. Then $\operatorname{head} M := M / \operatorname{rad} M$ is the largest semisimple quotient of M. Finally, the *heart* of M is $\mathcal{H}(M) := (\operatorname{rad} M)/(\operatorname{rad} M \cap \operatorname{soc} M)$ and is the module obtained by 'removing' the socle and head of M.

We can use generalisations of socles and radicals to 'take apart' modules and break them into socle factors or radical factors, at least for 'sufficiently nice' rings R such as group algebras for finite groups. We prefer to use radical factors here, which break modules down by way of their quotients and show their structure starting from the head and working down. Dually, we have a notion of socle factors and a socle series where one breaks the module down by taking successively larger submodules. We will only be working in terms of radical factors here, so we only give this definition. Recall here that we only talk about modules which are finitely generated in this thesis.

Definition 4.1.21

Given an R-module M, we define the i^{th} *radical factor* of M to be $\operatorname{rad}^{i-1} M / \operatorname{rad}^i M$, where $\operatorname{rad}^0 M := M$ and we define $\operatorname{rad}^{i+1} M := \operatorname{rad}(\operatorname{rad}^i M)$. The collection of radical factors of M is called its *radical series*.

Definition 4.1.22

Given an R-module M, a *composition series* for M is a sequence of submodules $0 =: M_0 \lneq M_1 \lneq \ldots \lneq M_n := M$ such that each M_i/M_{i-1} is irreducible.

The Jordan–Hölder theorem for modules [22, 3.11] states that if such a composition series exists then the *composition factors* M_i/M_{i-1} are unique (up to reordering and isomorphism). Since we are working with finite-dimensional vector spaces in this thesis, a composition series always exists for the modules we consider.

As well as taking general results from the theory of modules over an arbitrary ring, we also wish to return to our main area of interest and specialise to when $R = kG$ is the group ring for a (finite) group G. While we can look at various types of submodules of a module and see what they tell us, we can also see what happens when we consider this module upon restriction to a subgroup of G or perhaps see what modules for a subgroup can tell us about those for the larger group. For this, we of course need some way of moving between modules for a subgroup and for its overgroups which we will introduce now.

Definition 4.1.23

Given a subgroup H of G and a kG-module V, we define the *restriction* $\operatorname{Res}^G_H V$ of V to H to be V viewed as a H-module via the natural action. Formally, if $\varphi\colon G \to \mathrm{GL}(V)$ is a representation affording V and $\iota\colon H \hookrightarrow G$ is the inclusion map, then $\operatorname{Res}^G_H V$ is the module afforded by the representation $\varphi\iota\colon H \to \mathrm{GL}(V)$. Conversely, given a kH-module W, we define the *induced module* $\operatorname{Ind}^G_H W := W \otimes_{kH} kG$.

The notation above for induction and restriction is a little unwieldy, so we will try to avoid it where possible. To this end, we shall also denote the restriction of a kG-module V to a subgroup $H \leq G$ by V_H. Some authors also denote induced modules by V^G as in [1], but this will clash with our notation for fixed points so we will stick to $\operatorname{Ind}_H^G V$.

Much like the restriction of a module to a subgroup is of course a module for this subgroup, the induced module from H to G is a kG-module. One example of an induced module is the permutation module defined in Definition 4.1.15. One can check that the permutation module of G acting on cosets of H is isomorphic to $\operatorname{Ind}_H^G k$, where k is regarded as the trivial kG-module. This can be seen more clearly from the proof of the next lemma.

In the representation theory of finite groups, it is a common technique to move modules between subgroups and overgroups and use various relationships between them to obtain much more information than we may initially know from just one group's structure alone. Some of the most notable examples of this are Frobenius Reciprocity and Mackey's Formula, seen below, along with Clifford Theory, based on Clifford's Theorem [22, 11.1] which relates the representation theory of a finite group to that of its normal subgroups. We give a few such results to close out this section.

Lemma 4.1.24

Let $H \leq G$ be groups and let V be a kH-module. Then $\dim \operatorname{Ind}_H^G V = [G : H] \dim V$.

Proof: We show that $\operatorname{Ind}_H^G V \cong \bigoplus_{g \in G/H} g \otimes V$. To see this, recall that since a tensor product is bilinear then for any $h \in H$ we have that $h \otimes V = 1 \otimes hV = 1 \otimes V$. So if $g \in G$ lies in the coset $g'H$, then $g \otimes V = g'h \otimes V = g' \otimes V$ for some $h \in H$. So in particular, $gH \otimes V = \sum_{h \in H} gh \otimes V = \sum_{h \in H} g \otimes V = g \otimes V$.

Then $kG \otimes_{kH} V = \sum_{g \in G/H} gH \otimes V = \sum_{g \in G/H} g \otimes V$. This sum is direct, and so the result follows from the fact that $\dim(g \otimes V) = \dim V$. This latter statement holds since $\{g \otimes v \mid v \in \mathcal{B}\}$ is a basis for $g \otimes V$ given any basis $\mathcal{B}$ of V. ■

Theorem 4.1.25 (Frobenius Reciprocity)

Let $H \leq G$ be groups, W a kG-module and V a kH-module. Then

$$\operatorname{Hom}_H(V, \operatorname{Res}_H^G W) \cong \operatorname{Hom}_G(\operatorname{Ind}_H^G V, W).$$

Frobenius Reciprocity is also known by the name of its more general form, the Nakayama relations [6, Proposition 2.8.3].

Theorem 4.1.26 (Mackey's Formula) [1, III, Lemma 7]
Let H, $K \leq G$ be groups and V be a kH-module. Then

$$\operatorname{Res}_K^G \operatorname{Ind}_H^G V \cong \bigoplus_{s \in K\backslash G/H} \operatorname{Ind}_{K\cap H^s}^K \operatorname{Res}_{K \cap H^s}^{H^s} V^s$$

where V^s denotes the *conjugate* of V by s, with action given by $gv \coloneqq g^s v$. Note here that we are abusing notation and viewing $K\backslash G/H$ as *representatives* of (K, H)–double cosets of G rather than the double cosets themselves. This is a common abuse of notation, as with G/H, and we shall do it without comment in future.

Finally, to close out the section, we introduce the notion of a *character*. When working in coprime characteristic (this is equivalent to the characteristic zero case), characters completely determine the structure of a module.

Definition 4.1.27
Given a representation $\varphi\colon G \to \mathrm{GL}_n(k)$ of G in characteristic 0, we define the (ordinary) *character* χ of φ to be the function $\chi\colon G \to k$ where $\chi(g)$ is given by the trace $\operatorname{Tr}\varphi(g)$.

The character of a representation φ is constant on conjugacy classes and in fact determines the representation φ up to isomorphism. A sum of characters corresponds to a direct sum of the corresponding G-modules and a product of characters is the character for the tensor product of the corresponding G-modules. Given two characters χ and ψ of G, we define their inner product $\langle \chi, \psi \rangle \coloneqq \frac{1}{|G|} \sum_{g\in G} \chi(g)\psi(g^{-1})$.

Theorem 4.1.28 (Ordinary character orthogonality relations) [22, 9.26]
Let G be a finite group and k a field of characteristic coprime to $|G|$. Let $\operatorname{Irr}_k G = \{\chi_i \mid i \in I\}$. Then $\langle \chi_i, \chi_j \rangle = \delta_{ij}$.

From these orthogonality relations, we can see that we may use the inner product of characters to identify which simple modules lie inside a module. For example, if we take a module M with character χ and take some other simple module with character ψ, then $\langle \chi, \psi \rangle \neq 0$ only if the module corresponding to ψ is a summand of M.

We will also introduce an analogue to these 'ordinary' characters in the case where the characteristic of k divides $|G|$ which can be used to determine a module's composition factors, though not the way in which they are stuck together.

4.2 Cohomology of groups

Here we give a very brief introduction to the cohomology of groups. Underlying all of this is a lot of category theory and several very deep results and concepts which are given only passing mentions, if any. If the reader is not already familiar with the area, they should consider consulting one of the following references: for a categorical approach to this the reader is referred to [45, 68]; whereas for algebraic or topological approaches they are instead referred to [7, 13].

We begin by introducing some language and notation from category theory. Then we give a few more properties of Hom before moving on to the definition of projective modules, Ext and thus group cohomology. We then use the properties of Hom to give properties of Ext before providing a few useful results for calculating or bounding group cohomology in various situations.

Definition 4.2.1 [68, Definition A.1.1]
We define a *category* $\mathcal{C}$ to be a collection $\operatorname{Obj}\mathcal{C}$ of *objects* with, for any objects A and B, a set $\operatorname{Hom}_{\mathcal{C}}(A, B)$ of structure-preserving *morphisms*. We further require an *identity morphism* $\operatorname{Id}_A \in \operatorname{Hom}_{\mathcal{C}}(A, A)$ for each A, and a *composition function* from $\operatorname{Hom}_{\mathcal{C}}(A, B) \times$

$\mathrm{Hom}_{\mathcal{C}}(B, C) \to \mathrm{Hom}_{\mathcal{C}}(A, C)$ for every A, B and C. The composition of morphisms must be associative, and for any $f\colon A \to B$, $\mathrm{Id}_B \circ f = f = f \circ \mathrm{Id}_A$.

One example of a category is that of finite groups. This is a category whose objects are all finite groups and whose morphisms are simply group homomorphisms between said groups. For this thesis, we will primarily be working in the category R-mod of (left) modules over a ring R (which will usually be kG for k a field and G a finite group) with $\mathrm{Hom}_{R\text{-mod}}(A, B) = \mathrm{Hom}_R(A, B)$ the set of R-module homomorphisms between A and B.

Definition 4.2.2 [68, A.2]

Given two categories $\mathcal{C}$ and $\mathcal{D}$, we define a *(covariant) functor* $F\colon \mathcal{C} \to \mathcal{D}$ to be a mapping which associates to each object A in $\mathcal{C}$ a corresponding object $F(A)$ in $\mathcal{D}$, and to each morphism $\varphi\colon A \to B$ in $\mathcal{C}$ a corresponding morphism $F(\varphi)\colon F(A) \to F(B)$ in $\mathcal{D}$ such that $F(\mathrm{Id}_A) = \mathrm{Id}_{F(A)}$. We also require that for any two morphisms φ, ψ, $F(\varphi\psi) = F(\varphi)F(\psi)$ and that the following diagram commutes.

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[d, "F"] & B \arrow[d, "F"] \\
FA \arrow[r, "F\varphi"] & FB
\end{tikzcd}$$

Many common methods of constructing objects can be realised as functors. In particular, we have that $\mathrm{Hom}_R(-, B)$, $\mathrm{Hom}_R(A, -)$ and $- \otimes_R B$ are all functors from R-mod to the category Ab of abelian groups (while $A \otimes_R -$ is a functor from the category of *right* R-modules to Ab). Here, the $-$ in the above expressions is the space taken by the argument of the functor, *e.g.* $(- \otimes_R B)(A) = A \otimes_R B$.

Definition 4.2.3

We say a functor $F\colon \mathcal{C} \to \mathcal{D}$ is *contravariant* if for each morphism $\varphi\colon A \to B$ of objects of $\mathcal{C}$ there is a corresponding morphism $F\varphi\colon FB \to FA$ in $\mathcal{D}$.

Informally, one can say that a contravariant functor ‘reverses the arrows’ in any diagram to which it is applied, while a covariant functor preserves their directions. The functors $\mathrm{Hom}_R(A, -)$, $A \otimes_R -$ and $- \otimes_R B$ are covariant for all rings R, R-modules A and B whilst $\mathrm{Hom}_R(-, B)$ is contravariant.

We now introduce a few useful properties of the Hom functor when dealing with modules over a ring.

Theorem 4.2.4 (Tensor-Hom Adjunction) [68, Proposition 2.6.3]
Let R and S be rings. The functors $- \otimes_R B$ and $\mathrm{Hom}_S(A, -)$ are *adjoint*, *i.e.* we have a *natural* isomorphism

$$\mathrm{Hom}_S(A \otimes_R B, C) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)).$$

Lemma 4.2.5
If V and W are k–vector spaces then we have an isomorphism

$$\mathrm{Hom}(V, W) \cong V^* \otimes W.$$

Proof: Using Lemma 4.1.6,

$$\mathrm{Hom}(V, W) \cong \mathrm{Hom}(V, \mathrm{Hom}(W^*, k))) \cong \mathrm{Hom}(V \otimes W^*, k) \cong (V \otimes W^*)^* \cong V^* \otimes W$$

as required. ■

Lemma 4.2.6
Let k be a field and V and W be k–vector spaces. Then

$$\mathrm{Hom}(V, W) \cong \mathrm{Hom}(W^*, V^*)$$

Proof: This can be proved in a more elementary fashion by showing that the map $^*\colon \mathrm{Hom}(V, W) \to \mathrm{Hom}(W^*, V^*)$ given by $\varphi^*\colon \theta \mapsto \theta \circ \varphi$, where $\varphi\colon V \to W$ and $\theta\colon W \to k$, is an isomorphism. However, we will instead prove this using Lemmas 4.1.6 and 4.2.5 as follows.

$$\mathrm{Hom}(V, W) \cong \mathrm{Hom}((V^*)^*, W) \cong V^* \otimes W \cong W \otimes V^* \cong \mathrm{Hom}(W^*, V^*). \qquad ■$$

Note with the above result we may extend this to group rings kG by simply taking G–fixed points afterwards, and in fact this result allows us to use Frobenius Reciprocity (Theorem 4.1.25) regardless of which side of the Hom contains the induction. More formally,

Corollary 4.2.7

Let $H \leq G$ be groups, W a kG-module and V a kH-module. Then

$$\operatorname{Hom}_H(\operatorname{Res}^G_H W, V) \cong \operatorname{Hom}_G(W, \operatorname{Ind}^G_H V).$$

Note that here, and indeed in future, $\operatorname{Hom}_G := \operatorname{Hom}_{kG}$ and if the subscript ring is omitted we assume that we are working over the base field.

Proof: By Frobenius Reciprocity (Theorem 4.1.25) we have that

$$\operatorname{Hom}_H(V, \operatorname{Res}^G_H W) \cong \operatorname{Hom}_G(\operatorname{Ind}^G_H V, W)$$

and thus using Lemma 4.2.6 we see that

$$\operatorname{Hom}_H((\operatorname{Res}^G_H W)^*, V^*) \cong \operatorname{Hom}_G(W^*, (\operatorname{Ind}^G_H V)^*).$$

Then $(\operatorname{Res}^G_H W)^* \cong \operatorname{Res}^G_H(W^*)$ and by Theorem 4.2.4 and Lemma 4.2.5

$$\begin{aligned}
(\operatorname{Ind}^G_H V)^* &:= \operatorname{Hom}(V \otimes_{kH} kG, k) \\
&\cong \operatorname{Hom}_H(kG, \operatorname{Hom}(V, k)) \\
&\cong (kG)^* \otimes_{kH} \operatorname{Hom}(V, k) \\
&\cong kG \otimes_{kH} V^* \\
&\cong V^* \otimes_{kH} kG \\
&\cong \operatorname{Ind}^G_H(V^*),
\end{aligned}$$

as required. ■

Corollary 4.2.8

Let G be a group, k be a field and V, W be kG-modules. Then we have an isomorphism

$$\mathrm{Hom}_G(V, W) \cong \mathrm{Hom}_G(k, V^* \otimes W).$$

Proof: Using Theorem 4.2.4 and Lemma 4.2.5

$$\begin{aligned} \mathrm{Hom}(V, W) &\cong \mathrm{Hom}(k \otimes V, W) \\ &\cong \mathrm{Hom}(k, \mathrm{Hom}(V, W)) \\ &\cong \mathrm{Hom}(k, V^* \otimes W) \end{aligned}$$

and using the fact that $\mathrm{Hom}_G(A, B) \cong \mathrm{Hom}(A, B)^G$ we are done. ■

With all these properties of Hom out of the way, we now need to introduce exact sequences. They may seem strange at first, but encoding collections of modules and maps as exact sequences is actually incredibly useful in a variety of areas and gives us a way to bound dimensions of any objects appearing in the sequence.

Definition 4.2.9

We say that a sequence

$$\dots \to M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \xrightarrow{\varphi_3} \dots$$

is *exact* if for each i we have that $\ker \varphi_i = \mathrm{Im}\, \varphi_{i-1}$. Sequences of the form

$$0 \to A \to B \to C \to 0$$

are called *short exact sequences* and exact sequences with infinitely many terms are usually called *long* exact sequences.

We will need the following lemma in Chapter 5, so we provide it here.

Lemma 4.2.10

Let G be a finite group and k a field. Let V be a kG-module and $0 \to A \to B \to C \to 0$ a short exact sequence of kG-modules. Then

$$0 \to V \otimes A \to V \otimes B \to V \otimes C \to 0$$

is also a short exact sequence of kG-modules.

Proof: This holds for vector spaces as they are *flat*. To see this, let $\iota\colon A \to B$ and $\pi\colon B \to C$ be the kG-module homomorphisms in the above short exact sequence. In particular, ι and π are linear maps. Then the linear maps $\mathrm{Id}_V \otimes \iota\colon V \otimes A \to V \otimes B$ and $\mathrm{Id}_V \otimes \pi\colon V \otimes B \to V \otimes C$ (where we use $f \otimes g$ to denote the function defined by $(f \otimes g)(v \otimes w) = f(v) \otimes g(w)$) give us the above short exact sequence as a sequence of vector spaces. It then remains only to show that these homomorphisms are also kG-module homomorphisms, but of course this is clear since the identity map is always a kG-module homomorphism and the maps ι and π with which we started were also homomorphisms of kG-modules. ■

Definition 4.2.11

Let A, B and C be R-modules. Then we say that the short exact sequence

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\varepsilon} C \to 0$$

splits or is *split* if $B \cong A \oplus C$ via an isomorphism φ such that $\varphi \circ \iota$ is the natural embedding of A into $A \oplus C$ and $\varepsilon \circ \varphi$ is the natural projection from $A \oplus C$ onto C.

Equivalently, by the splitting lemma [22, Proposition 2.3], there exists $f\colon B \to A$ such that $f \circ \iota = \mathrm{Id}_A$ or there exists $g\colon C \to B$ such that $\varepsilon \circ g = \mathrm{Id}_C$.

Another very useful notion is that of free and projective modules. In particular, projective modules are of great importance in the representation theory of finite groups and we shall see them used heavily towards the end of Section 5.3.

Definition 4.2.12

We say that an R-module F is *free* if it has a basis, *i.e.* there exists some subset $A \subseteq F$ such that every element of F may be expressed uniquely as a linear combination of elements of A. When R is a field, this coincides with the definition of a basis of a vector space and as such much of the terminology also carries over to the general setting unchanged.

Note that an R-module F is free if and only if it is a direct sum of copies of R viewed as an R-module.

The above definition is a nice easy way to define free modules. If we instead wished to define them in a more categorical sense, then an R-module F would be defined to be *free on a set* $S \subseteq F$ if, for any R-module M with a function $f \colon S \to M$, there exists a unique R-module homomorphism $\varphi \colon F \to M$ commuting with the natural inclusion $\iota \colon S \to F$ as in the below diagram.

$$\begin{tikzcd}
 & F \arrow[dl, "\varphi"'] \\
M & S \arrow[l, "f"] \arrow[u, "\iota"]
\end{tikzcd}$$

Definition 4.2.13

We say that an R-module P is *projective* if, whenever we have two R-modules M and N with a homomorphism $\theta \colon P \to M$ and a surjective homomorphism $\psi \colon N \to M$, there exists $\varphi \colon P \to N$ such that the following diagram (with exact row) commutes:

$$\begin{tikzcd}
 & P \arrow[dl, "\exists\varphi"'] \arrow[d, "\theta"] & \\
N \arrow[r, "\psi"] & M \arrow[r] & 0
\end{tikzcd}$$

One may obtain the definition of an *injective* module from this diagram by *dualising* (roughly speaking, reversing all of the arrows).

The following result shows that, at least for our purposes, it is sufficient to deal only with projective modules.

Theorem 4.2.14 [1, §6, Theorem 4]

Let G be a finite group and k a field. Then a kG-module is projective if and only if it is injective.

Moreover, the next result then immediately follows from Theorem 4.2.14 and the fact that the dual of a projective module is injective (by the contravariance of $\mathrm{Hom}(-, k)$).

Lemma 4.2.15

Let G be a finite group and k a field. Then the dual of a projective module is also projective.

We now give a few useful properties and generalisations of projective modules. In all of the following cases, there is a dual result which holds for injective modules which may generally be obtained by dualising the associated diagram. These results, however, will not be stated since we make far more use of projective modules than injective ones.

Lemma 4.2.16 [45, Theorem 4.7]

Let R be a ring and P an R-module. The following statements are equivalent.

i) The module P is projective;

ii) The functor $\mathrm{Hom}_R(P, -)$ is *exact*;

iii) Every short exact sequence of the form $0 \to A \to B \to P \to 0$ splits;

iv) There exists a free module F of which P is a direct summand;

v) Whenever P is a quotient of some R-module M, P must be a direct summand of M.

Lemma 4.2.17 [22, Corollary 19.4]

Let k be a field, G a group, M a kG-module and P a projective kG-module. Then $M \otimes P$ is projective.

Lemma 4.2.18

Let k be a field and $H \leq G$ be groups. Then if V is a projective kH-module and W a projective kG-module, both $\mathrm{Ind}_H^G V$ and $\mathrm{Res}_H^G W$ are projective.

Proof: By Lemma 4.2.16, since V and W are projective then V is a summand of $kH^{\oplus n}$ and W a summand of $kG^{\oplus m}$ for some m, $n \geq 1$. Then $\operatorname{Ind}_H^G V$ is a summand of $\operatorname{Ind}_H^G kH^{\oplus n} \cong kG^{\oplus n}$ and $\operatorname{Res}_H^G W$ is a summand of $\operatorname{Res}_H^G kG^{\oplus m} \cong kH^{\oplus m[G:H]}$ and so are both projective. ■

Definition 4.2.19

Given groups $H \leq G$ and a field k, we say that a kG-module V is *relatively H-projective* if the exact sequence

$$0 \to N \to M \to V \to 0$$

of kG-modules is split whenever the exact sequence

$$0 \to N_H \to M_H \to V_H \to 0$$

of kH-modules is split. If the same as above holds for fixed N rather than V then we say that N is *relatively H-injective.* Note that relatively 1-projective modules are simply projective and all kG-modules are relatively G-projective.

Relative projectivity may seem like a condition that might never be satisfied in some nontrivial way, but in fact it's controlled entirely by the Sylow p-subgroups. More formally, this is the following result.

Lemma 4.2.20 [1, §9, Theorem 2]

If $H \leq G$ contains a Sylow p-subgroup of G and $\operatorname{char} k = p$ then every kG-module is relatively H-projective.

In order to ease notation in the future, we have this quick definition.

Definition 4.2.21

We say that a subgroup $H \leq G$ is a *trivial intersection subgroup* if, for all $g \in G$, we have that $H \cap H^g = H$ or 1.

The next result is a special case of the famous Green Correspondence, which may be found in [1, §11, Theorem 1].

Lemma 4.2.22 [1, §10, Theorem 1]
Suppose that $R \in \operatorname{Syl}_r G$ is a trivial intersection subgroup and $N_G(R) \leq H \leq G$. Then there is a correspondence between non-projective indecomposable kH-modules and non-projective indecomposable kG-modules. If U and V are such a pair, then we have that $\operatorname{Ind}_H^G U = V \oplus P$ for some projective kG-module P and $V_H = U \oplus Q$ for some projective kH-module Q.

The Green Correspondence itself does not require the Sylow p-subgroups to be trivial intersection subgroups as we have above, but instead of having a correspondence up to projective modules we only know the modules up to some relatively Q-projective module for a particular p-subgroup Q.

