Classification Problems for Finite Linear Groups

Hurley, Barry

2013-03-08

http://hdl.handle.net/10379/3498
Classification Problems for Finite Linear Groups

Barry Hurley

Ollscoil na hÉireann, Gaillimh
National University Of Ireland, Galway

Supervised by: Dr. Dane Flannery

Eanáir 2012
Coimriú

Is é an chloch is mó ar ár bpaidrín sa tráchtas seo ná grúpaí de chéim príomha, agus grúpaí atá sainmhínithe thar réimsí críochta. Má tá $q = p^a$ do $p$ príomha agus $a \in \mathbb{Z}^+$, tógaimid liosta d’fhoghrúpaí dolaghdaíthe dothuaslagtha de GL$(3, q)$ inar fior an méid seo a leanas:

- tá gach grúpa tugtha ag tacar giniúna paraiméadraithe de mhaitríseí
- níl grúpaí difríula ar an liosta comhchuingeach in GL$(3, q)$, agus
- foghrúpa dothuaslagtha dolaghdaíthe ar bith de GL$(3, q)$,
  tá sé GL$(3, q)$-chomhchuingeach le grúpa (amháin) ar an liosta.

Contents

1 Introduction  
   1.1 Outline  
   1.2 General approach  
   1.3 Implementation  

2 Preliminaries  
   2.1 Group extensions and cohomology  
   2.2 Some linear group theory  
      2.2.1 Basic terms  
      2.2.2 Actions on the underlying space  
   2.3 Fundamentals for the classification of linear groups  
   2.4 Linear group classification  
      2.4.1 The isomorphism question  
      2.4.2 The SL-transfer  
   2.5 Changing the field  
   2.6 Linear groups of prime degree  
   2.7 Congruence homomorphisms  

3 Finite linear groups of degree two  

4 Order conditions for finite matrix groups  
   4.1 Introduction to Blichfeldt-Dixon methods  
   4.2 The Blichfeldt-Dixon criterion for normality of Sylow subgroups  
   4.3 Existence of elements of composite order in finite linear groups  

5 Insoluble non-modular linear groups of degree three  
   5.1 Bounding group orders in degree 3  

1
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.2 Table of insoluble irreducible subgroups of $\text{GL}(3, q)$</td>
<td>120</td>
</tr>
<tr>
<td>8.2.3 Sample results</td>
<td>120</td>
</tr>
<tr>
<td>A Notation and terminology</td>
<td>124</td>
</tr>
<tr>
<td>A.1 Notation</td>
<td>124</td>
</tr>
<tr>
<td>A.2 Terminology</td>
<td>127</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>130</td>
</tr>
<tr>
<td>Bibliography</td>
<td>131</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

This thesis is concerned with classification problems for finite linear groups. Our main concern is with groups of prime degree, and groups defined over finite fields and fields of zero characteristic.

We provide a glossary of basic notation and terminology in Appendix A. In this thesis, omitted proofs are either well-known, or considered to be straightforward.

1.1 Outline

A major objective of the thesis is to classify completely, irredundantly, and explicitly, the insoluble irreducible subgroups of GL(3, q), for a prime power q. In other words, we will construct a list of irreducible insoluble subgroups of GL(3, q) in which

- each group is given by a parametrised generating set of matrices,
- different groups in the list are not conjugate in GL(3, q), and
- any insoluble irreducible subgroup of GL(3, q) is GL(3, q)-conjugate to a (single) group in the list.

This will also include a solution of the listing problem for the finite insoluble irreducible subgroups of GL(3, F) where F is any field of positive characteristic.

The computational algebra system MAGMA [4] has facilities for listing the irreducible subgroups of GL(2, q), and the irreducible soluble subgroups of GL(3, q); this is work by Flannery and O’Brien [11]. The results of this thesis complete the classification of irreducible subgroups of GL(n, q) for n < 4 and almost all characteristics.
1.2. GENERAL APPROACH

We also consider miscellaneous related topics: listings of the finite subgroups of $GL(n, \mathbb{F})$ for various fields $\mathbb{F}$ of characteristic zero and $n \leq 3$, and listing finite irreducible soluble subgroups of $GL(n, \mathbb{F})$ for prime $n$ and real fields $\mathbb{F}$.

As outlined above, by ‘classification’ we refer to the most exhaustive kind of classification that one could expect regarding linear groups – namely, by linear isomorphism (conjugacy in the ambient general linear group). While many classifications of linear groups have been obtained over the years, few are of this exhaustive type. The amount of work involved in extracting this sort of information from known lists of groups in the relevant projective special or general linear group is considerable.

We begin by providing some preliminary background material, which includes basic cohomology and linear group concepts. The next chapter gives an outline of the finite linear groups of degree 2. Some of the methods used recur in the degree 3 case; however, these cases are very different. Our solution for the degree 3 case is broken up into two parts: the non-modular groups and the modular groups. We start the degree 3 case by recalling methods in that degree over the field $\mathbb{C}$ introduced by Blichfeldt [2, 25]; these were (much later) generalised by Dixon [5]. We combine their arguments to give a fully modernised, self-contained and complete account of the finite irreducible insoluble linear groups of degree 3 over a non-modular field. Along the way, we obtain results applicable to other degrees and fields. In Chapter 6, we complete the listing of groups in the modular case and give the corresponding matrix generating sets. Here we recall and expand on results of Bloom [3], Feit [7] and Hartley [14]. In the penultimate chapter, we present a solution of the listing problem for the finite groups of degrees 2 and 3 over certain characteristic zero fields and rings of algebraic integers. This chapter applies some results and general methods of the previous chapters.

1.2 General approach

Let $G$ be an irreducible subgroup of $GL(n, q)$. Then $G$ is completely reducible over the algebraic closure $\mathbb{F}_q$ of $GF(q)$, with $\mathbb{F}_q$-irreducible parts of the same degree. Hence if $n$ is prime then $G$ is either abelian or absolutely irreducible. The insoluble irreducible subgroups of $GL(3, q)$ are therefore absolutely irreducible. Furthermore, such a group must be primitive over $GF(q)$ and $\mathbb{F}_q$, because otherwise it would be monomial (again using that the degree is prime), and a monomial linear group of degree less than 5 is soluble.

We begin by solving the listing problem over $\mathbb{F}_q$. The list over $GF(q)$ is then obtained by determining (using trace calculations) the groups over $\mathbb{F}_q$ that have conjugates in $GL(n, q)$,
and then rewriting those over GF(q). In practice, it is possible to carry out the latter task using the algorithm of Glasby and Howlett [12] for writing a finite absolutely irreducible group over a minimal field.

The classification of finite linear groups is a classical problem in group theory and early results go back to the very beginning of the subject. Much of the literature here deals with the groups over the complex field $\mathbb{C}$. To avail of the classical results in our attempt to list groups over finite fields, we can use a ‘reduction mod $p$’ homomorphism (also known as a congruence homomorphism, or Minkowski homomorphism) to ‘lift’ groups from positive to zero characteristic. The next two theorems and discussion give a flavour of the basic ideas.

**Theorem 1.2.1.** ([5], 3.4B, p.54) Let $G$ be a finite irreducible subgroup of $\text{GL}(n, \mathbb{C})$. Then $G$ is conjugate to a subgroup of $\text{GL}(n, F)$ for some algebraic number field $F$.

Let $G = \langle g_1, \ldots, g_r \rangle$ be a finite subgroup of $\text{GL}(n, \mathbb{C})$. We may assume $G \leq \text{GL}(n, \mathbb{F})$ where $\mathbb{F}$ is the number field of fractions of some integral domain $R$ (and so $R$ is the ring of integers of $\mathbb{F}$). Let $S$ denote the ring of fractions with denominators in the submonoid of $R$ generated by the denominators of the generators $g_i \in G$. Then $S$ is a finitely generated Dedekind domain. Note that $G \leq \text{GL}(n, S)$. Select a prime $p \in \mathbb{Z}$ where $p \neq 2$. Let $K$ be a maximal (i.e. proper prime) ideal of $S$ containing $p$ but not containing $2$, such that $p \notin K^2$. Let $f$ denote the natural epimorphism $S \to S/K$, extended entry-wise to $\text{GL}(n, S)$; thus $f$ maps $G$ into some $\text{GL}(n, \mathbb{F}_q)$. Moreover, under the conditions imposed on $K$, the kernel of $f$ is torsion-free. Thus any finite subgroup of $\text{GL}(n, \mathbb{C})$ is isomorphic to a linear group over a finite field. The converse is also true, with an extra proviso.

**Theorem 1.2.2.** ([5], 3.8, p.62) Let $G$ be a finite irreducible subgroup of $\text{GL}(n, \mathbb{F}_q)$. If $G$ has order co-prime to $q$ then $G$ is isomorphic (via a congruence homomorphism) to an irreducible subgroup of $\text{GL}(n, \mathbb{C})$.

To list the groups that can be ‘lifted’ (via the inverse of a congruence homomorphism) from positive to zero characteristic, we use the list of finite irreducible subgroups of $\text{SL}(3, \mathbb{C})$ with simple central quotient, given by Blichfeldt [2, 25]. We can transfer from $\text{SL}(3, \mathbb{C})$ to $\text{GL}(3, \mathbb{C})$ using adjunction of scalars. That is, if $G \leq \text{GL}(n, \mathbb{F})$ is insoluble irreducible, where $\mathbb{F}$ is algebraically closed, then there exists $H \leq \text{SL}(n, \mathbb{F})$ such that $H$ is insoluble irreducible, $HZ = GZ$ where $Z$ is the scalar subgroup of $\text{GL}(n, \mathbb{F})$, and $G/Z(G)$ is isomorphic to $H/Z(H)$. Also, $H$ is finite if $G$ is finite.

The next theorem characterises the groups that can be lifted.

**Theorem 1.2.3.** ([25]) Let $G$ be a finite insoluble primitive subgroup of $\text{GL}(3, \mathbb{C})$. Then $G/Z(G)$ is isomorphic to one of the following: $\text{Alt}(5)$, $\text{Alt}(6)$, $\text{PSL}(2, 7)$. Conversely, a
finite subgroup of $GL(3, \mathbb{C})$, with central quotient isomorphic to one of $Alt(5)$, $Alt(6)$ or $PSL(2, 7)$, is an insoluble primitive subgroup of $GL(3, \mathbb{C})$.

For the modular groups, a list of the abstract isomorphism types of central quotients is available in [3]. For all groups, there is also the separate issue of obtaining generating sets for listed groups, which we handle by ad hoc methods. The completion of the listing problem then involves

- solving central extension problems (i.e., given a finite abelian group $A$, and a finite group $B$, determine all groups $G$ containing $A$ as a central subgroup and such that $G/A \cong B$);

- solving the conjugacy problem in $GL(3, q)$, i.e., eliminating all $GL(3, q)$-conjugacy between groups in the final list.

We point out that, in general, the concepts of ‘non-modular’ and ‘liftable’ are not equivalent; we see this in the degree 3 case later in the thesis.

1.3 Implementation

We have implemented our lists in Magma. Since the procedures are a direct implementation of a theoretical solution of the classification problem, the computation is mainly field arithmetic (and perhaps some rewriting over smaller fields). A major issue is confirming the veracity of our implementation. Details of this, and some experimental results, are discussed in the final chapter.

We point out that by the nature of our solution of the listing problem, the only limitation in computing is imposed by Magma’s intrinsic functions for (finite) fields. Thus, unlike a direct approach to computing the conjugacy classes of irreducible subgroups of $GL(n, q)$, implementations of complete theoretical solutions to the listing will always be far superior.
Chapter 2

Preliminaries

We assume basic concepts, terminology and notation for groups, vector spaces, modules, algebras, rings and fields, as may be found in a text such as [24]. We also assume basic familiarity with ordinary character theory, as may be found in [17, Chapters 2 & 3]. The purpose of this chapter is to introduce some foundational results upon which we will build later in the thesis.

2.1 Group extensions and cohomology

We restrict our discussion to the case of central extensions. Let $G$ be a finite group and $C$ a finite abelian group. The set of all cocycles $G \times G \to C$ forms an abelian group $Z^2(G, C)$ under pointwise composition of maps. The set of all coboundaries is a subgroup $B^2(G, C)$ of $Z^2(G, C)$. The quotient $H^2(G, C) = Z^2(G, C)/B^2(G, C)$ is the second cohomology group of $G$ with coefficients in $C$. A coset of $B^2(G, C)$ is called a cohomology class. The cohomology class of $\psi \in Z^2(G, C)$ is denoted $[\psi]$.

Let $\psi \in Z^2(G, C)$ and define the group $E(\psi)$ as follows: the elements of $E(\psi)$ are the pairs $(x, c)$ where $x \in G$ and $c \in C$, and multiplication is $(x, c)(y, b) = (xy, cb\psi(x, y))$. It may be checked that associativity of this multiplication corresponds precisely to the cocycle identity. If $\psi \in B^2(G, C)$, say $\psi(x, y) = \phi(x)\phi(y)\phi(xy)^{-1}$, then $E(\psi)$ splits as the direct product $\{(1, c)\} \times \{(x, \phi(x)^{-1})\} \cong C \times G$. Conversely, suppose that

$$1 \to C \xrightarrow{f_1} E \xrightarrow{f_2} G \to 1$$

is a central short exact sequence, and choose a transversal $t$ for the cosets of $f_1(C)$ in $E$; that is, for each $x \in G$, select $t(x) \in E$ such that $f_2t(x) = x$. Then it may be checked
that the assignment \((x, y) \mapsto t(x)t(y)t(xy)^{-1}\) defines a cocycle \(G \times G \to C\). This cocycle depends on our choice of \(t\), but its cohomology class does not.

The above discussion leads to the following well-known theorem.

**Theorem 2.1.1.** \(|H^2(G, C)|\) is an upper bound on the number of different isomorphism types of central extensions of \(C\) by \(G\).

Now we examine the problem of actually calculating \(H^2(G, C)\). Several methods exist for this; we follow the one in [9].

The Schur multiplier \(H_2(G)\) of a finite group \(G\) is defined to be \(H^2(G, \mathbb{C}^\times)\). As a cohomology group, \(H_2(G)\) is abelian, and it is finite under the assumption that \(G\) is. Hopf’s formula, which we now describe, affords a method for computing \(H_2(G)\). Let \(G = F/R\), where \(F\) is free, and \(R\) is a normal subgroup of \(F\). Then \(R/[R, F]\) is central in \(F/[R, F]\). The quotient \(F/F'\) is a free abelian group of the same rank as \(F\). Since \(RF'/F'\) has finite index in \(F/F'\), \(R/[R, F]\cong RF'/F'\) is also free abelian of rank \(r\).

**Lemma 2.1.2.**

(i) \((R \cap F')/[R, F]\) is finite; in fact, \((R \cap F')/[R, F] \cong H_2(G)\).

(ii) \(R/[R, F]\) is a finitely generated abelian group, with torsion subgroup \((R \cap F')/[R, F]\).

**Proof.** See [19, p. 50, Theorem 2.4.6].

So the finitely generated abelian group \(R/[R, F]\) splits over its torsion subgroup:

\[
R/[R, F] = (R \cap F')/[R, F] \times S/[R, F],
\]

where the complement \(S/[R, F]\) of \((R \cap F')/[R, F] \cong H_2(G)\) in \(R/[R, F]\) is free abelian of rank \(r\).

**Corollary 2.1.3.** Assume the notation above. Then

(i) \(R/S \cong (R \cap F')/[R, F] \cong H_2(G)\).

(ii) \(F/S\) is a central extension of \(R/S \cong H_2(G)\) by \(F/R \cong G\).

(iii) \(R/S\) is contained in the derived subgroup of \(F/S\).

A Schur cover of \(G\) is a group \(E\) with a central subgroup \(M \cong H_2(G)\) such that \(E/M \cong G\) and \(M \leq E'\). The group \(F/S\) in Corollary 2.1.3 is a Schur cover of \(G\). We see that a Schur cover \(E\) definitely never splits over \(M\) if \(M\) is non-trivial; nor is \(E\) abelian if \(M\) is non-trivial. Unlike the multiplier, there may be more than one Schur cover (up to isomorphism) of a given finite group \(G\).
Lemma 2.1.4.  (i) $|H^2(G, H_2(G))|$ is an upper bound on the number of non-isomorphic Schur covers of $G$.

(ii) Another upper bound for the number of non-isomorphic Schur covers of $G$ is $|H^1(G, H_2(G))| = |\text{Hom}(G, H_2(G))| = |\text{Hom}(G/G', H_2(G))|$.

Proof. Part (i) is obvious by Theorem 2.1.1. Part (ii) is due to Schur. □

The bound of part (i) of Lemma 2.1.4 is not tight, as it counts all central extensions $E$ of $H_2(G)$ by $G$ and therefore includes unsuitable groups not satisfying the requirement $H_2(G) \leq E'$ in the definition of Schur cover. Neither is the bound of part (ii) tight.

We next give an overview of the Universal Coefficient theorem, which enables us to calculate $H^2(G, C)$ and thereby gives us a handle on the central extension problem for $C$ and $G$.


$$1 \to R/S \to F/S \to F/R \to 1$$

is a Schur cover of $G$, where the non-trivial maps are inclusion and projection. Let $\psi$ be a cocycle of this central extension. For any abelian group $C$, if we compose $\psi$ with any homomorphism $f : R/S \to C$, we obtain an element $f \circ \psi$ of $Z^2(G, C)$. The Universal Coefficient theorem states that the map from $\text{Hom}(H^2(G, C))$ into $H^2(G, C)$ defined in this way (i.e. $f \mapsto [f \circ \psi]$) is an embedding, and that $H^2(G, C)$ splits over its image. We state the Universal Coefficient theorem in an explicit form, as follows.

Theorem 2.1.5. $H^2(G, C) = I \times T$, where $I \cong \text{Hom}(G/G', C)$ and $T \cong \text{Hom}(H_2(G), C)$ is the image of the embedding $\text{Hom}(H_2(G), C) \hookrightarrow H^2(G, C)$, $f \mapsto [f \circ \psi]$, defined above.

Proof. See [9]. □

We now focus on the case of central extensions whose quotients are perfect groups; this is how insoluble finite linear groups frequently arise.

Lemma 2.1.6. Let $G$ be a finite perfect group. Then there is a single Schur cover $E$ of $G$ up to isomorphism. Moreover, $E$ is perfect.

Proof. Uniqueness of the cover (up to isomorphism) is a consequence of Lemma 2.1.4 (ii). Let $E$ be a Schur cover of $G$, with central subgroup $M \cong H_2(G)$ in $E'$, such that $E/M \cong G$. Now

$$E/M \cong G = G' \cong (E/M)' = E'M/M = E'/M$$

implies that $E = E'$. □
Lemma 2.1.6 allows us to speak of the Schur cover of a finite perfect group.

**Lemma 2.1.7.** If $|G|$ and $|C|$ are coprime then $H^i(G,C) = 0$.

*Proof.* See [19]. □

**Lemma 2.1.8.** Suppose that $G$ is a finite group with centre $Z$ such that $G/Z$ is perfect. Denote by $\tau$ the set of all primes dividing $|H_2(G/Z)|$. Then $G$ splits over $Z_{\tau'}$, the $\tau'$-subgroup of $Z$. That is, $G = H \times Z_{\tau'}$ where $H$ is a normal subgroup of $G$ such that $Z(H) = Z_{\tau}$ and $H/Z_{\tau} \cong G/Z$. The number of possible isomorphism types for $H$ is at most $|\text{Hom}(H_2(G/Z), Z_{\tau})|$. 

*Proof.* By Lemma 2.1.7, we can factor out the cohomology of the normal subgroup $Z/Z_{\tau'}$ of $G/Z_{\tau'}$:

$$H^2(G/Z_{\tau'}, Z_{\tau'}) \cong H^2((G/Z_{\tau'})/(Z/Z_{\tau'}), Z_{\tau'}) \cong H^2(G/Z, Z_{\tau'}).$$

(2.1)

Since $G/Z$ is perfect, we have by the Universal Coefficient theorem (Theorem 2.1.5) that

$$H^2(G/Z, Z_{\tau'}) \cong \text{Hom}(H_2(G/Z), Z_{\tau'}) = 0.$$  

(2.2)

Combining Eqs.(2.1) and (2.2) we get that $H^2(G/Z_{\tau'}, Z_{\tau'}) = 0$. So there is a subgroup $H$ of $G$ such that $G = H \times Z_{\tau'}$. Taking projections onto coordinates in the direct product, we see that $Z_{\tau} \leq Z(H)$. Since a central element of $H$ is central in $G$, it follows that $Z_{\tau} = Z(H)$. Now

$$G/Z = (HZ_{\tau'})/(Z_{\tau}Z_{\tau'}) \cong (HZ_{\tau'}/Z_{\tau'})/(Z_{\tau}Z_{\tau'}/Z_{\tau'}) \cong H/Z_{\tau}.$$ 

The last statement of the lemma is just the Universal Coefficient theorem again, for central extensions (like $H$) of $Z_{\tau}$ by the perfect group $G/Z$. □

**Lemma 2.1.9.** Suppose that $G$ is a finite group with centre $Z$ such that $G/Z$ is perfect. Then there exists a subgroup $U$ of $Z$ isomorphic to a quotient of $H_2(G/Z)$, such that $G$ contains a copy of a central extension $E$ of $U$ by $G/Z$, and $G = EZ$.

*Proof.* In the discussion before Theorem 2.1.5, we indicated how to obtain an isomorphism $\text{Hom}(H_2(G/Z), Z) \to H^2(G/Z, Z)$ by mapping each $f \in \text{Hom}(H_2(G/Z), Z)$ to $[f \circ \psi]$ where $\psi$ is a fixed cocycle for the Schur cover of $G/Z$. We have $G \cong E(f \circ \psi)$ for some $f$. Set $U = \text{im}(f)$. Of course, $U$ is a subgroup of $Z$ isomorphic to $H_2(G/Z)/\ker f$. Moreover, the set of pairs $(x, u)$ where $x \in G/Z$ and $u \in U$ forms a subgroup of $E(f \circ \psi)$, and is a central extension of $U \cong \{(1, u)\}$ by $G/Z$. □

We can replace ‘quotient of $H_2(G/Z)$’ in Lemma 2.1.9 by ‘subgroup of $H_2(G/Z)$’, since, for any finite abelian group $A$ and $B \leq A$, $A/B$ is isomorphic to a subgroup of $A$. 

---

2.1. GROUP EXTENSIONS AND COHOMOLOGY
2.2 Some linear group theory

2.2.1 Basic terms

Let $V$ be the $n$-dimensional vector space over a field $\mathbb{F}$. We write $\text{Mat}(n, \mathbb{F})$ for the $\mathbb{F}$-algebra of all $n \times n$ matrices over $\mathbb{F}$. We treat the elements of $V$ as column vectors with $\text{Mat}(n, \mathbb{F})$ acting on the left.

A linear group of degree $n$ over $\mathbb{F}$ is a subgroup of $\text{GL}(n, \mathbb{F})$. We can also define a linear group to be a subgroup of the group $\text{GL}(V)$ of all invertible $\mathbb{F}$-linear transformations of $V$. It is sometimes useful to distinguish between the two cases by defining the former group as a matrix group. Even more abstractly, a group is said to be linear if it admits a faithful finite-dimensional representation over a field $\mathbb{F}$. According to this definition every finite group is a linear group (via regular permutation representation of the group).

It is straightforward to define an isomorphism from $G \leq \text{GL}(V)$ onto a subgroup of $\text{GL}(n, \mathbb{F})$ after choosing a basis for $V$. Hence it may seem that the choice of basis is significant. However, the effect of changing the basis of $V$ is very easy to describe. Let $\theta_1 : G \to \text{GL}(n, \mathbb{F})$ and $\theta_2 : G \to \text{GL}(n, \mathbb{F})$ be representations of $G$ with respect to any two different bases. Then $\theta_2(g) = \theta_1(g)^A$ for all $g \in G$ and change of basis matrix $A$. $\theta_2$ is the composite of $\theta_1$ with a linear isomorphism, i.e. an isomorphism between subgroups of $\text{GL}(n, \mathbb{F})$ induced by an inner automorphism of $\text{GL}(n, \mathbb{F})$.

2.2.2 Actions on the underlying space

Let $V$ be an $n$-dimensional $\mathbb{F}$-space. The matrix algebra $\text{Mat}(n, \mathbb{F})$ is a faithful representation of the endomorphism algebra of $V$. By restriction, $V$ is a $G$-module for any $G \leq \text{GL}(n, \mathbb{F})$; more properly, $V$ is a module for the $\mathbb{F}$-enveloping algebra $\langle G \rangle_{\mathbb{F}}$ or $\mathbb{F}$-group algebra of $G$. Here, $\langle G \rangle_{\mathbb{F}}$ consists of all (finite) $\mathbb{F}$-linear combinations $\sum_{g \in G} \alpha_g g$ under matrix addition and multiplication and scalar multiplication in $\text{Mat}(n, \mathbb{F})$. Clearly $\langle G \rangle_{\mathbb{F}}$ is an epimorphic image of the group algebra $\mathbb{F}G$.

Each $G$-module $V$ determines a representation $G \to \text{GL}(V)$, and vice versa. The natural way of comparing $G$-modules is by isomorphism. This carries over to a notion of equivalence for $G$-representations.

**Lemma 2.2.1.** Let $\theta_1 : G \to \text{GL}(V_1)$ and $\theta_2 : G \to \text{GL}(V_2)$ be two representations of $G$, where the $V_i$ are $\mathbb{F}$-spaces of the same dimension. Then $V_1$ and $V_2$ are isomorphic as $G$-modules if and only if the representations $\theta_1$ and $\theta_2$ are equivalent, i.e. there exists $x \in \text{GL}(n, \mathbb{F})$ such that $\theta_1(g) = \theta_2(g)^x \forall g \in G$. 

---

12
If \( \theta_1, \theta_2 \) are equivalent representations of \( G \) then \( \theta_1 \) and \( \theta_2 \) have the same character, i.e. \( \text{tr}(\theta_1(g)) = \text{tr}(\theta_2(g)) \) for all \( g \in G \). Two ordinary (i.e. complex) representations of a group are equivalent if and only if they have equal characters (see [17, 2.9, p. 17]). Note that this statement may not be true for fields other than \( \mathbb{C} \). However, the statement is true in zero characteristic, and in positive characteristic when the representations are irreducible.

Equivalent representations \( \theta_1, \theta_2 \) of the same group \( G \) in \( \text{GL}(n, \mathbb{F}) \) have conjugate images; but not necessarily vice versa. That is, \( \theta_1(G) \) and \( \theta_2(G) \) may be conjugate in \( \text{GL}(n, \mathbb{F}) \) yet \( \theta_1 \) is not equivalent to \( \theta_2 \). We return to this issue in an upcoming subsection.