Definition 4.2.23
Given an R-module M, we define a *projective resolution* to be a long exact sequence

$$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$$

where each P_i is projective. Dualising this, we get the definition of an *injective resolution.*

Definition 4.2.24
A *chain complex* $\boldsymbol{C}$ of R-modules is a family of R-modules $\{C_n\}_{n\in\mathbb{Z}}$ with R-module maps $d = d_i \colon C_i \to C_{i-1}$ such that $d \circ d = 0$. These maps are called *differentials* or *boundary homomorphisms.* We define the submodule of n-cycles of $\boldsymbol{C}$ to be $\mathrm{Z}_n(\boldsymbol{C}) \coloneqq \ker d_n$ and the n-boundaries to be $\mathrm{B}_n(\boldsymbol{C}) \coloneqq \operatorname{Im} d_{n+1}$. We define the n^{th} *homology module* of $\boldsymbol{C}$ to be the quotient $\mathrm{H}_n(\boldsymbol{C}) \coloneqq \mathrm{Z}_n(\boldsymbol{C}) / \mathrm{B}_n(\boldsymbol{C})$. Similarly we have a *cochain complex* $\boldsymbol{C}$ defined in the same way, except we index differently and take the differentials (coboundary maps) to be $\partial = \partial^i \colon C^i \to C^{i+1}$ such that $\partial \circ \partial = 0$. The n-cocycles are defined to be $\mathrm{Z}^n(\boldsymbol{C}) \coloneqq \ker \partial^n$ and the n-coboundaries are $\mathrm{B}^n(\boldsymbol{C}) \coloneqq \operatorname{Im} \partial^{i-1}$. As before, we define the n^{th} *cohomology module* to be the quotient $\mathrm{H}^n(\boldsymbol{C}) \coloneqq \mathrm{Z}^n(\boldsymbol{C}) / \mathrm{B}^n(\boldsymbol{C})$.

Definition 4.2.25

Let M be an R-module. Now take a projective resolution

$$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$$

of M, denoted $\boldsymbol{P}$, and apply $\operatorname{Hom}(-, N)$ for some R-module N to each term to obtain the sequence

$$0 \to \operatorname{Hom}(P_0, N) \to \operatorname{Hom}(P_1, N) \to \operatorname{Hom}(P_2, N) \to \ldots$$

which is no longer necessarily exact. We then treat this as a cochain complex $\boldsymbol{C} = \operatorname{Hom}(\boldsymbol{P}, N)$ with coboundary maps induced from those of the original resolution and define $\operatorname{Ext}^n_R(M, N) \coloneqq \mathrm{H}^n(\boldsymbol{C})$. When $R = kG$ is a group ring, then we just denote this by $\operatorname{Ext}^n_G(M, N)$ instead of $\operatorname{Ext}^n_{kG}(M, N)$. One may also obtain $\operatorname{Ext}^n_R(M, N)$ by taking an injective resolution of N and applying $\operatorname{Hom}(M, -)$ to this instead.

One can see that the kernel of the map $\operatorname{Hom}(P_0, N) \to \operatorname{Hom}(P_1, N)$ is just $\operatorname{Hom}(M, N)$ since $\operatorname{Hom}(-, N)$ is a *left-exact* functor. We thus have that $\operatorname{Ext}^0_R(M, N) = \operatorname{Hom}(M, N)$ for all rings R, R-modules M, N. There is also another functor, $\operatorname{Tor}^R_n(M, N)$, obtained through a similar process using tensor products instead of Hom, but we will not define this here.

Definition 4.2.26

Given a group G and a kG-module V, we define the n^{th} *cohomology group* $\mathrm{H}^n(G, V) \coloneqq \operatorname{Ext}^n_G(k, V)$, where k is regarded as the trivial kG-module. There is a corresponding definition for group homology using Tor, but we again omit this.

Group cohomology may be thought of as something of a generalisation of taking the fixed points of a G-module, as we have that $\mathrm{H}^0(G, V) \cong \operatorname{Hom}_G(k, V) \cong V^G$. There are also very strong ties to extension theory as the group $\operatorname{Ext}^n_R(A, B)$ in general is in 1–1 correspondence with what we call n-extensions of R-modules, which are exact sequences

$$0 \to B \to X_n \to \cdots \to X_1 \to A \to 0.$$

Setting $n = 1$ we obtain the usual definition of an extension of an object A by B, that is an exact sequence

$$0 \to B \to E \to A \to 0.$$

The classification of such extensions is an important problem and has been investigated by a great many people due to the fact that one may theoretically construct any module as a sequence of extensions by simple modules. The same is true of groups, hence the importance of the finite simple groups and their classification.

Due to this correspondence between Ext and extensions of modules, we can note that if $\operatorname{char} k$ is coprime to $|G|$ then every G-module is completely reducible. That is, every G-module splits completely into a direct sum of all of its simple submodules. As such, there is only one way to extend one G-module by another in coprime characteristic, namely by a direct sum. We thus have that if the characteristic is coprime and $n > 0$ then $\operatorname{Ext}^n_G(V, W) = 0$ for all G-modules V and W in this characteristic.

We now give a few properties of the Ext functor which allow the manipulation of its arguments in various ways. Since the definition of Ext is dependent on Hom, many of these properties are just direct extensions of the Hom versions given earlier on in this chapter.

Lemma 4.2.27

Let U, V and W be kG-modules for a finite group G. Then $\operatorname{Ext}^n_G(U, V \oplus W) \cong \operatorname{Ext}^n_G(U, V) \oplus \operatorname{Ext}^n_G(U, W)$ and $\operatorname{Ext}^n_G(U \oplus V, W) \cong \operatorname{Ext}^n_G(U, W) \oplus \operatorname{Ext}^n_G(V, W)$.

Proof: We prove the first isomorphism=. The proof for the second is identical. As in the definition of Ext, we take a projective resolution $\boldsymbol{P}$ of U and apply $\operatorname{Hom}_G(-, V \oplus W)$ to make a sequence $\operatorname{Hom}_G(\boldsymbol{P}, V \oplus W)$. We then apply Lemma 4.1.7 to see that $\operatorname{Hom}_G(\boldsymbol{P}, V \oplus W) \cong \operatorname{Hom}_G(\boldsymbol{P}, V) \oplus \operatorname{Hom}_G(\boldsymbol{P}, W)$ and take cohomology to obtain the desired result. ■

Lemma 4.2.28

Let V and W be kG-modules for a finite group G. Then

$$\mathrm{Ext}_G^n(V, W) \cong \mathrm{Ext}_G^n(W^*, V^*).$$

Proof: We proceed as in the definition of Ext: take a projective resolution $\boldsymbol{P}$ of V and apply $\mathrm{Hom}_G(-, W)$ to this to obtain a sequence $\mathrm{Hom}_G(\boldsymbol{P}, W)$. Now, apply Lemma 4.2.6 to get $\mathrm{Hom}_G(\boldsymbol{P}, W) \cong \mathrm{Hom}_G(W^*, \boldsymbol{P}^*)$ and since $\boldsymbol{P}^*$ is an injective resolution of V^*, taking cohomology of these sequences gives us the required result. ■

Lemma 4.2.29

Let V and W be kG-modules for a finite group G. Then

$$\mathrm{Ext}_G^n(V, W) \cong \mathrm{Ext}_G^n(k, V^* \otimes W) \cong \mathrm{H}^n(G, V^* \otimes W).$$

Proof: As in the proof of Lemma 4.2.28, take a projective resolution $\boldsymbol{P}$ of V and apply $\mathrm{Hom}_G(-, W)$ and Lemma 4.2.5 to get $\mathrm{Hom}_G(\boldsymbol{P}, W) \cong \mathrm{Hom}_G(k, \boldsymbol{P}^* \otimes W)$. Since $\boldsymbol{P}^* \otimes W$ is an injective (by Lemma 4.2.17 and Theorem 4.2.14) resolution of $V^* \otimes W$, taking cohomology of these sequences gives the required result. ■

We now give a series of useful results regarding cohomology. We start with some nice characterisations of the low-dimensional cohomology for a finite group G. We have already talked about cohomology and extensions of modules, and we talked a little about how $\mathrm{H}^1(G, V)$ parameterises complements in semidirect products. At the time, however, we had not actually defined H^1, so we will revisit this briefly here.

Let G be a finite group and V a kG-module afforded by a representation $\varphi\colon G \to \mathrm{GL}(V)$. Then, regarding V as an additive abelian group we may form the semidirect product $V \rtimes_\varphi G$ of V and G, where the action of G on V is the same as its module action. Then, in some sort of natural way (covered in [13, Chapter IV, §2]), each element of $\mathrm{H}^1(G, V)$ gives rise to a different conjugacy class of complements to V in $V \rtimes G$.

Next, we recall the definition of an extension of modules above. There is an identical concept for groups. Let G and N be groups. Then a *group extension* of G by N is an exact sequence

$$1 \to N \to E \to G \to 1$$

of groups, with the same notion of equivalence as for modules. We may simply regard such a group extension as a group E with $N \trianglelefteq E$ such that $E/N \cong G$. However, the manner in which N is embedded into E is important as nonequivalent extensions can give rise to isomorphic groups E. Notice that a semidirect product satisfies this property, as $N \trianglelefteq N \rtimes G$, and $(N \rtimes G)/N \cong G$, so semidirect products are in fact group extensions. Much as a direct sum of modules can always be formed and is a split extension of modules, the semidirect product of two groups can always be formed and is a split group extension. One can check that this matches with the definition of a split exact sequence, too.

Then, when N is abelian, we have that group extensions of G by N are in 1–1 correspondence with $\mathrm{H}^2(G, N)$ and one may find a treatment of this in [13, Chapter IV, §3]. The result is true in greater generality than this (see [31]), indeed for nonabelian N except under certain conditions on $\mathrm{H}^3(G, Z(N))$, such extensions are in 1–1 correspondence with $\mathrm{H}^2(G, Z(N))$.

From this it should be clear that we often care quite a lot about $\mathrm{H}^1(G, V)$ and $\mathrm{H}^2(G, V)$ for various choices of V, and when V is a trivial module then we have a nice way to determine these cohomology groups. It is sufficient to work only with the 1-dimensional trivial module, since cohomology commutes with direct sums by Lemma 4.2.27. This first result can be proven directly without too much trouble, but we will instead just note that it follows from Theorem 4.2.42 further on in this section.

Lemma 4.2.30

Let G be a finite group and k 1-dimensional the trivial kG-module. Then $\mathrm{H}^1(G, k) \cong \mathrm{Hom}_G(G/G', k)$, where $G' = [G, G]$ is the derived subgroup of G.

An important corollary of the above result is that if G is perfect, then $\mathrm{H}^1(G, k) = 0$

for any field k. Remaining in the setting of perfect groups, we also have the following.

Definition 4.2.31

Let G be a finite perfect group. Then the *Schur multiplier* of G is $\mathrm{H}^2(G, \mathbb{C}^*)$, where $\mathbb{C}^*$ here is not the dual space of $\mathbb{C}$ but its multiplicative group of units with trivial G-action.

The Schur multiplier can also be defined to be $\mathrm{H}_2(G, \mathbb{Z})$, where the action of G on $\mathbb{Z}$ is trivial. This fact, and the definition, can both be found in [36, Definition 5.1.6]. This next lemma is due to the Schur multiplier's role as a *universal central extension*.

Lemma 4.2.32

Let G be a finite perfect group and k the 1-dimensional trivial kG-module where k is a field of characteristic p. Then $\mathrm{H}^2(G, k)$ is the p-part of the *Schur multiplier* of G.

Next, we have Shapiro's Lemma. This generalises Frobenius Reciprocity (Theorem 4.1.25) to Ext.

Theorem 4.2.33 (Shapiro's Lemma) [6, Corollary 2.8.4]

Given groups $H \leq G$, a kH-module V and a kG-module W, we have

$$\mathrm{Ext}^n_H(V, W) \cong \mathrm{Ext}^n_G(\mathrm{Ind}^G_H V, W).$$

As with Frobenius Reciprocity, we do not need to worry about which side of the Ext contains the induction as one may prove the following corollary by proceeding as in the above proofs (Lemmas 4.2.27 to 4.2.29) — take a projective resolution of the first argument and apply Corollary 4.2.7 to every term before taking cohomology.

Corollary 4.2.34

Given groups $H \leq G$, a kH-module V and a kG-module W, we have

$$\mathrm{Ext}^n_H(W, V) \cong \mathrm{Ext}^n_G(W, \mathrm{Ind}^G_H V).$$

We will refer to both of the above results as 'Shapiro's Lemma' in future.

Next, we have a result which allows us to move between dimensions for group cohomology. In general, this is very useful as it allows the low-dimensional cohomology to tell us about the higher-dimensional terms which are usually far more difficult to calculate.

Theorem 4.2.35 (Long exact sequence in (group) cohomology) [13, 6.1 (ii')]
Let G be a group and $0 \to U \to W \to V \to 0$ a short exact sequence of G-modules. Then we have a long exact sequence

$$0 \to U^G \to W^G \to V^G \to \mathrm{H}^1(G,U) \to \mathrm{H}^1(G,W) \to \mathrm{H}^1(G,V) \to \mathrm{H}^2(G,U) \to \cdots .$$

The above theorem is true for the Ext functor in general (and indeed the statement is identical) but we shall most commonly use it in the above form and so that is the only one that will be given.

We now very quickly introduce spectral sequences in order to understand another very useful result. This will be a very brief introduction to what is a very complicated tool in homological algebra. The interested reader is referred to [68, Chapter 5] for a more thorough introduction with some examples.

Definition 4.2.36
Similar to the notion of a chain complex, we define a *double complex* to be a family $\{M_{ij}\}_{i,j\in\mathbb{Z}}$ which may be regarded as a lattice where each row and column is its own chain (or cochain) complex. There are differing conventions regarding the differentials of a double complex and whether they commute or anti-commute. In this case, we use the same convention as [68, Chapter 5] which is that the differentials commute. This choice is not important for what follows though, since we will not be composing any differentials. A double complex is called a *first quadrant* complex if $M_{ij} = 0$ whenever $i < 0$ or $j < 0$.

Definition 4.2.37
A first quadrant *cohomology spectral sequence* (starting at E_0) consists of the following:

i) A family $\{\mathrm{E}_r^{pq}\}$ of objects defined for all integers p, q, $r \geq 0$.

ii) Maps $d_r^{pq} \colon \mathrm{E}_r^{pq} \to \mathrm{E}_r^{p+r,q-r+1}$ which are differentials of the cochain complex consisting of the domains of each map.

iii) Isomorphisms between E_{r+1}^{pq} and the homology of E_r at the spot E_r^{pq}.

Definition 4.2.38

Given a spectral sequence $\{\mathrm{E}_r^{pq}\}$, we define $\mathrm{B}_\infty^{pq} \coloneqq \bigcup_{r=a}^\infty \mathrm{B}_r^{pq}$ and $\mathrm{Z}_\infty^{pq} \coloneqq \bigcap_{r=a}^\infty \mathrm{Z}_r^{pq}$. Given these terms, we then define $\mathrm{E}_\infty^{pq} \coloneqq \mathrm{Z}_\infty^{pq} \,/\, \mathrm{B}_\infty^{pq}$.

Definition 4.2.39

We say that a spectral sequence *approaches* or *abuts to* H if we have a filtration (sequence of submodules)

$$\ldots \subseteq F^{p+1}\,\mathrm{H}^n \subseteq F^p\,\mathrm{H}^n \subseteq \ldots \subseteq \mathrm{H}^n$$

such that $\bigcup F^p\,\mathrm{H}^n = \mathrm{H}^n$, $\bigcap F^p\,\mathrm{H}^n = 0$ for all n and we have isomorphisms $\mathrm{E}_\infty^{pq} \cong F^p\,\mathrm{H}^{p+q} \,/ F^{p+1}\,\mathrm{H}^{p+q}$ for all p and q. If this happens, we write $\mathrm{E}_2^{pq} \Rightarrow \mathrm{H}^{p+q}$.

With all the notation out of the way, here is the result that we wanted to give.

Theorem 4.2.40 (Hochschild–Serre spectral sequence) [68, 6.8.2]

Let G be a group, $N \trianglelefteq G$ and V be a G-module. Then we have a convergent spectral sequence

$$\mathrm{E}_2^{pq} = \mathrm{H}^p(G/N, \mathrm{H}^q(N, V)) \Rightarrow \mathrm{H}^{p+q}(G, V).$$

In particular, the Hochschild–Serre spectral sequence says that if we have a group G with $N \trianglelefteq G$, then for any kG-module V we have that $\mathrm{H}^n(G, V)$ is a subquotient (quotient of a submodule) of

$$\bigoplus_{p+q=n} \mathrm{H}^p(G/N, \mathrm{H}^q(N, V)).$$

We see this used in Lemma 5.2.2. The following exact sequence also comes as a corollary of the Hochschild–Serre spectral sequence.

Theorem 4.2.41 (Exact sequence of low-degree terms) [68, 6.8.3]

Given a group G with normal subgroup N and a G-module V, the Hochschild–Serre spectral sequence gives us an exact sequence of low-degree terms

$$0 \to \mathrm{H}^1(G/N, V^N) \to \mathrm{H}^1(G, V) \to \mathrm{H}^1(N, V)^{G/N} \to \mathrm{H}^2(G/N, V^N) \to \mathrm{H}^2(G, V).$$

Finally, we give a means to relate cohomology of trivial modules to their integral homology which is sometimes better known. One example of the use of this theorem is to determine the cohomology of the trivial module for dihedral groups under certain circumstances.

Theorem 4.2.42 (Universal Coefficient Theorem for cohomology) [45, Theorem 15.1] Let G be a group and let V be a kG-module with trivial G-action. Then $\mathrm{H}^n(G, V) \cong \mathrm{Ext}^1_{\mathbb{Z}}(\mathrm{H}_{n-1}(G, \mathbb{Z}), V) \oplus \mathrm{Hom}(\mathrm{H}_n(G, \mathbb{Z}), V)$, where H_n is the n^{th} *group homology* and $\mathbb{Z}$ denotes the set of integers with a trivial G-action.

Note that the Universal Coefficient Theorem can be used to prove Lemma 4.2.30, we require only the additional information that $\mathrm{H}_1(G, \mathbb{Z}) \cong G/G'$ which one may find as equation (4.2) in [45, Chapter VI, §4].

To close out the section, we also give the following technical definition and result which we shall make use of later on.

Definition 4.2.43

Two kG-modules V and W are said to be *quasi-equivalent* if one may be obtained as a twist of the other via some automorphism σ of G, *i.e.* $V \cong W^\sigma$.

Lemma 4.2.44

Suppose that two kG-modules V and W are quasi-equivalent with $V = W^\sigma$. Then $\mathrm{H}^n(G, V) \cong \mathrm{H}^n(G, W)$ for all n.

Proof: Suppose that we have some homomorphism of kG-modules $\varphi \colon A \to B$. Then one may obtain a twisted homomorphism $\varphi^\sigma \colon A^\sigma \to B^\sigma$ by leaving the underlying linear map unchanged (note $A^\sigma = A$ as vector spaces) and noting that $\varphi^\sigma(g \cdot_\sigma a) = \varphi^\sigma(g^\sigma a) = g^\sigma \varphi^\sigma(a) = g \cdot_\sigma \varphi^\sigma(a)$, where $\cdot_\sigma$ denotes the twisted G-action on a kG-module. Then it is clear from this that such a twist preserves kernels and images of homomorphisms, and so in particular will preserve group cohomology as required. ■

4.3 Blocks and modular representation theory

Some of the work in Chapter 5 makes use of some facts from the theory of blocks in modular representation theory. We shall thus quickly introduce some of the relevant theory and results to avoid clutter later on. This section will introduce blocks quickly and discuss properties of Ext and projective modules in blocks. We will also introduce a structure known as the *Brauer graph*, which is a very useful tool when the Sylow p-subgroups of G are cyclic or dihedral (or the *defect group* of a block is cyclic or dihedral). We will primarily treat blocks as ideals of kG as in [1], but another common approach is to treat blocks by dealing with their *block idempotents* as in [33].

The main reference for this section is [33], though [22, 23, 24] are also good references and [1] is a great introductory reference for blocks and Brauer trees but is quick and short on detail by design. For a more modern reference, [21] also gives a very good introduction to this area.

For what follows, we let k be an algebraically closed field of characteristic p and G be a finite group.

We begin with a brief introduction to blocks themselves. We mainly just use blocks as a means of partitioning the irreducible kG-modules, but Proposition 4.3.5 in particular is very useful to us and in fact makes it clear that this partition into blocks is in some way meaningful.

Definition 4.3.1

The group algebra kG can be decomposed uniquely as a direct sum of minimal two-sided ideals $kG = B_1 \oplus B_2 \oplus \ldots \oplus B_n$. These ideals B_i are called the *blocks* of kG or *p-blocks* of G. Multiplication between these ideals is also such that if $x_i \in B_i$, $x_j \in B_j$ and $i \neq j$, then $x_i x_j \in B_i \cap B_j = 0$.

Definition 4.3.2

Let V be a kG-module. Then if $B_iV = V$ and $B_jV = 0$ for all $j \neq i$, we say that V *lies in* the block B_i.

Proposition 4.3.3 [1, §13, Proposition 2]

If V is a G-module, then V, like kG, has a unique decomposition $V = V_1 \oplus \ldots \oplus V_n$ where V_i lies in the block B_i of kG.

From this result it is clear that an irreducible module V does lie in a block, and it may only lie in one. Next, we introduce projective covers. These modules are particularly special as they are in one to one correspondence with irreducible modules, and are intricately tied to their extension theory.

Lemma 4.3.4 [1, §5 Theorem 3]

Given an irreducible kG-module V, there is a unique projective indecomposable module $\mathcal{P}(V)$ such that $\operatorname{head}\mathcal{P}(V) \cong \operatorname{soc}\mathcal{P}(V) \cong V$ called the *projective cover* of V. Similarly, for any indecomposable module M, there is a unique (up to isomorphism) projective cover $\mathcal{P}(M) \cong \mathcal{P}(\operatorname{head} M)$.

In an arbitrary algebra, there is no reason to suspect that the above statements hold. For example, the fact that $\mathcal{P}(V)$ has simple, isomorphic socle and head in fact follows from the fact that the group algebra kG is a *symmetric algebra* (see [22, §9A]). In other classes of algebras this need not be the case. It is not even guaranteed in general that one can take projective covers of modules over an arbitrary ring.

Proposition 4.3.5 [1, §13, Proposition 3]

Let V, $W \in \operatorname{Irr}_k G$. Then the following are equivalent:

i) V and W lie in the same block.

ii) There is a chain of irreducible kG-modules $V = V_1, V_2, \ldots, V_n = W$, such that V_i and V_{i+1} are composition factors of an indecomposable projective module.

iii) There is a chain of irreducible kG-modules $V = W_1, W_2, \ldots, W_n = W$, such that W_i and W_{i+1} coincide, or there is a non-split extension of one by the other.

Conditions i) and iii) of the above proposition essentially say that two modules V, $W \in \operatorname{Irr}_k G$ lie in the same block if and only if $\operatorname{Ext}^n_G(V, W) \neq 0$ for some $n \in \mathbb{N}_0$.

As said earlier, projective covers are in some way tied to the extension theory of modules. We will now give some results to show exactly how strong these ties are, but first we require some notation to simplify things a little.

Definition 4.3.6 [21, p. 46]

Let V be a kG-module. Then we define the *Heller translate* or *syzygy* ΩV of V to be the kernel of $\mathcal{P}(V) \twoheadrightarrow V$. So ΩV is a module such that

$$0 \to \Omega V \to \mathcal{P}(V) \to V \to 0$$

is exact. We then define $\Omega^{i+1} V := \Omega(\Omega^i V)$.

The Heller translate has a variety of nice properties. The most useful for our purposes will be the following two lemmas.