Given the exact correspondence between modules and representations, we apply certain terms to modules for \( G \) in \( V \), and to \( G \) itself.

The following important result is known as Schur’s lemma.

**Lemma 2.2.2.** Let \( U \) and \( W \) be irreducible \( G \)-modules. Then a homomorphism \( U \to W \) is either zero or an isomorphism.

One corollary of Schur’s lemma that we use frequently is that the centre of an irreducible linear group over an algebraically closed field consists entirely of scalar matrices. This is definitely not the case when the field is not algebraically closed.

If \( G \) is reducible then, because \( V \) has finite dimension, it has a \( G \)-composition series

\[
V = V_1 > V_2 > \cdots > V_{\ell} > V_{\ell+1} = \{0\}
\]

where \( \ell \geq 2 \), the \( V_i \) are \( G \)-submodules of \( V \), and \( V_i/V_{i+1} \) is an irreducible \( G \)-module. We can combine bases for each composition factor to obtain a basis for \( V \). With respect to this basis, elements \( g \) of \( G \) have block triangular form

\[
\begin{pmatrix}
\rho_1(g) & 0 & 0 & \cdots & 0 \\
* & \rho_2(g) & 0 & \cdots & 0 \\
* & * & \rho_3(g) & \cdots & 0 \\
& & & \ddots & \ddots \\
* & * & * & \cdots & \rho_\ell(g)
\end{pmatrix},
\]

(2.3)

where the homomorphisms \( g \mapsto \rho_i(g) \) are irreducible \( \mathbb{F} \)-representations of \( G \). Now suppose that \( G \) is completely reducible, i.e.

\[
V = V_1 \oplus \cdots \oplus V_k
\]

(2.4)

for irreducible \( G \)-submodules \( V_i \) of \( V \). Up to conjugacy in \( \text{GL}(n, \mathbb{F}) \), elements \( g \) of \( G \) have
block diagonal form

\[
\begin{pmatrix}
\rho_1(g) & 0 & 0 & \cdots & 0 \\
0 & \rho_2(g) & 0 & \cdots & 0 \\
0 & 0 & \rho_3(g) & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & \rho_k(g)
\end{pmatrix},
\]

(2.5)

where the homomorphisms \( g \mapsto \rho_i(g) \) are irreducible \( F \)-representations of \( G \). Re-ordering of the \( V_i \) in Eq.(2.4) corresponds to conjugation of the block diagonal form of \( G \) by a permutation matrix. Thus, we can assume that in the block diagonal form in (2.5), blocks corresponding to equivalent representations \( \rho_i \) are all grouped together. Moreover, we have

**Lemma 2.2.3.** Suppose that \( V = U_1 \oplus \cdots \oplus U_r \), where the \( G \)-modules \( U_i \) are all isomorphic to each other. Then there exists \( x \in \text{GL}(n,F) \) such that \( g^x = \text{diag}(\rho(g), \ldots, \rho(g)) \) where \( \rho \) is a representation \( G \to \text{GL}(m,F) \), \( m = \text{dim}_F(U_i) \), \( 1 \leq i \leq r \).

Note that we allow \( k = 1 \) in the definition of complete reducibility; an irreducible group is completely reducible. Not all reducible groups are completely reducible; for example over a finite field of characteristic \( p \), a linear \( p \)-group is unipotent, meaning that it can be conjugated to a group of unitriangular matrices.

Supposing that \( G \) is completely reducible, let Eq.(2.4) be a decomposition of \( V \) into irreducible \( G \)-submodules \( V_i \). The \( V_i \) fall into finitely many isomorphism types of irreducible \( G \)-submodules, so let \( \{U_i \mid 1 \leq i \leq k\} \) be a complete and irredundant set of representatives of these isomorphism types, and define \( W_i \) to be the direct sum of all submodules \( V_i \) in Eq.(2.4) that are isomorphic to \( U_i \). We call \( W_i \) a \( G \)-homogeneous component of \( V \). Note that if \( U \) is any non-zero irreducible \( G \)-submodule of \( V \) then the projection homomorphism \( \gamma_i : V \to V_i \) must be non-zero on \( U \) for some value \( j \) of \( i \). By Schur’s lemma, \( U \cong V_j \). It follows that \( \{U_i \mid 1 \leq i \leq k\} \) is a complete set of representatives for all isomorphism types of irreducible \( G \)-submodules of \( V \). Also, since \( \gamma_j \) being non-zero on \( U \) implies that \( U \cong V_j \), if \( W_{ij} \) is the homogeneous component containing \( V_j \), then in fact \( U \leq W_{ij} \). In other words, each \( G \)-homogeneous component \( W_i \) contains every submodule of \( V \) isomorphic to \( U_i \). This shows that for any completely reducible subgroup \( G \) of \( \text{GL}(V) \), the \( G \)-homogeneous components are canonically defined: starting from any decomposition in Eq.(2.4) and collecting together summands of the same isomorphism type, we always end up with the same homogeneous components (not just up to isomorphism; the modules will actually be equal).

There is a direct way to associate a completely reducible representation to any subgroup \( G \) of \( \text{GL}(n,F) \). That is, given all elements \( g \) of \( G \) in the form of (2.3), map \( g \) to the matrix in the form of (2.5). This map \( \theta \) is a group homomorphism. Obviously \( \theta(G) \) is
completely reducible. The kernel of $\theta$ is $G \cap \text{LT}(n, F)$, where $\text{LT}(n, F)$ is the group of (lower) unitriangular matrices in $\text{GL}(n, F)$.

Normal subgroups of irreducible linear groups are completely reducible and provide imprimitivity systems (for details see Clifford’s Theorem in the next section). Note that an imprimitive group may have a unique imprimitivity system, or it may have several. If $G \leq \text{GL}(n, F)$ has an imprimitivity system of size $n$ (its maximal possible size) then $G$ is monomial.

**Lemma 2.2.4.** Let $\text{Mon}(n, F)$ be the group of all monomial matrices in $\text{GL}(n, F)$, let $\text{D}(n, F)$ be the group of all diagonal matrices in $\text{GL}(n, F)$, and let $\text{Sym}(n)$ be the group of all permutation matrices in $\text{GL}(n, F)$. Then

- $\text{Mon}(n, F) = \text{D}(n, F) \rtimes \text{Sym}(n)$,

- the map $\pi : \text{Mon}(n, F) \to \text{Sym}(n)$ defined by $dt \mapsto t$ for $d \in \text{D}(n, F)$ and $t \in \text{Sym}(n)$ is an epimorphism with kernel $\text{D}(n, F)$.

**Lemma 2.2.5.** Suppose that $G \leq \text{Mon}(n, F)$ is irreducible. Then $\pi G$ is a transitive subgroup of $\text{Sym}(n)$.

For a given subgroup $M$ of $\text{Mon}(n, F)$, we call $M \cap \text{D}(n, F)$ the diagonal subgroup of $M$, and $\pi M \leq \text{Sym}(n)$ the permutation part of $M$. Thus $M$ is an extension of its diagonal subgroup by its permutation part.

**Lemma 2.2.6.** Suppose that $G \leq \text{GL}(n, F)$ is monomial, and let $S = \{V_1, \ldots, V_n\}$ be any imprimitivity system of size $n$ preserved by $G$. Denote by $\text{Stab}_G(S)$ the $G$-stabiliser of this system (i.e. subgroup of $G$ consisting of all elements that stabilise each $V_i$). Then there exists $x \in \text{GL}(n, F)$ such that $G^x$ consists of monomial matrices, and $G^x \cap \text{D}(n, F) = \text{Stab}_G(S)^x$.

Hence, we can consider any monomial group as consisting of monomial matrices up to linear isomorphism.

Imprimitive groups are block monomial, in the following sense. Suppose that $G \leq \text{GL}(n, F)$ is imprimitive and irreducible. Then all components of an imprimitivity system for $G$ are of the same dimension, $m$, say. Furthermore, up to conjugacy, $G$ is a group of $n/m \times n/m$ monomial matrices over $\text{Mat}(m, F)$.

**Theorem 2.2.7.** Let $G$ be a completely reducible nilpotent subgroup of $\text{GL}(n, F)$, where $F$ is algebraically closed. Then $G$ is monomial.

**Proof.** [32, Lemma 6] proves the claim for irreducible $G$, from which the general claim follows. □
2.3 Fundamentals for the classification of linear groups

Let \( F \) be a field and \( G \) a finite subgroup of \( \text{GL}(n, F) \). If the characteristic of \( F \) is zero, or is positive and does not divide \( |G| \), then \( G \) is said to be non-modular. On the other hand if \( \text{char} F > 0 \) divides \( |G| \) then \( G \) is modular. We also apply these terms to a single element \( g \) of \( \text{GL}(n, F) \) as they apply to \( \langle g \rangle \).

Lemma 2.3.1. If \( G \leq \text{GL}(n, F) \) is absolutely irreducible, then \( C_{\text{GL}(n,F)}(G) \) is scalar.

Corollary 2.3.2. \( \text{GL}(n, F) \) has absolutely irreducible abelian subgroups if and only if \( n = 1 \).

Theorem 2.3.3. (Maschke’s Theorem) If \( G \leq \text{GL}(n, F) \) has a completely reducible subgroup \( H \) such that \( |G : H| \) is not divisible by the characteristic of \( F \), then \( G \) is completely reducible. In particular if \( G \) is finite and non-modular then it is completely reducible.

Theorem 2.3.3 and Corollary 2.3.2 imply that, for any field \( F \), a non-modular finite order element of \( \text{GL}(n, F) \) can be diagonalised.

Theorem 2.3.4. (Clifford’s Theorem) Let \( F \) be any field, \( G \) be an irreducible subgroup of \( \text{GL}(n, F) \), \( V \) be the underlying \( n \)-dimensional \( F \)-vector space for \( \text{GL}(n, F) \) and \( N \) be a normal subgroup of \( G \). Then \( V \) is a completely reducible \( N \)-module:

\[
V = V_1 \oplus V_2 \oplus \cdots \oplus V_k,
\]

where the \( V_i \) are the \( N \)-homogeneous components, i.e. each \( V_i \) is a direct sum \( W_{i1} \oplus \cdots \oplus W_{il_i} \) of isomorphic irreducible \( N \)-submodules \( W_{ij} \) of \( V \), and summands from different components are not isomorphic as \( N \)-modules. Furthermore, under the matrix multiplication action of \( \text{GL}(n, F) \) on \( V \), the \( N \)-homogeneous components of \( V \) form an imprimitivity system for \( G \), and \( G \) permutes those components transitively.

Corollary 2.3.5. Let \( G \) be a primitive subgroup of \( \text{GL}(n, F) \) where \( F \) is algebraically closed. Then an abelian normal subgroup of \( G \) is scalar.

Proof. Let \( A \) be an abelian normal subgroup of \( G \). As the \( A \)-homogeneous components form a \( G \)-imprimitivity system, there can only be one component. The irreducible parts of this component correspond to irreducible abelian linear groups over an algebraically closed field, so are 1-dimensional. This means that \( A \) is scalar (cf. Lemma 2.2.3).

Theorem 2.3.6. Let \( G \) be an irreducible subgroup of \( \text{GL}(n, F) \). Then either \( G \) is absolutely irreducible, or there exists a field extension \( K \) of \( F \) of degree \( m > 1 \) dividing \( n \) such that \( G \) is isomorphic to an absolutely irreducible subgroup \( H \) of \( \text{GL}(n/m, K) \). Moreover, if \( G \) is primitive then \( H \) is primitive.
2.4. LINEAR GROUP CLASSIFICATION

Proof. See [35, 1.19, p.12].

Theorem 2.3.7. If $G$ is a finite absolutely irreducible subgroup of $\text{GL}(n, F)$ then there exists a finite extension $E$ of the prime subfield of $F$ such that $G$ is conjugate to a subgroup of $\text{GL}(n, E)$.

Proof. See [5, Theorem 3.4B, p.54].

So a finite absolutely irreducible matrix group over a field of positive characteristic can always be ‘written over’ a finite field (conjugated to a group over such a field). Over a field of characteristic zero, a finite group can be written over an algebraic number field.

2.4 Linear group classification

The criteria by which linear groups are classified vary. Linear groups have an abstract description (by isomorphism type); but since they are groups in action (on vector spaces), they can also be described in terms of the finer criterion of linear isomorphism arising from the action.

Lemma 2.4.1. Let $G \leq \text{GL}(n, F)$. Suppose that $G$ has property $P$, where

$$ P \in \{\text{ir/reducible, completely reducible, im/primitive, in/decomposable, absolutely irreducible}\}. $$

Then for any $H \leq \text{GL}(n, F)$ conjugate to $G$, $H$ also has property $P$.

In other words, linear isomorphism not only preserves abstract group properties, but also linear group properties. So in some settings we can obtain more than just the basic statement of the lemma. For example, if $G$ is completely reducible then a conjugate of $G$ has homogeneous components isomorphic to those of $G$; also if $G$ is imprimitive then a conjugate of $G$ preserves a ‘conjugate’ of each $G$-imprimitivity system. Thus linear isomorphism is the natural criterion by which to classify linear groups. For these reasons we are primarily concerned with classifying linear groups up to linear isomorphism, i.e. given the degree $n$, the field $F$, and a set of properties $P$, we aim to produce a complete irredundant list $\mathcal{L}_P$ of finite subgroups of $\text{GL}(n, F)$ satisfying $P$: every group in $\mathcal{L}_P$ satisfies $P$, and any subgroup of $\text{GL}(n, F)$ satisfying $P$ is $\text{GL}(n, F)$-conjugate to a single group in $\mathcal{L}_P$.

A computer implementation of a linear group classification should be as useful as possible. Thus, apart from the actual lists themselves, the implementation should return other
‘intrinsic’ properties of the listed groups that are already known in advance from the theoretical classification — that is, without computing information from the listed generating sets using other algorithms. This information might include a mixture of abstract group theoretic and linear group theoretic properties such as: orders; whether a listed group is soluble or nilpotent; the isomorphism type of the central quotient; whether a listed group is irreducible, and if not, a non-trivial module for it; whether a listed group is primitive, and if not, a non-trivial imprimitivity system for it; whether a listed group is absolutely irreducible; and so on.

As the next lemma illustrates, sometimes it is easy to obtain the classifications of subgroups of other classical groups given a classification of subgroups of the general linear group.

**Lemma 2.4.2.** Let \( \mathbb{F} \) be algebraically closed. Suppose that \( \mathcal{L} \) is a complete and irredundant list of the finite irreducible subgroups of \( \text{GL}(n, \mathbb{F}) \). Then \( \mathcal{L}^* = \mathcal{L} \cap \text{SL}(n, \mathbb{F}) \) is a complete and irredundant list of the finite irreducible subgroups of \( \text{SL}(n, \mathbb{F}) \).

When classifying finite groups over infinite fields, it is not even always true that there are finitely many groups, up to the classification criterion. We address this issue next.

**Proposition 2.4.3.** Suppose that \( G \) is a finite subgroup of \( \text{GL}(n, \mathbb{C}) \). Then there are only finitely many \( \text{GL}(n, \mathbb{C}) \)-conjugacy classes of subgroups of \( \text{GL}(n, \mathbb{C}) \) isomorphic to \( G \).

**Proof.** Select a complete set of representatives \( \rho_1, \ldots, \rho_k \) for the equivalence classes of ordinary irreducible representations of \( G \) of degree \( \leq n \) (this set is finite because the number of irreducible ordinary characters of \( G \) is the number of conjugacy classes in \( G \), see e.g. [17, 2.7, p.16]). Let \( H \leq \text{GL}(n, \mathbb{C}) \) and \( \theta : G \to H \) be an isomorphism. By Maschke’s theorem, \( H \) is conjugate to a group of block diagonal matrices: \( \{(\lambda_1(h), \ldots, \lambda_r(h)) \mid h \in H\} \), and \( \lambda_i \) is an irreducible ordinary representation of \( H \) of degree \( \leq n \). Hence, for each \( i \), \( \lambda_i\theta \) is equivalent to some \( \rho_{j(i)} \). Consequently, \( H \) is \( \text{GL}(n, \mathbb{C}) \)-conjugate to \( \{(\rho_{j(1)}(g), \ldots, \rho_{j(r)}(g)) \mid g \in G\} \). There are only finitely many ways to choose each \( \rho_{j(i)} \), so we are done. \( \square \)

**Proposition 2.4.4.** There are only finitely many conjugacy classes of finite primitive subgroups of \( \text{SL}(n, \mathbb{C}) \).

**Proof.** Any finite subgroup \( G \) of \( \text{GL}(n, \mathbb{C}) \) has an abelian normal subgroup \( A \) whose index is bounded above by a function of \( n \) (cf. [17, Theorem 14.12, p.249]). Suppose that \( G \) is primitive. Then \( A \) is scalar, by Corollary 2.3.5. Hence, if \( G \leq \text{SL}(n, \mathbb{C}) \) then \( |A| \leq n \); so, in fact \( |G| \) is bounded above (in terms of \( n \)). That is, there are only finitely many
isomorphism types of finite primitive subgroups of $\text{SL}(n, \mathbb{C})$. The result then follows from Proposition 2.4.3. □

2.4.1 The isomorphism question

Elements of the lists we produce in this thesis are representatives of conjugacy classes in their ambient full general linear groups. That is, elements of our lists are not linearly isomorphic. It is natural then, to ask whether distinct listed groups are abstractly isomorphic. More generally, we pose the isomorphism question for a subgroup $G$ of $\text{GL}(n, \mathbb{F})$: “if $H \leq \text{GL}(n, \mathbb{F})$ is abstractly isomorphic to $G$, must $H$ be linearly isomorphic to $G$?”

Equivalent representations have conjugate images; however, the converse is not true. The next straightforward theorem determines how equivalence of representations and conjugacy of their images are related.

**Theorem 2.4.5.** Let $\mathbb{F}$ be any field, and $G$ a finite group. Let $\mathcal{R} = \mathcal{R}(G, n, \mathbb{F})$ denote the set of equivalence classes $[\rho]$ of all faithful representations $\rho : G \to \text{GL}(n, \mathbb{F})$. Assuming that $\mathcal{R}$ is non-empty, define an action of $\text{Aut}(G)$ on $\mathcal{R}$ by

$$[\rho] \alpha = [\rho \alpha]; \quad [\rho] \in \mathcal{R}, \quad \alpha \in \text{Aut}(G).$$

Then the following hold:

(i) $\text{Stab}_{\text{Aut}(G)}([\rho]) \cong N_{\text{GL}(n, \mathbb{F})}(\rho(G))/C_{\text{GL}(n, \mathbb{F})}(\rho(G))$.

(ii) $[\rho]$ and $[\psi]$ are in the same $\text{Aut}(G)$-orbit if and only if $\rho(G)$ and $\psi(G)$ are $\text{GL}(n, \mathbb{F})$-conjugate.

(iii) The number of $\text{Aut}(G)$-orbits in $\mathcal{R}$ is the number of conjugacy classes of subgroups of $\text{GL}(n, \mathbb{F})$ that are isomorphic to $G$.

Note that the $\text{Aut}(G)$-action in Theorem 2.4.5 restricts to various subsets $\mathcal{R}_P$ of $\mathcal{R}$ of the linear groups satisfying a property $P$ as in Lemma 2.4.1, and then the conclusions of Theorem 2.4.5 hold true for the groups in $\mathcal{R}_P$.

**Corollary 2.4.6.** Retaining the same notation as above, the isomorphism question for a subgroup $G$ of $\text{GL}(n, \mathbb{F})$ with property $P$ has an affirmative answer if and only if $\text{Aut}(G)$ acts transitively on the set $\mathcal{R}_P$.

We will observe that the groups listed in Chapter 5 are covered by Corollary 2.4.6. Here is a lemma which we need in order to establish that fact.
Lemma 2.4.7. Suppose that $G$ is an absolutely irreducible subgroup of $\text{GL}(n, \mathbb{F})$ such that $N_{\text{GL}(n, \mathbb{F})}(G) = GZ$, where $Z$ denotes the scalars of $\text{GL}(n, \mathbb{F})$. If the number of inequivalent faithful absolutely irreducible representations of $G$ in $\text{GL}(n, \mathbb{F})$ is $|Z(G)||\text{Aut}(G)|/|G|$, then every absolutely irreducible subgroup of $\text{GL}(n, \mathbb{F})$ isomorphic to $G$ is conjugate to every other such subgroup of $\text{GL}(n, \mathbb{F})$.

Proof. Let $\rho$ be the identity representation on $G$. Since $\rho(G)$ is absolutely irreducible, $C_{\text{GL}(n, \mathbb{F})}(\rho(G)) = Z$. Then

$$|N_{\text{GL}(n, \mathbb{F})}(G) : C_{\text{GL}(n, \mathbb{F})}(G)| = |GZ : Z| = |G : Z(G)|.$$ 

Thus $|G : Z(G)|$ is the size of the $\text{Aut}(G)$-stabiliser of $[\rho]$, by Theorem 2.4.5 (i). Hence the $\text{Aut}(G)$-orbit of $[\rho]$ has length $|Z(G)||\text{Aut}(G)|/|G|$. By hypothesis and Theorem 2.4.5 (iii), the proof is then complete. \qed

2.4.2 The SL-transfer

When $\mathbb{F}$ is algebraically closed, there is a traditional method that reduces a classification problem for finite subgroups of $\text{GL}(n, \mathbb{F})$ to an analogous classification problem in $\text{SL}(n, \mathbb{F})$. It is usually easier to work in the latter setting (cf. Proposition 2.4.4). We shall refer to this method colloquially as the ‘SL-transfer’.

Lemma 2.4.8. Let $\mathbb{F}$ be any field, and $\overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$. Let $G$ be a finitely generated subgroup of $\text{GL}(n, \overline{\mathbb{F}})$, say $G = \langle g_1, \ldots, g_r \rangle$. For each $g_i$, select an $n^{th}$ root $\alpha_i$ of $\det(g_i)$ in $\overline{\mathbb{F}}$, and define $\theta(g_i) = \alpha_i^{-1}g_i$. Set $H = \langle \theta(g_1), \ldots, \theta(g_r) \rangle$. Then the following hold:

(i) $H \leq \text{SL}(n, \overline{\mathbb{F}})$.

(ii) $GZ = HZ$, where $Z$ denotes the scalars of $\text{GL}(n, \overline{\mathbb{F}})$.

(iii) Let $\mathbb{F}$ be algebraically closed. Then $H$ has property $P$ if and only if $G$ has property $P$, where $P \in \{ \text{ir/reducible, completely reducible, im/primitive, in/decomposable} \}$.

Now suppose furthermore that $G$ is absolutely irreducible. Then

(iv) $G/Z(G) \cong H/Z(H)$;

(v) $H$ is finite if $G/Z(G)$ is finite.

Proof. (i) This follows because each generator $\theta(g_i)$ of $H$ has determinant 1.
2.5. CHANGING THE FIELD

(ii) Clear from the definitions.

(iii) Since $G$ and $H$ differ only by scalars (of $\mathbb{F} = \mathbb{F}$), the properties $P$ are invariant under the $\text{SL}$-transfer: the $G$-submodules and $H$-submodules of the underlying space coincide.

(iv) Since $H$ is also absolutely irreducible, we have $Z(G) = G \cap Z$ and $Z(H) = H \cap Z$ by Schur’s lemma. The result follows from (ii).

(v) Since $Z(H) \leq \text{SL}(n, \mathbb{F})$ is scalar, it is isomorphic to a subgroup of the group of $n^{th}$ roots of unity in $\mathbb{F}$ and so is finite. This part then follows from (iv).

Note that the SL-transfer is easily carried out in practice, via generating sets. Note also that the map $\theta$ in Lemma 2.4.8 is not a homomorphism and cannot be canonically defined.

As we shall see, a group in the lists of Chapter 5 is determined by its central quotient and centre, i.e. by the isomorphism type of its central quotient and the order of its centre. Hence the isomorphism question has an affirmative answer for these groups.

2.5 Changing the field

We now recall some standard representation and character theory to do with changing the field of definition of a linear group; this may be found in [17, Chapters 9 & 15]. See also [5, Chapter 5].

**Theorem 2.5.1.** Let $G$ be a finite subgroup of $\text{GL}(n, \mathbb{F})$ where $\mathbb{F}$ is any field. If $G$ is completely reducible then $G$ is completely reducible as a subgroup of $\text{GL}(n, \mathbb{E})$ for any extension $\mathbb{E}$ of $\mathbb{F}$.

*Proof.* See [16, Chapter 7, §1].

**Theorem 2.5.2.** Let $\mathbb{F}$ be a field of positive characteristic. Suppose that $G$ is an irreducible subgroup of $\text{GL}(n, \mathbb{F})$, and $\text{tr}(G) \subseteq \mathbb{K}$ for some subfield $\mathbb{K}$ of $\mathbb{F}$. Then $G$ is conjugate to a subgroup of $\text{GL}(n, \mathbb{K})$.

*Proof.* See [5, 9.23, p.155].

Theorem 2.5.2 is not true in zero characteristic.

**Theorem 2.5.3.** (Deuring-Noether) Suppose that $G$ and $H$ are subgroups of $\text{GL}(n, \mathbb{F})$, such that $G$ and $H$ are $\text{GL}(n, \mathbb{K})$-conjugate for some field extension $\mathbb{K}$ of $\mathbb{F}$. Then $G$ and $H$ are $\text{GL}(n, \mathbb{F})$-conjugate.
2.6 Linear groups of prime degree

Let \( F \) be any field, \( p \) be a prime, and \( V \) be the underlying space for \( \text{GL}(p, F) \). In this section we state some of the restrictions on the structure of subgroups of \( \text{GL}(p, F) \).

**Lemma 2.6.1.** An irreducible imprimitive linear group of degree \( p \) is monomial.

**Lemma 2.6.2.** Let \( G \leq \text{GL}(p, F) \) be irreducible. Then a normal subgroup of \( G \) is either abelian or irreducible.

**Proof.** Let \( N \trianglelefteq G \). By Clifford’s theorem and primality of degree, \( V \) is either an irreducible \( N \)-module or a direct sum of 1-dimensional \( N \)-modules. In the latter case, \( N \) is diagonalisable and hence abelian. \( \square \)

**Lemma 2.6.3.** Let \( G \) be an irreducible non-abelian subgroup of \( \text{GL}(p, F) \).

(i) \( G \) is absolutely irreducible.

(ii) If \( G \) is primitive then every non-scalar normal subgroup of \( G \) is irreducible.

(iii) If \( p < 5 \) and \( G \) is insoluble, then \( G \) is primitive (over \( \overline{F} \)).

**Proof.** (i) If \( G \) is not absolutely irreducible then by Theorem 2.3.6 and the fact that \( p \) is prime, \( G \) is isomorphic to a subgroup of \( \text{GL}(1, K) \) for some extension \( K \) of \( F \), i.e. \( G \) is abelian.

(ii) Suppose that \( G \) is primitive, and let \( N \) be a normal non-scalar subgroup of \( G \). By Clifford’s theorem, \( V \) is \( N \)-homogeneous. Thus, if \( N \) were reducible then \( V \) would be a direct sum of isomorphic 1-dimensional \( N \)-modules, i.e. \( N \) would be scalar.

(iii) This follows from Lemma 2.6.1 and the fact that a monomial linear group in degree \( n \leq 4 \), as an extension of an abelian group by a subgroup of \( \text{Sym}(n) \), is soluble. \( \square \)

Hence, the subgroups of \( \text{GL}(3, q) \) that we list in Chapter 5 are absolutely irreducible and primitive over every extension of \( \text{GF}(q) \).

**Lemma 2.6.4.** Let \( F \) be algebraically closed. Suppose that \( G \) is an irreducible subgroup of \( \text{GL}(p, F) \) with a non-scalar normal abelian subgroup \( D \). Then \( D \) has \( p \) homogeneous components in \( V \). These components are precisely the irreducible \( D \)-submodules of \( V \), and they form an imprimitivity system for \( G \). In particular, \( G \) is monomial: \( G \) is conjugate to a group of monomial matrices in which the image of \( D \) consists of diagonal matrices.
2.6. LINEAR GROUPS OF PRIME DEGREE

Proof. Corollary 2.3.2, Clifford’s theorem and $D$ non-scalar imply that $V$ is a direct sum of pairwise non-isomorphic 1-dimensional (irreducible) $D$-modules $W_i$. The $W_i$ are in fact the $D$-homogeneous components of $V$, and they form a system of imprimitivity for $G$. □

**Lemma 2.6.5.** Let $G$ be an irreducible monomial subgroup of $\mathrm{GL}(p, F)$ with an abelian normal subgroup $D$ of index $p$. If $H$ is an irreducible monomial subgroup of $\mathrm{GL}(p, F)$ isomorphic to $G$ then $\pi G \cong \pi H \cong C_p$ is a transitive subgroup of $\mathrm{Sym}(p)$.

Proof. Let $A$ denote the image in $G$ of the diagonal subgroup of $H$ under an isomorphism $H \to G$. If $A \leq D$ then $G/A = AD/A \cong D/D \cap A$ is abelian. As this quotient is also isomorphic to a transitive permutation group of degree $p$, that permutation group is regular and so the quotient $G/A$ has size $p$, i.e. $|\pi H| = p$.

Now assume that $A < D$. Then $D/A$ is isomorphic to a non-trivial normal subgroup of a transitive permutation group of degree $p$. Thus $D/A$ is transitive and so, as it is also an abelian group, $D/A$ is regular. Hence $|D : A| = p$ and $|G : A| = p^2$. But $G/A$ is (isomorphic to) a transitive permutation group of degree $p$; it cannot have order $p^2$ because if it did it would be abelian and then regular. This final contradiction implies that $|\pi H| = p$. □

Next we present some criteria for irreducibility of monomial groups in prime degree.

**Lemma 2.6.6.** Suppose that $G$ is a finite soluble non-modular subgroup of $\mathrm{Mon}(p, F)$ such that $\pi G$ is a transitive subgroup of $\mathrm{Sym}(p)$, and let $D$ be the diagonal subgroup of $G$. Then $G$ is irreducible (i.e., absolutely irreducible) if and only if $D$ is non-scalar.

Proof. As a soluble transitive permutation group of prime degree $p$, $\pi G$ splits over a normal transitive cyclic subgroup $C$ of order $p$. Moreover, $\pi G/C$ is cyclic of order dividing $p - 1$ (see [15, Satz 3.6, p. 163]). Let $H$ be the normal subgroup of $G$ containing $D$ such that $\pi H = C$.

Suppose that $D$ is non-scalar. Then $H$ is non-abelian. Since $H$ is non-modular, it is isomorphic to a subgroup of $\mathrm{GL}(p, C)$ (see Theorem 2.7.3 below). By Ito’s theorem [17, 6.15, p. 84], the degree of an irreducible character of $H$ divides $p$. Since $H$ is non-abelian, this means that $H$ must be irreducible. It follows that $G$ is irreducible and so absolutely irreducible by Lemma 2.6.3.

It can be shown that $G$ is $\mathrm{GL}(p, F)$-conjugate to a subgroup $\hat{G}$ of $\mathrm{Mon}(p, F)$ containing $\pi G$ modulo scalars (cf. [11, Remark 6.3] and [11, Theorem 6.2]). Thus, if $G$ is irreducible then $D$ cannot be scalars; if it were, then $\hat{G}$ would fix the subspace of $V$ spanned by the all 1s vector and so would be reducible.
Note that Lemma 2.6.6 does not remain true if $G$ is insoluble; there exist finite insoluble monomial linear groups with scalar diagonal subgroup.

We continue with further results on monomial groups in prime degree.

**Theorem 2.6.7.** Let $\mathbb{F}$ be algebraically closed. Suppose that $G$ is an irreducible subgroup of $\text{GL}(p,\mathbb{F})$ with a normal abelian subgroup $D$ of index $p$. Then $G$ is monomial, and $G$ preserves either exactly 1 or exactly $p+1$ distinct imprimitivity systems of size $p$.

**Proof.** We begin by observing that $D$ does not consist entirely of scalar matrices; if it did then $G/Z(G)$ would be cyclic and so $G$ would be abelian. For the same reason, $G$ does not possess any scalar subgroups of index $p$.

The important point of the proof is that the set $\mathcal{Y}$ of distinct imprimitivity systems $S$ of $G$ of size $p$ (which is non-empty by monomiality of $G$) is in 1:1 correspondence with the set $\mathcal{N}$ of non-scalar abelian normal subgroups $A$ of $G$ of index $p$.

Let $f$ be the map from $\mathcal{Y}$ to the set of subgroups of $G$ defined by $f(S) = \text{Stab}_G(S) = \{g \in G \mid gU = U, \forall U \in S\}$. By Lemma 2.2.6, $G$ is conjugate to a monomial matrix group whose diagonal subgroup is the image of $\text{Stab}_G(S)$ under the conjugation. Hence, by Lemma 2.6.5, $\text{Stab}_G(S)$ is an abelian normal subgroup of $G$ of index $p$. This shows that $f$ maps $\mathcal{Y}$ into $\mathcal{N}$.

Conversely, if $A$ is a non-scalar abelian normal subgroup of $G$ of index $p$, then by Lemma 2.6.4, $V$ is a direct sum of pairwise non-isomorphic irreducible $A$-modules $W_i$ (the $A$-homogeneous components of $V$). Thus, the $W_i$ are the only 1-dimensional $A$-submodules of $V$. Moreover, $A$ is precisely the $G$-stabiliser of all of the $W_i$ (otherwise, $G$ itself is diagonal). So the map $h : \mathcal{N} \rightarrow \mathcal{Y}$ given by $h(A) = \{W_1, \ldots, W_p\}$ is well-defined.

Now $f(h(A))$ is a subgroup of $G$ leaving every element of $h(A)$ invariant. Obviously then $A \leq f(h(A))$. If $A \neq f(h(A))$ then (because $A$ has index $p$), we must have $f(h(A)) = G$. This implies that $G$ can be diagonalised; hence $A = f(h(A))$. Conversely, $h(f(S)) = S$ because the elements of $S$ are the unique 1-dimensional $f(S)$-submodules of $V$. Hence $\mathcal{Y}$ and $\mathcal{N}$ are in 1:1 correspondence, as claimed. So we finish the proof by counting the number $m$ of distinct abelian normal subgroups of $G$ of index $p$.

Assume that $m > 1$, and let $A \neq D$ be an abelian normal subgroup of $G$ of index $p$. Then $A \cap D$ has index $p$ in each of $A$ and $D$, and $A \cap D$ is scalar (because $G$ can be monomialised, with a diagonal subgroup of index $p$). Clearly, if $D$ has at least one scalar subgroup of index $p$, call it $X$, then $X$ is the unique scalar subgroup of $D$ of index $p$ (because otherwise $D$ would be scalar). We see that $m$ is the number of distinct subgroups of $G/X$ of order $p$. Now $|G : X| = |G : D| \cdot |D : X| = p^2$, and since $G/X$ is not cyclic (it has two different subgroups of order $p$), we see that $G/X \cong C_p \times C_p$. We note that the
distinct subgroups of order \( p \) in \( \langle a, b \mid a^p = b^p = 1, ab = ba \rangle \cong C_p \times C_p \) are \( \langle b \rangle \) and the \( \langle ab^i \rangle, 0 \leq i \leq p - 1 \). Thus \( m = p + 1 \), as required.

When \( G \) in Theorem 2.6.7 preserves \( p + 1 \) imprimitivity systems of size \( p \), \( G \) has a scalar subgroup of index \( p^2 \) — as observed in the proof of the theorem. That is, \( G \) is nilpotent.

In the rest of the section we are concerned with primitive groups in degree \( p \).

**Lemma 2.6.8.** Let \( \mathbb{F} \) be an algebraically closed field. Suppose that \( G \) is a primitive subgroup of \( \text{GL}(p, \mathbb{F}) \) such that \( G/\mathcal{Z}(G) \) is not simple. Then either \( G \) is an extension of a proper normal monomial subgroup by a permutation group of degree \( p + 1 \), or for every proper normal non-trivial subgroup \( N/\mathcal{Z}(G) \) of \( G/\mathcal{Z}(G) \), \( N \) is primitive.

*Proof.* Let \( N \trianglelefteq G \). By part (ii) of Lemma 2.6.3, \( N \) is irreducible. Suppose that \( N \) is imprimitive, so that \( N \) preserves an imprimitivity system \( \{U_1, \ldots, U_p\} \). If \( g \in G \) then \( \{gU_1, \ldots, gU_p\} \) is also an \( N \)-imprimitivity system: as \( G \) is primitive, \( N \) therefore has more than one imprimitivity system. Hence by Theorem 2.6.7, \( N \) has \( p + 1 \) distinct imprimitivity systems, which are permuted amongst themselves by \( G \). The kernel of the corresponding degree \( p + 1 \) permutation representation of \( G \) arising from this action is monomial. This completes the proof.

*Corollary 2.6.9.* Let \( G \) be a primitive insoluble subgroup of \( \text{GL}(p, \mathbb{F}) \), \( \mathbb{F} \) algebraically closed and \( p \leq 3 \). Then every normal subgroup of \( G \) not contained in \( \mathcal{Z}(G) \) is primitive.

*Proof.* We may suppose that \( G/\mathcal{Z}(G) \) is not simple. By Lemma 2.6.8, one of the following must be true:

(i) \( G \) is an extension of a proper normal monomial subgroup by a permutation group of degree 3 or 4; or

(ii) every proper normal subgroup \( L \) of \( G \) properly containing \( \mathcal{Z}(G) \) is primitive.

Case (i) cannot occur, because in degrees less than 5, permutation groups and monomial matrix groups are soluble.

Note again that degree \( p = 3 \) is special; Corollary 2.6.9 is not true for other \( p \).

**Lemma 2.6.10.** Suppose that \( G \) is a finite primitive subgroup of \( \text{GL}(p, \mathbb{F}) \) such that the socle \( S/\mathcal{Z}(G) \) of \( G/\mathcal{Z}(G) \) is non-abelian. Then \( S \) is irreducible and \( S/\mathcal{Z}(G) \) is simple.
2.7. CONGRUENCE HOMOMORPHISMS

Proof. By Lemma 2.6.2, \( S \) is an irreducible subgroup of \( \text{GL}(p, \mathbb{F}) \). Recall that the socle of a finite group is a direct product of simple groups. Since \( S/Z(G) \) is non-abelian, there exists a non-abelian normal simple subgroup \( S_1/Z(G) \) of \( S/Z(G) \). Note that \( S_1 \) is irreducible by Lemma 2.6.2; and hence absolutely irreducible by Lemma 2.6.3(i).

Let \( aZ(G) \) be a non-trivial element of \( S/Z(G) \) centralising \( S_1/Z(G) \). The map \( \varphi : S_1 \rightarrow Z(G) \) defined by \( s \mapsto [s, a] \) is a homomorphism, and \( \ker \varphi / Z(G) \) is a normal subgroup of \( S_1/Z(G) \). If \( \ker \varphi = S_1 \) then \( a \) centralises the absolutely irreducible group \( S_1 \), so is in \( Z(G) \). Thus, \( \ker \varphi \leq Z(G) \) which gives another contradiction; namely that \( S_1/\ker \varphi \), which is isomorphic to a subgroup of \( Z(G) \), is abelian. Thus \( S/Z(G) \) can only contain a single simple factor, and we are finished. □

Lemma 2.6.11. Let \( G \) be a finite primitive subgroup of \( \text{GL}(p, \mathbb{F}) \), \( p \leq 3 \), where \( \mathbb{F} \) is algebraically closed. Then \( G \) contains a normal primitive subgroup \( N \) such that \( N/Z(G) \) is a non-abelian simple group.

Proof. Set \( S/Z(G) := \text{soc}(G/Z(G)) \). Then \( S \) is primitive by Corollary 2.6.9. Suppose that \( S/Z(G) \) is abelian. Then \( S \) is nilpotent. However, as a non-abelian nilpotent group, \( S \) has a non-central (hence non-scalar) abelian normal subgroup. Since this contradicts Lemma 2.6.3 (i), the result follows from Lemma 2.6.10. □

2.7 Congruence homomorphisms

One useful feature of a congruence homomorphism is that it enables us to obtain explicit generating sets for groups, over a finite field, given generating sets for pre-images over an infinite field. We also need the concept of congruence homomorphism for an important special result below.

Lemma 2.7.1. Let \( G \) be a finite subgroup of \( \text{GL}(n, \mathbb{C}) \). Then there exists an algebraic number field \( \mathbb{A} \) such that \( G \) is conjugate to a subgroup of \( \text{GL}(n, \mathbb{A}) \).

Proof. This follows directly from Theorem 2.3.7. □

With \( G \) as in Lemma 2.7.1, it is possible to select a finitely generated integral domain \( \Delta \) such that \( G \leq \text{GL}(n, \Delta) \), a prime \( p \in \mathbb{Z} \), and a ring homomorphism \( \psi : \Delta \rightarrow \Delta/p\Delta \), such that the extension of \( \psi \) to all of \( G \leq \text{GL}(n, \Delta) \) maps into \( \text{GL}(n, q) \) for some power \( q \) of \( p \). Then the kernel of \( \psi \) on \( G \) is a normal \( p \)-subgroup of \( G \). We call \( \psi \) a congruence homomorphism (‘mod \( p \)’). More generally we have
Proposition 2.7.2. Let $G$ be a finite subgroup of $GL(n, \mathbb{F})$, $\mathbb{F}$ any field. Then for each prime $p > 2$ there exists a congruence homomorphism $\psi : G \to GL(n, q)$ for some power $q$ of $p$ such that the kernel of $\psi$ on $G$ is a $p$-group.

Proof. See [32, Chapter III] and [35, Chapter 4].

The following (which we noted previously) can also be proved by congruence homomorphism techniques.

Theorem 2.7.3. A finite non-modular subgroup $G$ of $GL(n, \mathbb{F})$ is isomorphic to a subgroup $H$ of $GL(n, \mathbb{C})$. In addition, $G$ is absolutely irreducible if and only if $H$ is irreducible.

Proof. See [5, Corollary 3.8, p.62].

Lemma 2.7.4. Let $G \leq GL(n, \mathbb{F})$, where $\mathbb{F}$ is a field of prime characteristic $p$. Suppose that $p > n$. If $G$ can be ‘lifted’ to $\mathbb{C}$, i.e. if $G$ is isomorphic to a subgroup $H$ of $GL(n, \mathbb{C})$, then any $p$-subgroup of $G$ is abelian.

Proof. Over $\mathbb{C}$, a $p$-subgroup $P$ of $H$ is monomial. But $p > n$ so the permutation part of $P$ is trivial i.e. $P$ is diagonal i.e. $P$ is abelian.

Lemma 2.7.5. Let $G$ be a finite irreducible subgroup of $GL(n, \mathbb{F})$, and suppose that $G$ has an element $g$ of prime power order $p^a$, where $p^{a-1} \geq n$. Then $G$ has a (non-trivial) normal $p$-subgroup containing $g^{p^{a-1}}$.

Proof. By Proposition 2.7.2, let $\psi$ be a congruence homomorphism of $G$ into $GL(n, \mathbb{E})$ where $\mathbb{E}$ is a (finite) field of characteristic $p$, such that the kernel of $\psi$ in $G$ is a $p$-group. Now $\psi(g)$ is a matrix of $p$-power order over a field of characteristic $p$, hence it is unipotent; meaning that $(\psi(g) - 1_n)^n = 0_n$. Thus $(\psi(g) - 1_n)^{p^{a-1}} = 0_n$, and expanding the left hand side of this identity and using char $\mathbb{E} = p$, we get that $\psi(g^{p^{a-1}}) = \psi(g)^{p^{a-1}} = 1_n$. 

Chapter 3

Finite linear groups of degree two

In this chapter, we give a classification of finite absolutely irreducible groups in degree 2 and characteristic zero. Some of this information is very well-known; for degree 2 groups over finite fields, we point to [11, Section 5] as a source of reference. The main arguments were essentially known to Klein and Jordan. Details of the classification are needed for the classification of non-modular groups carried out in Chapter 5. Chapter 7 also draws on the results of this chapter.

Let $K$ be a field with an automorphism $r \mapsto r^\sigma$ of order at most 2. An Hermitian form on the $n$-dimensional $K$-vector space $K^{(n)}$ is a nondegenerate biadditive form $f$ such that $f(ru,v) = rf(u,v)$ and $f(u,v) = f(v,u)$ for all $r \in K$ and $u,v \in K^{(n)}$.

**Lemma 3.0.1.** With $f$ as above, suppose that for all $u \in K^{(n)}$, $f(u,u) \in \{r \sigma r^\sigma \mid r \in K\}$, and $f(u,u) = 0$ if and only if $u = 0$. Then $K^{(n)}$ has a basis $\{u_1, \ldots, u_n\}$ such that $f(u_i, u_j) = \delta_{i,j}$.

A matrix $A$ of $GL(n, K)$ is called unitary if $AA^\top = I_n$ (here $A = [a_{ij}]_{ij}$). Of course, in the special case $K = \mathbb{R}$, a unitary matrix is more properly called orthogonal. We denote the subgroup of all unitary matrices in $GL(n, K)$ by $U(n)$ when $K = \mathbb{C}$, and by $O(n)$ when $K = \mathbb{R}$.

**Remark 3.0.2.** We defined uniquely $U(n)$ and $O(n)$ in terms of unitary and orthogonal matrices respectively. One may be tempted to call these respectively the unitary group and the orthogonal group. Indeed, some mathematical literature is misleading in this regard — a unitary group preserves a non-degenerate $\sigma$-Hermitian form with $\sigma \neq 1$ and an orthogonal group preserves a non-degenerate quadratic form. As such, the matrices which form respectively part of a unitary or orthogonal group may neither themselves be unitary nor orthogonal necessarily but rather each preserves an appropriate chosen form.
Proposition 3.0.3. Assume the hypotheses of Lemma 3.0.1. Suppose that $G \leq \text{GL}(n, \mathbb{K})$ preserves $f$, i.e. $f(ug, vg) = f(u, v)$ for all $u, v \in \mathbb{K}^{(n)}$ and $g \in G$. Then $G$ is conjugate to a group of unitary matrices.

Proof. If $u_1, \ldots, u_n$ is a basis of $\mathbb{K}^{(n)}$ as in Lemma 3.0.1, and $h$ is the matrix of $g \in G$ with respect to this basis, then it may be checked that $h$ is unitary. □

Corollary 3.0.4. (i) If $G$ is a finite subgroup of $\text{GL}(n, \mathbb{C})$ then $G$ is conjugate to a subgroup of $\text{U}(n)$.

(ii) Let $\mathbb{K}$ be any subfield of $\mathbb{R}$ containing square roots of all its positive elements. If $G$ is a finite subgroup of $\text{GL}(n, \mathbb{K})$ then $G$ is conjugate to a subgroup of $\text{O}(n)$.

Proof. Let $f$ be the usual complex Hermitian inner product $f$. Since for finite $G \leq \text{GL}(n, \mathbb{C})$ the Hermitian form $\hat{f}$ defined by $\hat{f}(u, v) = \sum_{g \in G} f(ug, vg)$ satisfies the hypotheses of Lemma 3.0.1, (i) follows from Proposition 3.0.3. The proof of (ii) is similar, taking $f$ to be the scalar product over $\mathbb{K}$. □

By Corollary 3.0.4 (i), classifying the finite subgroups of $\text{SL}(n, \mathbb{C})$ up to $\text{GL}(n, \mathbb{C})$-conjugacy (that is, up to $\text{SL}(n, \mathbb{C})$-conjugacy) is the same as classifying the finite subgroups of $\text{SU}(n) := \text{U}(n) \cap \text{SL}(n, \mathbb{C})$.

Coming down to degree 2, we first describe the standard explicit homomorphism of $\text{SU}(2)$ onto $\text{SO}(3) := \text{O}(3) \cap \text{SL}(n, \mathbb{R})$. This relies on the fact that $\text{SO}(3)$ consists of rotations in $\mathbb{R}^{(3)}$ about axes through the origin (see e.g. [30, Proposition I.4.1, p. 11]).

Define a monomorphism $\Theta$ from $\text{SU}(2)$ into the multiplicative group of the ring $\mathbb{Q}$ of quaternions as follows: $\Theta$ assigns the element of $\text{SU}(2)$ with first row $(t + xi, y + z) \in \mathbb{Q}$. The image of $\Theta$ is $\mathbb{Q}$, the group of unit quaternions. Then for each $q \in \mathbb{Q}$ define $\Lambda(q) : \mathbb{R}^{(3)} \to \mathbb{R}^{(3)}$ by

$$\Lambda(q) : v \mapsto q^{-1}vq,$$

where $v$ is regarded as an element of $\mathbb{Q}$ (with zero real part). The map $\Lambda$ is a homomorphism from $\mathbb{Q}$ into $\text{GL}(\mathbb{R}^{(3)})$. Choosing the basis $\{i, j, k\}$ of $\mathbb{R}^{(3)}$ yields a representation, which we also denote $\Lambda$, of $\mathbb{Q}$ in $\text{GL}(3, \mathbb{R})$. Indeed, if we write $q = \cos \beta - \sin \beta u$ for some unit vector $u \in \mathbb{R}^{(3)}$, then $\Lambda(q)$ is rotation about the axis parallel to $u$ through an angle $2\beta$. This implies that $\Lambda(q)$ maps $\mathbb{Q}$ onto $\text{SO}(3)$. Also we have ker $\Lambda = \{\pm 1\}$. Thus

Theorem 3.0.5. The composite map $\Lambda \Theta : \text{SU}(2) \to \text{SO}(3)$ is an epimorphism whose kernel is $\langle \text{diag}(-1, -1) \rangle$.  

29
So \( \Theta \theta \) induces an isomorphism between the central quotient \( \text{PSU}(2) \) of \( \text{SU}(2) \) and \( \text{SO}(3) \). There are several accounts of the famous classification of finite subgroups of \( \text{SO}(3) \) up to \( \text{SO}(3) \)-conjugacy. (We remark that by Corollary 3.0.4 (ii), this is a classification of the finite subgroups of \( \text{SL}(3, \mathbb{R}) \), up to conjugacy and isomorphism, at the same time.) For example, see [30, pp. 11–15]. To be very brief, apart from cyclic and dihedral groups, there are copies of \( \text{Alt}(4), \text{Sym}(4) \) and \( \text{Alt}(5) \), which are respectively the symmetry groups of a regular tetrahedron, cube, and regular icosahedron inscribed inside the unit sphere centred at the origin in \( \mathbb{R}^3 \). We postpone identification of explicit generators for each group in this classification until the proof of the next theorem.

Denote \( \langle \text{diag}(-1, -1) \rangle \) by \( Z \) and \( \zeta_n \) as a primitive \( n \)th root of unity.

**Theorem 3.0.6.** A finite subgroup \( G \) of \( \text{PSU}(2) \) is \( \text{PSU}(2) \)-conjugate to one and only one of the following groups:

(i) the cyclic group \( C_n Z/Z \), where \( C_n \) is the cyclic group \( \langle \text{diag}(\zeta_n, \zeta_n^{-1}) \rangle \) of order \( n, n \geq 1 \) (\( C_n \) contains \( Z \) if and only if \( n \) is even);

(ii) the dihedral group \( \hat{D}_n/Z \), where \( \hat{D}_n \) is the dicyclic group of order \( 4n, n \geq 2 \) (also called generalised quaternion if \( n \) is a power of \( 2 \)) generated by

\[
\begin{pmatrix}
\zeta_{2n} & 0 \\
0 & \zeta_{2n}^{-1}
\end{pmatrix}, \quad \begin{pmatrix}
0 & -1 \\
1 & 0
\end{pmatrix};
\]

(iii) \( A^*_4/Z \cong \text{Alt}(4) \), where \( A^*_4 \) is the (unique up to isomorphism) Schur cover of \( \text{Alt}(4) \), generated by

\[
A = \frac{1}{2} \begin{pmatrix}
1 - i & -1 - i \\
1 - i & 1 + i
\end{pmatrix}, \quad \begin{pmatrix}
-i & 0 \\
0 & i
\end{pmatrix};
\]

(iv) \( S^*_4/Z \cong \text{Sym}(4) \), where \( S^*_4 \) is the binary octahedral group, the Schur cover of \( \text{Sym}(4) \) generated by \( A \) as in (iii) and

\[
S = \begin{pmatrix}
\zeta_8^{-1} & 0 \\
0 & \zeta_8
\end{pmatrix}
\]

(v) \( A^*_5/Z \cong \text{Alt}(5) \), where \( A^*_5 \) is the (unique up to isomorphism) Schur cover of \( \text{Alt}(5) \) generated by \( A^*_4 \) and

\[
V = \frac{1}{2} \begin{pmatrix}
-i & 1 + \sqrt{5}/2 + (1 - \sqrt{5}/2)i \\
-(1 + \sqrt{5}/2) + (1 - \sqrt{5}/2)i & i
\end{pmatrix}.
\]
Proof. Let $\tilde{\Theta}$ be the isomorphism $\text{PSU}(2) \to Q_c := Q/\langle -1 \rangle$ induced by $\Theta$, and let $\Lambda$ be the isomorphism $Q_c \to \text{SO}(3)$ induced by $\Lambda$. Recall that $\Theta$ maps $\begin{pmatrix} t + xi & y + zi \\ -y + zi & t - xi \end{pmatrix} \in \text{SU}(2)$ to $t + xi + yj + zk \in Q$.