Lemma 4.3.7 [44, Proposition 1]

The Heller translate Ω is a permutation on the set of isomorphism classes of non-projective indecomposable kG-modules.

In [44], the above result is stated for 'weak-Frobenius algebras,' algebras in which the classes of injective and projective modules coincide. Group algebras for finite groups are one such example of these algebras. The above result is a consequence of the fact [44, 1.1] that $\Omega(A \oplus B) \cong \Omega A \oplus \Omega B$ for any two modules A and B, and tells us that the Heller translate of an indecomposable module is itself indecomposable.

Lemma 4.3.8 [2, Lemma 1]

Let U, V be kG-modules with V irreducible. Then, for any $n \geq 0$,

$$\operatorname{Ext}^n_G(U, V) \cong \operatorname{Hom}_G(\Omega^n U, V).$$

Proof: This follows from the long exact sequence in Ext corresponding to the short exact sequence $0 \to \Omega V \to \mathcal{P}(V) \to V \to 0$, coupled with the fact that $\mathrm{Ext}_G^n(\mathcal{P}(U), V) = 0$ for all $n \geq 1$ and that $\mathrm{Hom}_G(\mathcal{P}(U), V) \cong \mathrm{Hom}_G(U, V)$. To see this latter statement, we note that we have an embedding $\mathrm{Hom}_G(U, V) \hookrightarrow \mathrm{Hom}_G(\mathcal{P}(U), V)$ via composition with the projective covering map. This embedding is surjective since if we have any $\theta\colon \mathcal{P}(U) \twoheadrightarrow V$ then this must factor through $\mathcal{P}(V)$. We must then have that the image of $\Omega(U)$ must be all of $\mathcal{P}(V)$ to be able to map onto a simple module, but then θ induces a map on $\mathcal{P}(U)/\Omega(U) \cong U$ and so θ comes from some map in $\mathrm{Hom}_G(U, V)$. ■

Definition 4.3.9

A module V is said to be *periodic* of *period* n if $\Omega^n V \cong V$ for some $n \geq 1$.

From Lemma 4.3.8 we see that one can determine $\dim \mathrm{Ext}_G^n(U, V)$ by looking at the multiplicity of the irreducible module V in the head of $\Omega^n U$, so $\mathrm{H}^n(G, V)$ is simply the multiplicity of V in $\mathrm{head}\, \Omega^n k$. Similarly, by noting that $\mathrm{H}^n(G, V) \cong \mathrm{Ext}_G^n(V^*, k) \cong \mathrm{Hom}_G(\Omega^n V^*, k)$ (Lemma 4.2.28 and Lemma 4.3.8), we can see that $\mathrm{H}^n(G, V)$ is also the multiplicity of k in $\mathrm{head}\, \Omega^n V^*$. Combining this with the definition above, we see that periodic modules have periodic cohomology as the heads of the $\Omega^n V$ will repeat in the same way.

We now introduce a modular version of characters, known as *Brauer characters.* There are a lot of incredibly technical results and definitions that should be given in any proper treatment of this subject which we are going to try our best to avoid in the name of simplicity. One such proper treatment may be found in [22, §16–18]. We begin with the (rather technical) definition of a *p-modular system.* While we do not make explicit use of p-modular systems outside of this section it is important to use them here in order to ensure that the results given are actually correct. An example of a p-modular system is $(\mathbb{Q}_p, \mathbb{Z}_p, \mathbb{F}_p)$, where $\mathbb{Z}_p$ is the p-adic integers and $\mathbb{Q}_p$ its field of fractions, and one may obtain p-modular splitting systems for any extensions of $\mathbb{F}_p$. This is discussed in more detail at the beginning of Chapter 3 of [49].

Definition 4.3.10 [22, §16]

Let p be a prime. A p-modular system (K, R, k) is a *discrete valuation ring* R with field of fractions K, a maximal ideal $\mathfrak{p} = \pi R$ (where $\pi \in R$ is prime) and residue class field $k = R/\mathfrak{p}$ of characteristic p. In general it is not required for K to be a field of characteristic zero.

Definition 4.3.11

An element $g \in G$ is said to be *p-regular* if its order is not divisible by p. We denote by $G_{p'}$ the set of p-regular elements of G.

Definition 4.3.12 [22, Definition 17.4]

Let G be a finite group of exponent $m = p^a m'$ with m' coprime to the prime p and let (K, R, k) be a p-modular system for G with K a field of characteristic 0 containing an m^{th} root of unity. Let $\omega \in K$ be an m'^{th} root of unity and $f\colon R \to k$ be the quotient map by the unique maximal ideal of R. Then f is an isomorphism from $\langle \omega \rangle$ onto the group $\langle \overline{\omega} \rangle$ of m'^{th}roots of unity in k.

Let $g \in G$ be a p-regular element and V be a kG-module afforded by a representation φ. Then all eigenvalues of $\varphi(g)$ are m'^{th} roots of unity and thus lie in $\langle \overline{\omega} \rangle$. Denote the eigenvalues of $\varphi(g)$ by $\{\xi_1, \dots, \xi_n\}$ and define $\lambda(g) \coloneqq \sum_{i=1}^{n} f^{-1}(\xi_i)$. Then λ realises the trace of $\varphi(g)$ as an element of K. We define the *Brauer character* of V to be this function $\lambda\colon G_{p'} \to K$. As with ordinary characters, we have the same notion of inner products, this time taken over p-regular elements, $\langle \chi, \psi \rangle \coloneqq \frac{1}{|G|} \sum_{g \in G_{p'}} \chi(g)\psi(g^{-1})$.

We may sometimes abuse notation and refer to these as k-characters for brevity.

Mechanically, Brauer characters behave in a very similar way to ordinary characters. However, defining them rigorously is much more difficult and even the above definition is obfuscating a fair few details. The curious or sceptical reader should consult [22, §17] for more detail along with proofs that we can actually do the things done above.

The following theorem is actually a combination of a variety of results from [22, §18].

Theorem 4.3.13

Let G be a finite group and k a field. Then two kG-modules have the same Brauer characters if and only if they have the same composition factors.

Note that Brauer characters in characteristic zero are the same as ordinary characters, and composition factors over fields of characteristic zero are sufficient to determine a module up to isomorphism.

Definition 4.3.14

Let G be a finite group, (K, R, k) a p-modular system for G with k a field of characteristic $p > 0$ and K a characteristic zero splitting field for G. Denote by $\{\chi_i\}_{i=1}^{n}$ and $\{\psi_j\}_{j=1}^{m}$ the irreducible k- and K-characters, respectively. Then we define the *decomposition number* d_{ij} to be the multiplicity of χ_i as a summand of ψ_j. We also define the matrix $D = (d_{ij})$ to be the *decomposition matrix* of G over k, where each row indicates the number of occurrences of each irreducible kG-module in a given KG-module.

Definition 4.3.15 [22, Definition 18.4]

Let G be a finite group and (K, R, k) be a p-modular system for G. Let $\operatorname{Irr}_k G = \{V_i \mid i \in \{1, \ldots, n\}\}$ and let P_i be the projective cover of the simple module V_i. Let $c_i(M)$ denote the multiplicity of the simple module V_i as a composition factor of M, then we define the *Cartan matrix* $C = (c_{ij})$ by $c_{ij} = c_i(P_j)$.

So we see from this that the Cartan matrix tells us exactly what the irreducible constituents of the projective indecomposable modules for G are. Note that the definition we give above is in fact the transpose of the version given in [22], but by the following result that does not matter.

Lemma 4.3.16 [22, Corollary 18.10]

Let G be a finite group and (K, R, k) be a p-modular system for G with decomposition matrix D and Cartan matrix C. Then C is symmetric, and $C = DD^T$.

The reason for introducing all of the above machinery is to state the equivalent to Theorem 4.1.28 for Brauer characters, which will allow us to use Brauer characters to determine the composition factors of modules in characteristic p dividing $|G|$. This is Theorem 18.23 in [22].

Theorem 4.3.17 (Brauer character orthogonality relations)
Let (K, R, k) be a p-modular system for a finite group G with Cartan matrix C. Let $\operatorname{Irr}_k G = \{V_i \mid i \in \{1, \ldots, n\}\}$ and let P_i be the projective cover of the simple module V_i. Let χ_i be the Brauer character of V_i and ψ_i be the Brauer character of P_i. Then we have the following relations.

i) $\frac{1}{|G|}\langle \chi_i, \psi_j \rangle = \delta_{ij}$,

ii) $\frac{1}{|G|}\langle \chi_i, \chi_j \rangle = \gamma_{ij}$, where $C^{-1} = (\gamma_{ij})$,

iii) $\frac{1}{|G|}\langle \psi_i, \psi_j \rangle = c_{ij}$.

One of the goals of this section is to introduce *Brauer graphs*, but to talk about them properly and know when they are useful we need to be able to talk about *defect groups*. Defect groups are a particular kind of p-subgroup associated to a p-block which in some way determines how complicated this block can be, though to date it is in fact not known exactly what the defect group determines about the block. There are several famous conjectures on this subject, including Brauer's Height Zero conjecture [50, Conjecture 2.6] and Donovan's conjecture [30, Conjecture 1.1]. We of course begin with a definition. There are several equivalent definitions of defect groups, and many of these are very complicated. We have decided to take the definition used in [1], thus we must first introduce the notion of a *vertex*.

Theorem 4.3.18
Let U be an indecomposable kG-module. Then there exists a p-subgroup Q of G, unique up to G-conjugacy, such that U is relatively H-projective for $H \leq G$ if and only if Q is conjugate to a subgroup of H. We call Q a *vertex* of U.

For this next result, we must regard kG as a $k(G \times G)$-module via the action $(g, h)a = gah^{-1}$. Then $k(G \times G)$-submodules of kG are in fact its two-sided ideals and thus kG splits as a direct sum of its blocks as a $k(G \times G)$-module. With this in mind, we have the following result.

Theorem 4.3.19

As a $k(G \times G)$-module, a block B of kG has a vertex of the form δD where $\delta\colon G \to G \times G$ is the diagonal map $\delta(g) = (g, g)$ and $D \leq G$ is a p-subgroup. This p-subgroup D is called a *defect group* for B and is unique up to conjugacy.

We also have that any module contained in B has a vertex appearing as a subgroup of the defect group of the block.

Definition 4.3.20

A block B is said to be of *defect* d if its defect group has order p^d. We say that a block is of *maximal defect* if its defect groups are Sylow p-subgroups of G.

One can actually read off the defect of a block from the character table. As in [21, Definition 2.3.1], we see that if a Sylow p-subgroup of G has order p^a then the defect of a block B is the least d such that $p^{a-d} \mid \chi(1)$ for all ordinary characters χ lying in B. This equivalent definition also makes it clear that the principal block (the block containing k) must have maximal defect.

Lemma 4.3.21

A block B of defect zero contains only one irreducible module, which is also projective.

Proof: Such a block has the trivial group as a defect group, and thus any module in this block is relatively 1-projective, *i.e.* projective. Then by Theorem 4.2.14 and Lemma 4.2.16 there are no indecomposable modules containing this projective module apart from itself and thus there cannot be any other modules in this block by Proposition 4.3.5. ■

There is another important property of defect groups which one can see by reading the (again equivalent) definition of defect groups in [47, p. 278], which is the following.

Lemma 4.3.22

Let B be a p-block of a finite group G. Then a defect group D of B is a Sylow p-subgroup of $C_G(x)$ for some p-regular $x \in G$.

We do not say what the x in the previous lemma actually is, but it is useful to know the above as this alone is enough to impose some restrictions on defect groups in some circumstances. For example, it can be used to show that certain blocks of non-maximal defect must have cyclic defect groups, which would be very useful due to the following results.

Theorem 4.3.23 [1, §21, Lemma 5]

Let B be a p-block of a finite group G. If the defect groups of B are cyclic, then $\dim \operatorname{Hom}_G(V, W) \leq 1$ for all indecomposable V and irreducible W in B.

Note that in the language of [1], a simple module is 'short' and so the above result is indeed the same as cited. Note that this is all we require for a general result for all n, as follows.

Theorem 4.3.24

Let B be a p-block of a finite group G. If the defect groups of B are cyclic, then $\dim \operatorname{Ext}^n_G(V, W) \leq 1$ for all indecomposable V and irreducible W in B and all n.

Proof: Recall from Lemma 4.3.8 that $\operatorname{Ext}^n_G(V, W) \cong \operatorname{Hom}_G(\Omega^n V, W)$, and by Theorem 4.3.23 if $\Omega^n V$ is indecomposable then the result follows. But, by Lemma 4.3.7, the Heller translate takes indecomposable modules to indecomposable modules, so we are done. ■

Note that by duality of the above using Lemma 4.2.28 we have the same result for V irreducible and W indecomposable, as the duals of indecomposable and irreducible modules remain indecomposable and irreducible, respectively. A useful corollary of this result that we make use of later is the following.

Proposition 4.3.25

Let B be a block containing a single non-projective simple module V with a cyclic defect group. Then $\operatorname{Ext}^n_G(V, V) \cong k$ for all n.

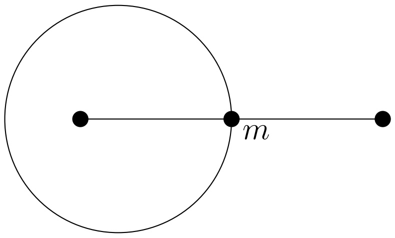
Proof: Since V is not projective and is the only module in its block, we must have that V lies in the head of $\Omega^n V$ for all n. Thus $\mathrm{Ext}^n_G(V,V) \neq 0$ for all n. But since the defect group of B is cyclic, we know that $\dim \mathrm{Ext}^n_G(V,V) \leq 1$ for all n and so we are done. ■

We now introduce a concept which is incredibly useful when the Sylow subgroups of G are known to be either cyclic or dihedral, the Brauer graph. This is a graph which encodes the structure of the projective modules and all indecomposable modules for algebras known as *Brauer graph algebras.* A good introduction to these algebras in a more general setting may be found in [5] or in [6, 4.18]. For our purposes, we just need to know that when the Sylow p-subgroups of G are cyclic or dihedral then kG is a Brauer graph algebra.

In the case where the Sylow subgroups are cyclic we instead have a Brauer *tree* due to Brauer [9], generalised by Thompson [67] and completed by Dade [25]. A relatively friendly introduction may be found in [1, p. V]. One can also find a good introduction in [21, Chapter 5].

Definition 4.3.26 [6, Definition 4.18.1]
A *Brauer graph* is a finite undirected graph (here we allow loops and multiple edges) where to each vertex v we assign a cyclic ordering of its incident edges and a *multiplicity* $m_v \geq 1$. If this graph is a tree with at most one *exceptional vertex* v with $m_v > 1$ then it is called a *Brauer tree.*

Brauer graphs are, of course, best explained through examples. Thus, below is an example of a Brauer graph which we shall see again later.



An algebra A is said to be a *Brauer graph algebra* (for some Brauer graph Γ) if there is a one to one correspondence between edges e_j of Γ and irreducible A-modules V_j such that $\mathcal{P}(V_j)$ may be described as follows: $\mathrm{head}\,\mathcal{P}(V_j) \cong \mathrm{soc}\,\mathcal{P}(V_j) \cong V_j$ and the heart

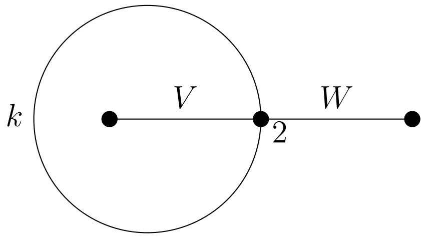
$\mathcal{H}(\mathcal{P}(V_j))$ (see Definition 4.1.20) is a direct sum of two uniserial modules corresponding to taking anticlockwise walks around the vertices u_j, w_j at either end of the edge e_j. So, our projective cover looks like this:

$$\begin{array}{cc} & V_j \\ \mathcal{P}(V_j): & U_j \oplus W_j \\ & V_j \end{array}$$

where U_j and W_j are uniserial corresponding to vertices u_j and w_j. To describe the structure of these modules, suppose that the multiplicity of u_j is m and the edges incident at u_j after e_j are (in order) $M_1, \ldots, M_k$. Then the composition factors of U_j will be, starting at the head and working down to the socle:

$$M_1,\ M_2,\ \ldots,\ M_k,\ \boldsymbol{V_j},\ M_1,\ \ldots,\ M_k,\ \boldsymbol{V_j},\ \ldots,\ M_k,$$

where V_j appears $m-1$ times and each M_i appears m times. So, if we take the example above with $m = 2$ (then this is the Brauer graph of the principal block of $\mathrm{PSL}_2(13)$ in characteristic 2, amongst others), we get the below graph.



Then our projective modules for this block (highlighting full cycles around the vertex with a bold module) are

$$
\begin{array}{ccc}
 & V & \\
 & & k \\
 & & W \\
 & & k \\
0 & \oplus & \boldsymbol{V} \\
 & & k \\
 & & W \\
 & & k \\
 & V &
\end{array}
\qquad\qquad
\begin{array}{ccc}
 & W & \\
k & & \\
V & & \\
k & & \\
\boldsymbol{W} & \oplus & 0 \\
k & & \\
V & & \\
k & & \\
 & W &
\end{array}
\qquad\qquad
\begin{array}{ccc}
 & k & \\
V & & W \\
k & & k \\
W & & V \\
\boldsymbol{k} & \oplus & \boldsymbol{k} \\
V & & W \\
k & & k \\
W & & V \\
 & k &
\end{array}
$$

where the left (resp. right) column is the uniserial module corresponding to the left (resp. right) vertex, and a zero column corresponds to a vertex with no other incident edges and multiplicity 1. So $\mathcal{P}(k)$ is such that $\operatorname{head}\mathcal{P}(k) \cong \operatorname{soc}\mathcal{P}(k) \cong k$ and $\mathcal{H}\,\mathcal{P}(k)$ is a direct sum of two uniserial modules with the indicated composition factors.

CHAPTER 5

HIGHER GROUP COHOMOLOGY

5.1 Introduction

Group cohomology is intricately tied with the extension theory of finite groups. If N is an abelian group with fixed action of another group G on N by automorphisms, then $\mathrm{H}^1(G, N)$ parameterises the conjugacy classes of complements to N in $N \rtimes G$, and $|\mathrm{H}^2(G, N)|$ is the number of equivalence classes of extensions of G by N. The first cohomology group $\mathrm{H}^1(G, N)$ is also linked to generating sets for groups and their modules [4, 38], and $\mathrm{H}^2(G, V)$ for V an irreducible G-module gives information about the number of relations needed in profinite presentations of G [39, 57].

Due to these various applications, it is natural to want to bound the cohomology of some group G and some G-module V, and in particular it is natural to start with the case where G is a finite simple group and V is an irreducible kG-module for k an algebraically closed field of characteristic r. The cohomology in this case has been investigated extensively, though still remarkably little is known. In 1986, Guralnick conjectured [37] that if V is a faithful irreducible kG-module then there exists some absolute constant c such that $\dim \mathrm{H}^1(G, V) \leq c$, and originally it was conjectured that $c = 2$. Since then, examples were found in 2003 and 2008 for groups of Lie type $G(p^n)$ in defining characteristic $(r = p)$ [11, 66] with 3-dimensional cohomology, and more recently in 2020 Lübeck [56, Theorem 4.7] found an irreducible module V in defining characteristic for $\mathrm{E}_6(q)$ with

$\dim \mathrm{H}^1(G, V) = 3537142$. Thus the Guralnick conjecture is likely false, but it is still important to study the behaviour of group cohomology.

Let G be a rank e finite group of Lie type, defined in characteristic p with Weyl group W. If $r \neq p$, the current best bounds for irreducible V are $\dim \mathrm{H}^1(G, V) \leq |W|^{\frac{1}{2}} + e - 1$ from [42] in 2019 (an improvement on [40] from 2011) with strong bounds when the B–fixed points $V^B = 0$ for B a Borel subgroup of G. In defining characteristic $r = p$, we instead have [63] from 2013 stating that, for any irreducible kG-module V,

$$\dim \mathrm{H}^1(G, V) \leq \max \left\{ \frac{z_p^{\frac{h^3}{6}+1} - 1}{z_p - 1}, \frac{1}{2}(h^2(3h-3)^3)^{\frac{h^2}{2}} \right\},$$

where $z_p = \lfloor \frac{h^3}{6}(1 + \log_p(h-1)) \rfloor$ and h is the Coxeter number of G. Referring to the above module for $\mathrm{E}_6(q)$, this bound amounts to roughly 10^{703} compared to the 10^6 that is the largest known example.

For second cohomology and higher, less is known but for example in [39] from 2007 it is shown that $\dim \mathrm{H}^2(G, V) \leq \frac{35}{2} \dim V$ for G any finite quasisimple group and V any G-module, or $\frac{37}{2} \dim V$ for G any finite group and V a faithful, irreducible G-module.

In some cases, we also know that a bound of a particular type exists, but we have no explicit expressions for them. For a finite group of Lie type in its defining characteristic, Cline, Parshall and Scott [19] showed that $\dim \mathrm{H}^1(G, V)$ (for V irreducible) is bounded by some constant dependent only upon the rank of G. More generally, Guralnick and Tiep [42] have showed that if G is a finite group and V an irreducible kG-module then $\dim \mathrm{H}^1(G, V)$ is bounded by some constant dependent only on r and the *sectional r-rank* of G (maximum r-rank of an elementary abelian section — quotient of a subgroup — of G). Very recently, the as-yet unpublished sequel to this work [43] generalises the result to show that, for arbitrary D and irreducible V, $\dim \mathrm{Ext}^n_G(D, V)$ is bounded by a constant dependent only on the sectional r-rank of G, $\dim D$ and n.

In this chapter, we generalise Theorem 2.2 from [40] to a larger class of groups, higher cohomology and reducible modules, giving

Theorem 1

Let G be a finite group and let $k = \overline{k}$ be a field of characteristic r. Suppose $H \leq G$ is such that $O_{r'}(H) = O^r(H)$ and suppose that $\mathcal{L}$ is the permutation module $\operatorname{Ind}_H^G k$ of G acting on cosets of H. Suppose V is a kG-module with $V^H = 0$. Then $\mathrm{H}^n(G, V) \cong \operatorname{Ext}_G^{n-1}(V^*, \mathcal{L}/\mathcal{L}^G)$.

In fact, $\mathcal{L}^G \cong k$ and so in future we shall talk about $\mathcal{L}/k$ rather than $\mathcal{L}/\mathcal{L}^G$. Of particular note is that when $n = 1$ one may then determine $\dim \mathrm{H}^1(G, V)$ by investigating the structure of $\operatorname{soc} \mathcal{L}/k$. More formally,

Corollary 1

Retain the above notation. Then if $V^H = 0$, $\mathrm{H}^1(G, V) \cong \operatorname{Hom}_G(V^*, \mathcal{L}/k)$.

The hypothesis $O_{r'}(H) = O^r(H)$ is vital to our arguments for the above theorem. It stems from Lemma 5.2.1, which one can see to be a generalisation of [40, Lemma 2.1] by taking B to be a Borel subgroup of a group of Lie type G and r to be any prime not equal to the defining characteristic of G. Using this lemma, specifically the statement that $V^H = 0$ if and only if $V^{O_{r'}(H)} = 0$, we can show that in fact $\mathrm{H}^n(H, V) = 0$ for all n when $V^H = 0$ and then a long exact sequence in Ext implies the main theorem. The use of this hypothesis permits the extension of [40, Theorem 2.2] from being a statement about irreducible modules for groups of Lie type to being a statement about any module for an arbitrary finite group.