If $G$ is cyclic of order $n$ then $\Lambda \tilde{\Theta}(G)$ is $\text{SO}(3)$-conjugate to the rotation about $i$ through $2\pi/n$. Hence $\tilde{\Theta}(G)$ is $Q_c$-conjugate to the coset modulo $\langle -1 \rangle$ with representative $\cos(\pi/n) - \sin(\pi/n)i$, and then $G$ is $\text{PSU}(2)$-conjugate to the cyclic group generated by the coset of $Z$ with representative $\text{diag}(\zeta_{2n}, \zeta_{2n}^{-1})$. Certainly $\langle \text{diag}(\zeta_{2n}^{-1}, \zeta_{2n})Z \rangle = C_n Z/Z$ if $n$ is odd, whereas if $n$ is even then $\langle \text{diag}(\zeta_{2n}^{-1}, \zeta_{2n})Z \rangle = C_{2n} Z/Z$.

Suppose that $G$ is dihedral of order $2n$, $n \geq 2$. Then $\Lambda \tilde{\Theta}(G)$ is $\text{SO}(3)$-conjugate to the group generated by the rotation through $2\pi/n$ about $i$, and the rotation through $\pi$ about $j$. Thus $\tilde{\Theta}(G)$ is $Q_c$-conjugate to $\langle \cos(\pi/n) - \sin(\pi/n)i, -j \rangle/\langle -1 \rangle$ and hence $G$ is $\text{PSU}(2)$-conjugate to $\hat{D}_n/Z$. Now $\hat{D}_n$ is an extension of $C_{2n}$ by a cyclic group of order 2; it has presentation $\langle g, h \mid g^{2n} = 1, h^2 = g^n, g^h = g^{-1} \rangle$, which defines a dicyclic group of order $4n$.

If $G \cong \text{Alt}(4)$ then $\tilde{\Theta}(G)$ is $Q_c$-conjugate to $\langle \frac{1}{2}(1 - i - j - k), -i \rangle/\langle -1 \rangle$ so that $G$ is $\text{PSU}(2)$-conjugate to $A_4^* / Z$ as claimed. Since $A^3 = \text{diag}(-1, -1)$ and

$$A \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} A^{-1} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

which squares to $\text{diag}(-1, -1)$, $A_4^*$ is a central extension of a cyclic group of order 2 by $\text{Alt}(4)$ such that $Z$ is contained in the derived subgroup of $A_4^*$. That is, $A_4^*$ is the unique Schur cover of $\text{Alt}(4)$.

Suppose that $G \cong \text{Sym}(4)$. Then $G$ is $\text{PSU}(2)$-conjugate to the subgroup of $\text{PSU}(2)$ generated by $AZ$ and $\Lambda^{-1} \left( \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right) = S$. Note that $A_4^*$ has index 2 in $S_4^*$. Thus $S_4^*$ is a Schur cover of $\text{Sym}(4)$.

Finally suppose that $G \cong \text{Alt}(5)$. It may be verified that $V^2, (GD)^2$, and $\langle \text{diag}(-i, i) \rangle V^3$ are all in $Z$. (Conversely, the entries in $V$ may be directly found by enforcing these constraints; any solution of the resulting system in the matrix entries will do, since we determine $G$ only up to conjugacy, and a single conjugacy class is guaranteed.) $\Lambda \tilde{\Theta}(G)$ is $\text{SO}(3)$-conjugate to $\Lambda \tilde{\Theta}(\langle A_4^*, V \rangle Z)$. Hence $G$ is certainly $\text{PSU}(2)$-conjugate to $A_5^* / Z$. Since the latter group is perfect, $Z$ is contained in the derived group of $A_5^*$, and so $A_5^*$ is the Schur cover of $\text{Alt}(5)$ as claimed. 

\[ \Box \]
Remark 3.0.7. Each of the groups in (ii)–(v) of Theorem 3.0.6 has centre $Z$. Also, $A_4^* = S_4^* \cap A_5^*$.

Theorem 3.0.8. Let $\mathcal{L}$ be the list of finite subgroups of SU(2) consisting of the groups $C_n$, $\hat{D}_m$, $A_4^*$, $S_4^*$ and $A_5^*$, as defined in Theorem 3.0.6, where $n \geq 1$ and $m \geq 2$. A finite subgroup of SU(2) is SU(2)-conjugate to one and only one of the groups in $\mathcal{L}$.

Proof. Of course $C_n$ is not isomorphic to any other group in $\mathcal{L}$. Neither can any of the remaining distinct groups be isomorphic, since their central quotients (being dihedral, Alt(4), Sym(4) or Alt(5)) are different. Hence, the claim on irredundancy of $\mathcal{L}$ is clear. We only have to show completeness.

Let $H$ be a finite subgroup of SU(2). By Theorem 3.0.6, $H^x Z / Z$ is equal to one of the groups $L / Z$ defined in (i)–(v) of that theorem, for some $x \in SU(2)$. This yields two possibilities: (1) $H^x = L$, or (2) $L = H^x \times Z$.

Suppose that $L = C_n Z$. If $n$ is even then (2) cannot occur, because in this case the subgroup of $L$ of index 2 contains $Z$, so (1) is true and consequently $H^x \in L$. If $n$ is odd then certainly $L = C_n \times Z$, but still $H^x = C_n \in \mathcal{L}$.

Suppose that $L = \hat{D}_n$. Every element of $\hat{D}_n$ not in $C_{2n}$ has order 4, so if $n \geq 3$ then $C_{2n}$ is the unique index 2 subgroup of $\hat{D}_n$, and $\hat{D}_n$ does not split over that. If $n = 2$ then $\hat{D}_n = Q_8$ has 3 subgroups of index 2, and still $\hat{D}_n$ does not split over any of them. Therefore (2) cannot occur in this case and $H^x \in \mathcal{L}$.

Suppose that $L = A_4^*$ and (2) is true. Thus $L$ has a subgroup isomorphic to Alt(4) complementing $Z$, and consequently its Sylow 2-subgroup is elementary abelian of order 8. But $\text{diag}(i, -i) \in L$ has order 4. Hence (2) cannot occur.

Suppose that $L = S_4^*$ and (2) is true. Thus $L$ has a subgroup isomorphic to Sym(4) complementing $Z$, and consequently its Sylow 2-subgroup is the direct product of $D_8$ with $Z$. This subgroup has exponent 4. But $S \in L$ has order 8. Hence (2) cannot occur here.

Suppose that $L = A_5^*$ and (2) is true. Then $L$ has a unique subgroup $K$ of index 2 that is isomorphic to Alt(5), and complements $Z$ in $L$. We know that $A_5^* \leq L$ and so if $A_4^* \leq K$ then $K \cap A_4^*$ is a subgroup of $A_4^*$ of index 2 not containing $Z$ — but then $A_4^* \cong \text{Alt}(4) \times Z$, which we have already established is false. Thus completeness of $\mathcal{L}$ is proved.

Remark 3.0.9. As a minor observation, we note that the description of $\mathcal{L}$ confirms that SU(2) has no dihedral subgroups of order $2n > 2$.

We are now able to classify up to GL(2, C)-conjugacy the finite irreducible subgroups of SL(2, C). This parallels [25, Chapter X], which recapitulates material from the earlier
book [2] by Blichfeldt. Our choice of generators (deriving from Theorem 3.0.6) is slightly different from Blichfeldt’s.

**Theorem 3.0.10.** The following are finite irreducible subgroups of $\text{SL}(2, \mathbb{C})$, and any such group is $\text{SL}(2, \mathbb{C})$-conjugate (that is, $\text{GL}(2, \mathbb{C})$-conjugate) to precisely one of them.

(i) $\hat{D}_n$, $n \geq 2$.

(ii) $A_4^*, S_4^*$, $A_5^*$.

The groups in (i) are monomial, and those in (ii) are primitive.

**Proof.** A finite subgroup $G$ of $\text{GL}(2, \mathbb{C})$ is irreducible if and only if it is non-abelian. By Theorem 3.0.8 (and Corollary 3.0.4 (i)), $G$ is therefore conjugate to one of the stated groups. Visibly $\hat{D}_n$ is monomial. If $G$ is one of $A_4^*, S_4^*$, $A_5^*$ and $G$ is imprimitive, then $G$ must be monomial. But then $G$ has an abelian subgroup $A$ of index 2. Since none of $\text{Alt}(4)$, $\text{Sym}(4)$ or $\text{Alt}(5)$ has an abelian subgroup of index 2, we would have to have $G = A \times Z$. But in the proof of Theorem 3.0.8 we specifically ruled this out. Hence $G$ is primitive.  

It will be useful to have a classification of the finite irreducible subgroups of $\text{GL}(2, \mathbb{C})$. As far as we are aware, this has never appeared in full anywhere previously. The classification is provided by the two results below, the first of which may be deduced from [10, Theorems 5.1 and 5.3] (and arguments from first principles for non-modular groups used in their proofs).

**Theorem 3.0.11.** Let $G$ be a finite irreducible monomial subgroup of $\text{GL}(2, \mathbb{C})$. Then $G$ is $\text{GL}(2, \mathbb{C})$-conjugate to one and only one of the following groups:

(i) $\left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \zeta_r & 0 \\ 0 & \zeta_r \end{pmatrix}, \begin{pmatrix} \zeta_s & 0 \\ 0 & \zeta_s^{-1} \end{pmatrix} \right\rangle$  

$\quad r \geq 1, s \geq 3$ and $2 \mid (r + s)$,

(ii) $\left\langle \begin{pmatrix} 0 & \zeta_r \\ \zeta_r & 0 \end{pmatrix}, \begin{pmatrix} \zeta_s & 0 \\ 0 & \zeta_s^{-1} \end{pmatrix} \right\rangle$  

$\quad 4 \mid r$, $2 \mid s$ and $s \geq 4$,

(iii) $\left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \zeta_r^{s+r} & 0 \\ 0 & \zeta_r^{s-r} \end{pmatrix}, \begin{pmatrix} \zeta_s^2 & 0 \\ 0 & \zeta_s^{-2} \end{pmatrix} \right\rangle$  

$\quad 4 \mid r$, $4 \mid s$ and $s \geq 8$.

The approach in the proof of the theorem foreshadows that in Chapter 5. It relies on Theorem 3.0.10 together with the SL-transfer and elementary cohomology theory. This result essentially follows from Theorems 5.4, 5.8 and 5.11 of [11] (see also [10, Theorem 5.4]), which are applicable to non-modular groups in general.
Theorem 3.0.12. Assume the notation of Theorem 3.0.6. Let $G$ be a finite primitive subgroup of $GL(2, \mathbb{C})$, with centre $\langle C \rangle$ of even order.

(i) If $G/Z(G) \cong \text{Alt}(4)$ and $\nu \notin \langle C \rangle$ is a scalar such that $\nu^3 = C$, then $G$ is conjugate to precisely one of $\langle A_4^*, C \rangle$ or $\langle \nu A, \text{diag}(-i, i) \rangle$.

(ii) If $G/Z(G) \cong \text{Sym}(4)$ and $\mu \notin \langle C \rangle$ is a scalar such that $\mu^2 = C$, then $G$ is conjugate to precisely one of $\langle S_4^*, C \rangle$ or $\langle A, \mu S, C \rangle$.

(iii) If $G/Z(G) \cong \text{Alt}(5)$ then $G$ is conjugate to $\langle A_5^*, C \rangle$.

Note that, up to conjugacy, the list of Theorem 3.0.10 is the intersection of the union of the lists in Theorems 3.0.11 and 3.0.12 with $SL(2, \mathbb{C})$.

Theorem 3.0.13. Let $G$ be a finite subgroup of $GL(2, \mathbb{C})$. Then $G$ is cyclic or else one the groups given in either Theorem 3.0.11 or 3.0.12.

Proof. Theorems 3.0.11 and 3.0.12 give all the finite irreducible subgroups of $GL(2, \mathbb{C})$. A finite reducible subgroup of $GL(2, \mathbb{C})$ is conjugate to a diagonal group and hence must be cyclic. \qed
Chapter 4

Order conditions for finite matrix groups

Blichfeldt [2, 25] pioneered the particular kind of linear group theory in this chapter. Here we address problems such as the following: for a given degree $n$, and possible order of a finite non-modular matrix group $G$ of degree $n$, what can we say about the Sylow structure of $G$, or the existence of elements of various orders in $G$. Moreover, J. D. Dixon [5] in the 1970s significantly extended some of Blichfeldt’s work beyond small degrees. Our aim is to provide an accessible and fully justified exposition of Dixon’s and Blichfeldt’s work on these problems. We point out that several results in [2, 25] are missing complete proofs, or contain minor errors. Other material relies on earlier sources, with no apparent connection to the result at hand; here we mention in particular a theorem of Kronecker quoted in [25, p. 240].

4.1 Introduction to Blichfeldt-Dixon methods

We set up some notation, which will be used throughout the chapter. Denote the polynomial ring over a ring $R$ in the indeterminate $X$ by $R[X]$. If $\eta \in \mathbb{C}$ then $\mathbb{Z}[\eta]$ is the image of $\mathbb{Z}[X]$ under the evaluation homomorphism that maps $f(X) \in \mathbb{Z}[X]$ to $f(\eta)$. Let $\zeta_m$ be a primitive $m^{th}$ root of unity in $\mathbb{C}$, and denote the $m^{th}$ cyclotomic polynomial by $\Phi_m(X)$.

Lemma 4.1.1. $\mathbb{Z}[\zeta_m] \cong \mathbb{Z}[X]/\Phi_m(X)\mathbb{Z}[X]$.

Proof. The kernel of the evaluation homomorphism $\mathbb{Z}[X] \rightarrow \mathbb{Z}[\zeta_m]$ consists of all $f(X)$ that have $\zeta_m$ as a root. Since $\Phi_m(X)$ is the minimal polynomial of $\zeta_m$ over $\mathbb{Q}$, we have $f(X) =$
Φ_m(X)q(X) for some q(X) ∈ ℚ[X]. Since Φ_m(X) ∈ ℤ[X] is monic, and f(X) ∈ ℤ[X], in fact q(X) ∈ ℤ[X] (or we can invoke Gauss’s lemma).

**Corollary 4.1.2.** Suppose that f(X) ∈ ℤ[X] and f(ζ_m) = 0 for some ζ_m. Then f(X) is divisible by Φ_m(X) in ℤ[X].

Let p ∈ ℤ be a prime.

**Lemma 4.1.3.** If e is coprime to m then Φ_m(ζ_p^e m) ≡ 0 mod pℤ[ζ_m] for all i ≥ 0.

**Proof.** Since Φ_m(X)p - Φ_m(X^p) ∈ pℤ[X], we get the result after taking X = ζ_m^e.

We use the above to ensure that maps on rings of algebraic integers of the form ℤ[η] are well-defined. The point is that an element of ℤ[η] does not have a unique expression as a linear combination of powers of η with integer coefficients, i.e. \( \sum_{i} a_i \eta^i = \sum_{i} b_i \eta^i \) does not necessarily imply that \( a_i = b_i \).

**Lemma 4.1.4.** Let r be a non-negative integer, and denote the ring of integers modulo p by ℤ_p. The map \( \theta : ℤ[ζ_m] \to ℤ_p[ζ_m] \cong ℤ[ζ_m]/pℤ[ζ_m] \) given by

\[
\theta : \sum_{i} a_i ζ_m^i \mapsto \sum_{i} [a_i]_p \cdot ζ_m^{p^i}
\]

is a ring homomorphism, where the \([ \cdot ]_p\) denotes reduction modulo p (in ℤ).

**Proof.** All that really needs to be verified is that \( \theta \) is well-defined. This follows from Corollary 4.1.2 and Lemma 4.1.3.

In the case that \( p^r \) is the largest power of p dividing m, as a shorthand we will denote the image of \( α \in ℤ[ζ_m] \) under the ring homomorphism \( \theta \) defined by Eq.(4.1) by \([ α ]_p\). Note that in general the finite ring \( ℤ_p[ζ_m] \) is not a field.

The next lemma is inspired by ideas from Blichfeldt [25, §118, pp. 246–247].

**Lemma 4.1.5.** Let G ≤ GL(n, ℂ) be finite of order m, with Sylow p-subgroup of order \( p^r \). Since \( \text{tr}(G) = \{ \text{tr}(g) \mid g ∈ G \} \subseteq ℤ[ζ_m] \), we may define the homomorphism as per Eq.(4.1) on \( \text{tr}(G) \). The subset

\[
N_p = \{ α ∈ G \mid [\text{tr}(ga)]_p = [\text{tr}(g)]_p \quad ∀ g ∈ G \}
\]

of G is a normal subgroup.
4.1. INTRODUCTION TO BLICHFELDT-DIXON METHODS

Proof. If \(a, b \in N_p\) then \([\text{tr}(g(ab))]_p = [\text{tr}((ga)b)]_p = [\text{tr}(ga)]_p = [\text{tr}(g)]_p\) for all \(g \in G\). Hence \(N_p\) is a subgroup of \(G\). If \(x \in G\) then \([\text{tr}(gx^{-1}ax)]_p = [\text{tr}(xgx^{-1}a)]_p = [\text{tr}(xgx^{-1})]_p = [\text{tr}(g)]_p\). So \(N_p\) is indeed normal in \(G\). □

Remark 4.1.6. \([\text{tr}(a)]_p \equiv n \mod p\mathbb{Z}[\zeta_m]\) for all \(a \in N_p\).

Lemma 4.1.7. Assuming the hypotheses and notation of Lemma 4.1.5, the following hold.

(i) If \(N_p\mathbb{Z}(G)/\mathbb{Z}(G)\) is not a \(p\)-group then \(p < n\).

(ii) If \(n \leq 3\) and \(G \leq \text{SL}(n, \mathbb{C})\), then \(N_p\mathbb{Z}(G)/\mathbb{Z}(G)\) is a (possibly trivial) normal \(p\)-subgroup of \(G/\mathbb{Z}(G)\).

Proof. (Cf. [25, §119, p. 247].) Suppose that there exists \(x \in N_p \setminus (\mathbb{Z}(G) \cap N_p)\) of order \(e\) say, where \(e \neq p\) is prime. Let \(\epsilon_1, \ldots, \epsilon_n\) be the eigenvalues of \(x\) (including multiplicities). Then for each \(j \geq 1\),

\[
\left\lfloor \sum_{k=1}^{n} \epsilon_k^j \right\rfloor_p \equiv \left\lfloor \text{tr}(x^j) \right\rfloor_p \equiv n \mod p\mathbb{Z}[\zeta_m].
\] (4.2)

Fix \(i\). Multiplying both sides of Eq.(4.2) by \(\left\lfloor \epsilon_i^{-j} \right\rfloor_p\) and then summing over \(j\) yields

\[
\left\lfloor \sum_{k=1}^{n} \sum_{j=1}^{e} (\epsilon_i^{-1} \epsilon_k)^j \right\rfloor_p \equiv n \left\lfloor \sum_{j=1}^{e} \epsilon_i^{-j} \right\rfloor_p \mod p\mathbb{Z}[\zeta_m].
\] (4.3)

Now for any \(e\)th root of unity \(\epsilon \neq 1\), \(\sum_{j=1}^{e} \epsilon^j = 0\). Thus, the right hand side of Eq.(4.3) is \(en \mod p\mathbb{Z}[\zeta_m]\) if \(\epsilon_i = 1\), and is \(0 \mod p\mathbb{Z}[\zeta_m]\) otherwise. On the left hand side, let \(l_i\) be the number of \(k\) such that \(\epsilon_k = \epsilon_i\); note that \(1 \leq l_i \leq n - 1\) since \(x\) is non-scalar. Hence the left hand side of Eq.(4.3) is \(el_i \mod p\mathbb{Z}[\zeta_m]\), and so

\[
l_i \equiv \begin{cases} n & \epsilon_i = 1 \\ 0 & \epsilon_i \neq 1 \end{cases} \mod p
\] (4.4)

as \(e\) is invertible mod \(p\) (the only rational algebraic integers are ordinary integers). In particular, this proves (i).

Now suppose that \(n = 3\) and \(G \leq \text{SL}(n, \mathbb{C})\), so that \(p = 2\) by (i). Since \(x\) is non-scalar, at least one of its eigenvalues has multiplicity 1. By Eq.(4.4), an eigenvalue of \(x\) with multiplicity 1 must be 1, and the remaining eigenvalue has multiplicity 2. But then we get the contradiction that \(x^2 = 1\). □
Remark 4.1.8. (i) In the situation of Lemma 4.1.7 (i), for degrees \( n \leq 5 \), \( G \) must be soluble (since the only allowable primes dividing \(|G|\) are 2 and 3).

(ii) Lemma 4.1.7 (ii) cannot be extended beyond degree 3. For example, in degree 4, an element with two eigenvalues each of multiplicity 2 does not give a contradiction against Eq.(4.4).

When we later refer to Lemmas 4.1.5 and 4.1.7, we will need to demonstrate in certain situations that \( N_p \) is non-trivial — in fact, is non-central.

Proposition 4.1.9. Let \( G \) be a finite subgroup of \( GL(n, \mathbb{C}) \). Suppose that \( G \) has an element \( x \) of order \( p^s q^t \), \( s \geq 1 \), where \( p \) and \( q \) are distinct primes, \( x^{p^s} \) is scalar, and \( x^p \) has pairwise distinct eigenvalues. Then the following hold.

(i) \( x^q \in N_p \), where \( N_p \) is as defined in Lemma 4.1.5.

(ii) If \( x^q \notin Z(G) \) then \( N_p \) is a non-central normal subgroup of \( G \).

Proof. This proposition generalises results of Blichfeldt [25, pp. 248–249]. Part (ii) is a trivial consequence of part (i), by Lemma 4.1.5. We recall that the effect of the homomorphism defined by Eq.(4.1) on \(|G|\)th roots of unity is to raise them to the power \( p^r \mod p \mathbb{Z}[\zeta] \), where \( \zeta = \zeta_{|G|} \) and \( p^r \) is the order of a Sylow \( p \)-subgroup of \( G \).

Up to conjugacy, \( x \) is diagonal. So let \( x = \text{diag}(x_1, \ldots, x_n) \). Let \( u \) be any element of \( G \), with main diagonal entries \( u_1, \ldots, u_n \) say. Then

\[
\begin{pmatrix}
\text{tr}(u) & 1 & \ldots & 1 \\
\text{tr}(ux^q) & x_1^q & \ldots & x_n^q \\
\text{tr}(ux^p) & x_1^p & \ldots & x_n^p \\
\vdots & \vdots & \ddots & \vdots \\
\text{tr}(ux^{(n-1)p}) & x_1^{(n-1)p} & \ldots & x_n^{(n-1)p}
\end{pmatrix}
\begin{pmatrix}
-1 \\
\vdots \\
\vdots \\
1 \\
u_1 \\
u_2 \\
\vdots \\
u_n
\end{pmatrix}
= \begin{pmatrix}
0 \\
0 \\
\vdots \\
0
\end{pmatrix}_{(n+1) \times 1}, \quad (4.5)
\]

and from this it follows that

\[
\det\left(
\begin{pmatrix}
\text{tr}(u) & 1 & \ldots & 1 \\
\text{tr}(ux^q) & x_1^q & \ldots & x_n^q \\
\text{tr}(ux^p) & x_1^p & \ldots & x_n^p \\
\vdots & \vdots & \ddots & \vdots \\
\text{tr}(ux^{(n-1)p}) & x_1^{(n-1)p} & \ldots & x_n^{(n-1)p}
\end{pmatrix}
\right) = 0. \quad (4.6)
\]

We now apply the homomorphism in Eq.(4.1) to Eq.(4.6). (Note that it was necessary to first eliminate the \( u_i \)s from Eq.(4.5), because the homomorphism is defined on \( \mathbb{Z}[\zeta] \) and \( u_i \)
4.2 The Blichfeldt-Dixon criterion for normality of Sylow subgroups

In this section we expand and modify work of Dixon [5, pp. 90–94]. The main result is Theorem 4.2.3, which was essentially observed by Blichfeldt in a special case (see [25, §117, Theorem 13]).

We start with a technical lemma, which amends and amplifies [5, Lemma 5.5, p. 91] with a view to its later application in the proof of Lemma 4.2.2 below.

Lemma 4.2.1. Let $p$ be prime, $m$ be a positive integer coprime to $p$, and $m_1, \ldots, m_s$ be the distinct primes dividing $m$. Define

$$
\epsilon_i := \begin{cases} 
1, & i = 0 \\
(-1)^t, & i > 0 \text{ and } \zeta_m^i = \prod_{k=1}^t \zeta_{m_{j_k}} \text{ for some distinct } j_k \\
0, & \text{otherwise.}
\end{cases}
$$
Suppose that \( \alpha = \sum_{i=0}^{m-1} a_i \zeta^i_m \in \mathbb{Z}[\zeta_m] \) and \( \alpha \equiv 0 \mod p\mathbb{Z}[\zeta_u] \) where \( u = p^r m, \ r \geq 0 \). Then
\[
\tilde{\alpha} := \sum_{i=0}^{m-1} a_i \epsilon_i \equiv 0 \mod p.
\]

**Proof.** For each \( i, \)
\[
\sum_{k=1}^{m} \left( \prod_{l=1}^{s} (1 - \zeta^{-k}_{m_l}) \right) \zeta_m \epsilon_i = \sum_{k=1}^{m} \zeta_m \epsilon_i + \sum_{1 \leq j_1 < \ldots < j_t \leq s} (-1)^t (\zeta_{m_{j_1}} \cdots \zeta_{m_{j_t}})^{-k} \zeta_m \epsilon_i
\]
\[
= \begin{cases} 
\sum_{1 \leq j_1 < \ldots < j_t \leq s} (-1)^t \sum_{k=1}^{m} ((\zeta_{m_{j_1}} \cdots \zeta_{m_{j_t}})^{-1} \zeta_m)^k, & \zeta_m \epsilon_i \neq 1 \\
\sum_{l=1}^{s} (1 - \zeta^{-k}_{m_l}) \zeta_m \epsilon_i, & m, \\
0, & \text{otherwise}.
\end{cases}
\]

Also,
\[
\sum_{k=1}^{m} ((\zeta_{m_{j_1}} \cdots \zeta_{m_{j_t}})^{-1} \zeta_m)^k = \begin{cases} 
m, & \zeta_m = \zeta_{m_{j_1}} \cdots \zeta_{m_{j_t}} \\
0, & \text{otherwise}.
\end{cases}
\]

Now either there is no sequence \( 1 \leq j_1 < \cdots < j_t \leq s \) such that \( \zeta_m \epsilon_i = \zeta_{m_{j_1}} \cdots \zeta_{m_{j_t}} \), or there is a unique sequence \( 1 \leq j_1 < \cdots < j_t \leq s \) such that \( \zeta_m \epsilon_i = \zeta_{m_{j_1}} \cdots \zeta_{m_{j_t}} \). Therefore
\[
\sum_{k=1}^{m} \left( \prod_{l=1}^{s} (1 - \zeta^{-k}_{m_l}) \zeta_m \epsilon_i \right) = m \epsilon_i.
\]

Now let \( k \leq m \) be a positive integer coprime to \( m \), so that \( k = p^t e \) for some \( e \) coprime to \( u \). Using Lemma 4.1.3 (and cf. Lemma 4.1.4), we may check readily that the map
\[
\sum_{i=0}^{u-1} a_i \zeta^i_u \mapsto \left( \sum_{i=0}^{u-1} a_i \zeta^i_u \right) + p\mathbb{Z}[\zeta_u]
\]
is a well-defined ring homomorphism \( \mathbb{Z}[\zeta_u] \rightarrow \mathbb{Z}[\zeta_u]/p\mathbb{Z}[\zeta_u] \). Therefore \( \alpha \in p\mathbb{Z}[\zeta_u] \) implies that
\[
\sum_{i=0}^{m-1} a_i \zeta^i_m \epsilon_i \in p\mathbb{Z}[\zeta_u].
\]

Since \( \prod_{l=1}^{s} (1 - \zeta^{-k}_{m_l}) \in \mathbb{Z}[\zeta_u] \) we then get
\[
\sum_{i=0}^{m-1} a_i \sum_{k=1}^{m} \left( \prod_{l=1}^{s} (1 - \zeta^{-k}_{m_l}) \zeta^i_m \right) \epsilon_i \in p\mathbb{Z}[\zeta_u].
\]

(4.10)
4.2. THE BLICHFELDT-DIXON CRITERION FOR NORMALITY OF SYLOW SUBGROUPS

The second summation in Eq. (4.10) can actually be taken over all indices \( k \), for if \( k \) is not coprime to \( m \) then some factor \( 1 - \zeta_m^{-k} \) is zero and the \( k \)th term contributes nothing to the sum. By Eq. (4.9), we therefore get

\[
m \sum_{i=0}^{m-1} a_i \epsilon_i \in p\mathbb{Z}[\zeta_m],
\]

i.e. \( m \sum_{i=0}^{m-1} a_i \epsilon_i \in p\mathbb{Z} \). Hence \( \sum_{i=0}^{m-1} a_i \epsilon_i \in p\mathbb{Z} \), since \( m \) and \( p \) are coprime. \( \square \)

We make some comments on Lemma 4.2.1 and its proof. The map \( \zeta_m \mapsto \epsilon_i \) is the same as that explicated by Blichfeldt in [25, pp. 243–244]. Notice also that for a fixed expression of \( \alpha \) as a \( \mathbb{Z} \)-linear combination of powers of \( \zeta_m \), the definition of \( \alpha \) depends only on the choice of the Sylow subgroup generators \( \zeta_m \) in \( \langle \zeta_m \rangle \). The freedom allowed in this choice will be vital in proving the following deep result. Again, the proof is a slight amendment and fully justified version of Dixon’s reasoning [5, pp. 92–94]. His proof is a major extension of Blichfeldt’s proof in degree 3.

**Lemma 4.2.2.** Let \( G \) be a finite subgroup of \( \text{GL}(n, \mathbb{C}) \). Suppose that \( p > 2n \) is a prime dividing \( |G| \), such that \( G \) does not have a normal Sylow \( p \)-subgroup. Then there exists a non-constant polynomial \( \ell(X) \in \mathbb{Z}_p[X] \) of degree at most \( n - 1 \) such that

\[
\{ \ell(h) \mid h \in \mathbb{Z}_p \} \subseteq \{0, \pm1, \ldots, \pm n\} \mod p.
\]

**Proof.** Our first objective is to obtain a certain congruence mod \( p \), from Lemma 4.2.1 and manipulations in rings of algebraic integers containing the traces of elements of \( G \). This will give us the required \( \mathbb{Z}_p \)-polynomial.

Say \( |G| = p^r \cdot m \) where \( m \) is coprime to \( p \), and let \( \zeta = \zeta_{p^r} \cdot m \), so that \( \langle \zeta \rangle = \langle \zeta_{p^r}, \zeta_m \rangle \). We employ the following repeatedly: if \( a_1, \ldots, a_k \in \mathbb{Z}[\zeta] \) then

\[
(a_1 + \cdots + a_k)^{p^r} \equiv a_1^{p^r} + \cdots + a_k^{p^r} \mod p\mathbb{Z}[\zeta].
\]

Thus

\[
a^{p^r} \in \mathbb{Z}[\zeta_m] \mod p\mathbb{Z}[\zeta] \quad \forall a \in \mathbb{Z}[\zeta].
\]

Select a non-trivial \( p \)-element \( x \) of \( G \), with minimal polynomial \( f(X) \) of degree \( d \). The coefficients of \( f(X) \) are elements of \( \mathbb{Z}[\zeta_{p^r}] \). We claim that, for each integer \( h \geq 0 \), there are unique \( \alpha_{h,i} \in \mathbb{Z}[\zeta_{p^r}] \) such that

\[
X^h = \sum_{i=0}^{d-1} \alpha_{h,i}(X - 1)^i + f(X)g(X)
\]

(4.13)
for some \( g(X) \in \mathbb{Z}[\zeta_{p^r}][X] \). If \( h \leq d - 1 \) then this is clear: put \( g(X) = 0 \), \( \alpha_{h,i} = 0 \) for all \( i > h \), and \( \alpha_{h,i} = \binom{h}{i} \) for \( i \leq h \). If \( h \geq d \) then existence and uniqueness of the \( \alpha_{h,i} \) are guaranteed after division in \( \mathbb{C}[X] \) of \( X^h \) by the monic polynomial \( f(X) \in \mathbb{Z}[\zeta_{p^r}][X] \).

Let \( y \) be any \( p \)-element of \( G \). Taking \( X = x \) in Eq.(4.13), multiplying both sides by \( y \) and then taking traces, yields

\[
\text{tr}(x^hy) = \sum_{i=0}^{d-1} \alpha_{h,i} \text{tr}((x - 1)^iy).
\]

(4.14)

Set \( \tau_h \) to be the sum of the \( p^r \)th powers of the eigenvalues of \( x^hy \) (including multiplicities). By Eqs.(4.11) and (4.14),

\[
\tau_h \equiv \sum_{i=0}^{d-1} \alpha_{h,i}^p \text{tr}((x - 1)^iy)^{p^r} \mod p\mathbb{Z}[\zeta];
\]

(4.15)

and \( \text{tr}((x - 1)^iy)^{p^r} \in p\mathbb{Z}[\zeta_{p^r}] \mod p\mathbb{Z}[\zeta] \) by Eq.(4.12).

Next, we concentrate on the terms \( \alpha_{h,i}^p \) in Eq.(4.15), finding a more explicit description of them. If \( h \leq d - 1 \) then \( \alpha_{h,i}^p \equiv \binom{h}{i} \mod p \). So let us suppose that \( h \geq d \). By Eq.(4.11), \( f(X)^{p^r} \equiv (X^{p^r} - 1)^d \mod p\mathbb{Z}[\zeta][X] \). Then from Eqs.(4.13) and (4.11),

\[
X^{hp^r} \equiv \sum_{i=0}^{d-1} \alpha_{h,i}^p (X^{p^r} - 1)^i + (X^{p^r} - 1)^d g(X)^{p^r} \mod p\mathbb{Z}[\zeta][X].
\]

(4.16)

Now since \( g(X) \in \mathbb{Z}[\zeta_{p^r}][X] \), we have \( g(X)^{p^r} \in \mathbb{Z}[X^{p^r}] \mod p\mathbb{Z}[\zeta][X] \), again by Eq.(4.11). In fact we may take \( g(X)^{p^r} \in \mathbb{Z}[X^{p^r} - 1] \mod p\mathbb{Z}[\zeta][X] \), by change of variable. Subtracting Eq.(4.16) from \( X^{hp^r} = \sum_{i=0}^{h} \binom{h}{i} (X^{p^r} - 1)^i \) gives

\[
\sum_{i=0}^{h} c_i (X^{p^r} - 1)^i \in p\mathbb{Z}[\zeta][X]
\]

(4.17)

where \( c_i = \binom{h}{i} - \alpha_{h,i}^p \) for \( 0 \leq i \leq d - 1 \) and \( c_i \in \mathbb{Z} \) for \( d \leq i \leq h \). It is clear from Eq.(4.17) that each of the coefficients \( c_i \) is in \( p\mathbb{Z}[\zeta] \). Hence

\[
\alpha_{h,i}^p \equiv \binom{h}{i} \mod p\mathbb{Z}[\zeta]
\]

for all \( h \) and \( i \). Then inserting into Eq.(4.15) gives

\[
\tau_h \equiv \sum_{i=0}^{d-1} \binom{h}{i} \text{tr}((x - 1)^iy)^{p^r} \mod p\mathbb{Z}[\zeta].
\]

(4.18)
We rewrite Eq.(4.18) as
\[ \tau_h \equiv \sum_{i=0}^{d-1} a_i(h)\beta_i \mod p\mathbb{Z}[\zeta] \quad (4.19) \]
where each \( a_i(h) \) is a polynomial in \( h \) over \( \mathbb{Z}_p \) of degree \( i \leq d - 1 \leq n - 1 \), and \( \beta_i \in \mathbb{Z}[\zeta_m] \), \( \beta_i \equiv \text{tr}((x - 1)^i y^{pr}) \mod p\mathbb{Z}[\zeta] \), by Eq.(4.12).

By definition, \( \tau_h \in \mathbb{Z}[\zeta_m] \). We apply Lemma 4.2.1 to Eq.(4.19), obtaining
\[ t_h \equiv \sum_{i=0}^{d-1} a_i(h)b_i \mod p \quad (4.20) \]
where \( t_h = \bar{\tau}_h \) and \( b_i = \tilde{\beta}_i \). (in the notation of Lemma 4.2.1).

The derivation of Eq.(4.20) achieves the first objective of the proof. To complete the proof, we bring in the hypotheses that \( p > 2n \), and that \( G \) does not have a normal Sylow \( p \)-subgroup.

We can choose the \( p \)-element \( y \) so that \( xy \) is not a \( p \)-element. Since \( \tau_h \) is a sum of \( n \) powers of \( \zeta_n \), \( |t_h| \leq n \) by Lemma 4.2.1. In particular, since the order of \( y \) divides \( p^r \), \( \tau_0 = n \) and so \( t_0 = n \). On the other hand, since \( xy \) is not a \( p \)-element, \( \tau_1 \in \mathbb{Z}[\zeta_m] \) must contain at least one non-trivial power of \( \zeta_m \). If one of these powers yields \(-1\) in applying Lemma 4.2.1 then \( t_1 \neq n \). If all such powers yield \( 1 \) then \( m \) is divisible by more than one prime, and we make a different choice of some \( \zeta_m \) in Lemma 4.2.1 so that in re-applying the lemma, at least one non-trivial power of \( \zeta_m \) that previously yielded \( 1 \) now yields \(-1\) or \( 0 \). So it is always possible to arrange that \( t_1 \neq n \).

Let \( \ell(X) = \sum_{i=0}^{d-1} a_i(X)[b_i]_{p^r} \). The preceding paragraph shows that \( \ell(X) \) is not a constant polynomial in \( \mathbb{Z}_p[X] \). For if it were then \( p \) would have to divide \((n - t_1)\), but \( 0 < n - t_1 \leq 2n < p \). Now \( |t_h| \leq n \), so \( \ell(h) \in \{0, \pm 1, \ldots, \pm n\} \mod p \). Since the degree of \( \ell(h) \) is no more than \( d - 1 \leq n - 1 \), this completes the proof. \( \square \)

**Theorem 4.2.3.** Let \( G \) be a finite subgroup of \( \text{GL}(n, \mathbb{C}) \). If \( p > (2n+1)(n-1) \) is a prime dividing \( |G| \), then \( G \) has a normal Sylow \( p \)-subgroup.

**Proof.** (Cf. [5, Theorem 5.5, pp. 92–94].) Suppose that \( G \) does not have a normal Sylow \( p \)-subgroup. Then there is \( \ell(X) \in \mathbb{Z}_p[X] \) as in Lemma 4.2.2. Define an equivalence relation \( \sim \) on \( \mathbb{Z}_p \) by
\[ h_1 \sim h_2 \iff \ell(h_1) \equiv \ell(h_2) \mod p. \]

By Lemma 4.2.2, the number \( e \) of equivalence classes is at most \( 2n + 1 \). On the other hand, the maximum size of an equivalence class is \( n-1 \), because every element in a class is a root of a polynomial of degree at most \( n-1 \) over the field \( \mathbb{Z}_p \). It follows that the minimum total
number of equivalence classes in $\mathbb{Z}_p$ is $p/(n-1)$. Thus $p/(n-1) \leq e \leq 2n+1$, contrary to the hypothesis $p > (2n+1)(n-1)$.

Theorem 4.2.3 is an extraordinary result. It may be stated equivalently as follows.

**Theorem 4.2.4.** Let $G$ be a finite non-modular subgroup of $\text{GL}(n, \mathbb{F})$. If $G$ has more than one Sylow $p$-subgroup, then $p \leq (2n+1)(n-1)$.

Feit and Thompson improved upon the above: they showed that if $p > 2n+1$ then a Sylow $p$-subgroup of a finite subgroup $G$ of $\text{GL}(n, \mathbb{C})$ is normal. (Moreover, that Sylow subgroup is abelian. See [8], [17, p. 248], and cf. Lemma 2.7.4.) However, their proof makes use of deep methods from character theory. We have chosen not to rely on Feit and Thompson’s theorem; our intention in this section was to provide a completely accessible treatment of the Blichfeldt-Dixon result (Theorem 4.2.4), which is lacking in the literature. Moreover, the methods used to prove Theorem 4.2.4 set the stage for some of the manipulations in the next chapter.

### 4.3 Existence of elements of composite order in finite linear groups

In this section we give an account of techniques (once more essentially due to Blichfeldt and Dixon) for proving the existence of elements of composite order $mn$ in a finite irreducible linear group, when the existence of elements of orders $m$ and $n$ is known.

Blichfeldt’s approach in [2, 25] relies crucially on a result attributed to Kronecker [21]. However, neither that result, nor a proof of it, actually appears in [21]. To sidestep this obscurity, we present a simplified version of Dixon’s re-telling of a proof due to Brauer (see [5, §5.3, pp. 84–87]). Only basic character theory and Galois theory are required.

Denote the $m$th cyclotomic field by $\mathbb{Q}_m$, i.e. $\mathbb{Q}_m = \mathbb{Q}(\zeta_m)$. The degree of $\mathbb{Q}_m$ as an extension of $\mathbb{Q}$ is the degree $\varphi(m)$ of $\Phi_m(X)$. The field extension $\mathbb{Q}_m/\mathbb{Q}$ is a Galois abelian extension, i.e. the Galois group $\text{Gal}(\mathbb{Q}_m/\mathbb{Q})$ is abelian. For proofs of these facts and of the following lemma, see e.g. [18, pp. 310–313].

**Lemma 4.3.1.** (i) $\mathbb{Q}_r \cap \mathbb{Q}_s = \mathbb{Q}_{\gcd(r,s)}$; (ii) $\langle \mathbb{Q}_r, \mathbb{Q}_s \rangle = \mathbb{Q}_{\text{lcm}(r,s)}$.

Let $\alpha$ be an element of some cyclotomic field. We call the smallest positive integer $r$ such that $\alpha \in \mathbb{Q}_r$ the **cyclotomic level** of $\alpha$. If $G$ is a finite subgroup of $\text{GL}(n, \mathbb{C})$ then $\text{tr}(g)$ has a defined cyclotomic level for each $g \in G$. 


4.3. EXISTENCE OF ELEMENTS OF COMPOSITE ORDER IN FINITE LINEAR GROUPS

Lemma 4.3.2. If $\alpha \in \mathbb{Q}_m$ has cyclotomic level $r$ then $r$ divides $m$.

Proof. This follows immediately from Lemma 4.3.1 (i).

Lemma 4.3.3. If $g \in \text{GL}(n, \mathbb{C})$ has finite order, then the cyclotomic level of $\text{tr}(g)$ divides $|g|$.

Proof. As $\text{tr}(g) \in \mathbb{Q}_{|g|}$, the result is clear by Lemma 4.3.2.

Lemma 4.3.4. Suppose that $g \in \text{GL}(n, \mathbb{C})$ has prime order $p > n + 1$. Then $\text{tr}(g)$ has cyclotomic level $p$.

Proof. Let $m_i$ denote the multiplicity of $\zeta_p^i$ as an eigenvalue of $g$, and define $f(X) = \sum_{i=0}^{p-1} m_i X^i \in \mathbb{Z}[X]$. By Lemma 4.3.3, if $a := \text{tr}(g)$ does not have cyclotomic level $p$ then $a \in \mathbb{Q}$. Further, $f(X) - a$ is divisible by $\Phi_p(X) = X^{p-1} + \cdots + X + 1$, so we must have $m_1 = \cdots = m_{p-1}$. But if $m_1 > 0$ then $n = m_0 + \sum_{i=1}^{p-1} m_i \geq p - 1$, contradicting $n < p - 1$. Hence $m_1 = 0$, i.e. $g = 1$, another contradiction.

The next theorem has roots going back to an exercise in [25, p. 268]. It can be proved for any number of primes (see [5, Lemma 5.3B, p. 85]). We give a proof for just two primes.

Theorem 4.3.5. Let $G$ be a finite irreducible subgroup of $\text{GL}(n, \mathbb{C})$ of order divisible by $pq$, where $p$, $q$ are distinct primes. Suppose that $G$ has elements $g, h$ such that $\text{tr}(g)$ has cyclotomic level $p^i$ and $\text{tr}(h)$ has cyclotomic level $q^j$, $i, j \geq 1$. Then $G$ has an element of order $p^i q^j$.

Proof. Say $|G| = p^r q^s t$, where $t$ is coprime to both $p$ and $q$. Define $l = p^{i-1} q^{j-1} t$ and $m = p^i q^j t$. By Lemma 4.3.2, $\text{tr}(g) \notin \mathbb{Q}_l$ and $\text{tr}(h) \notin \mathbb{Q}_m$. However, because $p^i$ divides $m$ and $q^j$ divides $l$, we have $\text{tr}(g) \in \mathbb{Q}_m$ and $\text{tr}(h) \in \mathbb{Q}_l$. Hence there exist $\alpha \in \text{Gal}(\mathbb{Q}_l/\mathbb{Q}_l)$ and $\beta \in \text{Gal}(\mathbb{Q}_l/\mathbb{Q}_m)$ such that $\alpha(\text{tr}(g)) \neq \text{tr}(g)$ and $\beta(\text{tr}(h)) \neq \text{tr}(h)$; whereas $\beta(\text{tr}(g)) = \text{tr}(g)$ and $\alpha(\text{tr}(h)) = \text{tr}(h)$.

Suppose that for all $y \in G$, either $\alpha(\text{tr}(y)) = \text{tr}(y)$ or $\beta(\text{tr}(y)) = \text{tr}(y)$. Since $\alpha \beta = \beta \alpha$,

$$\text{tr}(y) - \alpha(\text{tr}(y)) - \beta(\text{tr}(y)) + \beta \alpha(\text{tr}(y)) = 0$$ (4.21)

for all $y \in G$. The linear dependence in Eq.(4.21) between the irreducible characters $\text{tr}$, $\alpha \text{tr}$, $\beta \text{tr}$ and $\beta \alpha \text{tr}$ of $G$ implies that they cannot all be distinct. However, these characters certainly are distinct, as we see from their values on $g$ and $h$.

It follows that $G$ must have an element $x$ such that $\text{tr}(x) \notin \mathbb{Q}_l$ and $\text{tr}(x) \notin \mathbb{Q}_m$. Hence the cyclotomic level $c$ of $\text{tr}(x)$ must be divisible by $p^i$; if not then $c$ divides $l$ and hence $\text{tr}(x) \in \mathbb{Q}_c \subseteq \mathbb{Q}_l$. Similarly $c$ is divisible by $q^j$. We are done by Lemma 4.3.3. □
4.3. EXISTENCE OF ELEMENTS OF COMPOSITE ORDER IN FINITE LINEAR GROUPS

To conclude the chapter, we say a little about the approach taken by Blichfeldt to prove Theorem 4.3.5. In [25, §6, pp. 240–241], a special case of the following is cited as a consequence of a theorem of Kronecker [21]. (The problem of determining linear dependencies between roots of unity is a classical one, on which much work has been undertaken; see [23] for recent progress.)

**Theorem 4.3.6.** Suppose that \( \alpha_i \in \mathbb{C}, 1 \leq i \leq n, \) are roots of unity such that \( \sum_{i=1}^{n} \alpha_i = 0. \) Then there exist roots of unity \( \mu_1, \ldots, \mu_l, \beta_1, \ldots, \beta_m, \) primes \( p_1, \ldots, p_m \leq n, \) and primitive \( p_i \)th roots of unity \( \omega_i, \) such that the sequence \( (\alpha_1, \ldots, \alpha_n, \mu_1, -\mu_1, \ldots, \mu_l, -\mu_l) \) equals

\[
(\beta_1, \beta_1 \omega_1, \ldots, \beta_1 \omega_1^{p_1-1}, \beta_2, \beta_2 \omega_2, \ldots, \beta_2 \omega_2^{p_2-1}, \ldots, \beta_m, \beta_m \omega_m, \ldots, \beta_m \omega_m^{p_m-1})
\]

(4.22)

up to re-ordering.

Let us call a sequence of roots of unity summing to zero that may be re-ordered into a sequence of the form in (4.22) ‘arrangeable’. Theorem 4.3.6 includes the possibility \( l = 0. \) But it is easily seen why the original sequence \( (\alpha_1, \ldots, \alpha_n) \) may need to be expanded to obtain an arrangeable sequence. For example, \( (\omega, \ldots, \omega^{p-1}, -\mu, -\mu^2, \ldots, -\mu^{q-1}) \), where \(|\omega| = p, |\mu| = q, p, q \) distinct primes, becomes arrangeable only after the addition of \((1, -1)\).

For another example, note that \( \Phi_{15}(\zeta_3 \zeta_5) = 0 \) implies that the sequence of roots

\[
(\zeta_3^2 \zeta_5^3, -\zeta_3 \zeta_5^2, \zeta_3^2, -\zeta_3 \zeta_5^4, \zeta_5^3, -\zeta_3 \zeta_5, 1)
\]

sums to zero. However, this sequence is definitely not arrangeable. We add pairs of cancelling roots to obtain the arrangeable sequence

\[
(\zeta_3^2 \zeta_5^3, -\zeta_3 \zeta_5^2, \zeta_3^2, -\zeta_3 \zeta_5^4, \zeta_5^3, -\zeta_3 \zeta_5, 1, -\zeta_3, \zeta_3, -\zeta_3 \zeta_5^2, \zeta_3 \zeta_5^3).
\]

This example is minimal: it is a shortest sequence of roots of unity that sums to zero that is not arrangeable.

As Theorem 4.3.6 indicates, the possibilities for the roots of unity in a vanishing sum of \( n \) roots are related to the primes in decompositions of \( n \) as a sum of primes. This is also the content of the following result, due to Lam and Leung [23].

**Theorem 4.3.7.** Suppose that \( \alpha_1, \ldots, \alpha_n \in \mathbb{C} \) are \( m \)th roots of unity such that \( \sum_{i=1}^{n} \alpha_i = 0, \) and denote by \( \pi \) the set of all primes that appear in the prime factorisation of \( m. \) Then \( n = \sum_{p_i \in \pi} a_i p_i \) where the \( a_i \) are non-negative integers.

Thus, the number of summands in a vanishing sum of roots of unity of order dividing \( pq, \) where \( p \) and \( q \) are primes, is \( ap + bq \) for some non-negative integers \( a, b. \) Moreover, if \( (\alpha_1, \ldots, \alpha_n) \) sums to zero and is not arrangeable, then some \( \alpha_i \) must have order divisible by at least three distinct primes. Here is another immediate corollary.
Corollary 4.3.8. Let \( g \) be an element of \( \text{GL}(n, \mathbb{C}) \) of finite order. If \( \text{tr}(g) = 0 \) then for some primes \( p_1, \ldots, p_m \) such that \( \sum_{i=1}^{m} p_i = n \), \( |g| \) is divisible by each of \( p_1, \ldots, p_m \).

As a trivial consequence, we note that a finite order element of \( \text{GL}(n, \mathbb{C}) \) with zero trace, \( n \leq 3 \), has order divisible by \( n \).

Blichfeldt’s proof of Theorem 4.3.5 starts with the simple fact that if \( G \) is a finite irreducible subgroup of \( \text{GL}(n, \mathbb{C}) \), then, for any pair of elements \( g, h \) of \( G \) we have \( \text{tr}(g)\text{tr}(h) = \frac{n}{|G|} \sum_{x \in G} \text{tr}(gh^x) \). The idea is to take \( g \) of order \( p \) and \( h \) of order \( q \), use the fact that \( \text{tr}(g)\text{tr}(h) \) has cyclotomic level \( pq \), and then apply the ‘Kronecker theorem’ to deduce that some \( gh^x \) has an eigenvalue of order divisible by \( pq \).
Chapter 5

Insoluble non-modular linear groups of degree three

We are now in a position to classify the finite irreducible insoluble non-modular linear groups of degree 3. The field of definition $\mathbb{F}$ is kept general until the last stage, when we obtain lists in $\text{GL}(3, q)$. Early parts of the chapter draw on Blichfeldt’s work, albeit with independent and more general proofs. The bulk of this chapter is completely new.

Essentially, as we touched upon in Section 2.7, the theory of finite linear groups is two-fold: either the characteristic of the field of definition divides group orders (the modular case), or it does not (the non-modular case). In this chapter, we attend to the non-modular case, whereas in the next chapter, we will deal with the modular case.

The various tasks undertaken can be broken down as follows:

• determining the possible isomorphism types, for which it is sufficient to restrict the discussion to finite complex matrix groups;

• classification questions such as changing the field characteristic, for which we consequently prefer a discussion that is independent of the field of definition more or less.

We keep Theorem 2.7.3 in mind. Also, note that if $G \leq \text{GL}(n, \mathbb{F})$ is finite non-modular then $\mathbb{F}$ contains primitive $e^{th}$ roots of unity for all $e > 1$ dividing $|G|$.
5.1 Bounding group orders in degree 3

Section 4.2 derived the restriction on primes dividing orders of our groups by fairly elementary and completely explicated means. It did so at some length however. We could have avoided this length by simply appealing to the Feit-Thompson improvement [8]. However, we now seek to bound group orders, and further ingenious elementary arguments in the same vein will be needed for this. We have filled in all details that were omitted from [2, 25].