If one wanted to obtain results similar to those of Guralnick–Tiep for all groups of Lie type, one might wish to use the common technique of an induction on the rank of G. In order to take this approach, we would need to know what the cohomology of the rank 1 groups of Lie type is. In any case, it is interesting to know what happens for the small rank groups of Lie type as this may be of use in forming conjectures or performing calculations in higher ranks. As such, the bulk of this chapter is made up of a complete, explicit determination of all cross characteristic cohomology for irreducible modules for $G \in \{\mathrm{PSL}_2(q), \mathrm{Sz}(q)\}$ for all prime powers q for which G is defined. As a corollary to this, we also obtain a complete determination of $\operatorname{Ext}_G^i(V, W)$ for all irreducible V, W.

5.2 General results

Notation

For the remainder of this chapter, let $k = \overline{k}$ be a field of characteristic r, G be a finite group and, unless otherwise specified, Hom shall denote Hom_G.

We begin by generalising a lemma and theorem from [40], whilst also providing a shorter proof of the original theorem as a special case.

Lemma 5.2.1

Suppose H is a finite group, k a field of characteristic r and V a kH-module. If $O_{r'}(H) = O^r(H) =: A$ then the following statements are equivalent.

i) $V^H \neq 0$,

ii) H has trivial composition factors on V,

iii) $V^A \neq 0$,

iv) $(V^*)^H \neq 0$.

Proof: That i) implies ii) is clear, and that ii) implies iii) follows from the fact that $r \nmid |A|$. To see that iii) implies i), we note that the r-group H/A acts on V^A so we have that $(V^A)^{H/A} \neq 0$ and so $V^H \neq 0$. Thus i)–iii) are equivalent. It remains only to show that iv) is equivalent to the rest; to see this, note that using i) $\iff$ iii) we have

$$V^H \neq 0 \iff V^A \neq 0 \iff (V^*)^A \neq 0 \iff (V^*)^H \neq 0,$$

as required. ■

Lemma 5.2.2

Suppose H is a finite group such that $O_{r'}(H) = O^r(H)$. Then if V is a kH-module with $V^H = 0$, we have that $\mathrm{H}^n(H, V) = 0$ for all n.

Proof: Let $A := O_{r'}(H) = O^r(H)$. Note that we have an exact sequence of groups $1 \to A \to H \to H/A \to 1$, and thus from the Hochschild–Serre spectral sequence (Theorem 4.2.40) we can see that $\mathrm{H}^n(H,V)$ is a subquotient (quotient of a submodule) of

$$\bigoplus_{i+j=n} \mathrm{H}^i(H/A, \mathrm{H}^j(A,V)) \cong \mathrm{H}^n(H/A, V^A) \oplus \bigoplus_{\substack{i+j=n \\ i\neq n}} \mathrm{H}^i(H/A, \mathrm{H}^j(A,V)).$$

We may then note that $V^H = 0$ so $V^A = 0$ by Lemma 5.2.1 and $\mathrm{H}^j(A,V) = 0$ for all $j > 1$ since $r \nmid |A|$, thus the above module is 0 and so $\mathrm{H}^n(H,V) = 0$ for all n. ■

Theorem 5.2.3

Suppose G is a finite group, $k = \overline{k}$ a field of characteristic r, V a kG-module and $H \leq G$ is such that $O_{r'}(H) = O^r(H) =: A$. Let $\mathcal{L}$ be the permutation module of G acting on cosets of H. Then if $V^H = 0$, we have that $\dim \mathrm{H}^n(G,V) = \dim \mathrm{Ext}_G^{n-1}(V^*, \mathcal{L}/\mathcal{L}^G) = \dim \mathrm{Ext}_G^{n-1}(V^*, \mathcal{L}/k)$.

Proof: We first note that we have the exact sequence

$$0 \to k \to \mathcal{L} \to \mathcal{L}/k \to 0$$

and we may apply $\mathrm{Hom}_G(V^*, -)$ to this to obtain a long exact sequence with segments of the form

$$\cdots \to \mathrm{Ext}_G^{n-1}(V^*, \mathcal{L}) \to \mathrm{Ext}_G^{n-1}(V^*, \mathcal{L}/k) \to \mathrm{Ext}_G^{n}(V^*, k) \to \mathrm{Ext}_G^{n}(V^*, \mathcal{L}) \to \cdots$$

which, using Shapiro's Lemma (Theorem 4.2.33) and Lemma 4.2.28, reduces to

$$\cdots \to \mathrm{H}^{n-1}(H,V) \to \mathrm{Ext}_G^{n-1}(V^*, \mathcal{L}/k) \to \mathrm{H}^n(G,V) \to \mathrm{H}^n(H,V) \to \cdots . \qquad (\star)$$

Then, applying Lemma 5.2.2 it follows that $\mathrm{H}^n(G,V) \cong \mathrm{Ext}_G^{n-1}(V^*, \mathcal{L}/k)$ as required. ■

An important observation is that when $n = 1$ we get

Corollary 5.2.4

Retain all of the above notation. If $V^H = 0$, then $\dim \mathrm{H}^1(G, V) = \dim \mathrm{Hom}(V^*, \mathcal{L}/k)$.

In particular, when V is irreducible we have that $\dim \mathrm{H}^1(G, V)$ is the multiplicity of V^* in the socle of $\mathcal{L}/k$. This also gives the following corollaries.

Corollary 5.2.5

Retain notation as above. Let V be an irreducible kG-module which is not a composition factor of $\mathcal{L}$. Then $\mathrm{H}^1(G, V) = 0$.

Or, for a consequence of this corollary that can simply be read off from character degrees, we have the following.

Corollary 5.2.6

Let G be a finite group and V an irreducible kG-module. If $\dim V > [G : H]$ for some $H \leq G$ such that $O_{r'}(H) = O^r(H)$, then $\mathrm{H}^1(G, V) = 0$.

One example where the previous corollaries are useful is for $G = S_p$, the symmetric group of prime degree p. G has a subgroup S_{p-1} of index p, and $O_{p'}(S_{p-1}) = O^p(S_{p-1}) = S_{p-1}$ as it has p'-order. Then by the previous corollary we can say that $\mathrm{H}^1(G, V) = 0$ for any irreducible V of dimension greater than p, or using Corollary 5.2.5 we can say that $\mathrm{H}^1(G, V) = 0$ for all V apart from the unique nontrivial constituent of the permutation module on S_{p-1}. Note that $\mathrm{H}^1(G, k) = 0$ by Lemma 4.2.30 since G is perfect.

A major application of these results is to the area of finite groups of Lie type in cross characteristic, since any Borel subgroup of such groups satisfies the conditions on H of all above theorems. This then gives the following theorem as a special case.

Theorem 5.2.7 [40, Theorem 2.2]

Let G be a finite group of Lie type defined in characteristic $p \neq r$ and let $B \leq G$ be a Borel subgroup. For an irreducible kG-module V with $V^B = 0$ we have that $\dim \mathrm{H}^1(G, V)$ is the multiplicity of V^* in $\mathrm{soc}\, \mathcal{L}/k$. Alternatively, $\dim \mathrm{H}^1(G, V) = \dim \mathrm{Hom}(V^*, \mathcal{L}/k)$.

Though our result also generalises to $\mathrm{H}^n(G, V) \cong \mathrm{Ext}_G^{n-1}(V^*, \mathcal{L}/k)$ and does not require that V be irreducible.

Notation

For the remainder of the section, assume that G is a finite group of order divisible by r containing a subgroup H such that $O_{r'}(H) = O^r(H)$.

We can use Theorem 5.2.3 repeatedly to obtain $\mathrm{H}^n(G, V)$ as the first cohomology of some tensor product of modules. To do this, take a projective resolution $\boldsymbol{P}$ of V^*

$$\cdots \to P_2 \to P_1 \to P_0 \to V^* \to 0$$

and then apply $\mathrm{Hom}_G(-, \mathcal{L}/k)$ to this to obtain

$$0 \to \mathrm{Hom}_G(P_0, \mathcal{L}/k) \to \mathrm{Hom}_G(P_1, \mathcal{L}/k) \to \dots$$

then from Corollary 4.2.8 we see that this is the same as

$$0 \to \mathrm{Hom}_G(k, P_0^* \otimes \mathcal{L}/k) \to \mathrm{Hom}_G(k, P_1^* \otimes \mathcal{L}/k) \to \dots.$$

Now, taking the cohomology of the cochain complexes $\mathrm{Hom}_G(\boldsymbol{P}, \mathcal{L}/k)$ and $\mathrm{Hom}_G(k, \boldsymbol{P}^* \otimes \mathcal{L}/k)$ from the previous two expressions therefore gives $\mathrm{Ext}^n_G(V^*, \mathcal{L}/k) \cong \mathrm{H}^n(G, V \otimes \mathcal{L}/k)$. Thus if enough can be understood about such tensor products, we could obtain another avenue by which to attack higher cohomology. Further, the following result is immediate from ($\star$).

Proposition 5.2.8

Suppose $r \nmid |H|$. Then

$$\dim H^1(G, V) = \dim \mathrm{Hom}(V^*, \mathcal{L}/k) - \dim V^H$$

and

$$\mathrm{H}^n(G, V) \cong \mathrm{Ext}^{n-1}_G(V^*, \mathcal{L}/k) \cong \mathrm{H}^{n-1}(G, V \otimes \mathcal{L}/k)$$

for any $n \geq 2$.

An important note here is that this retrieves the main result for higher cohomology without requiring that $V^H = 0$, and gives an easy calculation to determine $\mathrm{H}^1(G, V)$ when $V^H \neq 0$.

Often, it is far easier to determine Hom between modules than it is to determine Ext^n_G. As such, we repeatedly apply Proposition 5.2.8 to obtain the following result which does not require explicit calculation of Ext.

Proposition 5.2.9

Suppose $r \nmid |H|$. Then

$$\dim \mathrm{H}^2(G, V) = \dim \mathrm{Hom}_G(V^*, (\mathcal{L}/k)^{\otimes 2}) - \dim \mathrm{Hom}_H(V^*, \mathcal{L}/k).$$

Proof: Applying Proposition 5.2.8 to $\mathrm{H}^2(G, V)$, then again to $\mathrm{H}^1(G, V \otimes \mathcal{L}/k)$ gives

$$\begin{aligned}
\dim \mathrm{H}^2(G, V) &= \dim \mathrm{H}^1(G, V \otimes \mathcal{L}/k) \\
&= \dim \mathrm{Hom}_G((V \otimes \mathcal{L}/k)^*, \mathcal{L}/k) - \dim(V \otimes \mathcal{L}/k)^H \\
&= \dim \mathrm{Hom}_G(V^*, (\mathcal{L}/k)^{\otimes 2}) - \dim \mathrm{Hom}_H(k, V \otimes \mathcal{L}/k) \\
&= \dim \mathrm{Hom}_G(V^*, (\mathcal{L}/k)^{\otimes 2}) - \dim \mathrm{Hom}_H(V^*, \mathcal{L}/k)
\end{aligned}$$

and the result follows. ■

The above result is much more in the spirit of Theorem 5.2.7, as it reduces the study of $\mathrm{H}^2(G, V)$ for any V to the study of the structure of fixed modules $(\mathcal{L}/k)^{\otimes 2}$ and $\mathcal{L}/k$. Note in the above that if we also have $V^H = 0$ then we may replace $\dim \mathrm{Hom}_H(V^*, \mathcal{L}/k)$ by $\dim \mathrm{Hom}_H(\mathcal{L}, V) = \sum_{g \in H\backslash G/H} \dim V^{H \cap H^g}$ using Mackey's Formula (Theorem 4.1.26). Thus for example when $p \neq r$ in the case of $G = G(p^n)$ a group of Lie type and $H = B$ a Borel subgroup, it is easy to understand what $B \cap B^g$ is and if one knows enough about the action of root subgroups on V then one may reduce the bound given by $\dim \mathrm{Hom}_G(V^*, (\mathcal{L}/k)^{\otimes 2})$ significantly. Further, if enough is known about the structure of $(\mathcal{L}/k)^{\otimes 2}$ then we can get a bound on $\mathrm{H}^2(G, V)$, and studying the structure of $\mathcal{L}$ and V as

H-modules can be used to reduce this bound. A very similar method generalises this to all n with increasing tensor powers of $\mathcal{L}/k$.

One could attempt to obtain a bound for $\mathrm{H}^2(G, V)$ by noting that $\dim \mathrm{H}^1(G, V \otimes \mathcal{L}/k)$ is at most the number of composition factors of $V \otimes \mathcal{L}/k$ with nonzero cohomology. However, even in the case of $\mathrm{PSL}_2(q)$ this would give bounds of approximately $2 \dim V$ (by using the structure of $\operatorname{soc} \mathcal{L}$ from §4 of [40] and the minimum dimensions of irreducible modules of groups of Lie type from [41]), which ends up being far worse than the bounds obtained in [39] and of course far worse than the true values obtained in the remainder of this chapter. That being said, it is possible to use the results of [40, 42] to slightly improve some of the bounds for $\mathrm{SL}_3(q)$ and $\mathrm{SL}_4(q)$ in [39] by carefully reading the proofs and inserting the improved bounds for $\mathrm{H}^1(G, V)$ wherever possible.

5.3 Cohomology of $\mathrm{PSL}_2(q)$

A common technique for proving results about finite groups of Lie type is induction on the rank of G, and such an approach may be suitable in this case. Even if such an approach proved unsuitable, it is interesting to investigate the cohomology of the rank 1 groups in detail as this can assist with forming conjectures or performing calculations in higher rank groups and the rank 1 groups are still of independent interest. We begin with $\mathrm{PSL}_2(q)$ for $q = p^n$ a prime power.

We completely determine the cohomology of all irreducible kG-modules V, for $k = \overline{k}$ a field of characteristic $r \neq p$ when $G = \mathrm{PSL}_2(q)$. For this, we need to know what the irreducible modules for $\mathrm{PSL}_2(q)$ are. We therefore reproduce the character tables for $\mathrm{PSL}_2(q)$ below for convenience. There are three cases to consider, $q \equiv 1 \mod 4$, $q \equiv 3 \mod 4$ and q even. The odd cases may be found in [29, §38] and the even case, along with decomposition numbers for all cases, can be found in [14]. We begin with the case where $q \equiv 1 \mod 4$. In all of the tables below, γ and δ are distinct elements of order p, and α and β are elements of maximum order dividing $q-1$ and $q+1$, respectively. Also, ρ and

σ are primitive $|\alpha|^{\text{th}}$ and $|\beta|^{\text{th}}$ roots of unity in $\mathbb{C}$, respectively.

In the first table, $q \equiv 1 \mod 4$ and $i \leq \frac{1}{4}(q-5)$, and $j,\ l,\ m \leq \frac{1}{4}(q-1)$ are positive integers.

In the second table, $q \equiv 3 \mod 4$ and $i,\ j,\ l \leq \frac{1}{4}(q-3)$, and $m \leq \frac{1}{4}(q+1)$ are positive integers.

Finally, for the last table, q is even and $i,\ l \leq \frac{q}{2}-1$ and $j,\ m \leq \frac{q}{2}$ are positive integers.

The structure of a Borel subgroup B of G, and the permutation module $\mathcal{L} := \operatorname{Ind}_B^G k$, will be important for this section, so we give a little bit of information about B before we begin. As discussed in Section 2.3, G has a split BN-pair and so $B \cong Q \rtimes T$ where $Q \in \operatorname{Syl}_p G$ and $T \cong C_{\frac{1}{2}(q-1)}$ is a maximal torus lying in B. Without loss of generality we let $B = \langle \alpha, \gamma \rangle$ be the image in G of the upper triangular matrices, $T = \langle \alpha \rangle$ be the image of the diagonal matrices and Q be the image of the upper unitriangular matrices.

We will need to use Mackey's Formula (Theorem 4.1.26) with $H = K = B$ in what follows, so we will describe a partition of G into (B, B)–double coset representatives. Since $N_G(T)/C_G(T) = N_G(T)/T \cong C_2$, again since G has a split BN-pair, we have that $G = B1B \cup B\tau B$ for any $\tau \in N_G(T) \setminus T$ and so $\{1, \tau\}$ is a complete set of (B, B)–double coset representatives for G. Again without loss of generality we may take τ to be the image in G of the matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and from this it is clear to see that $B \cap B^\tau = T$.

We also need some understanding of how the irreducible kG-modules are constructed. Some of these modules are obtained from a Borel subgroup, so we also need to know a little bit about the representation theory of B. In particular, we want to know about the 1-dimensional kB-modules. These 1-dimensional representations of B are simply homomorphisms from B into the group of units of k. However, this is an abelian group and thus (for $q > 3$) $B' = [B, B] = Q$ must lie in the kernel of any such representation. As such, 1-dimensional representations of B correspond precisely to irreducible representations of its abelianisation $B/B' \cong T$ and in fact are just irreducible kT-modules with trivial actions of Q imposed upon them (this process is often called *inflation*).

Naturally, the character tables only give us a complete answer when the characteristic

	1	γ	δ	α^l	β^m
1	1	1	1	1	1
ξ_1	$\frac{1}{2}(q+1)$	$\frac{1}{2}(1+\sqrt{q})$	$\frac{1}{2}(1-\sqrt{q})$	$(-1)^l$	0
ξ_2	$\frac{1}{2}(q+1)$	$\frac{1}{2}(1-\sqrt{q})$	$\frac{1}{2}(1+\sqrt{q})$	$(-1)^l$	0
θ_j	$q-1$	-1	-1	0	$-(\sigma^{jm}+\sigma^{-jm})$
φ	q	0	0	1	-1
χ_i	$q+1$	1	1	$\rho^{il}+\rho^{-il}$	0

Table 5.1: Character table for $\mathrm{PSL}_2(q)$, $q \equiv 1 \mod 4$.

	1	γ	δ	α^l	β^m
1	1	1	1	1	1
η_1	$\frac{1}{2}(q-1)$	$\frac{1}{2}(\sqrt{-q}-1)$	$-\frac{1}{2}(1+\sqrt{-q})$	0	$(-1)^{m+1}$
η_2	$\frac{1}{2}(q-1)$	$-\frac{1}{2}(1+\sqrt{-q})$	$\frac{1}{2}(\sqrt{-q}-1)$	0	$(-1)^{m+1}$
θ_j	$q-1$	-1	-1	0	$-(\sigma^{jm}+\sigma^{-jm})$
φ	q	0	0	1	-1
χ_i	$q+1$	1	1	$\rho^{il}+\rho^{-il}$	0

Table 5.2: Character table for $\mathrm{PSL}_2(q)$, $q \equiv 3 \mod 4$.

	1	γ	α^l	β^m
1	1	1	1	1
θ_j	$q-1$	-1	0	$-(\sigma^{jm}+\sigma^{-jm})$
φ	q	0	1	-1
χ_i	$q+1$	1	$\rho^{il}+\rho^{-il}$	0

Table 5.3: Character table for $\mathrm{PSL}_2(q)$, q even.

of k is coprime to $|G|$ and so we shall briefly discuss how the above characters behave upon descent to the modular case. The specific decomposition of the ordinary characters into Brauer characters depends upon whether r divides $q-1$, $q+1$ or both (*i.e.* $r=2$) and we treat each of these cases individually when needed. However, there are some pieces of information that remain similar or the same across all cross characteristic cases and so we outline these before we begin.

In particular, the list of character degrees for G does not change too much and we can in fact give consistent notation for the irreducible kG-modules for remainder of this section. To find the construction of the irreducible characters in characteristic zero, see [29, §38] and combine with [14, I–VI, VIII] for an elementary description of the irreducible characters in the modular case. A thorough discussion of this (with lots of heavy machinery) for $\mathrm{SL}_2(q)$ may also be found in [8, Chapter 9] and then the irreducible representations of $\mathrm{PSL}_2(q)$ are those which have $Z(\mathrm{SL}_2(q))$ in their kernels. First, we let k be an algebraically closed field of characteristic $r \nmid q$, and as usual we shall use k to denote the 1-dimensional trivial kG-module or its restriction to some subgroup.

Now, fix a maximal torus in a Borel subgroup $T = \langle \alpha \rangle \leq B = \langle \alpha, \gamma \rangle \leq G$. We wish to obtain a family of irreducible kG-modules by inducing them from 1-dimensional kB-modules and for this it is sufficient to consider only the $N_G(T) \cong D_{q-1}$–conjugacy classes of such modules. To see this, recall that 1-dimensional kB-modules are essentially just irreducible kT-modules (so $N_G(T)$ acts on them) and irreducible representations of an abelian group correspond to its elements (in this case, if $T = \langle \alpha \rangle$ then for each i we may obtain a representation $\varphi_{\alpha^i} \colon \alpha \mapsto \sigma^i$ for $\sigma \in k$ an $|T|^{\mathrm{th}}$ root of unity). Then since α and α^{-1} are conjugate in $N_G(T)$, the corresponding kT-modules are also conjugate in $N_G(T)$ (and thus in G). As such, their inflations to B are isomorphic when induced from B to G.

Let $\{k = X_1, X_2, \ldots, X_a\}$ be a set of representatives of $N_G(T)$ conjugacy classes of 1-dimensional irreducible kT-modules, inflated to B, where a depends on q and r. We have three possibilities for $\mathrm{Ind}_B^G X_i$. If $i = 1$, then $\mathcal{L} \coloneqq \mathrm{Ind}_B^G X_1 = \mathrm{Ind}_B^G k$ has dimension $q+1$ and contains at most two nontrivial irreducible constituents, though the precise structure of this module varies on a case by case basis. The shape of $\mathcal{L}$ is described in the section 'Rank one groups' in [40] and we shall present this information again later on when necessary. If $r \neq 2$, $\mathcal{L}$ has a unique nontrivial irreducible constituent which we shall denote by V for the remainder of this section. Note that we do not give $\dim V$ here as this also depends on the characteristic r. When $r = 2$ then we have two nontrivial irreducible constituents of $\mathcal{L}$, each of dimension $\frac{1}{2}(q-1)$, and without loss of generality we shall denote these by V and W.

For $i > 1$, X_i is nontrivial and we have two possible structures: either $\operatorname{Ind}_B^G X_i$ is irreducible or it is not. Except for one case when $q \equiv 1 \mod 4$, $\operatorname{Ind}_B^G X_i =: M_i$ is irreducible of dimension $q+1$. When $q \equiv 1 \mod 4$, T contains an involution which is therefore normalised by the action of $N_G(T) \cong D_{q-1}$. We choose notation so that, when $q \equiv 1 \mod 4$, X_a is the irreducible kB-module corresponding to this involution. Then $\operatorname{Ind}_B^G X_a =: M_a$ has two distinct irreducible constituents of dimension $\frac{1}{2}(q+1)$ which we shall denote M_{a1} and M_{a2}.

More mysteriously, yet still somewhat similarly, G has modules of dimensions dividing $q-1$ which are obtained as constituents of nontrivial modules induced from a Singer cycle, S (subgroup of order $\frac{1}{(q+1,2)}(q+1)$, or index $q(q-1)$). Let $\{N_1, \dots, N_b\}$ denote the modules obtained in this way up to $N_G(S)$-conjugacy (see [29, §38, Steps 6, 7]), where again b depends on q and r. As with the modules M_i, except for $q \equiv 3 \mod 4$, all of these modules are irreducible of dimension $q-1$. When $q \equiv 3 \mod 4$, we choose notation so that N_b is the kG-module corresponding to the involution in S. Then N_b is not irreducible but has two distinct irreducible constituents of dimension $\frac{1}{2}(q-1)$ which we shall denote N_{b1} and N_{b2}.

We also use the following decomposition of kB-modules.

Lemma 5.3.1

Let $B = Q \rtimes T$ as before. Then as a kB-module, $kQ \cong k \oplus P_1 \oplus P_2$ for q odd and $k \oplus P_3$ for q even where the P_i are projective irreducible kB-modules. Further, if Y is a kB-module, we have a decomposition $Y = Y^Q \oplus P$ where P is a semisimple projective kB-module.