We first work towards establishing which prime powers can divide the order of the central quotient of one of our groups.

Lemma 5.1.1. Suppose that \( \ell(h) = ah^2 + bh + c \in \mathbb{Z}_{11}[h] \), where either \( a \neq 0 \) or \( b \neq 0 \). Then the set of residues mod 11 of \( \ell(h) \) as \( h \) runs over \( \mathbb{Z}_{11} \) is not contained in \( S = \{0, \pm 1, \pm 2, \pm 3\} \).

Proof. For a prime \( p \) and fixed \( b, c \in \mathbb{Z}_p \) where \( b \neq 0 \), we have \( h \mapsto bh + c \) is an injective map on \( \mathbb{Z}_p \). So we may assume that \( a \neq 0 \). Completing the square, we see that it suffices to take \( b = 0 \). Whatever the value of \( a \), as \( h \neq 0 \) runs over \( \mathbb{Z}_{11} \), \( ah^2 \) runs completely over either the set of non-zero quadratic residues or the set of quadratic non-residues mod 11. Then, whatever the value of \( c \), \( \ell(h) \) definitely has a value outside \( S \). \( \square \)

Lemma 5.1.2. Suppose that \( \ell(h) = ah^2 + bh + c \in \mathbb{Z}_{13}[h] \), where either \( a \neq 0 \) or \( b \neq 0 \). Then the set of residues mod 13 of \( \ell(h) \) as \( h \) runs over \( \mathbb{Z}_{13} \) is not contained in \( \{0, \pm 1, \pm 2, \pm 3\} \).

Proof. Cf. the proof of Lemma 5.1.1. \( \square \)

Corollary 5.1.3. Suppose that \( G \) is a finite non-modular subgroup of \( \text{GL}(3, \mathbb{F}) \) whose order is divisible by a prime \( p > 7 \). Then \( G \) has a normal Sylow \( p \)-subgroup.

Proof. (Note that this is immediate from Feit and Thompson’s result [8].) By Theorem 4.2.4, we have to show that if \( p = 11 \) or \( p = 13 \) then \( G \) has a normal Sylow \( p \)-subgroup. But this follows from Lemmas 4.2.2, 5.1.1, and 5.1.2. \( \square \)

Lemma 5.1.4. Let \( G \) be a finite group, with \( \text{soc}(G) \) non-abelian simple. Then \( G \) has no normal non-trivial \( p \)-subgroups.

Corollary 5.1.5. Let \( G \) be a finite non-modular subgroup of \( \text{GL}(3, \mathbb{F}) \) such that the socle of \( G/Z(G) \) is non-abelian simple. Then the prime divisors of \( |G : Z(G)| \) lie in \( \{2, 3, 5, 7\} \).

Proof. Let \( p > 7 \) be a prime, and suppose that \( p \) divides \( |G : Z(G)| \). By Corollary 5.1.3, \( G \) has a normal Sylow \( p \)-subgroup \( P \). Since \( P \leq Z(G) \) by Lemma 5.1.4, if \( xZ(G) \in G/Z(G) \)
has order $p$ then $x^e$ is a $p$-element for some $e$ coprime to $p$. That is $x^e \in P$, and then $x = x^{ae} x^{bp} \in Z(\mathcal{G})$ for some integers $a, b$. Thus $p \nmid |G : Z(\mathcal{G})|$. □

We could use the SL-transfer to obtain the conclusion of Corollary 5.1.5, but this would require the extra hypothesis of irreducibility.

Henceforth unless stated otherwise, $G \leq GL(3,F)$ is finite irreducible insoluble non-modular and $F$ is any field. By Lemma 2.6.3, $G$ is absolutely irreducible (so e.g. its centre is scalars) and primitive over $\overline{F}$. Thus $S/Z(\mathcal{G}) = soc(G/Z(\mathcal{G}))$ is non-abelian simple and $S$ is primitive by Lemma 2.6.11.

**Lemma 5.1.6.** A non-trivial $p$-element of $G/Z(\mathcal{G})$, $p$ prime, has order in $\{2, 3, 4, 5, 7\}$.

**Proof.** By Corollary 5.1.5, the allowable values of $p$ are 2, 3, 5, 7. Suppose that $G/Z(\mathcal{G})$ has an element $gZ(\mathcal{G})$ of order $p^a$, where $a \geq 3$ if $p = 2$ and $a \geq 2$ if $p \in \{3, 5, 7\}$. Write $g = g_p g_p'$, where $g_p$ is a generator of the Sylow $p$-subgroup of $\langle g \rangle$, and $g_p' \in \langle g \rangle$ has $p'$-order. Since $p^a$ divides $|g|$, $p^a \leq |g_p|$. Hence $g_p^{\frac{|g_p|}{p^a}} \in Z(\mathcal{G})$, which means that $g_p' \in Z(\mathcal{G})$ because $|g_p'|$ is coprime to $p$. Thus $|g_p Z(\mathcal{G})| = p^a$. By Lemma 2.7.5, $G$ has a normal $p$-subgroup containing $g_p^{p^a-1}$, so that $G/Z(\mathcal{G})$ has a non-trivial normal $p$-subgroup, contradicting Lemma 5.1.4. □

The next two lemmas are a generalisation of Blichfeldt’s arguments in [25, Chapter XII] using a more modern approach but essentially following a similar line of reasoning.

**Lemma 5.1.7.** Suppose that $g \in GL(n, F)$ is diagonalisable, with an eigenvalue of multiplicity $n - 1$. Then for any $x \in GL(n, F)$, $\langle g, g^x \rangle$ leaves invariant a proper non-trivial subspace of $V$.

**Proof.** By conjugation, we may assume that $g = diag(\alpha, \ldots, \alpha, \beta)$. Let $v$ denote the vector with a single non-zero entry 1 in the $n^{th}$ position. Hence the $n^{th}$ column of $x$ and $x^{-1}$ are respectively $xv$ and $x^{-1}v$. We set $xv := (y_1, \ldots, y_n)\top$ and $x^{-1}v := (x_1, \ldots, x_n)\top$. Then $v$ is an eigenvector for $g$, and $x^{-1}v$ is an eigenvector for $g^x$. Also
\[ gx^{-1}v = (\beta - \alpha)x_nv + \alpha x^{-1}v \in \text{span}_F(v, x^{-1}v) \]
and \[ g^xv = x^{-1}(\alpha xv + (\beta - \alpha)y_nv) = \alpha v + (\beta - \alpha)y_nv = \text{span}_F(v, x^{-1}v). \] □

By Lemma 5.1.6, an element of $G$ of projective order a non-trivial power of 2 has projective order 2 or 4.

**Lemma 5.1.8.** (i) No element of $G$ of projective order 4 or 7 has a repeated eigenvalue.
5.1. BOUNDING GROUP ORDERS IN DEGREE 3

(ii) Suppose that $G$ contains an element of projective order 5 with a repeated eigenvalue. Then, up to conjugacy in $\text{GL}(3, \mathbb{F})$, $G$ contains (commuting) elements of the form $\text{diag}(-1, -1, \epsilon)$ and $\text{diag}(\zeta, \zeta^{-1}, \eta)$.

Proof. Suppose that the projective order of $g \in G$ is $m$, where $m = 4, 5$ or 7, and $g$ has a repeated eigenvalue. Replacing $g$ by $gz$ for an appropriate scalar $z$, we may assume that $g \notin \text{Z}(G)$ has a repeated eigenvalue and $|g| = m$.

For any $x \in G$, the completely reducible group $H = \langle g, g^x \rangle \leq G$ has an irreducible part of degree $\leq 2$ by Lemma 5.1.7. If $g$ commutes with $g^x$ for all $x \in G$, then $\langle g^x : x \in G \rangle$ is a non-central abelian normal subgroup of $G$ of prime power order, contradicting Lemma 5.1.4. For exactly the same reason, if $m = 4$ then $g^2$ does not commute with $(g^2)^x$ for some $x \in G$. So in all cases of $m$ we are able to choose $x \in G$ such that $g^2$ does not commute with $(g^2)^x$. With such a choice of $x$, $H$ is non-abelian and has an irreducible part of degree 2.

Let $\rho$ be the projection of $H$ onto its 2-dimensional irreducible part. If $[\rho(g), \rho(g^x)] = 1$ then because the other irreducible part of $H$ is 1-dimensional, we have $[g, g^x] = 1$. Hence $[\rho(g), \rho(g^x)] \neq 1$. For the same reason, $[\rho(g^2), \rho(g^{2x})] \neq 1$. Thus $\rho(H)$ cannot be monomial, because in a monomial group of degree 2 the squares of elements all commute with each other. Hence $\rho(H)$ has central quotient $\text{Alt}(4)$ or $\text{Sym}(4)$ or $\text{Alt}(5)$, by Theorem 3.0.12. This gives an immediate contradiction when $m = 7$, just by orders, and so proves one of the statements in (i). Suppose that $m = 5$; then $\rho(H)$ contains $\text{diag}(-1, -1)$ and a non-scalar element of order 3. This proves (ii).

Suppose now that $m = 4$. Since $\rho(g)^4 = 1$ but $\rho(g)$ is not central in $\rho(H)$, $\rho(g)$ has projective order 2 or 4 in $\rho(H)$. However, if $\rho(g)$ had projective order 2, then $\rho(g^2)$ would commute with $\rho(g^{2x})$. Hence $\rho(g)$ and $\rho(g^x)$ both have projective order 4. Since the Sylow 2-subgroups of $\text{Alt}(4)$ and $\text{Alt}(5)$ are elementary abelian, the central quotient of $\rho(H)$ could therefore only be $\text{Sym}(4)$. However, in $\text{Sym}(4)$, the squares of any two 4-cycles commute with each other. This contradiction completes the proof of part (i), and thus of the whole lemma.

Lemma 5.1.9. $G$ does not contain an element with projective order in $\{15, 21, 35\}$.

Proof. Invoking the SL-transfer (see Section 2.4.2), we assume that $G \leq \text{SL}(3, \mathbb{F})$. Let $x \in G$ have projective order $pq$. If $p = 3$ or 5 and $q = 7$ then $x^p$ has pairwise distinct eigenvalues by Lemma 5.1.8, and so by Proposition 4.1.9 and Lemma 4.1.7 we get the contradiction that $G/\text{Z}(G)$ has a non-trivial normal $p$-subgroup. Taking $p = 3$ and $q = 5$ produces a contradiction as before, by Lemma 5.1.8: $G$ contains a non-central normal $r$-subgroup where $r = 2$ or 3.
Lemma 5.1.10. Let $H$ be a finite group of order $2m$, $m$ odd. Then $H$ has a (normal, soluble) subgroup of index 2.

Lemma 5.1.11. A Sylow 2-subgroup of $G/Z(G)$ has order 4 or 8.

Proof. We make some trivial but necessary opening remarks. First, $|G : Z(G)|$ is even (because an odd order group is soluble). Secondly, a Sylow 2-subgroup of $G/Z(G)$ must have order greater than 2, by Lemma 5.1.10.

Via the SL-transfer we assume that $G \leq \text{SL}(3, \mathbb{F})$. Hence $Z(G)$ has order dividing 3, and so the Sylow 2-subgroups of $G$ and of $G/Z(G)$ have the same order. Let $S$ be a Sylow 2-subgroup of $G$. Then $S$ is monomial (over $\mathbb{F}$) by Theorem 2.2.7. We bound the order of the diagonal subgroup $D$ of $S$. Note that $D$ has index 1 or 2 in $S$. Remember also by Lemma 5.1.6 that $D$ (as $S$) has exponent dividing 4. The largest subgroup $T$ of $D(3, \mathbb{F})$ of exponent 4 is isomorphic to $C_4 \times C_4 \times C_4$; it is generated by $\text{diag}(\iota, 1, 1)$ and its cyclic shifts, where $\iota$ is a primitive fourth root of unity in $\mathbb{F}$ ($\iota$ exists because $G$ has even order and is non-modular).

Then $T \setminus \text{SL}(3, \mathbb{F}) = \langle \text{diag}(\iota, 1, -\iota) \rangle \times \langle \text{diag}(1, \iota, -\iota) \rangle \cong C_4 \times C_4$.

Each subgroup of $T \setminus \text{SL}(3, \mathbb{F})$ of order greater than 4 contains an element of order 4 with a repeated eigenvalue. Therefore $|D| \leq 4$ by Lemma 5.1.8, and then $|S| \leq 2 \cdot 4 = 8$ as required.

Lemma 5.1.12. A Sylow 3-subgroup of $G/Z(G)$ has order 3 or 9, or $G$ contains an element of order 9 with repeated eigenvalues.

Proof. By Ito’s famous theorem ([17, 6.15, p.84]), 3 divides the index of every abelian normal subgroup of $G$; hence $|G/Z(G)|$ is certainly divisible by 3. As in the previous proof, we enforce the SL-transfer. Let $S/Z(G)$ be a Sylow 3-subgroup of $G/Z(G)$. Then $S$ is a Sylow 3-subgroup of $G$.

By Lemma 5.1.6, the diagonal subgroup $D$ of the monomial group $S$ is contained in the subgroup of $D(3, \mathbb{F}) \cap \text{SL}(3, \mathbb{F})$ whose elements cube to scalars. That group has order 27, being generated by $\text{diag}(\zeta_9, \zeta_9, \zeta_9^{-2})$ and $\text{diag}(\zeta_9, \zeta_9^4, \zeta_9^4)$. Thus, if $S$ is diagonal, then either $|S| \leq 9$, or $S$ contains a scalar of order 3 and so $|S/Z(G)| \leq 9$. If $S \neq D$ then $D$ contains the scalar subgroup of order 3, because $S$ has a non-trivial centre, centralised by a cycle of order 3. In this case, then, $|S/Z(G)| \leq 3 \cdot 27/3 = 27$, and if $|S/Z(G)| = 27$ then e.g. $\text{diag}(\zeta_9, \zeta_9, \zeta_9^{-2}) \in S$ up to conjugacy.

Lemma 5.1.13. For $p \in \{5, 7\}$, a Sylow $p$-subgroup of $G/Z(G)$ has order dividing $p$. 

52
5.1. BOUNDING GROUP ORDERS IN DEGREE 3

Proof. We assume that $G \leq \text{SL}(3,\mathbb{F})$; so the orders of Sylow $p$-subgroups of $G$ and of $G/Z(G)$ are the same, for each $p$.

Let $S$ be a Sylow $p$-subgroup of $G$. By Lemma 5.1.6, $S$ has exponent $p$. Also, $S$ is diagonalisable (as a monomial group with trivial permutation part). Up to conjugacy,

$$S \leq T = \langle \text{diag}(\omega, \omega^{-1}, 1), \text{diag}(1, \omega, \omega^{-1}) \rangle \cong C_p \times C_p, \quad |\omega| = p.$$ 

Note that $T$ contains the element $\text{diag}(\omega, \omega, \omega^{-2})$ of order $p$. If $p = 7$ then $|S| \leq 7$ by Lemma 5.1.8. Suppose now that $p = 5$ and $|S| > 5$. By Lemma 5.1.8, $G$ contains an element with eigenvalues $-\zeta_3, -\zeta_3^2, 1$. This gives a contradiction by Proposition 4.1.9 and Lemma 4.1.7. □

Lemma 5.1.14. Suppose that $|G : Z(G)|$ is divisible by (i) $35$; (ii) $3^3 \cdot 5$; (iii) $3^3 \cdot 7$. Then $G$ has an element of projective order (i) $35$; (ii) $15$; (iii) $21$, respectively.

Proof. Assume that $G \leq \text{SL}(3,\mathbb{C})$, by Theorem 2.7.3 and the SL-transfer. Part (i) follows from Lemma 4.3.4 and Theorem 4.3.5. For the other two parts, we begin by noting that if $|G : Z(G)|$ is divisible by 27, then $G$ has an element $g$ of order 9 with a repeated eigenvalue $\lambda$ of order 9, by Lemma 5.1.12. We see that $\text{tr}(g)$ has cyclotomic level 9 (since $\text{tr}(g) = \lambda^7 + 2\lambda$, and then $\text{tr}(g) \in \mathbb{Q}_3$ implies that $\Phi_9(X) = X^6 + X^3 + 1$ divides $X^7 + aX^3 + 2X + b$ for some $a, b \in \mathbb{Q}$, which is obviously false). Now we can apply Lemma 4.3.4 and Theorem 4.3.5 to conclude that $G$ has an element of order $9q$, where $q = 5$ in case (ii) and $q = 7$ in case (iii). Therefore $|G : Z(G)|$ has an element of order $3q$. □

Theorem 5.1.15. $|G : Z(G)|$ is not divisible by (i) $35$ (ii) $3^3 \cdot 5$ or (iii) $3^3 \cdot 7$.

Proof. This follows directly from Lemmas 5.1.14 and 5.1.9. □

The culmination of Lemma 5.1.6 and the results from Lemma 5.1.11 to Theorem 5.1.15 is that

$$|G : Z(G)| \in \{2^a 3^b 5^c 7^d \mid 2 \leq a \leq 3, \ 1 \leq b \leq 2, \ (c,d) \in \{(0,1), (1,0)\}\}.$$ 

(Note that $(c,d)$ cannot be $(0,0)$ since a group of order $2^a 3^b$ is soluble: the Burnside $p^aq^b$ Theorem.) Hence we get just eight possibilities for $|G : Z(G)|$. Keeping in mind that $G/Z(G)$ has a normal non-abelian simple subgroup, we can dispose of some candidate orders by the Classification of Finite Simple Groups (further Blichfeldt-like methods could also be used). First, we note that $|\text{soc}(G/Z(G))| \in \{60, 168, 360, 504\}$, and hence $|G : Z(G)| \not\in \{84, 252\}$. We next dispose of the orders 120 and 180. To do this we use some of the cohomological machinery from Section 2.1 of Chapter 2 (this will be called on in the
next section too). Any of the statements about the structure of the groups involved can be easily checked, e.g. using MAGMA \cite{magma} (in particular, its SmallGroups library).

A group of order 120 with socle $\text{Alt}(5)$ is isomorphic to $\text{Sym}(5)$. The derived quotient and Schur multiplier of $\text{Sym}(5)$ are both of order 2, so that an extension of $\text{Sym}(5)$ by $C_3$ splits, by the Universal Coefficient theorem (Theorem 2.1.5). Thus, an irreducible group in $\text{SL}(3, \mathbb{C})$ with central quotient $\text{Sym}(5)$ contains an irreducible copy of $\text{Sym}(5)$. However, inspection of the ordinary character table of $\text{Sym}(5)$ shows that it does not have a faithful irreducible representation in $\text{GL}(3, \mathbb{C})$.

There is a single insoluble group of order 180 up to isomorphism, namely $\text{Alt}(5) \times C_3$. If $L \leq \text{SL}(3, \mathbb{C})$ is irreducible and has central quotient $\text{Alt}(5) \times C_3$ then $L$ contains a copy of $\text{Alt}(5)$ by the Universal Coefficient theorem (the multiplier of $\text{Alt}(5)$ has size 2). But this subgroup isomorphic to $\text{Alt}(5)$ is irreducible, and as it centralises a subgroup $C$ of order 9, $C$ must be scalars; this gives a contradiction.

There are two insoluble groups of order 504: one is simple, the other is $\text{PSL}(2, 7) \times C_3$. The simple group $\text{PSL}(2, 7)$ has multiplier of order 2. Also, as a copy of $\text{PSL}(2, 7)$ in $\text{GL}(3, \mathbb{C})$ is irreducible, if it centralises a $C_3$ then that $C_3$ is scalars: hence there is just the one candidate for a central quotient of order 504, and it is simple (cf. the previous paragraph). The simple group of order 504 has trivial multiplier, and an elementary abelian Sylow 2-subgroup that is necessarily monomial. But in $\text{SL}(3, \mathbb{C})$, a monomial group of exponent 2 can have order at most 4.

We are now down to just three orders: 60, 168 and 360. In fact, we have shown that $G$ (if it exists) has non-abelian simple central quotient (there are unique simple groups of these orders; and there is no group of order 360 with simple socle of order 60).

**Theorem 5.1.16.** If $G$ is a finite non-modular insoluble irreducible subgroup of $\text{GL}(3, \mathbb{F})$, $\mathbb{F}$ any field, then $G/\mathbb{Z}(G)$ must be isomorphic to one of $\text{Alt}(5)$, $\text{Alt}(6)$, or $\text{PSL}(2, 7)$.

Amongst other things, we will show in the next section that all isomorphism types as in Theorem 5.1.16 arise; moreover, each group $G$ is determined solely by $|\mathbb{Z}(G)|$ and the isomorphism type of $G/\mathbb{Z}(G)$.

### 5.2 Putting it all together: the final list

In this section we obtain a full solution to the problem of listing the finite non-modular insoluble irreducible subgroups of $\text{GL}(3, \mathbb{F})$, $\mathbb{F}$ any field. Theorem 5.1.16 is implicit throughout.
5.2. PUTTING IT ALL TOGETHER: THE FINAL LIST

5.2.1 Abstract structure of the groups

Recall that (due to Lemma 2.1.6) we can speak of the Schur cover of a finite non-abelian simple group.

**Lemma 5.2.1.** Suppose $G$ is a finite non-modular irreducible subgroup of $\text{GL}(3, \mathbb{F})$ with central quotient $\text{Alt}(5)$. Then $G$ splits over its centre: $G = A_5 \times Z(G)$ where $A_5 \cong \text{Alt}(5)$.

*Proof.* Since the Schur multiplier of $\text{Alt}(5)$ has order 2, by Lemma 2.1.9 either $G$ contains a copy $A_5$ or a Schur cover copy $\hat{A}_5$ of $\text{Alt}(5)$, which supplements $Z(G)$ in $G$. Since $Z(G)$ is scalars, $A_5$ or $\hat{A}_5$ has to be (absolutely) irreducible. Its character table shows that $\hat{A}_5$ has no faithful irreducible representation in $\text{GL}(3, \mathbb{C})$. \qed

The next result guarantees that all of our listed groups have the required properties.

**Lemma 5.2.2.** Let $\mathbb{F}$ be any field. Suppose that $G$ is a finite non-modular subgroup of $\text{GL}(3, \mathbb{F})$ such that $G/Z(G)$ is isomorphic to one of $\text{Alt}(6)$ or $\text{PSL}(2, 7)$, or $G$ contains a copy $A_5$ of $\text{Alt}(5)$. Then $G$ is an insoluble absolutely irreducible subgroup of $\text{GL}(3, \mathbb{F})$. Furthermore, $G$ is primitive (over $\mathbb{F}$, and over every extension of $\mathbb{F}$).

*Proof.* By Lemma 2.6.3, all we need to do is show that $G$ is irreducible. Suppose that $G$ is reducible. Then there is an irreducible representation $\alpha : G \to H \leq \text{GL}(2, \mathbb{F})$ with kernel $K \leq Z(G)$. As $H$ is an insoluble irreducible non-modular subgroup of $\text{GL}(2, \mathbb{F})$, we see by Theorem 3.0.12 and the hypotheses, that $G$ contains $A_5 \cong \text{Alt}(5)$. Then $K \cap A_5 = 1$ implies that $\text{GL}(2, \mathbb{C})$ contains a copy of $\text{Alt}(5)$, which is false. \qed

The slight difficulties for $\text{Alt}(5)$ arise because $\text{GL}(3, \mathbb{F})$ has reducible subgroups with central quotient $\text{Alt}(5)$, coming from the Schur cover of $\text{Alt}(5)$ in degree 2.

**Lemma 5.2.3.** Suppose that $G$ is a finite non-modular subgroup of $\text{GL}(3, \mathbb{F})$ with central quotient $G/Z(G) \cong \text{Alt}(6)$. Then $G$ is absolutely irreducible and $G = \langle 3.A_6, Z(G) \rangle$ where $3.A_6$ is the non-split central extension of $Z_3 \neq 1$ by $\text{Alt}(6)$.

*Proof.* Cf. the proof of Lemma 5.2.1. The Schur multiplier of $\text{Alt}(6)$ has order 6, so by Lemma 2.1.9 there are three possibilities: $G$ contains either a copy of $\text{Alt}(6)$, or a central extension of $C_2$ by $\text{Alt}(6)$, or a central extension of $C_3$ by $\text{Alt}(6)$ (if $G$ contains the Schur cover of $\text{Alt}(6)$ then the latter two cases hold). Simply checking character tables confirms that neither $\text{Alt}(6)$ nor the non-split extension of $C_2$ by $\text{Alt}(6)$ has an irreducible representation in $\text{GL}(3, \mathbb{C})$. \qed
Lemma 5.2.4. Suppose that $G$ is a finite non-modular subgroup of $GL(3, F)$ with central quotient $GL(3, 2) \cong PSL(2, 7)$. Then $G$ is absolutely irreducible and $G = P \times \mathbb{Z}(G)$ where $P \cong PSL(2, 7)$.

Proof. Since the Schur multiplier of $PSL(2, 7)$ has order 2, by Lemma 2.1.9 we only have to rule out the possibility that $G$ contains the Schur cover of $PSL(2, 7)$. But the character table of the cover exhibits only two degree three representations, and those representations are not faithful. □

So in Lemmas 5.2.1, 5.2.3, and 5.2.4, we have already determined quite a lot about the structure of our list groups. Next, we solve the conjugacy problem.

5.2.2 Solution of the conjugacy problem

When we transfer to the positive characteristic setting, as usual we have different exceptional primes for different groups. The set of exceptional primes for each of our core groups are as follows:

<table>
<thead>
<tr>
<th>Group</th>
<th>Exceptional primes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alt(5)</td>
<td>{2, 3, 5}</td>
</tr>
<tr>
<td>Alt(6)</td>
<td>{2, 3, 5}</td>
</tr>
<tr>
<td>PSL(2, 7)</td>
<td>{2, 3, 7}</td>
</tr>
</tbody>
</table>

Lemma 5.2.5. Let $G$ be an absolutely irreducible subgroup of $GL(n, \mathbb{F})$ isomorphic to $Alt(5)$, and suppose that $GL(n, \mathbb{F})$ does not have a subgroup containing $G$ with central quotient $Sym(5)$. If $Alt(5)$ has precisely two inequivalent faithful absolutely irreducible representations in $GL(n, \mathbb{F})$. Then any two absolutely irreducible subgroups of $GL(n, \mathbb{F})$ isomorphic to $Alt(5)$ are conjugate to each other.