Proof: Let $Y \in \operatorname{Irr}_k Q$ be nontrivial. Then since Q is abelian, $\dim Y = 1$. Then by Lemma 4.1.24, $\dim \operatorname{Ind}_Q^B Y = [B : Q] = |T| = \frac{1}{(q-1,2)}(q-1)$ and $\operatorname{Ind}_Q^B Y$ is projective by Lemma 4.2.18.

We now show that $\operatorname{Ind}_Q^B Y$ is irreducible. Note that T acts on the set of irreducible kQ-modules. In particular, for each $x \in Q$ there is a unique character χ_x of Q and for $t \in T$ we have $t \colon \chi_x \mapsto \chi_{x^t}$ under its action on Q. The orbits of this action thus correspond to conjugacy classes in the action of T on Q, of which there are 3 for q odd and 2 for q even. One conjugacy class contains only the identity in either case, and the remainder is made up of orbits of length $|T|$.

Since Y is nontrivial, the orbit of Y under T has length $\frac{1}{(q-1,2)}(q-1) = |T| = \dim \operatorname{Ind}_Q^B Y$ and so $\operatorname{Ind}_Q^B Y$ is an irreducible kB-module. As a result, we see that $kQ \cong k \oplus P_1 \oplus P_2$ as a kB-module for q odd and $kQ \cong k \oplus P_3$ for q even, as required. ■

We will also frequently use the following consequence of Frobenius Reciprocity (Theorem 4.1.25).

Lemma 5.3.2

Let Y be an irreducible kG-module. Then $Y^B \neq 0$ precisely when Y embeds in $\operatorname{head} \mathcal{L}$, where $\mathcal{L} := \operatorname{Ind}_B^G k$.

Proof: First, recall that $\dim Y^B = \dim \operatorname{Hom}_B(k, Y)$. Then by Frobenius Reciprocity, $\operatorname{Hom}_B(k, Y) \cong \operatorname{Hom}_G(\mathcal{L}, Y)$ and the latter is nonzero precisely when Y lies in the head of $\mathcal{L}$. ■

Lemma 5.3.2 is particularly helpful because we know precisely which modules lie in $\operatorname{head} \mathcal{L}$. In particular, in two of the three cases we are about to consider, this is only the trivial module.

Before we split our considerations into three cases, we first prove the below result which holds in two of them.

Proposition 5.3.3

Suppose that $r \nmid \frac{1}{2}(q+1)$. Then the modules N_i are projective for all i, as are N_{b1} and N_{b2}.

Proof: We first note that N_i is relatively B-projective. If $r > 2$ then this is because B contains a Sylow r-subgroup of G. Otherwise, by [14, VIII(a)], N_i lies in a block of non-maximal defect. Since a defect group of the block in which N lies is the Sylow 2-subgroup of the centraliser of some 2-regular element by Lemma 4.3.22 and is not equal to a whole Sylow 2-subgroup of G, one such group must lie in T. Then since a vertex of N_i must lie in a defect group of its block, by Theorem 4.3.18 we must have that N_i is relatively T-projective and thus relatively B-projective.

Suppose that the restriction $(N_i)_B$ is anything other than $P_i \oplus P_j$ (or P_3 if q is even) in the notation of Lemma 5.3.1 for some i, j. Then in particular, some non-projective irreducible B-module X_j must embed in $(N_i)_B$, so $\operatorname{Hom}_B(X_j, N_i) \neq 0$ and thus $\operatorname{Hom}_G(\operatorname{Ind}_B^G X_j, N_i) \neq 0$. This is impossible since $\operatorname{Ind}_B^G X_j = M_j$ and N_i have no irreducible constituents in common. Thus $(N_i)_B$ is projective, and since N_i is relatively B-projective (since B contains a vertex for N_i) we have that N_i must be a projective G-module. The same holds for N_{b1} and N_{b2} using only one of P_1 or P_2 in place of $P_i \oplus P_j$ (note N_{b1} and N_{b2} may only exist for odd q and $r \neq 2$). ■

Investigating the cohomology of $G := \mathrm{PSL}_2(q)$ splits naturally into three separate cases: $r = 2$, or r is odd and $r \mid q - 1$ or r is odd and $r \mid q + 1$. We shall consider the case where $2 \neq r \mid q - 1$ first.

Case 1: r odd and $r \mid q - 1$

We continue assuming that B is a Borel subgroup of G. Then B contains a Sylow r-subgroup of G and consequently all kG-modules are relatively B-projective by Lemma 4.2.20. For a description of the notation used for the irreducible kG-modules we refer the reader to the discussion on page 106. In this case, from [40, Rank 1 groups] we have that $\mathcal{L} \cong k \oplus V$. By Lemma 5.3.2, the only modules Y with $Y^B \neq 0$ are those appearing in head $\mathcal{L} \cong k \oplus V$.

To see how the ordinary characters decompose in this case, one should consult cases I, III and V in [14]. We now elaborate further on the irreducible kG-modules in this particular case.

Let $n_{r'}$ denote the r'-part of n. That is, $n_{r'}$ is an integer such that $n = n_{r'}r^m$ where $r \nmid n_{r'}$. Then since T is cyclic, it may be written as a direct product of a cyclic r-group and some group of r' order. As such, in characteristic r, $|\mathrm{Irr}_k\, T| = |T|_{r'}$ since the irreducible kT-modules are simply inflations of irreducible modules for its cyclic r' direct factor. When $|T|$ is even, so $q \equiv 1 \mod 4$, T contains an involution which is conjugate to itself under the action of $N_G(T)$. Thus, when $q \equiv 1 \mod 4$ we have $a = \frac{1}{2}|T|_{r'} + 1$ and otherwise $a = \frac{1}{2}(|T|_{r'} - 1) + 1$. Since r does not divide $|S|$, this is the same as in characteristic zero and so $b = \frac{1}{2}|S| = \frac{1}{4}(q+1)$ when $q \equiv 3 \mod 4$ and $b = \frac{1}{2}(|S| - 1)$ otherwise.

We begin with a quick lemma.

Lemma 5.3.4

Let G, B and k be as above and Y and Z be kG-modules. Then if $\mathrm{Ext}^1_B(Y, Z) = 0$, $\mathrm{Ext}^1_G(Y, Z) = 0$. In particular, for any kG-module Y, if $\mathrm{H}^1(B, Y) = 0$ then $\mathrm{H}^1(G, Y) = 0$.

Proof: Note that if we have an exact sequence of kG-modules

$$0 \to Z \to E \to Y \to 0$$

for some E, this then restricts down to an exact sequence of kB-modules

$$0 \to Z_B \to E_B \to Y_B \to 0.$$

If $\mathrm{Ext}^1_B(Y, Z) = 0$ then the latter sequence must split. Then since Y is relatively B-projective by Lemma 4.2.20, we have that the former sequence also splits by definition of relative projectivity and so $\mathrm{Ext}^1_G(Y, Z) = 0$. The result then follows since $\mathrm{H}^1(G, Z) = \mathrm{Ext}^1_G(k, Z)$. ■

Proposition 5.3.5

Let $1 < i \leq a$. Then $\mathrm{H}^n(G, M_i) = 0$ for all n.

This follows from Lemma 5.2.2 and Shapiro's Lemma (Corollary 4.2.34) as $O_{r'}(B) =$

$O^r(B)$ and $M_i^B = 0$ by Lemma 5.3.2, but we would like to use arguments relating to the structure of G to prove it instead. This is done through the following lemmas.

Lemma 5.3.6

Let H be a finite group and k a field of characteristic r. Let Y be any kH-module and let $A := O_{r'}(H)$. Then $\mathrm{H}^1(H, Y) \cong \mathrm{H}^1(H/A, Y^A)$.

Proof: Using the exact sequence of low-degree terms from the Hochschild–Serre spectral sequence (Theorem 4.2.41), we see

$$0 \to \mathrm{H}^1(H/A, Y^A) \to \mathrm{H}^1(H, Y) \to \mathrm{H}^1(A, Y)^{H/A} \to \cdots,$$

and $\mathrm{H}^1(A, Y) = 0$ due to coprime action. This yields the required isomorphism. ■

This is now all we need to prove the above result.

Proof of Proposition 5.3.5. Recall that $M_i = \mathrm{Ind}_B^G X_i$ is irreducible when i is neither 1 nor a (and the latter case is irreducible for $q \not\equiv 1 \mod 4$). We will consider $i = 1$ in a later result, so for the following suppose that $1 < i \leq a$. We begin by proving that $\mathrm{H}^2(G, M_i) = 0$.

We have an exact sequence

$$0 \to M_i \to M_i \otimes \mathcal{L} \to M_i \otimes \mathcal{L}/k \to 0$$

by Lemma 4.2.10 which gives rise to a corresponding long exact sequence in cohomology

$$0 \to M_i^A \to (M_i \otimes \mathcal{L})^A \to (M_i \otimes \mathcal{L}/k)^A \to \mathrm{H}^1(A, M_i) \to \cdots.$$

The action of $A = O_{r'}(B)$ is coprime, so $\mathrm{H}^1(A, M_i) = 0$ and so $\dim(M_i \otimes \mathcal{L}/k)^A = \dim(M_i \otimes \mathcal{L})^A - \dim M_i^A$. Also, by Lemma 5.3.2, $M_i^A = M_i^B = 0$. Thus we have that

$(M_i \otimes \mathcal{L})^A \cong (M_i \otimes \mathcal{L}/k)^A$. Then using Mackey's Formula (Theorem 4.1.26), we see that

$$\begin{aligned}(M_i)_B = (\operatorname{Ind}_B^G X_i)_B &\cong \bigoplus_{g\in\{1,\tau\}} \operatorname{Ind}_{B\cap B^g}^B X_i^g \\ &\cong X_i \oplus \operatorname{Ind}_T^B X_i^\tau \qquad (\dagger)\end{aligned}$$

where τ is as defined on p. 104. Then since X_i^τ is 1-dimensional (and not projective), its restriction to T remains irreducible (and not projective) and by Lemma 4.2.22 we have that $\operatorname{Ind}_T^B X_i^\tau \cong Y \oplus P$ for some non-projective (hence 1-dimensional) module Y and some projective module P.

Note that by Theorem 5.2.3, combined with Lemma 4.2.29, we have $\mathrm{H}^2(G, M_i) \cong \mathrm{H}^1(G, M_i \otimes \mathcal{L}/k)$. Then since $\mathcal{L} \cong k \oplus V$ and $\mathrm{H}^1(G, M_i) \cong \operatorname{Hom}_G(M_i^*, \mathcal{L}/k) = 0$, we see that

$$\mathrm{H}^1(B, M_i) \cong \mathrm{H}^1(G, M_i \otimes \mathcal{L}) \cong \mathrm{H}^1(G, M_i \otimes k) \oplus \mathrm{H}^1(G, M_i \otimes V) \cong \mathrm{H}^1(G, M_i \otimes V)$$

by Shapiro's Lemma with induction in the second coordinate (Corollary 4.2.34). Then by Lemma 5.3.6, $\mathrm{H}^1(B, M_i) \cong \mathrm{H}^1(B/A, M_i^A)$. But $M_i^A = 0$ as seen above, so combining the above gives

$$\mathrm{H}^2(G, M_i) \cong \mathrm{H}^1(G, M_i \otimes V) \cong \mathrm{H}^1(B, M_i) = \mathrm{H}^1(B/A, M_i^A) = 0.$$

If $i = a$ and $q \equiv 1 \mod 4$, $M_i = M_a$ is not irreducible. Then we have an exact sequence

$$0 \to M_{a1} \to M_a \to M_{a2} \to 0$$

which we may restrict down to B to get

$$0 \to (M_{a1})_B \to (M_a)_B \to (M_{a2})_B \to 0.$$

The latter must then split since $\operatorname{Ind}_B^G(X_a)$ is semisimple as a kB-module (modulo projectives, though these turn out to also be simple) as seen in (†). Thus since all kG-modules are relatively B-projective the former sequence must split and so we have that $\operatorname{Ind}_B^G X_a = M_a \cong M_{a1} \oplus M_{a2}$. Consequently, $\mathrm{H}^2(G, M_{a1}) = \mathrm{H}^2(G, M_{a2}) = 0$ since these must be summands of $\mathrm{H}^2(G, M_a) = 0$.

We now complete the proof by induction. Suppose that $\mathrm{H}^{n-1}(G, M_i) = 0$. Then by Theorem 5.2.3 we have $\mathrm{H}^n(G, M_i) \cong \mathrm{H}^{n-1}(G, M_i \otimes \mathcal{L}/k)$ and we also observe that

$$\mathrm{H}^n(G, M_i) \cong \mathrm{H}^{n-1}(G, M_i \otimes V) \oplus \mathrm{H}^{n-1}(G, M_i \otimes k) \cong \mathrm{H}^{n-1}(G, M_i \otimes \mathcal{L}) \cong \mathrm{H}^{n-1}(B, M_i).$$

But we know the structure of M_i as a B-module from (†), thus making heavy use of Shapiro's Lemma (Theorem 4.2.33) and a dash of Lemma 4.2.22,

$$\begin{aligned}
\mathrm{H}^{n-1}(B, M_i) &\cong \mathrm{H}^{n-1}(B, X_i) \oplus \mathrm{H}^{n-1}(B, \operatorname{Ind}_T^B X_i^\tau) && \text{(by (†))}\\
&\cong \mathrm{H}^{n-1}(B, X_i) \oplus \mathrm{H}^{n-1}(T, X_i^\tau) && \text{(Corollary 4.2.34)}\\
&\cong \mathrm{H}^{n-1}(B, X_i) \oplus \mathrm{H}^{n-1}(T, X_i) && \text{(Lemma 4.2.44)}\\
&\cong \mathrm{H}^{n-1}(B, X_i) \oplus \mathrm{H}^{n-1}(B, X_i \oplus P) && \text{(Lemma 4.2.22)}\\
&\cong \mathrm{H}^{n-1}(B, X_i) \oplus \mathrm{H}^{n-1}(B, X_i) &&\\
&\cong \mathrm{H}^{n-1}(G, \operatorname{Ind}_B^G X_i) \oplus \mathrm{H}^{n-1}(G, \operatorname{Ind}_B^G X_i) && \text{(Corollary 4.2.34)}\\
&\cong \mathrm{H}^{n-1}(G, M_i) \oplus \mathrm{H}^{n-1}(G, M_i) &&\\
&= 0
\end{aligned}$$

where P is some projective kB-module. Thus we see that $\mathrm{H}^{n-1}(B, M_i)$ is zero if $\mathrm{H}^{n-1}(G, M_i)$ is. But $H^{n-1}(B, M_i) \cong \mathrm{H}^n(G, M_i)$ and so $\mathrm{H}^n(G, M_i) = 0$ if $\mathrm{H}^{n-1}(G, M_i) = 0$. The required result then holds by induction since $\mathrm{H}^2(G, M_i) = 0$. The same argument holds for M_{a1} and M_{a2}. ■

Next, we deal with constituents of $\mathcal{L}$.

Proposition 5.3.7

We have the following:

$$\mathrm{H}^n(G,k) \cong \begin{cases} 0 & n \equiv 1,\,2 \mod 4, \\ k & n \equiv 0,\,3 \mod 4. \end{cases} \qquad \mathrm{H}^n(G,V) \cong \begin{cases} 0 & n \equiv 0,\,3 \mod 4, \\ k & n \equiv 1,\,2 \mod 4. \end{cases}$$

Proof: Recall that $\mathcal{L} \cong k \oplus V$ and also that $V \otimes \mathcal{L} \cong \operatorname{Ind}_B^G V$. We thus have, using the structure of V as a B-module and Shapiro's Lemma (Theorem 4.2.33),

$$\mathrm{H}^n(B,k) \cong \mathrm{H}^n(G,\mathcal{L}) \cong \mathrm{H}^n(G,k) \oplus \mathrm{H}^n(G,V).$$

We then see that $\mathrm{H}^n(G,\mathcal{L}) = \mathrm{H}^n(B,k) \cong \mathrm{H}^n(T,k)$ by Lemma 4.2.22 since $R \in \operatorname{Syl}_r B$ is a trivial intersection group and $T = N_B(R)$. We then also know that $\mathrm{H}^n(T,k)$ is 1-dimensional since T is a cyclic group of order divisible by r. It is now sufficient to determine $\mathrm{H}^n(G,k)$ since we know that $\dim \mathrm{H}^n(G,k) + \dim \mathrm{H}^n(G,V) = 1$. To do this, we make use of Lemma 4.2.22 since k is clearly a non-projective indecomposable module for both G and $N := N_G(R) = N_G(T)$ and so $\operatorname{Ind}_N^G k \cong k \oplus P$ for some projective kG-module P. Thus $\mathrm{H}^n(G,k) \cong \mathrm{H}^n(N,k)$. But N is a dihedral group and so its cohomology is well-known, but may also be easily determined using the Universal Coefficient Theorem for cohomology (Theorem 4.2.42) and the integral homology of N. We thus have that

$$\mathrm{H}^n(G,k) \cong \mathrm{H}^n(N,k) \cong \begin{cases} 0 & n \equiv 1,\,2 \mod 4, \\ k & n \equiv 0,\,3 \mod 4, \end{cases}$$

and the result follows. ■

Finally, we have the following from Proposition 5.3.3.

Proposition 5.3.8

The modules N_i are projective for all i, as are N_{b1} and N_{b2}.

Case 2: r odd and $r \mid q+1$

We next consider the case where r is odd and divides $q+1$. In this case, a Sylow r-subgroup of G lies in S and so we cannot use the properties of the Borel subgroup that were used in the previous case. As before, the structure of $\mathcal{L}$ will be important in this case so we note that the section on rank 1 groups in [40] tells us that $\mathcal{L}$ has radical factors k, V, k, where V is as described on p. 106. As such, no nontrivial irreducible kG-modules Y have $Y^B \neq 0$ by Lemma 5.3.2.

In this case, r does not divide $|T|$ and so we have that $a = \frac{1}{2}|T| + 1$ for $q \equiv 1 \mod 4$ and $a = \frac{1}{2}(|T| - 1) + 1$ otherwise. As for the Singer cycle, we have $b = \frac{1}{2}|S|_{r'} + 1$ for $q \equiv 3 \mod 4$ and $b = \frac{1}{2}(|S|_{r'} - 1)$ otherwise. Note that if S is an r-group and $q \not\equiv 3 \mod 4$ then in fact $b = 0$, and in this case the only irreducible kG-module of dimension $q-1$ is V. This information can be found in [14, II, IV, VI].

We proceed by investigating the projective kG-modules.

Proposition 5.3.9

The modules M_i are projective for all i, and so are M_{a1} and M_{a2}.

Proof: The Borel subgroup B is an r'-subgroup, thus all kB-modules are projective and hence so are their induced modules. For M_a, note that when $q \equiv 1 \mod 4$ we have an exact sequence

$$0 \to M_{a1} \to M_a \to M_{a2} \to 0$$

with M_a projective. Then M_a cannot be a projective indecomposable module since it has only two constituents which are not isomorphic, thus $M_a = M_{a1} \oplus M_{a2}$ is projective and so M_{a1} and M_{a2} must be projective. ■

Next, we deal with all of those irreducible modules for which there is no cohomology.

Proposition 5.3.10

We have $\mathrm{H}^n(G, N_i) = \mathrm{H}^n(G, N_{b1}) = \mathrm{H}^n(G, N_{b2}) = 0$ for all n.

Proof: For this proof, let $i \in \{1, \ldots, b-1, b, b1, b2\}$ for simplicity since no change in the argument is required to account for the case where N_b is reducible. We have $N_i^B = 0$ by Lemma 5.3.2. Since none of the modules N_i lie in the principal block we have that $\operatorname{Ext}_G^n(V^*, W) \cong \mathrm{H}^n(G, V \otimes W) = 0$ for all n. Now, we note that we have an exact sequence

$$0 \to V \to \mathcal{L}/k \to k \to 0$$

and again using Lemma 4.2.10 we get an exact sequence

$$0 \to N_i \otimes V \to N_i \otimes \mathcal{L}/k \to N_i \to 0.$$

This then gives the segment of the long exact sequence in cohomology

$$\cdots \to \mathrm{H}^1(G, N_i \otimes V) \to \mathrm{H}^1(G, N_i \otimes \mathcal{L}/k) \to \mathrm{H}^1(G, N_i) \to \mathrm{H}^2(G, N_i \otimes V) \to \cdots .$$

By the above we know that $\mathrm{H}^n(G, N_i \otimes V) = 0$ for all n. This tells us that $\mathrm{H}^1(G, N_i) \cong \mathrm{H}^1(G, N_i \otimes \mathcal{L}/k)$, but we know that $\mathrm{H}^1(G, N_i \otimes \mathcal{L}/k) \cong \mathrm{H}^2(G, N_i)$ by Theorem 5.2.3 and Lemmas 4.2.5 and 4.2.29. Following this along the exact sequence, we see that $\mathrm{H}^n(G, N_i) \cong \mathrm{H}^{n+1}(G, N_i)$ for all $n \geq 1$, and since $\mathrm{H}^1(G, N_i) = 0$ we have that $\mathrm{H}^n(G, N_i) = 0$ for all n. ■

Finally, we are back to dealing with the constituents of $\mathcal{L}$.

Proposition 5.3.11

We have

$$\mathrm{H}^n(G, k) \cong \begin{cases} 0 & n \equiv 1,\ 2 \mod 4, \\ k & n \equiv 0,\ 3 \mod 4, \end{cases} \qquad \mathrm{H}^n(G, V) \cong \begin{cases} 0 & n \equiv 0,\ 3 \mod 4, \\ k & n \equiv 1,\ 2 \mod 4. \end{cases}$$

Proof: We begin with k. Since $r \neq 2$ we have that $R \in \operatorname{Syl}_r G$ is a trivial intersection subgroup, and so $\mathrm{H}^n(G, k) \cong \mathrm{H}^n(N_G(R), k)$ by Lemma 4.2.22. But $N_G(R)$ is a dihedral group and so the cohomology is known as in the proof of Proposition 5.3.7, giving

$$\mathrm{H}^n(G,k) \cong \begin{cases} 0 & n \equiv 1,\ 2 \mod 4, \\ k & n \equiv 0,\ 3 \mod 4. \end{cases}$$

We then note that we have an exact sequence

$$0 \to k \to \mathcal{L} \to \mathcal{L}/k \to 0$$

from which we obtain the segment of the long exact sequence in cohomology

$$0 \to \mathrm{H}^1(G,k) \to \mathrm{H}^1(G,\mathcal{L}) \to \mathrm{H}^1(G,\mathcal{L}/k) \to \mathrm{H}^2(G,k) \to \mathrm{H}^2(G,\mathcal{L}) \to \cdots$$

and note that B is an r' group, so $\mathcal{L}$ is projective. Thus, continuing as above, $\mathrm{H}^n(G,k) \cong \mathrm{H}^{n-1}(G,\mathcal{L}/k)$ for each $n \geq 2$. We then look at the long exact sequence in cohomology corresponding to

$$0 \to V \to \mathcal{L}/k \to k \to 0$$

namely

$$0 \to \mathrm{H}^1(G,V) \to \mathrm{H}^1(G,\mathcal{L}/k) \to \mathrm{H}^1(G,k) \to \mathrm{H}^2(G,V) \to \mathrm{H}^2(G,\mathcal{L}/k) \to \cdots .$$

Since $\mathrm{H}^1(G,k) = 0$ by Lemma 4.2.30 as G is perfect and $\mathrm{H}^2(G,\mathcal{L}/k) \cong \mathrm{H}^3(G,k) \cong k$ by the above, we see that $\mathrm{H}^2(G,V) \cong k$. Continuing along the sequence in this way, one obtains the required result. ■

Case 3: $r = 2$

Finally, we consider the case where $\operatorname{char} k = 2$. This is more difficult than the previous cases since the Sylow 2-subgroups of G are not cyclic and the heart of $\mathcal{L}$ is no longer irreducible. We are no longer able to get as strong a result by proceeding as in the previous cases, so a different and more general approach has been taken. As an upside, this does mean the results later on in this section are more general and may be applied to other groups with similar representation theory. In particular, the results from now onwards hold for any group with the given Brauer graphs below.