Proof. Letting $Z$ denote the full scalar subgroup of $GL(n, \mathbb{F})$, we have that

$$Alt(5) \cong G/Z \leq N_{GL(n, \mathbb{F})}(G)/Z$$

is isomorphic to a subgroup of $Aut(Alt(5)) \cong Sym(5)$ and $N_{GL(n, \mathbb{F})}(G)/Z$ is isomorphic to a subgroup of $Aut(Alt(5)) \cong Sym(5)$. If $N_{GL(n, \mathbb{F})}(G) \neq GZ$ then we get a contradiction against the hypothesis that $GL(n, \mathbb{F})$ does not contain an absolutely irreducible subgroup with central quotient $Sym(5)$. The number of inequivalent faithful absolutely irreducible representations of $G$ in $GL(n, \mathbb{F})$ is $|Z(G)||Aut(G)|/|G|$, so we are done by Lemma 2.4.7. □
Corollary 5.2.6. Let $G$ be a finite irreducible non-modular subgroup of $GL(3, \mathbb{F})$ with central quotient $Alt(5)$. Then any irreducible subgroup of $GL(3, \mathbb{F})$ with central quotient $Alt(5)$ and centre of order $|Z(G)|$ is conjugate to $G$, and isomorphic to $Alt(5) \times Z(G)$.

Proof. By Lemma 5.2.1, $G \cong Alt(5) \times Z(G)$. We know by Lemma 2.4.2 (especially part (v) of that lemma) and the classification of finite irreducible insoluble subgroups of $GL(3, \mathbb{F})$ to this point (Theorem 5.1.16) that $GL(3, \mathbb{F})$ does not have a subgroup containing $G$ with central quotient $Sym(5)$. The character table of $Alt(5)$ supplies the remaining hypothesis of Lemma 5.2.5. □

We could frame the following two lemmas more generally, as per Lemma 5.2.5.

Lemma 5.2.7. Let $G$ be a non-modular subgroup of $GL(3, \mathbb{F})$ with central quotient $Alt(6)$. Then any subgroup of $GL(3, \mathbb{F})$ with central quotient $Alt(6)$ and centre of order $|Z(G)|$ is conjugate to $G$, and $G \cong \langle 3.A_6, Z(G) \rangle$, where $3.A_6$ is the non-split central extension of the $3$-subgroup $Z_3 \neq 1$ of $Z(G)$ by $Alt(6)$.

Proof. We use Lemma 2.4.7 again. Let us assume that $G \cong 3.A_6$, as $G$ certainly contains this as a splitting subgroup, by Lemma 5.2.3. We have that $G$ is absolutely irreducible so $Z(G) = Z \cap G$, $Z$ the scalars of $GL(3, \mathbb{F})$. Then

$$Alt(6) \cong GZ/Z \leq N_{GL(3, \mathbb{F})}(G)/Z$$

is isomorphic to a subgroup of $Aut(A_6)$, and $N_{GL(3, \mathbb{F})}(G)/Z$ is isomorphic to a subgroup of $Aut(3.A_6)$. Now $|Aut(3.A_6)| = 1440$, so $|Z(G)||Aut(G)|/|G| = 4$. If $N_{GL(3, \mathbb{F})}(G) \neq GZ$ then $SL(3, \mathbb{F})$ has a finite absolutely irreducible non-modular subgroup with central quotient of order greater than 360, by Lemma 2.4.2. This contradicts Theorem 5.1.16. Finally, the character table of $G$ shows that $G$ has exactly 4 (Galois conjugate) inequivalent faithful irreducible representations of degree 3. Hence Lemma 2.4.7 again gives the result. □

Lemma 5.2.8. Let $G$ be a non-modular subgroup of $GL(3, \mathbb{F})$ with central quotient $PSL(2, 7)$. Then any subgroup of $GL(3, \mathbb{F})$ with central quotient $PSL(2, 7)$ and centre of order $|Z(G)|$ is conjugate to $G$, and $G \cong PSL(2, 7) \times Z(G)$.

Proof. The argument is familiar from the preceding proofs, i.e. we proceed by checking that the hypotheses of Lemma 2.4.7 hold. Assume that $G \cong PSL(2, 7)$, by Lemma 5.2.4. Then

$$PSL(2, 7) \cong GZ/Z \leq N_{GL(3, \mathbb{F})}(G)/Z.$$
Also Aut(PSL(2, 7)) has a subgroup of index 2 isomorphic to PSL(2, 7). Lemma 2.4.2 and Theorem 5.1.16 then force \( N_{GL(3, F)}(G) = GZ \). Since \( G \) has precisely \( |Z(G)||\text{Aut}(G)|/|G| = 2 \) inequivalent irreducible representations of degree 3, we are done. \( \square \)

We end this subsection by stating the important conclusion following from Corollary 5.2.6, Lemma 5.2.7, and Lemma 5.2.8.

**Theorem 5.2.9.** Finite non-modular irreducible insoluble subgroups of \( GL(3, F) \) are isomorphic to each other if and only if they are \( GL(3, F) \)-conjugate to each other.

Thus, the groups that we eventually list are not only not conjugate, they are not isomorphic. Moreover, the isomorphism type of each listed group is determined solely by its central quotient and the order of its centre.

### 5.2.3 Generating sets of matrices

We can now define generating sets for the ‘core’ groups that will appear in our lists; each listed group will simply be one of the core groups adjoined by scalars.

Generators for all three core groups (in \( SL(3, F) \)) are provided by Blichfeldt in [25, pp. 250-251]. We opt for an alternative derivation using presentations that lead to generating sets involving the least number of possible generators. Of course, any generating set whose elements generate a group isomorphic to the core group in question is valid. Here we set \( p := \text{char } F \).

**Lemma 5.2.10.** Suppose that \( p \notin \{2, 3, 5\} \). Define the following elements of \( GL(3, \bar{F}) \):

\[
B = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}, \quad A = -\frac{1}{2} \begin{pmatrix} 1 & \mu_2 & \mu_1 \\ \mu_2 & \mu_1 & 1 \\ \mu_1 & 1 & \mu_2 \end{pmatrix}
\]

where \( \mu_1 \) and \( \mu_2 \) are two distinct roots of \( \mu^2 - \mu - 1 = 0 \), i.e. over the complex field \( \mu = (1 \pm \sqrt{5})/2 \). Then \( A_5 := \langle A, B \rangle \) is an irreducible subgroup of \( GL(3, \bar{F}) \) isomorphic to Alt(5).

**Proof.** Note that \( H := \langle a, b \mid a^2 = b^3 = (ab)^5 = 1 \rangle \) is a presentation of Alt(5). Define a map \( \theta : H \to \langle A, B \rangle \) by \( a \mapsto A \) and \( b \mapsto B \). Since relations in \( H \) are satisfied by \( \langle A, B \rangle \) under \( \theta \) it follows that \( \theta \) is a group epimorphism. Since Alt(5) is simple, it follows that \( \theta \) is in fact an isomorphism. \( \square \)
5.2. PUTTING IT ALL TOGETHER: THE FINAL LIST

Explanation of derivation for matrix generators

Any element of $\text{GL}(3, \mathbb{F})$ of order 3 can be chosen as our order 3 conjugacy class representative. We use the matrix $B$ as given. To find $A$, we solve for possible values for a $3 \times 3$ matrix using the constraints of the generator relations for $\text{Alt}(5)$.

Let $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$.

Taking $A^2 = I$, we get a set of nine equations. Due to symmetry, there is some redundancy. In addition, we have the constraint $(AB)^5 = 1$.

Hence we seek a corresponding matrix $C = AB$ such that $C^5 = 1$. Let $\lambda_1, \lambda_2, \lambda_3$ represent the three roots of the characteristic equation for $C$. We have that

$$(C - \lambda_1)(C - \lambda_2)(C - \lambda_3) = C^3 - \text{tr}(C)C^2 + \left(\sum_i c_{ii}\right)C - \det(C) \quad (5.1)$$

where $c_{jk}$ denotes the cofactor of the matrix $C$ at position $j,k$. It is straightforward to verify that the roots $1, \zeta_5, \zeta_5^4$ satisfy Eq.(5.1). Equating coefficients, we find that

- $C^2 : a_{13} + a_{21} + a_{32} = \mu$
- $C^1 : a_{21}a_{32} - a_{22}a_{31} + a_{13}a_{32} - a_{12}a_{33} + a_{21}a_{13} - a_{11}a_{23} = \mu$
- $C^0 : a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{21}a_{12}a_{33} + a_{21}a_{13}a_{32} + a_{31}a_{12}a_{23} - a_{31}a_{13}a_{22} = 1$

where $\mu$ is a root of $X^2 - X - 1 \in \overline{\mathbb{F}}$. Solving, we get the matrix $A$ as shown in Theorem 5.2.10. The other two cases below (i.e. Lemmas 5.2.11, 5.2.12) follow a similar approach.

**Lemma 5.2.11.** Suppose that $p \notin \{2, 3, 5\}$, define

$$H = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, K = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ \beta_1 & \beta_2 & 1 \end{pmatrix}.$$ 

where $\beta_1$ and $\beta_2$ are roots of $\beta_2^2 + \mu \beta_2 + \mu^2 = 0$ and $\mu$ satisfies (as in Lemma 5.2.10) $\mu^2 - \mu - 1 = 0$, i.e. over the complex field $\beta_1 = \zeta_3(1 \pm \sqrt{5})/2$ and $\beta_2 = \zeta_3 \beta_1$. Then $3A_6 = \langle H, K \rangle$ is an irreducible subgroup of $\text{GL}(3, \overline{\mathbb{F}})$ isomorphic to the unique non-split central extension of $C_3$ by $\text{Alt}(6)$.

**Proof.** A presentation for the 3-cover of $\text{Alt}(6)$ is given by
Then the list anyway.

Proof. The theorem is implicit in everything that has gone before, but we spell out a proof if $p \not\in \{2, 3, 7\}$ in each case and because $p$ divides $\ker \theta = C_3$ in $\langle h, k \rangle$. Let $z = (hk)^5$ be a word in $\langle h, k \rangle$. One can check that $\langle z \rangle$ is the cyclic group that generates $C_3$. It is easily verified that $\theta(z)$ is non-trivial and therefore $\ker \theta = 1$. Hence $\theta$ is in fact an isomorphism. \hfill \Box

**Lemma 5.2.12.** Suppose that $p \not\in \{2, 3, 7\}$ and define

$$S = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} -1 & \alpha_1 & 0 \\ 0 & 1 & 0 \\ 0 & \alpha_2 & -1 \end{pmatrix}$$

where $\alpha_1$ and $\alpha_2$ are roots of $\alpha^2 + \alpha + 2 = 0$, i.e. over the complex field $\alpha = \frac{1}{2}(-1 \pm \sqrt{-7})$. Then $L_2(7) = \langle S, R \rangle$ is an irreducible subgroup of $GL(3, \overline{\mathbb{F}})$ isomorphic to $PSL(2, 7) \cong GL(3, 2)$.

*Proof.* A presentation for $PSL(2, 7)$ is $(r^2 = s^3 = (rs)^7 = [r, s]^4 = 1)$. Similarly to Lemma 5.2.10, we can define an isomorphism by $s \mapsto S$ and $r \mapsto R$. \hfill \Box

Note that the groups defined in Lemmas 5.2.10–5.2.12 are in $SL(3, \mathbb{F})$. We can now assemble a proto-list of irreducible insoluble non-modular subgroups of $GL(3, \mathbb{F})$.

**Theorem 5.2.13.** For $\langle z \rangle$ ranging over the finite order scalars of $GL(3, \mathbb{F})$, define the following lists $\mathcal{L}_i$ of subgroups of $GL(3, \mathbb{F})$.

- $\mathcal{L}_1$: all groups $\langle A_5, z \rangle$, where $A_5$ is as defined in Lemma 5.2.10 for $p \not\in \{2, 3, 5\}$.
- $\mathcal{L}_2$: all groups $\langle 3.A_6, z \rangle$, where $3.A_6$ is as defined in Lemma 5.2.11 for $p \not\in \{2, 3, 5\}$ and either 3 does not divide $|z|$ or 9 divides $|z|$.
- $\mathcal{L}_3$: all groups $\langle L_2(7), z \rangle$ where $L_2(7)$ is as in Lemma 5.2.12 for $p \not\in \{2, 3, 7\}$.

Then the list $\mathcal{L} := \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3$ consists entirely of finite non-modular irreducible insoluble subgroups of $GL(3, \mathbb{F})$. Moreover, a non-modular irreducible insoluble subgroup of $GL(3, \mathbb{F})$ is $GL(3, \overline{\mathbb{F}})$-conjugate to one and only one group in $\mathcal{L}$.

*Proof.* The theorem is implicit in everything that has gone before, but we spell out a proof anyway.

The fact that the groups in $\mathcal{L}$ are irreducible and insoluble was observed in Lemmas 5.2.10–5.2.12. They are non-modular by the restriction on $p$ in each case and because if $p > 0$ then $|z|$ divides $p^r - 1$ for some $r \geq 1$. 

60
Distinct groups in \( \mathcal{L} \) are not isomorphic. Since isomorphic groups have isomorphic central quotients, then by Lemmas 5.2.10–5.2.12 if \( G \in \mathcal{L}_i \) is isomorphic to \( H \in \mathcal{L}_j \) then \( i = j \). Hence \( |Z(G)| = |Z(H)| \) implies that \( G = H \) (cf. Theorem 5.2.9).

Let \( G \) be a finite non-modular irreducible insoluble subgroup of \( \text{GL}(3, \mathbb{F}) \). By Theorem 5.1.16, \( G/Z(G) \) is isomorphic to one of \( \text{Alt}(5) \), \( \text{Alt}(6) \), or \( \text{PSL}(2, 7) \). Therefore, Corollary 5.2.6 and Lemmas 5.2.7, 5.2.8 & 5.2.10–5.2.12 show that \( G \) is \( \text{GL}(3, \overline{\mathbb{F}}) \)-conjugate to one of the groups in \( \mathcal{L} \).

**Corollary 5.2.14.** Let \( \mathcal{L}' \) be the sublist of \( \mathcal{L} \) as defined in Theorem 5.2.13 consisting of all groups that are conjugate to subgroups of \( \text{GL}(3, \mathbb{F}) \). Let \( \mathcal{L}'' \) be the list obtained from \( \mathcal{L}' \) by replacing each \( G \in \mathcal{L}' \) such that \( G \not\leq \text{GL}(3, \mathbb{F}) \) by a conjugate of \( G \) in \( \text{GL}(3, \mathbb{F}) \).

Then \( \mathcal{L}'' \) is a complete and irredundant list of \( \text{GL}(3, \overline{\mathbb{F}}) \)-conjugacy class representatives of the finite irreducible insoluble non-modular subgroups of \( \text{GL}(3, \mathbb{F}) \).

**Proof.** First, \( \mathcal{L}'' \) clearly consists of groups of the stated kind, that are pairwise non-conjugate in \( \text{GL}(3, \mathbb{F}) \). Let \( G \leq \text{GL}(3, \mathbb{F}) \) be finite irreducible insoluble non-modular. By Theorem 5.2.13 and the definition of \( \mathcal{L}'' \), \( G^x = H \in \mathcal{L}'' \) for some \( x \in \text{GL}(3, \mathbb{F}) \). Since \( G \) and \( H \) are both subgroups of \( \text{GL}(3, \mathbb{F}) \), the Deuring-Noether theorem (Theorem 2.5.3) completes the proof.

Corollary 5.2.14 sets the agenda to complete this chapter; that is, there are two major steps remaining:

1. Determine the sublist \( \mathcal{L}' \) of \( \mathcal{L} \);
2. Construct the list \( \mathcal{L}'' \) from \( \mathcal{L}' \).

To carry out these tasks we first need to amass the necessary information about existence of roots in finite fields.

### 5.2.4 Some elementary number theory

From now on, \( p = \text{char} \mathbb{F} > 0 \).

**Lemma 5.2.15.** Let \( p \) and \( r \) be distinct odd primes, and let \( q \) be a power of \( p \).

(i) If \( \log_p q \) is even then \( \sqrt{r} \in \text{GF}(q) \).

(ii) Suppose that \( \log_p q \) is odd and \( p \equiv 1 \mod 4 \) or \( r \equiv 1 \mod 4 \). Then \( \sqrt{r} \in \text{GF}(q) \) if and only if \( q \) is a quadratic residue mod \( r \).
(iii) Suppose that \( \log_p q \) is odd and \( p \equiv r \equiv 3 \mod 4 \). Then \( \sqrt{r} \in \text{GF}(q) \) if and only if \( q \) is a quadratic non-residue mod \( r \).

Proof. Since \( \sqrt{r} \in \text{GF}(p^2) \), part (i) is clear. Henceforth \( \log_p q \) is odd. We note that if \( \sqrt{r} \in \text{GF}(q) \) then \( \sqrt{r} \in \text{GF}(p) \); otherwise \( \text{GF}(q) \) contains \( \text{GF}(p^2) \).

(ii) If \( \sqrt{r} \in \text{GF}(q) \) then \( (\frac{r}{p}) = (\frac{p}{r}) = 1 \) by quadratic reciprocity, so that \( p \) and thus \( q \) is a quadratic residue mod \( r \). On the other hand if \( q \) is a quadratic residue mod \( r \) then so too is \( p \), because \( \log_p q \) is odd. That is, \( \sqrt{r} \in \text{GF}(p) \subseteq \text{GF}(q) \) by reciprocity again.

(iii) Here \( (\frac{r}{p}) = - (\frac{p}{r}) \), and reasoning as in part (ii) proves the statement. \( \Box \)

In Lemma 5.2.10, \( \sqrt{5} \in \text{GF}(q) \) is necessary and sufficient to write both matrix generators over the input field \( \text{GF}(q) \).

**Corollary 5.2.16.** Let \( q \) be a power of an odd prime \( p \neq 5 \). Then \( \sqrt{5} \in \text{GF}(q) \) if and only if \( q \equiv 1 \mod 5 \).  

Lemma 5.2.11 is covered by the next result.

**Lemma 5.2.17.** Let \( q \) be a power of an odd prime \( p \neq 3, 5 \), and let \( \zeta_3 \in \text{GF}(q) \). Then \( \sqrt{5}, \zeta_3 \in \text{GF}(q) \) if and only if \( q \equiv 1 \mod 3 \) and \( q \equiv 1 \mod 5 \).

Proof. Of course, \( \zeta_3 \in \text{GF}(q) \) if and only if \( q \equiv 1 \mod 3 \). If \( \log_p q \) is even then \( \sqrt{5} \in \text{GF}(q) \) by Lemma 5.2.15 (i), and \( q \) is a quadratic residue mod 5. When \( \log_p q \) is odd, part (ii) of Lemma 5.2.15 implies that \( \sqrt{5} \in \text{GF}(q) \) if and only if \( q \equiv 1 \mod 5 \). \( \Box \)

The perfect core group in Lemma 5.2.12 is in \( \text{GL}(3, q) \) as long as \( \sqrt{-7} \in \text{GF}(q) \).

**Lemma 5.2.18.** Let \( q \) be a power of an odd prime \( p \neq 7 \). Then \( \sqrt{-7} \in \text{GF}(q) \) if and only if \( q \equiv 1 \mod 2 \) or \( 2 \mod 4 \).

Proof. Suppose that \( q \equiv 1 \mod 4 \): so \( \sqrt{-7} \in \text{GF}(q) \) if and only if \( \sqrt{7} \in \text{GF}(q) \). If \( q \) is a square then \( \text{GF}(q) \) certainly contains \( \sqrt{7} \). If \( \log_p q \) is odd then \( p \equiv 1 \mod 4 \), and we have the result by Lemma 5.2.15 (ii).

Now suppose that \( q \equiv 3 \mod 4 \), so \( p \equiv 3 \mod 4 \) and \( \log_p q \) is odd. Then \( \sqrt{-7} \in \text{GF}(q) \) if and only if \( \sqrt{7} \notin \text{GF}(q) \). By Lemma 5.2.15 (iii), the latter holds precisely when \( q \) is a quadratic residue mod 7, just as before. \( \Box \)
5.2. PUTTING IT ALL TOGETHER: THE FINAL LIST

5.2.5 The list over finite fields

We now have enough information to assemble our final list of groups over finite fields, combining Theorem 5.2.13 with the results of the previous subsection. In all statements below, \( q = p^a \) for \( p \) prime and \( a \in \mathbb{Z}^+ \).

**Theorem 5.2.19.** Suppose

\[
\begin{align*}
a &\equiv 0 \mod 2, \ q \in \{1, 7, 13, 19\} \mod 30 \\
or \\
a &\equiv 1 \mod 2, \ q \in \{\pm1, \pm11\} \mod 30
\end{align*}
\]

and define

\[
\bar{L}_1 = \{A_5 \times C_r : \ r \mid (q - 1)\},
\]

where \( A_5 \) is as in Lemma 5.2.10. Then \( \bar{L}_1 \) is a list of finite irreducible non-modular subgroups of \( \text{GL}(3, q) \) with central quotient \( \text{Alt}(5) \). Moreover any such subgroup of \( \text{GL}(3, q) \) is \( \text{GL}(3, q) \)-conjugate to one and only one group in \( \bar{L}_1 \).

**Proof.** We refer to \( \mathcal{L}_1 \) in Theorem 5.2.13. If \( A_5 = \langle A, B \rangle \) is conjugate to a subgroup of \( \text{GL}(3, q) \) then \( \text{tr}(AB) = \frac{1}{2}(1 \pm \sqrt{5}) \in \text{GF}(q) \), i.e. \( \sqrt{5} \in \text{GF}(q) \). By Theorems 2.5.2 and Corollary 5.2.16 we infer the following restrictions on \( q \) and \( a \) for the list of finite irreducible non-modular subgroups of \( \text{GL}(3, q) \) with central quotient \( \text{Alt}(5) \).

\[
\begin{array}{c}
\text{(i)} \\
\begin{tabular}{ll}
a &\equiv 0 \mod 2 \\
q &\equiv 1 \mod 2 \\
q &\equiv \pm1 \mod 3 \\
q &\not\equiv 0 \mod 5
\end{tabular} & \text{or,} & \begin{tabular}{ll}
a &\equiv 1 \mod 2 \\
q &\equiv 1 \mod 2 \\
q &\equiv \pm1 \mod 3 \\
q &\equiv \pm1 \mod 5
\end{tabular}
\end{array}
\]

In the case of (i), the restriction on \( a \) necessarily restricts \( q \equiv 1 \mod 3 \). A simple application of the Chinese remainder theorem for both cases gives the required result. Furthermore, by Theorem 2.5.2, we have that each subgroup is conjugate to one and only one group in the list.

\[
\begin{array}{c}
\begin{tabular}{ll}
a &\equiv 0 \mod 2 \\
q &\equiv 1 \mod 2
\end{tabular} & \text{or} & \begin{tabular}{ll}
a &\equiv 1 \mod 2 \\
q &\equiv 1 \mod 2 \\
q &\equiv \pm1 \mod 3 \\
q &\equiv \pm1 \mod 5
\end{tabular}
\end{array}
\]

**Theorem 5.2.20.** Suppose

\[
\begin{align*}
a &\equiv 0 \mod 2, \ q \in \{1, 7, 13, 19\} \mod 30 \\
or \\
a &\equiv 1 \mod 2, \ q \in \{1, 19\} \mod 30
\end{align*}
\]
and define
\[
\tilde{L}_2 = \{(3.A_6) \times C_r : 3 \nmid r \mid (q - 1)\} \\
\cup \{(3.A_6) \circ C_{3r} C_{9r} : 9 \mid (q - 1), r \mid \frac{q - 1}{9}\}
\]
where \(3.A_6\) is as in Lemma 5.2.11. Then \(\tilde{L}_2\) is a list of finite irreducible non-modular subgroups of \(\text{GL}(3, q)\) with central quotient \(\text{Alt}(6)\). Moreover any such subgroup of \(\text{GL}(3, q)\) is \(\text{GL}(3, q)\)-conjugate to one and only one group in \(\tilde{L}_2\).

**Proof.** We refer to \(L_2\) in Theorem 5.2.13. If \(3.A_6 = \langle H, K \rangle\) is conjugate to a subgroup of \(\text{GL}(3, q)\) then \(\text{tr}(HK) = \beta_2\) and \(\text{tr}(HK^3) = \beta_1\) and so \(-\zeta_3(1 + \sqrt{5})/2 \in \text{GF}(q)\), i.e. \(\zeta_3, \sqrt{5} \in \text{GF}(q)\). Corollary 5.2.17 gives the following restrictions on \(q\) and \(a\) for the list of finite irreducible non-modular subgroups of \(\text{GL}(3, q)\) with central quotient 3.\text{Alt}(6).

<table>
<thead>
<tr>
<th>(a \equiv 0) mod 2</th>
<th>or</th>
<th>(a \equiv 1) mod 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>(q \equiv 1) mod 2</td>
<td></td>
<td>(q \equiv 1) mod 2</td>
</tr>
<tr>
<td>(q \equiv \pm 1) mod 3</td>
<td></td>
<td>(q \equiv 1) mod 3</td>
</tr>
<tr>
<td>(q \not\equiv 0) mod 5</td>
<td></td>
<td>(q \equiv \pm 1) mod 5</td>
</tr>
</tbody>
</table>

The result follows similarly to the previous theorem. \(\square\)

**Theorem 5.2.21.** Suppose
\[
a \equiv 0 \mod 2, \quad q \in \{1, 13, 19, 25, 31, 37\} \mod 42
\]
or
\[
a \equiv 1 \mod 2, \quad q \in \{1, 11, 23, 25, 29, 37\} \mod 42
\]
and define
\[
\tilde{L}_3 = \{L_2(7) \times C_r : r \mid (q - 1)\},
\]
where \(L_2(7)\) is as in Lemma 5.2.11. Then \(\tilde{L}_3\) is a list of finite irreducible non-modular subgroups of \(\text{GL}(3, q)\) with central quotient \(\text{PSL}(2, 7) \cong \text{GL}(3, 2)\). Moreover any such subgroup of \(\text{GL}(3, q)\) is \(\text{GL}(3, q)\)-conjugate to one and only one group in \(\tilde{L}_3\).

**Proof.** If \(L_2(7)\) has a conjugate in \(\text{GL}(3, q)\) then \(\text{tr}(SR) = \alpha_2\) and \(\text{tr}(S^2R) = \alpha_1\) are in \(\text{GF}(q)\), i.e. \(\frac{1}{2}(-1 \pm \sqrt{-7}) \in \text{GF}(q)\). Hence by Theorem 5.2.13 and Lemma 5.2.18, we get the following restrictions on \(q\) and \(a\):

<table>
<thead>
<tr>
<th>(a \equiv 0) mod 2</th>
<th>or</th>
<th>(a \equiv 1) mod 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>(q \equiv 1) mod 2</td>
<td></td>
<td>(q \equiv 1) mod 2</td>
</tr>
<tr>
<td>(q \equiv \pm 1) mod 3</td>
<td></td>
<td>(q \equiv 1) mod 3</td>
</tr>
<tr>
<td>(q \not\equiv 0) mod 5</td>
<td></td>
<td>(q \equiv \pm 1) mod 5</td>
</tr>
</tbody>
</table>
If $\sqrt{-7} \in \text{GF}(q)$ then $R \in \text{GL}(3, q)$, so $L_2(7) \leq \text{GL}(3, q)$. A similar argument as before gives the result. \hfill \Box

Combining the previous results in this subsection, we obtain the final classification of the chapter.