Again, the notation for this case is set out on p. 106. Here, $\mathcal{L}$ is indecomposable with radical factors k, $V \oplus W$, k and so again by Lemma 5.3.2 there are no nontrivial irreducible kG-modules with B–fixed points. When $q \equiv 3 \mod 4$, $\mathcal{L}$ is projective (since B is a $2'$-group) and indecomposable with head k and is thus isomorphic to $\mathcal{P}(k)$. The only irreducible modules lying in the principal block are k, V and W. The remaining irreducible modules do not behave too different to the other cases, though the modules M_{a1}, M_{a2}, N_{b1} and N_{b2} never appear since, in characteristic 2, the involution in T or S gives rise to the trivial module as its corresponding representation.

When $q \equiv 1 \mod 4$, S has odd order and so $b = \frac{1}{2}(|S| - 1) = \frac{1}{4}(q - 1)$. The order of T is now even, so there are $|T|_{2'}$ irreducible kT-modules, and so $a = \frac{1}{2}(|T|_{2'} - 1)$.

Similarly, when $q \equiv 3 \mod 4$, T has odd order and so $a = \frac{1}{2}(|T| - 1) = \frac{1}{4}(q - 3)$. Mimicking the above discussion, we also see that $b = \frac{1}{2}(|S|_{2'} - 1)$. Again, this information may be found in Burkhardt's paper [14, VIII].

Proposition 5.3.12

If Y is one of the modules M_i, N_j then $\mathrm{H}^n(G, Y) = 0$ for all n.

Proof: Referring to [14, p. 91] or [8, Theorem 7.1.1], we see that the above modules all lie outside the principal block. Thus $\mathrm{Ext}^n_G(k, Y) = \mathrm{H}^n(G, Y) = 0$ for all n by Proposition 4.3.5.

■

Proposition 5.3.13

When $q \equiv 1 \mod 4$, N_i is projective for all i. When $q \equiv 3 \mod 4$, M_i is projective for all i.

Proof: When $q \equiv 3 \mod 4$, the Borel subgroup, from which the modules M_i are induced, is an r'-subgroup and so these modules are projective by Lemma 4.2.18. For the N_i with

$q \equiv 1 \mod 4$, this is part of Proposition 5.3.3. ■

We also know the cohomology of k due to Fong and Milgram:

Proposition 5.3.14 [34, Theorem 8.1]

Let k be the trivial kG-module. Then $\dim \mathrm{H}^n(G,k)$ is given by the coefficient of x^n in the Poincaré series

$$P(x) = \frac{1+x^3}{(1-x^2)(1-x^3)} = 1 + x^2 + 2x^3 + x^4 + \dots .$$

For the cohomology of the remaining two modules, however, we bring in some extra machinery. We will make use of Brauer graphs and knowledge of the structure of the projective covers of modules for blocks with Brauer graphs.

The reader unfamiliar with Brauer graphs should refer to the end of Section 4.3 during what follows. We give below the Brauer graphs for $\mathrm{PSL}_2(q)$ in characteristic 2, which differs dependent on whether $q \equiv \pm 1 \mod 4$. These may be found in [28, §2, (4) & (5)], but the multiplicities of the vertices are not determined there. Thus before we give the Brauer graphs, we must determine the multiplicities at each vertex. We shall denote by m the multiplicity of the vertex at which both V and W are incident and determine the remaining multiplicities in the following lemmas. The case where $q \equiv 3 \mod 4$ is easy:

Lemma 5.3.15

Let $q \equiv 3 \mod 4$. Then the multiplicities of the two vertices at which k is incident are both 1.

Proof: This follows immediately from the fact that $\mathcal{L}$ is projective, since B is a $2'$-group. ■

Lemma 5.3.16

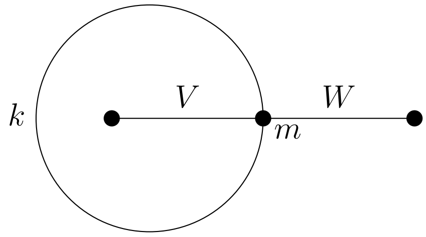
Let $q \equiv 1 \mod 4$. Then the multiplicities of the two vertices at which k is *not* incident are both 1.

Proof: This may be determined using the Ext quiver given in [32, p. 295]. An Ext quiver of a block is a directed graph whose vertices are the irreducible kG-modules lying in this block, and we draw $\dim \operatorname{Ext}^1_G(Y,Z)$ arrows between the vertices Y and Z (see p. 15 of the same book for this definition). As such, this quiver encodes the dimensions of $\operatorname{Ext}^1_G(Y,Z)$ for all Y, Z in a given block. The quiver in question is given below, where we know k is the central vertex since we know $\mathrm{H}^1(G,V) \cong \mathrm{H}^1(G,W) \cong k$ and so k must be connected to both other vertices.

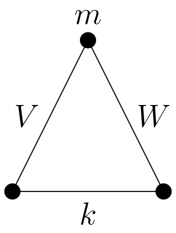
$$\begin{tikzcd} V \arrow[r, shift left] & k \arrow[l, shift left] \arrow[r, shift left] & W \arrow[l, shift left] \end{tikzcd}$$

In particular, in the above quiver we see that no module is connected to itself. This means that $\operatorname{Ext}^1_G(Y,Y) = 0$ for all irreducible Y in the principal block. In particular, $\operatorname{Ext}^1_G(V,V) = \operatorname{Ext}^1_G(W,W) = 0$. ■

Knowing the above facts, and the shape of the Brauer graphs for the principal block of $\mathrm{PSL}_2(q)$ from [28], we now give the Brauer graphs for G below (where m depends on q).



$q \equiv 1 \mod 4$



$q \equiv 3 \mod 4$

Using this, we can see that the projective indecomposable modules for $q \equiv 1 \mod 4$ are (using a bold letter to indicate a complete cycle around a vertex)

$$\begin{array}{ccccccccccc}
 & V & & & & W & & & & k & \\
 & & k & & k & & & & V & & W \\
 & & W & & V & & & & k & & k \\
 & & k & & k & & & & W & & V \\
0 & \oplus & \boldsymbol{V} & & \boldsymbol{W} & \oplus & 0 & & \boldsymbol{k} & \oplus & \boldsymbol{k} \\
 & & \vdots & & \vdots & & & & \vdots & & \vdots \\
 & & W & & V & & & & k & & k \\
 & & k & & k & & & & W & & V \\
 & V & & & & W & & & & k &
\end{array} \tag{‡}$$

and for $q \equiv 3 \mod 4$ we get the following.

$$\begin{array}{ccccccccccc}
 & V & & & & W & & & & & \\
 & & W & & V & & & & & & \\
 & & \boldsymbol{V} & & \boldsymbol{W} & & & & & & \\
 & & W & & V & & & & & k & \\
k & \oplus & \boldsymbol{V} & & \boldsymbol{W} & \oplus & k & & V & \oplus & W \\
 & & \vdots & & \vdots & & & & & k & \\
 & & \boldsymbol{V} & & \boldsymbol{W} & & & & & & \\
 & & W & & V & & & & & & \\
 & V & & & & W & & & & &
\end{array} \tag{$\blacklozenge$}$$

In all cases, the modules given in bold repeat $m-1$ times. Before proceeding, we introduce another piece of notation.

Definition 5.3.17

Given two kG-modules Y and Z, we say $Y \sim Z$ to indicate that Y and Z have the same radical factors, *i.e.* $\operatorname{rad}^{i-1} Y / \operatorname{rad}^i Y \cong \operatorname{rad}^{i-1} Z / \operatorname{rad}^i Z$ for all i. Suppose that Y has radical factors Y_1, Y_2, $\ldots$, Y_n. Then we denote the equivalence class of modules with this radical series by $[Y_1 \mid Y_2 \mid \ldots \mid Y_n]$ and say that $Y \sim [Y_1 \mid Y_2 \mid \ldots \mid Y_n]$. Note that here we begin at the head and move through the radical layers, so that $\operatorname{head} Y \cong Y_1$ and $\operatorname{soc} Y \hookrightarrow Y_n$ (this is not an isomorphism since, for example, a module of shape $[V \mid W] \oplus V$ has socle $W \oplus V$ but shape $[V \oplus V \mid W]$). If all of the radical factors Y_i given above are irreducible, then we say that Y is a *uniserial* module as it has a unique composition series.

Finally, given a uniserial kG-module Y with radical factors $Y_1, \ldots, Y_n$ and a semisimple kG-module Z we abuse this notation somewhat and write $[Y \mid Z]$ for a module of shape $[Y_1 \mid \ldots \mid Y_n \mid Z]$ and $[Y \oplus Z]$ for a module of shape $[Y_1 \oplus Z \mid \ldots \mid Y_n]$.

With all of our machinery in place, we are now ready to determine the cohomology for G.

Proposition 5.3.18

Suppose $q \equiv 1 \mod 4$. Then

$$\mathrm{H}^n(G, V) \cong \mathrm{H}^n(G, W) \cong \begin{cases} k & n \equiv 1 \mod 3, \\ 0 & \text{otherwise.} \end{cases}$$

Proof: We proceed by examining the structure of $\Omega^n V$ for $n \leq 3$. Since the choice of notation for V and W was arbitrary, this also proves the result for W. Denote $\mathcal{HP}(V)$ and $\mathcal{HP}(W)$ by X_V and X_W respectively, and let $\mathcal{HP}(k) \cong Y_1 \oplus Y_2$ with $\operatorname{head} Y_1 \cong V$ and $\operatorname{head} Y_2 \cong W$. Then one can immediately see from the definition that $\Omega V \cong \operatorname{rad} \mathcal{P}(V)$ has shape $[X_V \mid V]$.

To determine $\Omega^2 V$, we must first take the projective cover of ΩV and find the kernel of this covering map. Since $\Omega V \sim [X_V \mid V] \sim [k \mid Y_2]$, we see that $\mathcal{P}(\Omega V) \cong \mathcal{P}(\operatorname{head} \Omega V) \cong \mathcal{P}(k)$. In particular, we note that ΩV is uniserial. We therefore require a submodule $\Omega^2 V$ of $\mathcal{P}(k)$ such that $\mathcal{P}(k)/\Omega^2 V \cong \Omega V$.

Let L and R denote the submodules of $\mathcal{P}(k)$ of respective shapes $[Y_1 \mid k]$ and $[Y_2 \mid k]$, corresponding to taking the left and right hand sides of the picture of $\mathcal{P}(k)$ as seen in (‡). Then since $\mathcal{P}(k)/\Omega^2 V$ is uniserial, we know that $(L + \Omega^2 V)/\Omega^2 V$ and $(R + \Omega^2 V)/\Omega^2 V$ are both submodules of this uniserial module and thus one must contain the other. We also know that $\operatorname{soc}^2 R \nsubseteq \Omega^2 V$ (where $\operatorname{soc}^2 R$ is the 'bottom two layers' of R, of shape $[V \mid k]$) since $\mathcal{P}(k)/\operatorname{soc}^2 R$ has no quotients of shape ΩV. As such, $R \cap \Omega^2 V = \operatorname{soc} \mathcal{P}(k) \cong k$ and so $R/k \cap (\Omega^2 V)/k = 0$. Finally, since $\dim L = \dim R = \dim \Omega^2 V$, we see that $R + \Omega^2 V = \operatorname{rad} \mathcal{P}(k)$ and so $R/k + (\Omega^2 V)/k = \mathcal{H} \mathcal{P}(k)$. Thus $(\Omega^2 V)/k$ is a complement to R/k in $\mathcal{H} \mathcal{P}(k)$ and so $(\Omega^2 V)/k \cong L/k$. This yields $\Omega^2 V$ of shape $[Y_1 \mid k]$.

Finally, $\mathcal{P}(\Omega^2 V) \cong \mathcal{P}(\operatorname{head} Y_1) \cong \mathcal{P}(V)$ and clearly any map $\mathcal{P}(V) \twoheadrightarrow [Y_1 \mid k]$ must have kernel V, giving $\Omega^3 V \cong V$. Thus V is a periodic module, so $\Omega^4 V \cong \Omega(\Omega^3 V) = \Omega V$ and so we can determine the dimension of $\mathrm{H}^i(G, V)$ for all i by just counting the multiplicity of k in the head of $\Omega^n V$ for n at most 3. The required result then follows from Lemma 4.3.8 using the fact that $\operatorname{head} \Omega V \cong k$, $\operatorname{head} \Omega^2 V \cong V$ and $\operatorname{head} \Omega^3 V \cong V$. ■

For the next case, we again use the above approach, but since the projective module we are investigating is not uniserial (and indeed none of k, V or W are even periodic!) things are more complicated. We determine the structure of $\Omega^n V$ by carefully following the diagonal extensions present at each step and determining which extensions must therefore be present in its Heller translate. We recommend that the reader draws the associated pictures for the below arguments (and those which follow) and keeps them in mind at all times as they should greatly aid understanding. We will present some such pictures in the below proof, but in future they will be omitted in the name of brevity.

Proposition 5.3.19

Suppose $q \equiv 3 \mod 4$ and let V, W be as above. Then

$$\dim \mathrm{H}^n(G, V) = \dim \mathrm{H}^n(G, W) = \left\lceil \frac{n}{3} \right\rceil.$$

Recall again that as our decision as to which module is V and which is W was arbitrary, it suffices to only prove the result for one. We will prove the above in a similar manner to the previous proposition, examining the structure of $\Omega^n V$ and counting the multiplicity of k in its head. Before giving the proof, we must first set out some notation. Throughout this discussion and the proof which follows, the reader is encouraged to refer often to (♦).

Let Y_V, Y_W be such that $\mathcal{H}\mathcal{P}(V) \cong k \oplus Y_V$ and $\mathcal{H}\mathcal{P}(W) \cong Y_W \oplus k$. Then we can easily see that ΩV has shape $[k \oplus Y_V \mid V]$, which has projective cover $\mathcal{L} \oplus \mathcal{P}(W)$.

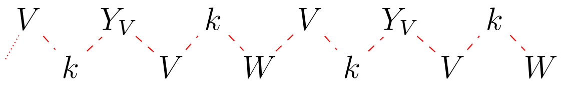
Throughout the proof, we investigate extensions of a collection of six modules, appearing as submodules of ΩV and Ωk. We briefly examine these below and in particular show that they are periodic.

We first observe that, since head $Y_V \cong W$, $\mathcal{P}(W) \twoheadrightarrow [Y_V \mid V]$ with kernel of shape $[k \mid W]$, onto which $\mathcal{L}$ surjects with kernel of shape $[V \mid k]$ which is in turn covered by $\mathcal{P}(V)$ with kernel $[Y_V \mid V]$ again.

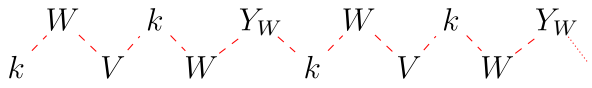
We also note that $\mathcal{P}(W) \twoheadrightarrow [W \mid k]$ with kernel of shape $[Y_W \mid W]$, which is covered by $\mathcal{P}(V)$ with kernel $[k \mid V]$ and which one may in turn cover with $\mathcal{L}$ and kernel $[W \mid k]$, returning us to the module shape we started with. We illustrate the periodicity of the modules in question below.

$$\begin{tikzcd}
 & \begin{matrix} V \\ k \end{matrix} \arrow[dl, bend right, "\Omega"'] \\
\begin{matrix} Y_V \\ V \end{matrix} \arrow[dr, bend right, "\Omega"'] & \\
 & \begin{matrix} k \\ W \end{matrix} \arrow[uu, bend right, "\Omega"']
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \begin{matrix} W \\ k \end{matrix} \arrow[dl, bend right, "\Omega"'] \\
\begin{matrix} Y_W \\ W \end{matrix} \arrow[dr, bend right, "\Omega"'] & \\
 & \begin{matrix} k \\ V \end{matrix} \arrow[uu, bend right, "\Omega"']
\end{tikzcd}$$

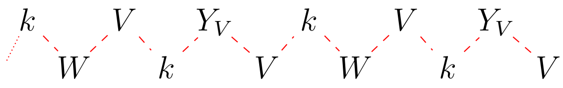
We aim to prove that all of $\Omega^n V$, aside from one irreducible constituent, is made up of a series of diagonal extensions of the above periodic modules. To do this, we must set out yet more notation. Specifically, when n is odd then $\Omega^n V$ is a diagonal extension of k by two modules E_n and F_n and when n is even then $\Omega^n V$ is a diagonal extension of V by two modules which we shall also denote by E_n and F_n. These modules are such that E_{2n} has shape

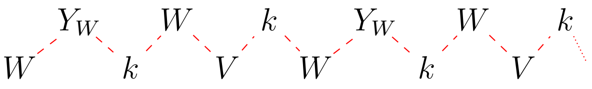


and F_{2n} has shape

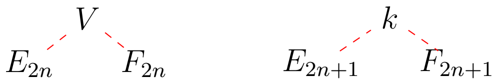


where each red dashed line indicates a non-split extension and the dotted line indicates that the pattern continues in this way. Each E_{2n} and F_{2n} contains n of the periodic modules mentioned above, so one can see that above we have drawn E_{12} and F_{12} (with possible continuations). Next, E_{2n+1} and F_{2n+1} have respective shapes





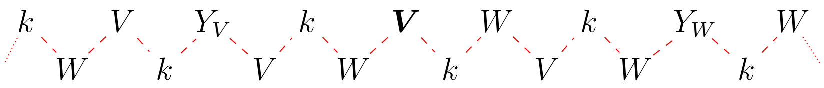
where E_{2n+1} contains $n+1$ of the periodic modules seen above and F_{2n+1} contains n (so we have drawn E_{11} and F_{13}). We will show that the shape of $\Omega^{2n}V$ is as on the left below, and the shape of $\Omega^{2n+1}V$ is as on the right. Here the k is part of a diagonal non-split extension with the V on the right hand side of E_{2n+1} and the W on the left hand side of F_{2n} and similarly the V is part of a diagonal non-split extension with W and k.



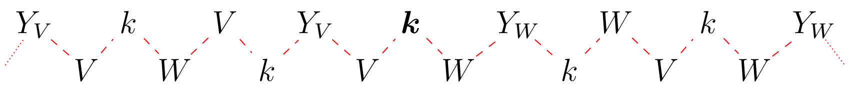
In full, we claim the following.

Lemma 5.3.20

The module $\Omega^{2n}V$ is of shape



and $\Omega^{2n+1}V$ is of shape



where we have put the irreducible module between E_n and F_n in bold.

Proof: We show that $\Omega^n V$ is as above by induction. For our base case, we observe that $\Omega^0 V \cong V$ is already of the required form. The bold V in $\Omega^{2n}V$ contributes an additional module of shape $[Y_V \mid V]$ to $\Omega^{2n+1}V$ which we associate to E_{2n+1}, and similarly the bold k in $\Omega^{2n+1}V$ contributes an additional $[W \mid k]$ to $\Omega^{2n+2}V$ which we associate to F_{2n+2}. We will show this more formally below, and show that if $\Omega^n V$ is of the required shape then so is $\Omega^{n+1}V$ by dealing with each of the E_n and F_n, then patching together the required extensions between these components to obtain the required result.

In particular, we show that $\Omega F_{2n} \sim F_{2n+1}$, $\Omega E_{2n+1} \sim E_{2n+2}$, E_{2n+1} is an extension of ΩE_{2n} by $[Y_V \mid V]$ and F_{2n+2} is an extension of ΩF_{2n+1} by $[W \mid k]$.

We first show that $\Omega F_{2n} \sim F_{2n+1}$. Due to the layout of the extensions as drawn above, it is sufficient to only consider a small case. To see this, note that F_6 is a quotient of F_{2n} (by a submodule of shape F_{2n-6}) for all $n \geq 3$. More formally, we take the short exact sequence

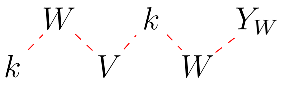
$$0 \to F_{2n-6} \xrightarrow{\theta_1} F_{2n} \xrightarrow{\theta_2} F_6 \to 0$$

and take the short exact sequence corresponding to the projective covering map for each term. Rotating the above short exact sequence so that it is vertical, we then get the following diagram (with φ_i determined afterwards).

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \Omega F_{2n-6} \arrow[r] \arrow[d, dashed, "\varphi_1"] & \mathcal{P}(F_{2n-6}) \arrow[r, "p_1"] \arrow[d] & F_{2n-6} \arrow[r] \arrow[d, "\theta_1"] & 0 \\
0 \arrow[r] & \Omega F_{2n} \arrow[r] \arrow[d, dashed, "\varphi_2"] & \mathcal{P}(F_{2n}) \arrow[r, "p_2"] \arrow[d] & F_{2n} \arrow[r] \arrow[d, "\theta_2"] & 0 \\
0 \arrow[r] & \Omega F_6 \arrow[r] \arrow[d] & \mathcal{P}(F_6) \arrow[r, "p_3"] \arrow[d] & F_6 \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Observe that $\mathcal{P}(F_{2n}) \cong \mathcal{P}(F_{2n-6}) \oplus \mathcal{P}(F_6)$ for each n, so that we may take the arrows in the middle column to be the inclusion map from $\mathcal{P}(F_{2n-6})$ to $\mathcal{P}(F_{2n})$ and projection map from $\mathcal{P}(F_{2n})$ onto $\mathcal{P}(F_6)$, respectively. We wish to take φ_1 and φ_2 to be (restrictions of) the same maps, but must check that their images would indeed be in the desired places. For this, it is sufficient to check that the two right-hand squares commute and this can be seen immediately from the shape of F_{2n} and its projective cover. Finally, exactness of the left-hand column may be verified directly, but also follows from the Nine (or 3×3) Lemma (appears as Exercise 1.3.2 in [68]). This gives us ΩF_{2n} as a known extension of ΩF_6 by ΩF_{2n-6} and so knowing ΩF_2, ΩF_4 and ΩF_6 tells us the shape of ΩF_{2n} for all n.

The smallest n from which we may obtain all the required information is 6, thus this is the case we shall consider. We first give F_6 for convenience.



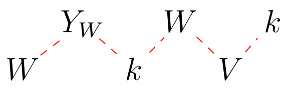
The following argument will be vital for much of the rest of this chapter. In order to save trees, we will not be drawing all of the below representations of modules and their extensions in future. The projective cover of F_6 is

$$\begin{matrix} W \\ Y_W \oplus k \\ W \end{matrix} \bigoplus \begin{matrix} k \\ V \oplus W \\ k \end{matrix} \bigoplus \begin{matrix} V \\ k \oplus Y_V \\ V \end{matrix}$$

where the quotients highlighted in red indicate areas in F_6 in which there is no choice as to which projective module will cover it. Conversely, the constituents highlighted in blue indicate areas in which there are at least two *(a priori)* possible coverings — for example, a module of shape $[V \oplus W \mid k]$ could (since such modules are not unique) have a covering by $\mathcal{P}(V) \oplus \mathcal{P}(W)$ such that $\mathcal{P}(V) \twoheadrightarrow [V \mid k]$ and $\mathcal{P}(W) \twoheadrightarrow W$, one such that $\mathcal{P}(V) \twoheadrightarrow V$ and $\mathcal{P}(W) \twoheadrightarrow [W \mid k]$ or some covering in which the copy of k is diagonal between $\mathcal{P}(V)$ and $\mathcal{P}(W)$.

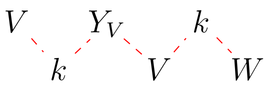
Taking note of the extensions in the second row of F_6 (as drawn above), we see that V must be in an extension of both W and k, and W in an extension of k and Y_W. This indicates that these three modules must correspond to some diagonal quotient of the corresponding projective cover. Thus in the modules highlighted in blue above, our quotient involves some diagonal submodule of the constituents of adjacent (as written) projective covers. For example, the non-split extension of shape $[W \oplus k \mid V]$ must stem from taking V as a diagonal submodule of head $Y_W \oplus V$ in $\mathcal{P}(W) \oplus \mathcal{P}(k)$. Similarly, the non-split extension $[k \oplus Y_W \mid W]$ must stem from taking W as a diagonal submodule of $W \oplus \operatorname{soc} Y_V$ in $\mathcal{P}(k) \oplus \mathcal{P}(V)$.

It then remains to see what a covering map of the described shape has as its kernel. The diagonal submodules occurring in the previous paragraph give rise to diagonal extensions of the heads of the kernel of the covering map. For example, covering $[W \oplus k \mid V]$ as described above results in an extension of shape $[V \mid Y_V \oplus k]$ in its kernel. Similarly, the described covering of $[k \oplus Y_W \mid W]$ gives an extension of shape $[W \mid k \oplus V]$. Patching these together, we obtain ΩF_6 of shape



which is the same shape as F_7, as required. A subset of this argument also yields ΩF_2 and ΩF_4.

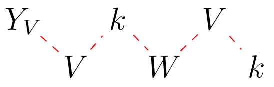
We next show that E_{2n+1} is an extension of ΩE_{2n} by $[Y_V \mid V]$. As before, we need only consider a small case since E_{2n} is an extension of E_6 by E_{2n-6} for all $n \geq 3$ and so we give E_6 below.



The projective cover of this, with colour highlights as in the previous case, is then

$$\begin{array}{c} V \\ Y_V \oplus k \\ V \end{array} \bigoplus \begin{array}{c} W \\ k \oplus Y_W \\ W \end{array} \bigoplus \begin{array}{c} k \\ V \oplus W \\ k \end{array} .$$

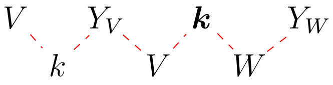
We may then proceed in a similar manner to the F_6 case above. The extension $[V \oplus Y_V \mid k]$ must come from a diagonal k in $k \oplus k$ in $\mathcal{P}(V) \oplus \mathcal{P}(W)$ and the extension $[Y_V \oplus k \mid V]$ can only come from a diagonal V in $\operatorname{soc} Y_W \oplus V$ from $\mathcal{P}(W) \oplus \mathcal{P}(k)$. Patching together the extensions this gives us in ΩE_6, we obtain ΩE_6 of shape



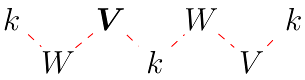
We then note that 'attaching' $[Y_V \mid V]$ on the right via an extension $[Y_V \mid k \oplus V]$ gives us the shape of E_7, as required. A subset of this argument also yields ΩE_2 and ΩE_4.

Applying exactly the same argument (using the same extensions seen above and noting that E_5 and F_7 are respective quotients of E_{2n+1} and F_{2n+1} by E_{2n-5} and F_{2n-5}) yields $\Omega E_{2n+1} \sim E_{2n+2}$ and we also get F_{2n+2} as an extension of ΩF_{2n+1} by $[W \mid k]$ via an extension $[W \mid k \oplus V]$.

We now return to $\Omega^n V$. In particular, we need to deal with the interface between E_n, F_n and V or k. Suppose that we have a module of the required form for some even n. Then the V in the middle is part of an extension of shape $[V \mid W \oplus k]$. To cover this extension, we would need to take a diagonal submodule of $W \oplus \operatorname{head} Y_V$ in $\mathcal{P}(k) \oplus \mathcal{P}(V)$ and a diagonal k in $k \oplus k$ in $\mathcal{P}(V) \oplus \mathcal{P}(W)$. Such a covering would then have kernel of shape



where we have put the k in bold above to illustrate where this should lie in $\Omega^{2n+1}V$ as drawn before the start of this proof. This corresponds to attaching an additional module of shape $[Y_V \mid V]$ to the right hand side of ΩE_{2n}, as discussed above. We can then see that if $\Omega^{2n}V$ is of the required form, then $\Omega^{2n+1}V$ is of the required form. It remains only to show that if $\Omega^{2n+1}V$ is as claimed, then so is $\Omega^{2n+2}V$. We do this in the same manner as the even case, investigating the non-split extension $[k \mid V \oplus W]$ in the middle. To cover this again requires a diagonal V as part of $\operatorname{soc} Y_W \oplus V$ in $\mathcal{P}(W) \oplus \mathcal{P}(k)$ and a diagonal W as part of $W \oplus \operatorname{soc} Y_V$ in $\mathcal{P}(k) \oplus \mathcal{P}(V)$. Such a covering would then give a kernel of shape



where V is bold for the same reason as k above. Similarly to the previous case, this corresponds to attaching a module of shape $[W \mid k]$ to the left hand side of F_{2n+1} as discussed earlier. This shows that if $\Omega^{2n+1}V$ is as claimed, then so is $\Omega^{2n+2}V$. Since $\Omega^0 V \cong V$ is of the required form, we are then done. ■

Now that we know the shape of $\Omega^n V$ for all $n \geq 0$, we are able to determine the dimensions of $\mathrm{H}^n(G, V)$ and $\mathrm{H}^n(G, W)$ for all n by investigating the modules present in its head.

Proof of Proposition 5.3.19. The result will follow from counting the multiplicity of k in $\operatorname{head}\Omega^n V$ by Lemma 4.3.8. For this, we need only count how many times k appears in the heads of E_n and F_n, along with the module given in the centre of $\Omega^n V$. Due to the structure of these modules, we may work modulo 6 for this. We see that E_n contains $\left\lceil \frac{n}{6} \right\rceil$ copies of n in its head when $n \equiv 0$, 2, 4 or 5 $\mod 6$ and $\left\lfloor \frac{n}{6} \right\rfloor$ otherwise. Similarly, F_n contains $\left\lceil \frac{n}{6} \right\rceil$ copies of k in its head when $n \equiv 0$ or 4 $\mod 6$ and $\left\lfloor \frac{n}{6} \right\rfloor$ otherwise. Finally, the module given in bold is trivial when n is odd.

We prove the case where $n \equiv 5 \mod 6$ here and leave the remaining cases to the reader. From the above, we have

$$\left\lceil \frac{n}{6} \right\rceil + 1 + \left\lfloor \frac{n}{6} \right\rfloor = 2\left\lceil \frac{n}{6} \right\rceil = 2\left(\frac{n}{6} + \frac{1}{6}\right) = \frac{n}{3} + \frac{1}{3} = \left\lceil \frac{n}{3} \right\rceil$$

copies of k in $\operatorname{head}\Omega^n V$, as required.

As our decision as to which module is V and which is W was arbitrary, we may swap them without loss of generality and thus the result holds for both. ■

The following results are direct corollaries of the above analysis, and follow from simply noting other aspects of the structures investigated above.

Corollary 5.3.21

Suppose $q \equiv 1 \mod 4$. Let V, W be as above and let $n > 0$. Then

$$\begin{aligned} \mathrm{Ext}^n_G(W,V) &= \mathrm{Ext}^n_G(V,W) = 0, \\ \mathrm{Ext}^n_G(W,W) &\cong \mathrm{Ext}^n_G(V,V) \cong \begin{cases} 0 & n \equiv 1 \mod 3, \\ k & \text{otherwise.} \end{cases} \end{aligned}$$

Proof: This follows directly from examining the heads of $\Omega^n V$ (a periodic module) given in the proof of Proposition 5.3.18. ■

Corollary 5.3.22

Suppose $q \equiv 3 \mod 4$. Let V, W be as above and let $n > 0$. Then

$$\begin{aligned} \dim \mathrm{Ext}^n_G(V,W) &= \dim \mathrm{Ext}^n_G(W,V) = \left\lceil \frac{n}{3} \right\rceil, \\ \dim \mathrm{Ext}^n_G(W,W) &= \dim \mathrm{Ext}^n_G(V,V) = \begin{cases} \frac{n}{3} + 1 & n \equiv 0 \mod 3, \\ \left\lfloor \frac{n}{3} \right\rfloor & n \equiv 1 \mod 3, \\ \left\lceil \frac{n}{3} \right\rceil & n \equiv 2 \mod 3. \end{cases} \end{aligned}$$

Proof: We repeat the above process, but counting multiplicities of V and W in $\operatorname{head} \Omega^n V$ instead. As before, V and W may be swapped without loss of generality. We first deal with $\mathrm{Ext}^n_G(V,W)$. The method of counting is identical to above except we may ignore the bold module in $\Omega^n V$ (see Lemma 5.3.20) entirely. One can observe as before that W appears in the head of E_n with multiplicity $\left\lfloor \frac{n}{6} \right\rfloor$ if $n \equiv 2 \mod 6$ and $\left\lceil \frac{n}{6} \right\rceil$ otherwise, and similarly for F_n with multiplicity $\left\lceil \frac{n}{6} \right\rceil$ if $n \equiv 0$, 2, 4 or $5 \mod 6$ and $\left\lfloor \frac{n}{6} \right\rfloor$ otherwise. We thus get that W appears with multiplicity $\left\lfloor \frac{n}{6} \right\rfloor + \left\lceil \frac{n}{6} \right\rceil = \left\lceil \frac{n}{3} \right\rceil$ for $n \equiv 0$, 1, 2, or $3 \mod 6$, and $\left\lceil \frac{n}{6} \right\rceil + \left\lceil \frac{n}{6} \right\rceil = \left\lceil \frac{n}{3} \right\rceil$ for $n \equiv 4$, $5 \mod 6$.

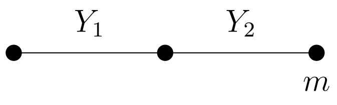
Finally, we deal with $\mathrm{Ext}^n_G(V,V)$. Again, one may verify that V appears in the head of E_n with multiplicity $\left\lceil \frac{n}{6} \right\rceil$ if $n \equiv 0$, 3 or $5 \mod 6$ and $\left\lfloor \frac{n}{6} \right\rfloor$ otherwise, and exactly the same for F_n. Also, V appears once in the head as the bold module whenever n is even and not otherwise. Adding these numbers gives the required result. ■

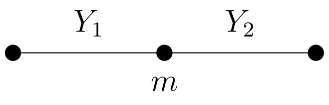
5.4 Extensions in $\mathrm{PSL}_2(q)$

Using the methods of the previous section, we can also determine $\mathrm{Ext}^n_G(Y, Z)$ for all Y, $Z \in \mathrm{Irr}_k\, G$ in other non-defining characteristics. For odd characteristic, the Brauer trees of these blocks are given in [14] though we summarise this information below. In the below discussion, B_0 denotes the principal block and B_1 denotes the block containing only M_{a1} and M_{a2} or N_{b1} and N_{b2}, dependent on which pair exists in the given situation.

The blocks for G containing two modules fall into two cases, case 1 holds for B_0 whenever r is odd and $r \mid q + 1$ and case 2 holds for B_0 whenever r is odd and $r \mid q - 1$, along with B_1 whenever it exists. All other blocks have cyclic defect groups, contain only a single simple module and can be dealt with separately.

For some exceptional multiplicity m, cases 1 and 2 respectively have Brauer trees





and Cartan matrices

$$\begin{pmatrix} 2 & 1 \\ 1 & m+1 \end{pmatrix} \qquad\qquad \begin{pmatrix} m+1 & m \\ m & m+1 \end{pmatrix}$$

where in case 1, the first column represents Y_1 (corresponding to the trivial module for our purposes) and the second Y_2 (corresponding to V). Using the above trees, we see that in case 1, $\mathcal{P}(Y_1) \sim [Y_1 \mid Y_2 \mid Y_1]$ and $\mathcal{P}(Y_2)$ has heart $Y_1 \oplus Z$ where $Z \sim [Y_2 \mid Y_2 \mid \ldots \mid Y_2]$. In case 2, both projective covers are uniserial of the same length with $\mathcal{P}(Y_i) \sim [Y_i \mid Y_j \mid Y_i \mid \ldots \mid Y_j \mid Y_i]$ for $i \neq j$. Note that when $m = 1$ in case 1, we will get a different answer as $\mathrm{Ext}^1_G(Y_2, Y_2) = 0$ and $Z = 0$. This happens in $\mathrm{PSL}_2(q)$ when the r-part of $q + 1$ is 3.

Proposition 5.4.1

Let B be a block with Brauer tree as in case 1 (for $m \neq 1$) with simple modules Y_1, Y_2.

Then $\mathrm{Ext}_G^n(Y_2, Y_2) \cong k$ for all n, and, for $i \neq j$,

$$\mathrm{Ext}_G^n(Y_1, Y_1) \cong \begin{cases} 0 & n \equiv 1,\ 2 \mod 4, \\ k & n \equiv 0,\ 3 \mod 4, \end{cases} \qquad \mathrm{Ext}_G^n(Y_i, Y_j) \cong \begin{cases} 0 & n \equiv 0,\ 3 \mod 4, \\ k & n \equiv 1,\ 2 \mod 4. \end{cases}$$

If $m = 1$, then instead $\mathrm{Ext}_G^n(Y_2, Y_2) \cong \mathrm{Ext}_G^n(Y_1, Y_1)$ for all n.

Proof: We proceed as before by computing $\Omega^n Y_i$. In both cases we see that the simple modules are periodic. This gives (immediately, since $\Omega^n Y_1$ is uniserial for all n) $\Omega^n Y_1$ of shapes $[Y_2 \mid Y_1]$, $[Z \mid Y_2]$ and $[Y_1 \mid Y_2]$ for $n = 1$, 2, 3, and $\Omega^4(Y_1) \cong Y_1$. When $m = 1$, note that $Z = 0$ and so $\Omega^2 Y_1 \cong Y_2$ and so can stop here (one may also deduce the required result from the fact that if $m = 1$ then Y_1 and Y_2 may be swapped without loss of generality). Otherwise, when $m > 1$, we must work harder.

For Y_2, the Heller translates are not all uniserial so some additional thought is required. We of course have $\Omega Y_2 \sim [Y_1 \oplus Z \mid Y_2]$. The projective cover of this is then $\mathcal{P}(Y_1) \oplus \mathcal{P}(Y_2)$, and the Y_2 in $\operatorname{soc} \Omega Y_2$ must stem from a diagonal submodule of $Y_2 \oplus \operatorname{soc} Z$ (taking any module 'higher up' in Z would result in $\Omega^2 Y_2$ being decomposable) in $\mathcal{P}(Y_1) \oplus \mathcal{P}(Y_2)$, yielding $\Omega^2 Y_2 \sim [Y_2 \oplus Y_1 \mid Y_1 \oplus Y_2]$. Similarly, the Y_2 in $\operatorname{soc} \Omega^2 Y_2$ comes from a diagonal submodule of $\operatorname{head} Z \oplus Y_2$ in $\mathcal{P}(Y_2) \oplus \mathcal{P}(Y_1)$ and so we obtain $\Omega^3 Y_2 \sim [Y_1 \oplus Z \mid Y_2]$. From this it immediately follows that $\Omega^4 Y_2 \cong Y_2$. The dimensions of Ext_G^n may be read off from the shapes of these modules, and the result follows. ■

Proposition 5.4.2

Let B be a block with Brauer tree as in case 2 with simple modules Y_1, Y_2. Then, for $i \neq j$,

$$\mathrm{Ext}_G^n(Y_i, Y_i) \cong \begin{cases} 0 & n \equiv 1,\ 2 \mod 4, \\ k & n \equiv 0,\ 3 \mod 4, \end{cases} \qquad \mathrm{Ext}_G^n(Y_i, Y_j) \cong \begin{cases} 0 & n \equiv 0,\ 3 \mod 4, \\ k & n \equiv 1,\ 2 \mod 4. \end{cases}$$

Proof: As before, we compute $\Omega^n Y_i$. One sees immediately from the shape of the projective covers that $\Omega Y_1 \sim \mathcal{P}(Y_2)/Y_2$, and then $\Omega^2 Y_1 \cong Y_2$. Since the choice of Y_1 or Y_2 was arbitrary, this determines the structure of all $\Omega^n Y_i$ for both i and the result follows. ■

The only remaining case is now made up of blocks containing a single non-projective simple module, *i.e.* all modules not in B_0 or B_1 mentioned above (k, V, W, M_{a1}, M_{a2}, N_{b1} and N_{b2}) and not shown to be projective by Proposition 5.3.3, Proposition 5.3.9 or Proposition 5.3.13. This case is dealt with by Proposition 4.3.25. To see this, note that either the Sylow r-subgroups of G are cyclic or $r = 2$ and they are dihedral. In the even case, the principal block is the only block of maximal defect and otherwise the defect group of any block B is a Sylow 2-subgroup of the centraliser of some 2-regular element by Lemma 4.3.22. In particular, such a group must be cyclic if it is not the whole Sylow 2-subgroup of G. To summarise, we have proven the following.

Corollary 5.4.3

Let Y be one of the following simple modules.

- M_i, $i \notin \{1, a, a1, a2\}$, for odd $r \mid q - 1$ or $r = 2$ and $q \equiv 1 \mod 4$,

- N_i, $i \notin \{b, b1, b2\}$, for odd $r \mid q + 1$ or $r = 2$ and $q \equiv 3 \mod 4$.

Then Y is the only simple module in its block, is not projective, and $\mathrm{Ext}^n_G(Y, Y) \cong k$ for all n.

5.5 Extensions and cohomology in $\mathrm{Sz}(q)$

We next deal with the Suzuki groups $G := \mathrm{Sz}(q)$ or ${}^2\mathrm{B}_2(q)$ for $q = 2^{2n+1}$, since the Sylow r-subgroups of these groups in non-defining characteristics are cyclic and so methods used before all apply. In particular, the Brauer trees are known due to Burkhardt [15] for the Suzuki groups for all such cases and so we know the structure of the projective modules in these cases very well.

We will not require any structural information about $\mathrm{Sz}(q)$ as the results are determined completely by the structure of the projective modules (thus the Brauer trees), but the curious reader should consult [18, Chapters 13, 14] for more. These groups have order $|\mathrm{Sz}(q)| = q^2(q-1)(q^2+1)$ which factors as $q^2(q-1)(q-s+1)(q+s+1)$, where $s^2 = 2q$, and so the study of the cross characteristic representation theory of these groups splits naturally into the three cases $r \mid q-1$, $r \mid q-s+1$ and $r \mid q+s+1$. We will examine each of these cases in turn. In order to do this we reproduce the character table of $\mathrm{Sz}(q)$ from [15] and label the complex characters accordingly.

Let x, y and z be elements of $\mathrm{Sz}(q)$ of orders $q-1$, $q+s+1$ and $q-s+1$, respectively, and let f and t be elements of respective orders 4 and 2. Powers of these elements give a set of conjugacy class representatives for G. Now, let ω, η and ζ be primitive $(q-1)^{\mathrm{th}}$, $(q-s+1)^{\mathrm{th}}$ and $(q+s+1)^{\mathrm{th}}$ complex roots of unity, respectively, and let $\varepsilon_d := \zeta^d + \zeta^{-d} + \zeta^{qd} + \zeta^{-qd}$ and $\delta_e := \eta^e + \eta^{-e} + \eta^{qe} + \eta^{-qe}$. Finally, let a, $u \leq \frac{1}{2}(q-2)$; b, $l \leq \frac{1}{4}(q+s)$; c, $v \leq \frac{1}{4}(q-s)$ and of course $i = \sqrt{-1}$, where a, b, c, l, u and v are all positive integers. Then the ordinary character table of G is as below.

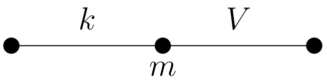
	1	x^a	y^b	z^c	t	f	f^{-1}
1	1	1	1	1	1	1	1
Π	q^2	1	-1	-1	0	0	0
Γ_1	$\frac{s}{2}(q-1)$	0	1	-1	$-\frac{s}{2}$	$\frac{si}{2}$	$-\frac{si}{2}$
Γ_2	$\frac{s}{2}(q-1)$	0	1	-1	$-\frac{s}{2}$	$-\frac{si}{2}$	$\frac{si}{2}$
Ω_u	q^2+1	$\omega^{ua}+\omega^{-ua}$	0	0	1	1	1
Θ_l	$(q-1)(q-s+1)$	0	$-\varepsilon_{lb}$	0	$s-1$	-1	-1
Λ_v	$(q-1)(q+s+1)$	0	0	$-\delta_{vc}$	$-s-1$	-1	-1

Table 5.4: Character table for $\mathrm{Sz}(q)$

Due to the way $\mathrm{Irr}_k\, G$ is partitioned into blocks, $\mathrm{Ext}^n_G(V, W)$ is zero for most choices of irreducible modules V and W. We will only deal with the cases where it may be nontrivial, so if a particular pair of irreducible modules is not mentioned below then one can safely assume that all extensions between them split.

Case 1: $r \mid q-1$

In this case, the modules with characters Γ_i, θ_i and Λ_i lie in blocks of defect zero and thus are projective. The principal r-block of G consists of two modules, k and V, where k is the trivial module as usual and $\dim V = q^2$. The remaining modules lie alone in blocks of maximal defect and so all Ext groups are known by Proposition 4.3.25. From [15, p. 423], the principal block has Brauer tree with the below shape and exceptionality $m = \frac{r^x-1}{2}$, where r^x is the r-part of $q-1$.



We see that in fact this is the same Brauer tree as for 'case 2' in Section 5.4, and so we already know the answer for the principal block. Specialising Proposition 5.4.2, we obtain the following result.

Proposition 5.5.1

Let V be the nontrivial irreducible module lying in the principal block. Then $V = V^*$, thus $\mathrm{H}^n(G,V) \cong \mathrm{Ext}^n_G(V,k)$, for all n and

$$\mathrm{H}^n(G,k) \cong \mathrm{Ext}^n_G(V,V) \cong \begin{cases} 0 & n \equiv 1,\, 2 \mod 4, \\ k & n \equiv 0,\, 3 \mod 4, \end{cases} \qquad \mathrm{H}^n(G,V) \cong \begin{cases} k & n \equiv 1,\, 2 \mod 4, \\ 0 & n \equiv 0,\, 3 \mod 4. \end{cases}$$

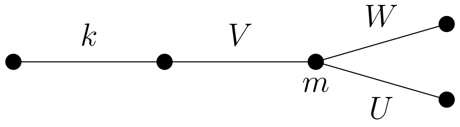
The following result is immediate from Proposition 4.3.25.

Proposition 5.5.2

Let W be any non-projective irreducible module outside the principal block (so W has character Ω_i for some i). Then $\mathrm{Ext}^n_G(W,W) \cong k$ for all n.

Case 2: $r \mid q-s+1$

In this case, the modules with characters Ω_i and θ_i are projective and the principal r-block of G contains 4 modules k, U, V and W. Here, $V \cong \mathcal{HL}$ (where $\mathcal{L}$ is the permutation module of G acting on some Borel subgroup of G as usual) has dimension $q^2 - 1$ and $U \cong W^*$ each have dimension $\frac{s}{2}(q-1)$. The remaining modules lie alone in blocks of maximal defect. From [15, p. 424], the Brauer tree for the principal r-block of G is as below with exceptionality $m = \frac{r^x - 1}{4}$ where r^x is the r-part of $q - s + 1$.



From this, we see that the projective modules in the principal block are as follows: $\mathcal{P}(k) \cong \mathcal{L} \sim [k \mid V \mid k]$, $\mathcal{P}(U) \sim [U \mid W \mid V \mid U \mid \ldots \mid V \mid U]$, $\mathcal{P}(W) \sim [W \mid V \mid U \mid W \mid \ldots \mid V \mid U \mid W]$ and $\mathcal{H}\mathcal{P}(V) \cong k \oplus X_V$ where $X_V \sim [U \mid W \mid V \mid \ldots \mid U \mid W]$.

Theorem 5.5.3

The value of $\mathrm{Ext}^n_G(M, N)$, for M, N in the principal r-block of G, is nonzero for precisely the values of n modulo 8 given in the below table. Here, the entry in row M, column N gives the values of n modulo 8 for which $\mathrm{Ext}^n_G(M, N) \cong k$.

	k	U	V	W
k	0, 7	2, 3	1, 6	4, 5
U	4, 5	0, 7	3, 6	1, 2
V	1, 6	1, 4	0, 2, 5, 7	3, 6
W	2, 3	5, 6	1, 4	0, 7

The proof of Theorem 5.5.3 is best split into two, thus it is given as the combination of the following two propositions.

Proposition 5.5.4

The dimensions of $\mathrm{Ext}^n_G(M, N)$ are as in the table in Theorem 5.5.3 for $(M, N) \in \{k, U, V, W\}^2 \setminus \{(V, V)\}$.

Proof: Throughout, the reader should refer to the structure of the projective modules given before Theorem 5.5.3. We proceed in the usual way, examining the structure of $\Omega^n k$.

Let X_U and X_W denote $\mathcal{H}\mathcal{P}(U)$ and $\mathcal{H}\mathcal{P}(W)$, respectively, and note that $\operatorname{head} X_U \cong W$, $\operatorname{head} X_V \cong U$ and $\operatorname{head} X_W \cong V$. Where $\operatorname{head} \Omega^n V$ is simple, the structure of $\Omega^{n+1} V$ may be immediately read off from the shape of $\mathcal{P}(\Omega^n V)$.

First, note that Ωk has shape $[V \mid k]$ and thus $\Omega^2 k$ must have shape $[X_V \mid V]$. Then $\Omega^3 k \cong U$ and so $\Omega^4 k \cong \Omega U$ has shape $[X_U \mid U]$. This then immediately gives $\Omega^5 k \cong W$, leading to $\Omega^6 k \cong \Omega W$ with shape $[X_W \mid W]$. Finally, this gives $\Omega^7 k$ of shape $[k \mid V]$ and thus $\Omega^8 k \cong k$, so as in the previous case we see that k, U and W are periodic of period 8. By examining the heads of these modules (and using the fact that $\operatorname{Ext}^n_G(M, N) \cong \operatorname{Ext}^n_G(N^*, M^*)$) we obtain the desired result. ■

Proposition 5.5.5

The dimensions of $\operatorname{Ext}^n_G(V, V)$ are as in the table in Theorem 5.5.3. In particular, $\operatorname{Ext}^n_G(V, V) \cong k$ precisely when $n \equiv 0$, 2, 5 or 7 $\mod 8$.

Proof: As with the previous case, we examine the structure of $\Omega^n V$ while referring continually to the structure of the projective modules given before Theorem 5.5.3. We first provide the shapes of $\Omega^n V$ for $n = 1, \ldots, 8$.

$$\begin{array}{llllllll}
\Omega V \sim & \begin{array}{c} k \oplus X_V \\ V \end{array} & \Omega^2 V \sim & \begin{array}{c} V \\ k \oplus U \end{array} & \Omega^3 V \sim & X_U & \Omega^4 V \sim & \begin{array}{c} U \\ W \end{array} \\
\Omega^5 V \sim & X_W & \Omega^6 V \sim & \begin{array}{c} k \oplus W \\ V \end{array} & \Omega^7 V \sim & \begin{array}{c} X_W \\ k \oplus W \end{array} & \Omega^8 V \cong & V
\end{array}$$

The cases where $\Omega^{n-1} V$ has a simple head may be read off directly from the structure of its projective cover.

For $\Omega^2 V$, note that the V in $\operatorname{soc} \Omega V$ must come from a diagonal submodule of $\mathcal{H}\mathcal{L} \oplus \operatorname{soc} X_U$ in $\mathcal{L} \oplus \mathcal{P}(U)$. Similarly, for $\Omega^7 V$, the V in $\operatorname{soc} \Omega^6 V$ must come from a diagonal submodule of $\mathcal{H}\mathcal{L} \oplus \operatorname{head} X_W$ in $\mathcal{L} \oplus \mathcal{P}(W)$. The result then follows by examining the heads of the above modules. ■

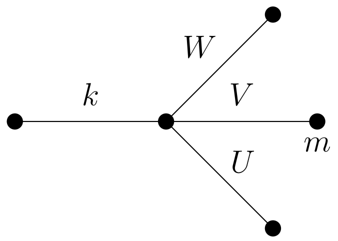
Proposition 5.5.6

For all non-projective irreducible modules M outside of the principal block (these are the modules with characters Λ_i), we have $\mathrm{Ext}^n_G(M, M) \cong k$ for all n.

Proof: This is a direct consequence of Proposition 4.3.25. ■

Case 3: $r \mid q + s + 1$

In this final case for the Suzuki groups, the modules with characters Ω_i and Λ_i are projective and the principal r-block of G contains 4 simple modules: k, U, V and W where $U^* \cong W$, $\dim U = \dim W = \frac{s}{2}(q-1)$ and $\dim V = (q-1)(q-s+1)$. The remaining modules lie alone in blocks of maximal defect as before. From [15, p. 423], the principal block has the below Brauer tree with exceptionality $m = \frac{r^x-1}{4}$ where r^x is the r-part of $q + s + 1$.



Using this, we see that $\mathcal{P}(k) \sim [k \mid U \mid V \mid W \mid k]$, $\mathcal{P}(U) \sim [U \mid V \mid W \mid k \mid U]$ and $\mathcal{P}(W) \sim [W \mid k \mid U \mid V \mid W]$. Finally, $\mathcal{P}(V)$ is not uniserial but has heart $X \oplus Y$ where $X \sim [W \mid k \mid U]$ and $Y \sim [V \mid V \mid \ldots \mid V]$ is a uniserial 'stack of Vs,' containing V as a composition factor with multiplicity $m-1$.

Theorem 5.5.7

In the same notation as Theorem 5.5.3, we have that $\mathrm{Ext}^n_G(M, N) \cong k$ for $n \mod 8$ as below for M, N in the principal block provided $m \neq 1$, *i.e.* the r-part of $q + s + 1$ is not 5.

	k	U	V	W
k	0, 7	1, 2	3, 4	5, 6
U	5, 6	0, 7	1, 2	3, 4
V	3, 4	5, 6	all	1, 2
W	1, 2	3, 4	5, 6	0, 7

When the r-part of $q+s+1$ is 5, we instead have $\mathrm{Ext}_G^n(V,V) \cong k$ for $n \equiv 3,\ 4 \mod 8$ and is zero otherwise.

The proof of Theorem 5.5.7 is, as in the previous case, best done in two parts and so the proof is given by the combination of the next two propositions.

Proposition 5.5.8

The dimensions of $\mathrm{Ext}_G^n(M,N)$ are as in Theorem 5.5.7 for $(M,N) \in \{k,\ U,\ V,\ W\}^2 \setminus \{(V,V)\}$. Further, when the r-part of $q+s+1$ is 5, $\mathrm{Ext}_G^n(V,V) \cong k$ for $n \equiv 3,\ 4 \mod 8$ and is zero otherwise.

Proof: We proceed as usual, by investigating the structure of $\Omega^n k$ and referring frequently to the structure of the projective modules as given before Theorem 5.5.7. As most of the projective modules are uniserial in this case, we may read off the structure of $\Omega^n k$ immediately for each n.

Doing this, one sees that $\Omega k \sim [U \mid V \mid W \mid k]$ and so $\Omega^2 k \cong U$. Then $\Omega^3 k \cong \Omega U \sim [V \mid W \mid k \mid U]$ onto which $\mathcal{P}V$ surjects with kernel $\Omega^4 k \sim [Y \mid V]$. This is again covered by $\mathcal{P}(V)$ with kernel $\Omega^5 k \sim [W \mid k \mid U \mid V]$, and then of course $\Omega^6 k \cong W$, so $\Omega^7 k \cong \Omega W \sim [k \mid U \mid V \mid W]$. Finally, we see that $\Omega^8 k \cong k$ and thus k, U and W are periodic modules of period 8. The result follows by noting where various modules occur in the head of $\Omega^n k \cong \Omega^{n-2} U \cong \Omega^{n-6} W$. Finally, to obtain $\mathrm{Ext}_G^n(V,k)$ we simply note that $\mathrm{Ext}_G^n(V,k) \cong \mathrm{Ext}_G^n(k^*,V^*) \cong \mathrm{H}^n(G,V)$ with similar results for $\mathrm{Ext}_G^n(V,U)$ and $\mathrm{Ext}_G^n(V,W)$.

To derive the result when the r-part of $q+s+1$ is 5, note that in this case we have $m=1$ and so $Y=0$. Replacing Y by 0 in the above calculations then yields the required result, since $\Omega^4 k \cong V$ ■

Proposition 5.5.9

Suppose that the r-part of $q+s+1$ is not 5. Then $\mathrm{Ext}_G^n(V,V) \cong k$ for all n.

Proof: We prove this by investigating the structure of $\Omega^n V$. As usual, the reader should refer frequently to the structure of the projective modules as given before Theorem 5.5.7.

The shapes of $\Omega^n V$ for $n \leq 4$ are given below as radical factors. Recall that Y is uniserial with composition factors $m-1 \neq 0$ copies of V.

$$\Omega V \sim \begin{array}{c} W \oplus Y \\ k \\ U \\ \quad V \end{array} \qquad \Omega^2 V \sim \begin{array}{c} W \oplus V \\ k \oplus W \\ U \\ V \end{array} \qquad \Omega^3 V \sim \begin{array}{c} k \oplus V \\ U \oplus W \oplus Y \end{array} \qquad \Omega^4 V \sim \begin{array}{c} V \oplus k \\ W \oplus U \\ k \oplus V \end{array}$$

The structure of ΩV is clear from the structure of $\mathcal{P}(V)$. For the remainder, we must see how $\Omega^{n-1}V$ appears as a quotient of $\mathcal{P}(\Omega^{n-1}V) \cong \mathcal{P}(\operatorname{head} \Omega^{n-1}V)$.

To find $\Omega^2 V$, note that we must have $\mathcal{P}(W) \twoheadrightarrow [W \mid k \mid U]$ and $\mathcal{P}(V) \twoheadrightarrow Y$, but the final copy of V in $\operatorname{soc} \Omega V$ may then be covered by either projective. Indeed, the particular extension of V seen in ΩV may be regarded as a diagonal submodule of $\operatorname{soc} Y \cong V$ in $\mathcal{P}(V)$ and the copy of V in $\mathcal{P}(W)$. Taking the kernel from this covering gives $\Omega^2 V$ as seen above.

Similarly, for $\Omega^3 V$, we again require $\mathcal{P}(W) \twoheadrightarrow [W \mid k \mid U]$ and this time $\mathcal{P}(V)$ must cover $[V \mid W]$. The extension of V from $\operatorname{soc} \Omega^2 V$ may then be regarded as a diagonal submodule of $\operatorname{head} Y$ in $\mathcal{P}(V)$ and the copy of V in $\mathcal{P}(W)$. The kernel of this covering then gives $\Omega^3 V$ as above.

Given the shape of $\Omega^3 V$, a projective covering of this must have $\mathcal{P}(k) \twoheadrightarrow [k \mid U]$ and $\mathcal{P}(V) \twoheadrightarrow [V \mid W \oplus Y / \operatorname{soc} Y]$. We then have a diagonal submodule of $V \oplus \operatorname{soc} Y$ in $\mathcal{P}(k) \oplus \mathcal{P}(V)$. This gives $\Omega^4 V$ as above.

We also have the following:

$$\Omega^5 V \sim \begin{array}{c} V \oplus U \\ W \oplus \operatorname{rad} Y \\ k \oplus V \end{array} \qquad \Omega^6 V \sim \begin{array}{c} V \oplus U \\ W \oplus V \\ k \\ U \end{array} \qquad \Omega^7 V \sim \begin{array}{c} V \\ W \\ k \oplus Y \\ U \end{array} \qquad \Omega^8 V \cong V.$$

To obtain $\Omega^5 V$, we again note that $\mathcal{P}(k)$ must cover $[k \mid U]$ and $\mathcal{P}(V)$ must cover $[V \mid W \mid k]$

and take a diagonal submodule of $V \oplus \operatorname{head} Y$ in $\mathcal{P}(k) \oplus \mathcal{P}(V)$. Similarly for $\Omega^6 V$ we must have that $\mathcal{P}(U)$ must cover U and $\mathcal{P}(V)$ must cover the remainder, and we take a diagonal submodule of $V \oplus \operatorname{soc} Y$ from $\mathcal{P}(U) \oplus \mathcal{P}(V)$ to account for the extension between V and $U \oplus V$ in $\operatorname{soc} \Omega^5 V$.

Next, we must have $\mathcal{P}(U) \twoheadrightarrow U$ and $\mathcal{P}(V) \twoheadrightarrow [V \mid W \mid k \mid U]$ in $\Omega^6 V$ and we require a diagonal submodule of $V \oplus \operatorname{head} Y$ in $\mathcal{P}(U) \oplus \mathcal{P}(V)$ to account for the diagonal extension between V and $V \oplus U$ in $\Omega^6 V$. This gives $\Omega^7 V$ as seen above, and finally $\Omega^8 V \cong V$ as $\Omega^7 V \sim \mathcal{P}(V)/V$.

We therefore see that V is also periodic of period 8. The result then follows from the fact that V is present precisely once in $\operatorname{head} \Omega^n V$ for all n. ■

Finally for this case, the following result is a direct consequence of Proposition 4.3.25.

Proposition 5.5.10

Let M be any non-projective irreducible kG-module outside of the principal block (then M has character Θ_i for $(q+s+1)_{r'} \nmid i$). Then $\operatorname{Ext}^n_G(M, M) \cong k$ for all n.

BIBLIOGRAPHY

[1] J. L. Alperin. *Local Representation Theory.* Cambridge University Press, 1993.

[2] J. L. Alperin. Periodicity in groups. *Illinois Journal of Mathematics* 21.4 (1977), pp. 776–783.

[3] M. Aschbacher. *Finite Group Theory.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2000.

[4] M. Aschbacher and R. M. Guralnick. Some applications of the first cohomology group. *Journal of Algebra* 90.2 (1984), pp. 446–460.

[5] I. Assem and S. Trepode. *Homological Methods, Representation Theory, and Cluster Algebras.* Springer, 2018.

[6] D. J. Benson. *Representations and Cohomology: Volume 1, Basic Representation Theory of Finite Groups and Associative Algebras.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1991.

[7] D. J. Benson. *Representations and Cohomology: Volume 2, Cohomology of Groups and Modules.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1998.

[8] C. Bonnafé. *Representations of* $\mathrm{SL}_2(\mathbb{F}_q)$. Springer, 2010.

[9] R. Brauer. Investigations on group characters. *Annals of Mathematics* 42.4 (1941), pp. 936–958.

[10] J. N. Bray, D. F. Holt, and C. M. Roney-Dougal. *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*. London Mathematical Society Lecture Note Series. Cambridge University Press, 2013.

[11] J. N. Bray and R. A. Wilson. Examples of 3-dimensional 1-cohomology for absolutely irreducible modules of finite simple groups. *Journal of Group Theory* 11.5 (2008), pp. 669–673.

[12] T. Breuer, R. M. Guralnick, A. Lucchini, A. Maróti, and G. P. Nagy. Hamiltonian cycles in the generating graphs of finite groups. *Bulletin of the London Mathematical Society* 42.4 (2010), pp. 621–633.

[13] K. S. Brown. *Cohomology of Groups*. Graduate Texts in Mathematics. Springer, 1982.

[14] R. Burkhardt. Die Zerlegungsmatrizen der Gruppen $\mathrm{PSL}(2, p^f)$. *Journal of Algebra* 40.1 (1976), pp. 75–96.

[15] R. Burkhardt. Über die Zerlegungszahlen der Suzukigruppen $\mathrm{Sz}(q)$. *Journal of Algebra* 59.2 (1979), pp. 421–433.

[16] P. J. Cameron. *Permutation groups*. London Mathematical Society Student Texts. Cambridge University Press, 1999.

[17] R. W. Carter. *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*. Wiley Classics Library. Wiley, 1993.

[18] R. W. Carter. *Simple Groups of Lie Type*. Wiley, 1989.

[19] E. T. Cline, B. J. Parshall, and L. L. Scott. Reduced standard modules and cohomology. *Transactions of the American Mathematical Society* 361.10 (2009), pp. 5223–5261.

[20] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*. Clarendon Press, 1985.

[21] D. A. Craven. *Representation Theory of Finite Groups: a Guidebook*. Springer, 2019.

[22] C. W. Curtis and I. Reiner. *Methods of Representation Theory: With Applications to Finite Groups and Orders*. Vol. 1. Pure and Applied Mathematics. Wiley, 1981.

[23] C. W. Curtis and I. Reiner. *Methods of Representation Theory: With Applications to Finite Groups and Orders*. Vol. 2. Pure and Applied Mathematics. Wiley, 1987.

[24] C. W. Curtis and I. Reiner. *Representation Theory of Finite Groups and Associative Algebras*. American Mathematical Society, 1966.

[25] E. C. Dade. Blocks with cyclic defect groups. *Annals of Mathematics* 84.1 (1966), pp. 20–48.

[26] L. E. Dickson. *Linear Groups*. BG Teubner Leipzig, 1901.

[27] J. D. Dixon. The probability of generating the symmetric group. *Mathematische Zeitschrift* 110.3 (1969), pp. 199–205.

[28] P. W. Donovan and M. R. Freislich. The indecomposable modular representations of certain groups with dihedral Sylow subgroup. *Mathematische Annalen* 238.3 (1978), pp. 207–216.

[29] L. Dornhoff. *Group Representation Theory. Part A, Ordinary Representation Theory*. Monographs and Textbooks in Pure and Applied Mathematics. M. Dekker, 1971.

[30] C. W. Eaton, F. Eisele, and M. Livesey. Donovan's conjecture, blocks with abelian defect groups and discrete valuation rings. *Mathematische Zeitschrift* (2019), pp. 1–16.

[31] S. Eilenberg and S. MacLane. Cohomology theory in abstract groups II: group extensions with a non-abelian kernel. *Annals of Mathematics* 48.2 (1947), pp. 326–341.

[32] K. Erdmann. *Blocks of Tame Representation Type and Related Algebras*. Springer, 2006.

[33] W. Feit. *The Representation Theory of Finite Groups*. Elsevier, 1982.

[34] P. Fong and R. J. Milgram. On the geometry and cohomology of the simple groups $\mathrm{G}_2(q)$ and $^3\mathrm{D}_4(q)$. *Group Representations: Cohomology, Group Actions, and Topology: Summer Research Institute on Cohomology, Representations, and Actions of Finite Groups, July 7-27, 1996, University of Washington, Seattle* 63 (1998), p. 221.

[35] D. Gorenstein. *Finite Groups.* AMS Chelsea Publishing Series. American Mathematical Society, 2007.

[36] D. Gorenstein, R. Lyons, and R. Solomon. *The Classification of the Finite Simple Groups, Number 3.* Mathematical Surveys and Monographs. American Mathematical Society, 1998.

[37] R. M. Guralnick. "The dimension of the first cohomology group". *Representation Theory II Groups and Orders.* Springer, 1986, pp. 94–97.

[38] R. M. Guralnick and C. G. Hoffman. "The first cohomology group and generation of simple groups". *Groups and Geometries.* Springer, 1998, pp. 81–89.

[39] R. M. Guralnick, W. M. Kantor, M. Kassabov, and A. Lubotzky. Presentations of finite simple groups: profinite and cohomological approaches. *Groups, Geometry, and Dynamics* 1.4 (2007), pp. 469–523.

[40] R. M. Guralnick and P. H. Tiep. First cohomology groups of Chevalley groups in cross characteristic. *Annals of Mathematics* 174.1 (July 2011), pp. 543–559.

[41] R. M. Guralnick and P. H. Tiep. Low-dimensional representations of special linear groups in cross characteristics. *Proceedings of the London Mathematical Society* 78.1 (1999), pp. 116–138.

[42] R. M. Guralnick and P. H. Tiep. Sectional rank and cohomology. *Journal of Algebra* (2019), To appear.

[43] R. M. Guralnick and P. H. Tiep. Sectional rank and Cohomology II (2020). arXiv: 2005.02543 [math.GR].

[44] A. Heller. Indecomposable representations and the loop-space operation. *Proceedings of the American Mathematical Society* 12.4 (1961), pp. 640–643.

[45] P. J. Hilton and U. Stammbach. *A Course in Homological Algebra.* Graduate Texts in Mathematics. Springer-Verlag, 1971.

[46] J. E. Humphreys. *Linear Algebraic Groups.* Graduate Texts in Mathematics. Springer, 2012.

[47] I. M. Isaacs. *Character theory of finite groups.* Courier Corporation, 1994.

[48] W. M. Kantor and A. Lubotzky. The probability of generating a finite classical group. *Geometriae Dedicata* 36.1 (Oct. 1990), pp. 67–87.

[49] G. Karpilovsky. *Group Representations.* Vol. 4. Elsevier, 1995.

[50] R. Kessar and G. Malle. Local-global conjectures and blocks of simple groups. *Groups St Andrews 2017 in Birmingham* 455 (2019), p. 70.

[51] P. B. Kleidman and M. W. Liebeck. *The Subgroup Structure of the Finite Classical Groups.* Cambridge University Press, 1990.

[52] A. W. Knapp. *Basic Algebra.* Springer, 2006.

[53] S. Lang. *Algebra.* Addison-Wesley, 1965.

[54] M. W. Liebeck and A. Shalev. Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky. *Journal of Algebra* 184.1 (1996), pp. 31–57.

[55] M. W. Liebeck and A. Shalev. The probability of generating a finite simple group. *Geometriae Dedicata* 56.1 (June 1995), pp. 103–113.

[56] F. Lübeck. Computation of Kazhdan–Lusztig polynomials and some applications to finite groups. *Transactions of the American Mathematical Society* 373 (2020), pp. 2331–2347.

[57] A. Lubotzky. Pro-finite presentations. *Journal of Algebra* 242.2 (2001), pp. 672–690.

[58] A. Lucchini and A. Maróti. On the clique number of the generating graph of a finite group. *Proceedings of the American Mathematical Society* 137.10 (2009), pp. 3207–3217.

[59] A. Lucchini and A. Maróti. Some results and questions related to the generating graph of a finite group. *Ischia Group Theory 2008* (2009), pp. 1–4.

[60] A. Lucchini, A. Maróti, and C. M. Roney-Dougal. On the generating graph of a simple group. *Journal of the Australian Mathematical Society* 103.1 (2017), pp. 91–103.

[61] G. Malle and D. Testerman. *Linear Algebraic Groups and Finite Groups of Lie Type*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2011.

[62] N. E. Menezes, M. Quick, and C. M. Roney-Dougal. The probability of generating a finite simple group. *Israel Journal of Mathematics* 198.1 (2013), pp. 371–392.

[63] A. E. Parker and D. I. Stewart. First cohomology groups for finite groups of Lie type in defining characteristic. *Bulletin of the London Mathematical Society* 46.2 (2013), pp. 227–238.

[64] J. P. Saunders. Cohomology of $\mathrm{PSL}_2(q)$ (2020). arXiv: `2002.04183 [math.RT]`.

[65] J. P. Saunders. Maximal cocliques in $\mathrm{PSL}_2(q)$. *Communications in Algebra* 47.10 (2019), pp. 3921–3931.

[66] L. L. Scott. Some new examples in 1-cohomology. *Journal of Algebra* 260.1 (2003), pp. 416–425.

[67] J. G. Thompson. Vertices and sources. *Journal of Algebra* 6.1 (1967), pp. 1–6.

[68] C. A. Weibel. *An Introduction to Homological Algebra*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1995.

[69] R. A. Wilson. *The Finite Simple Groups*. Graduate Texts in Mathematics. Springer London, 2012.