**Theorem 5.2.22.** Let $\bar{L}_i$, $1 \leq i \leq 3$, be as in Theorems 5.2.19, 5.2.20 and 5.2.21. Then $\bar{L} = \bigcup_{i=1}^{3} \bar{L}_i$ is a list of irreducible non-modular insoluble subgroups of $\text{GL}(3, q)$. Moreover any such subgroup of $\text{GL}(3, q)$ is $\text{GL}(3, q)$-conjugate to one and only one group in $\bar{L}$. 

65
Chapter 6

Insoluble modular linear groups of degree three

In this chapter we list the modular irreducible insoluble subgroups of $GL(3, q)$. We begin by determining which of the groups $G$ given in Theorems 5.2.19–5.2.21 can be lifted for characteristics dividing $|G|$. We obtain a complete and irredundant list of insoluble modular subgroups of $PSL(3, q)$ by combining the list of liftable groups in exceptional characteristics with a list of isomorphism types of such groups from Bloom [3] (which deals with odd $q$) and a list from Hartley [14] (dealing with even $q$). We emphasise our reliance on Bloom’s work in [3] which is vital in solving the relevant central extension problems in this chapter.

Note that Feit [7, pp.76-77] presents a ‘list’ of insoluble modular subgroups of $SL(3, q)$, citing Bloom, Hartley and Mitchell. Our approach enables us to derive a complete and irredundant list of all insoluble irreducible subgroups of $GL(3, q)$ which fully addresses the conjugacy issue in both $SL(3, q)$ and $GL(3, q)$.

6.1 Notation

Throughout this chapter: $q$ is a prime power, $p$ is a prime, and $n$ is a positive integer. We adopt the following notation:

- $\zeta_u$: a primitive $u$th root of unity in a specified field,
- $\mathcal{S} = \{(n, q) \mid n \geq 3, \text{ or } n = 2 \text{ and } q > 3\}$,
- $\hat{o}_s(t) = \max\{j \mid s^j \text{ divides } t\}$ for $s, t \in \mathbb{Z}^+$, and
- $(x; y)$: the greatest common divisor of $x$ and $y$.

Also, we extend the definition of $\hat{o}$ to a set $\mathcal{T}$ of positive integers: $\hat{o}_s(\mathcal{T}) = \{\hat{o}_s(t) \mid t \in \mathcal{T}\}$. 

66
Similar to Remark 3.0.2, we stress that a particular unitary group depends on some chosen non-degenerate form. Formally, $U$ is a unitary subgroup of $GL(n, q^2)$ if $U = \{ A \in GL(n, q^2) \mid \bar{A}^\top JA = J \}$ for some non-singular symmetric matrix $J$ where $\bar{A}$ is obtained by replacing each entry $a_{ij}$ in $A$ by $a_{ij}^{q}$.

### 6.1.1 Linear group notational differences

There are some differences between our notation for linear groups and that of the main references for this chapter: Bloom [3] and Hartley [14]. We clarify these here.

- Hartley uses $LF$ (Linear Fractional Group) for $PSL$ and $HO$ (Hyperorthogonal) in place of $PSU$.
- Bloom uses $U$ for a special unitary group and $U^*$ for a general unitary group.

In order to avoid confusion and ambiguity, we use $GU(n, q)$ and $SU(n, q)$ to mean, respectively, a general unitary group and a special unitary group in $GL(n, q^2)$. We follow the practice that a prefix ‘P’ denotes the linear group modulo its centre.

### 6.2 Preliminary results

**Lemma 6.2.1.** Suppose that $G$ is a perfect group such that $G/Z(G)$ is simple. If $N$ is a proper normal subgroup of $G$, then $N \leq Z(G)$.

Unless otherwise stated, we assume $(n, q) \in S$ for the remainder of this section. Thus $SL(n, q)$ is perfect and $PSL(n, q)$ is simple. The same is true of $SU(n, q)$ and $PSU(n, q)$, respectively, if further $q > 2$ when $n = 3$.

**Lemma 6.2.2.** $PSL(n, q)$ has a faithful representation of degree $n$ over $GF(q)$ if and only if $(n; q - 1) = 1$, in which case $PSL(n, q) \cong SL(n, q)$.

**Proof.** Suppose that $P \cong PSL(n, q)$ is a subgroup of $GL(n, q)$. If $P \not\leq SL(n, q)$ then $P \cap SL(n, q) = 1$, and we get the contradiction that $|P \cdot SL(n, q)| > |GL(n, q)|$. Thus $P \leq SL(n, q)$. Denote the centre of $SL(n, q)$ by $Z$. Then $P \cap Z = 1$, and so $SL(n, q) = P \times Z$, by orders again. Hence $P \leq SL(n, q)$. The result follows from Lemma 6.2.1.☐

**Lemma 6.2.3.** If $(n; q - 1) = 1$ then $PGL(n, q) \cong SL(n, q) \cong PSL(n, q)$.

**Corollary 6.2.4.** $PSL(3, q)$ has a faithful representation of degree $3$ over $GF(q)$ if and only if $3 \nmid q - 1$, in which case $PGL(3, q) \cong PSL(3, q) \cong SL(3, q)$.
Lemma 6.2.5. Suppose that $q > 2$ if $n = 3$. Then $PSU(n, q)$ has a faithful representation in $GU(n, q^2)$ if and only if $(n; q + 1) = 1$, in which case $PSU(n, q) \cong SU(n, q) \cong PGU(n, q)$.

Proof. Since $|SU(n, q)| = (n; q + 1)|PSU(n, q)|$, $SU(n, q)$ is perfect and $PSU(n, q)$ is simple, the proof is along the same lines as the proof of Lemma 6.2.2. □

Corollary 6.2.6. For $q > 2$, $PSU(3, q)$ has a faithful representation in $GL(3, q^2)$ if and only if $3 \mid (q + 1)$, in which case $PGU(3, q) \cong PSU(3, q) \cong SU(3, q)$.

Lemma 6.2.7. Let $K$ be an algebraically closed field and $L$ be a subfield of $K$. Suppose $G$ is a subgroup of $GL(n, L)$ irreducible over $K$. Then, modulo scalars, $N_{GL(n, K)}(G) \leq GL(n, L)$.

Proof. See [11, Lemma 5.15, p. 482]. □

Lemma 6.2.8. Let $P = PSL(n, q)$ for $n \in \{2, 3\}$. Then the Schur multiplier $H_2(P)$ is

(i) $Z_2$, if $(n, q) \in \{(2, 4), (3, 2), (2, 3)\}$,

(ii) $Z_6$, if $n = 2$ and $q = 9$,

(iii) $Z_4 \times Z_{12}$, if $n = 3$ and $q = 4$,

(iv) $Z_m$, for all other values of $q$, where $m = (n; q - 1)$.

In case (iv), $SL(n, q)$ is the unique Schur cover of $P$.

Proof. See [19, Theorem 7.1.1, p. 246] (which cites Steinberg). □

Lemma 6.2.9. Set $S = SL(n, q)$ and $G = GL(n, q)$. Suppose that $X \unlhd G$ and $X \cap S = 1$. Then $G/X$ is isomorphic to a subgroup of $G$.

Proof. Either $S \leq X$ or $X \leq Z := Z(G)$ (see e.g. [32, Theorem 3, p. 63]). Since $X \cap S = 1$, this forces $X \leq Z$. Then since $Z$ is cyclic, there are subgroups $Y$ and $T$ of $Z$ such that $X \leq T$, $S \cap Z \leq Y$, $Z = T \times Y$ and $|T|, |Y|$ are coprime. Thus $G = T \times \langle S, \alpha \rangle$ where $\alpha = \text{diag}(1, \ldots, 1, a)$ for some $a$ of order $|Y|$. Note that $\bar{S} := \langle S, \alpha \rangle = S \rtimes \langle \alpha \rangle$.

Now, set $|X| = k$ and define a homomorphism $\theta : G \to G$ by

$$\theta : t \bar{s} \mapsto t^k \bar{s}; \quad t \in T, \; \bar{s} \in \bar{S}.$$ 

We have $\ker \theta = \{t \in T \mid t^k = 1\} = X$. Thus $G/X \cong \theta(G) \leq G$ as required. □

Corollary 6.2.10. With the notation and hypotheses of Lemma 6.2.9, $G/X$ is isomorphic to a reducible subgroup of $GL(n + 1, q)$.

Lemma 6.2.11. Both Lemma 6.2.9 and Corollary 6.2.10 hold for $S$ replaced by $SU(n, q)$, $G$ replaced by $GU(n, q)$, and $X \leq G$ normal in $GL(n, q^2)$.

68
6.2. PRELIMINARY RESULTS

6.2.1 Normality of linear groups in extension groups

The main purpose of this subsection is to consider the following question where ‘Ω’ is replaced by each of ‘L’ and ‘U’:

if \( D \in D(n, \mathbb{GF}(q)) \), when is \( \langle D, S\Omega(n,q) \rangle \) a non-split extension of \( S\Omega(n,q) \) distinct from all elements of the set \( \{ S\Omega(n, q^\alpha), G\Omega(n, q^\alpha) \mid \alpha \in \mathbb{Z}^+ \} \)?

As an essential starting point, we consider the question of normality of special and general linear groups in extension groups; the case of unitary groups follows the same fundamental lines. From there, we answer the question posed above in full for the case \( n = 3 \). These results for \( n = 3 \) shall serve as a vital contribution to producing the lists given later in this chapter.

For each subgroup \( H \) of \( GL(n,q) \) we define an equivalence relation \( \sim_H \) on \( GL(n, GF(q)) \) by \( x \sim_H x' \) iff \( \langle H, x \rangle = \langle H, x' \rangle \). The \( \sim_H \)-equivalence classes are written \([x]_H\).

**Proposition 6.2.12.** If \((i; |x|) = (j; |x|)\) then \( x^i \sim_H x^j \) for any \( H \leq GL(n,q) \).

**Theorem 6.2.13.** An element \( x \) of \( GL(n, GF(q)) \) normalises \( GL(n,q) \) if and only if \( x = x_1 z \) where \( x_1 \in GL(n,q) \) and \( z \in GL(n, GF(q)) \) is scalar.

**Proof.** Since \( GL(n,q) \) is absolutely irreducible, this is an immediate consequence of Lemma 6.2.7. \(\square\)

We now shift attention to the case of \( SL(n,q) \) as this is of primary interest. Let \( \Delta_1 = \text{diag}(d_1, \ldots, d_n) \in SL(n, GF(q)) \).

**Corollary 6.2.14.** If \( \Delta_1 \) normalises \( SL(n,q) \) then \( d_i^\alpha \in GF(q)^\times \forall i \).

**Proof.** Again, this follows easily from Lemma 6.2.7. \(\square\)

Let \( F = GF(q) \) and \( D = \text{diag}(d_1, \ldots, d_n) \) where each \( d_i \) is some primitive \( k_i^\text{th} \) root of unity in \( F[\zeta_{k_i}]^\times \). We shall call \( D \)

- a \( \delta^m \)-type matrix if \( \forall i, k_i \mid m; \)
- a \( \delta_s^m \)-type matrix if \( \forall i, k_i \mid mu \) and \( \exists i \text{ s.t. } k_i \nmid u \), where \( u = (m; s) \).

**Lemma 6.2.15.** \( \Delta_1 = AB \) where \( A \) is a \( \delta^{q-1} \)-type matrix and \( B \) is \( \delta_{q-1}^n \)-type.

**Corollary 6.2.16.** Suppose that \( \Delta_1' = A'B \) where \( A' \) is \( \delta^{q-1} \)-type. Then \( \Delta_1' \sim_{SL(n,q)} \Delta_1 \); in fact \( \Delta_1 \sim_{SL(n,q)} B \).
6.2. PRELIMINARY RESULTS

Proof. The first part is clear since \( A, A' \in \text{SL}(n, q) \). For the second part, take \( A' \) to be the identity matrix. \qed

As a consequence of Corollary 6.2.16, in order to find distinct classes \([\Delta_1]_{\text{SL}(n, q)}\), it is only necessary to consider the different possible choices of \( \delta_{q-1}^n \)-type matrices.

**Corollary 6.2.17.** Suppose that \((q - 1; n) = 1\). Then the number of distinct \([\Delta_1]_{\text{SL}(n, q)}\) classes is \(|\{d \mid d \text{ divides } n, d > 1\}|\).

Proof. By Corollary 6.2.16, we can assume without loss of generality that \( \Delta_1 \) is \( \delta_{q-1}^n \)-type. Since \((q - 1; n) = 1\), each \( d_i \) must be an \( n \)th (not necessarily primitive) root of unity. By Theorem 6.2.13, each \( d_i \) can be written as \( \alpha_{ij} d_j, \alpha_{ij} \in \text{GF}(q)^\times \). Since all \( d_i \) are \( n \)th roots of unity, the only possible value for each \( \alpha_{ij} \) is 1. Hence all \( d_i \) are equal and thus the same primitive root of unity. The possibilities for these are precisely the (non-unit) divisors of \( n \). By Proposition 6.2.12, there can be no other classes. \qed

**Corollary 6.2.18.** If \( n \geq 3 \) then not all entries \( d_i \) in \( \Delta_1 \) can be distinct.

Proof. Again, we only need to consider the \( \delta_{q-1}^n \)-type part. Let \( t = n \cdot (n; q - 1) \). If the \( d_i \) are pairwise distinct, then the only possibilities are all different \( t \)th roots of unity. If \((n; q - 1) < n\), the result is clear by a simple counting argument. Suppose that \((n; q - 1) = n\) and so \( t = n^2 \). In this case, \( \{d_1, \ldots, d_n\} = \{\zeta_{n^2}^k, \zeta_{n^2}^{2k}, \ldots, \zeta_{n^2}^{(n-1)n}\} \), where \( k \nmid n := (n; q - 1) \).

Hence
\[
1 = \det(\Delta_1) = \zeta_{n^2}^{n k} \zeta_{n^2}^{n \sum_{j=0}^{n-1} j} = \zeta_{n^2}^{nk} \zeta_{n^2}^{(n-1)/2}.
\]

It follows that
\[
\zeta_{n^2}^k = 1, \quad \text{when } n \text{ is odd};
\]
\[
-\zeta_{n^2}^k = 1, \quad \text{when } n \text{ is even}.
\] (6.1)

But \( k \nmid n \), so the odd case in 6.1 cannot happen. The even case is only true if \( n = 2 \). \qed

**Corollary 6.2.19.** Let \( S\Omega(3, q) \in \{\text{SL}(3, q), \text{SU}(3, q)\} \). Up to conjugacy in \( S\Omega(3, \text{GF}(q)) \) there is only one subgroup of \( S\Omega(3, \text{GF}(q)) \) which is both a non-split extension of \( S\Omega(3, q) \) and contains \( S\Omega(3, q) \) as a subgroup of index 3.

Proof. Let \( s = \hat{\alpha}_3(q - 1) \). Applying Corollary 6.2.18, we can deduce the unique possibility \( \text{SL}(3, q)^3 = \langle \text{SL}(3, q), \text{diag}(\zeta_{3+1}, \zeta_{3+1}^{-2}, \zeta_{3+1}) \rangle \) up to conjugacy. A similar argument holds for \( \text{SU}(3, q) \). \qed
Corollary 6.2.20. Let $S\Omega(3,q) \in \{\text{SL}(3,q),\text{SU}(3,q)\}$ and $G\Omega(3,q)$ be the corresponding general linear/unitary group. Apart from the subgroup given in Corollary 6.2.19, up to conjugacy in $G\Omega(3,\overline{\text{GF}(q)})$, there is one additional subgroup of $G\Omega(3,\overline{\text{GF}(q)})$ which is both a non-split extension of $S\Omega(3,q)$ and contains $S\Omega(3,q)$ as a subgroup of index 3.

Proof. Denote $s = \hat{o}_3(q-1)$ as before. We take the additional generator as in Corollary 6.2.19 and multiply by the only relevant scalar $\text{diag}(\zeta_3 s+1,\zeta_3 s+1,\zeta_3 s+1)$. □

We denote the extensions of $S\Omega(3,q)$ by $C_3$ in Corollaries 6.2.19 and 6.2.20 by $S\Omega(3,q)_3$ and $S\Omega(3,q)_{3,3}$ respectively.

6.3 The modular lists for $\text{SL}(3,p^a)$ and $\text{GL}(3,p^a)$

6.3.1 Exceptional characteristics

Lemma 6.3.1. The modular insoluble irreducible subgroups of $\text{SL}(3,p^a)$ that can be lifted are precisely:

\begin{align*}
A_5 & \quad \text{when } (p = 3 \text{ and } 2 \mid a) \text{ or } p = 5, \\
3.A_6 & \quad \text{when } p \in \{2,5\} \text{ and } 2 \mid a, \\
L_2(7) & \quad \text{when } (p = 3 \text{ and } 2 \mid a) \text{ or } p = 7.
\end{align*}

Proof. We can eliminate certain characteristics by elementary character table arguments. For $A_5$ we need solutions to $\mu^2 - \mu - 1 = 0$ and so 2 must divide $a$ when $p = 2$ or 3. Now, we can disallow the possibility $p = 2$ altogether since if $2 \mid a$ then $\text{Alt}(5)$ will be reducible in $\text{SL}(3,2^a)$ because $\text{Alt}(5) \cong \text{SL}(2,4)$. The set of matrix generators as per Lemma 5.2.10 can be lifted directly to characteristic 3 when 2 divides $a$ and also to characteristic 5.

Since $3.A_6$ requires $\zeta_3$, we have that $p \neq 3$ and if $p \in \{2,5\}$ then $2 \mid a$. (It is interesting to note that identifying $\zeta_3$ with 1 produces a copy of $\text{Alt}(6)$ in $\text{GL}(3,p^a)$ from $\text{GL}(3,\mathbb{C})$.) We can use the generators given in Lemma 5.2.11 and directly lift these to characteristic $p \in \{2,5\}$ when $2 \mid a$.

$L_2(7)$ requires non-trivial solutions to $\alpha^2 + \alpha + 2 = 0$ so we cannot have $p = 2$. It also follows that 2 must divide $a$ when $p = 3$. The generators given in Lemma 5.2.12 lift for $p = 3$ when $2 \mid a$, and for $p = 7$. □

Remark 6.3.2. Note that $L_2(7) \cong \text{GL}(3,2)$ and so this group will indeed appear in a list of modular insoluble irreducible subgroups of $\text{SL}(3,p^a)$ when $p = 2$ and $2 \nmid a$. However, the important point here is that the previous theorem deals with groups that can be lifted and this is not an example of one of these groups.
6.3.2 Subgroups of $\text{PSL}(3, p^a)$

Lemma 6.3.3. Let $G$ be an insoluble irreducible subgroup of $\text{GL}(3, q)$. Then $G/Z(G)$ does not have a non-trivial normal elementary abelian subgroup.

Proof. Suppose that $N$ is a normal subgroup of $G$ properly containing $Z(G)$ such that $N/Z(G)$ is elementary abelian. Note that $N$ is nilpotent and completely reducible over the algebraic closure of $\text{GF}(q)$. Thus $N$ is monomial by Theorem 2.2.7. However, by Corollary 2.6.9, $N$ is primitive. This contradiction proves that $N$ cannot exist. □

The next theorem is a combination of Lemma 6.3.1, an extraction of Theorem 1.1 from Bloom [3] and the results of Hartley [14]. There is some intersection between the list of groups in Lemma 6.3.1 and the other two lists; we ensure that such groups are listed only once. We name the only possible extension groups for $\text{PSL}$ and $\text{PSU}$ in (a$^+$) and (b$^+$) below as $\text{PGL}$ and $\text{PGU}$. The other possibilities $\text{SL}$ and $\text{SU}$ cannot occur as their centres are non-trivial (for these particular cases) whereas the centre of $\text{PSL}(3, q)$ is trivial. Bloom also omits groups that contain a normal elementary abelian subgroup; Lemma 6.3.3 shows that we do not need to consider these.

Theorem 6.3.4. Let $\hat{G}$ be an insoluble modular subgroup of $\text{PSL}(3, p^a)$ not containing a normal elementary abelian subgroup. Then $\hat{G}$ is isomorphic to one of the following groups.

<table>
<thead>
<tr>
<th>Sublist I</th>
<th>Sublist III [when $3 \mid (p^a-1)$]:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) $\text{PSL}(3, p^b)$; $b \mid a$.</td>
<td>(a$^+$) $\text{PGL}(3, p^b)$; $3b \mid a$, $3 \mid (p^b-1)$.</td>
</tr>
<tr>
<td>(b) $\text{PSU}(3, p^b)$; $2b \mid a$.</td>
<td>(b$^+$) $\text{PGU}(3, p^b)$; $6b \mid a$, $3 \mid (p^b+1)$, $p^b \neq 2$.</td>
</tr>
<tr>
<td>(c) $\text{PSL}(2, p^b)$, $p \neq 2$, $b \mid a$, (c$^#$) $\text{PGL}(2, p^b)$; $p^b \neq 3$.</td>
<td></td>
</tr>
<tr>
<td>Sublist II [when $p = 3$ and $2 \mid a$]:</td>
<td>Sublist IV [when $p = 2$ and $2 \mid a$]:</td>
</tr>
<tr>
<td>(d) $\text{Alt}(5)$, $\text{PSL}(2, 7)$.</td>
<td>(e) $\text{Alt}(5)$, $\text{Alt}(6)$.</td>
</tr>
<tr>
<td>Sublist V [when $p = 5$ and $2 \mid a$]:</td>
<td>(f) $\text{Alt}(6)$, $\text{Alt}(6).2$, $\text{Alt}(7)$.</td>
</tr>
</tbody>
</table>

Moreover $\text{PSL}(3, p^a)$ has exactly one subgroup $\hat{G}$ of each type mentioned (for each indicated value of $p$ and $b$), up to conjugacy in $\text{GL}(3, p^a)/Z(\text{SL}(3, p^a))$.

We need another lemma to ensure that the groups listed are non-isomorphic. Henceforth, we will refer to the set of groups identified with the same label [i.e. any of (a), . . . , (f), (c$^#$), (a$^+$), (b$^+$)] as a family (of groups). If we label a set of groups within one of the main labels [(a), . . . , (f), (c$^#$), (a$^+$), (b$^+$)], then we will call this set a subfamily (of groups).
Lemma 6.3.5. For \( p, a, \) and \( b \) ranging as indicated, any two groups listed in Theorem 6.3.4 which differ in at least one of these three parameters are non-isomorphic.

Proof. All possible isomorphisms between PSL and PSU are given in [20, Prop. 2.9.1, p. 43]. Repetition from \( \text{PSL}(2, 7) \cong \text{PSL}(3, 2) \) clearly does not occur. By orders, \( \text{PSL}(2, p^b) \not\cong \text{PGL}(2, p^b) \) for odd \( p \), which is the constraint stated. This ensures no isomorphic copies in Sublist I.

All possible isomorphisms, between PSL and alternating groups together with those between SU and alternating groups, are also addressed in [20, Prop. 2.9.1, p. 43]. Repeats due to the isomorphisms \( \text{PSL}(2, 5) \cong \text{Alt}(5) \) and \( \text{PSL}(2, 9) \cong \text{Alt}(6) \) do not occur due to constraints on \( p \) and \( b \). So this ensures that there are no isomorphic copies amongst families (a)–(f) and (e\#).

For families (a+) and (b+), we have that \( \text{PGL}(3, q) \cong \text{PSL}(3, q) \) only when \( 3 \nmid (q - 1) \). Since we only list \( \text{PGL}(3, p^b) \) when \( 3 \mid (p^b - 1) \), there is no overlap between families (a) and (a+). Also, \( \text{PSU}(3, q) \cong \text{PGU}(3, q) \) only when \( 3 \nmid (q + 1) \) and no overlap occurs between families (b) and (b+) because we list \( \text{PGU}(3, p^b) \) only when \( 3 \mid (p^b + 1) \). The groups \( \text{PGU}(3, q) \) and \( \text{PGL}(3, \bar{q}) \) for any pair of prime powers \( q, \bar{q} \geq 2 \) are never isomorphic just by orders. This completes the proof. \( \square \)

6.3.3 Subgroups of \( \text{SL}(3, p^a) \)

The case \( 3 \nmid (p^a - 1) \)

Corollary 6.3.6. Suppose \( 3 \nmid (p^a - 1) \) and let \( G \) be an insoluble irreducible modular subgroup of \( \text{SL}(3, p^a) \). Then \( G \) is isomorphic to one and only one of the following groups.

Sublist I:

(a) \( \text{SL}(3, p^b); b \mid a \)

(b) (when \( p = 3 \), \( 2 \mid a \)): \( \text{SU}(3, 3^b); 2b \mid a \)

(c) \( \text{PSL}(2, p^b), \begin{cases} p \neq 2, b \mid a, \\ p^b \neq 3. \end{cases} \)

(c\#) \( \text{PGL}(2, p^b) \)

Sublist II [when \( p = 3 \) and \( 2 \mid a \)]:

(d) \( \text{Alt}(5), \text{PSL}(2, 7) \).

\( \text{SL}(3, p^a) \) has exactly one group of each isomorphism type mentioned (for each indicated value of \( p \) and \( b \)), up to conjugacy in \( \text{GL}(3, p^a) \). Furthermore, this is also a list of isomorphism types of insoluble modular subgroups of \( \text{PGL}(3, p^a) \).
6.3. THE MODULAR LISTS FOR $\text{SL}(3, p^a)$ AND $\text{GL}(3, p^a)$

**Proof.** We derive the above list from Theorem 6.3.4 and refer to families and sublists from there. For each $b | a$, we have that $(p^b - 1) | (p^a - 1)$, and hence $3 | (p^a - 1) \implies 3 | (p^b - 1)$.

By virtue of Corollary 6.2.4, $\text{SL}(3, p^b)$ corresponds to (a).

We change the entry in (b) because if $2b | a$, then $p^a$ must be a square in which case $p^a \in \{0, 1\}$ (mod 3). The added condition $3 | (p^a - 1)$ therefore enforces $p = 3$.

No change is required for groups listed in (c) and (d).

Sublists III–V are clearly irrelevant here.

By Corollary 6.2.4 and since $3 \nmid (p^a - 1)$, we have $\text{SL}(3, p^a) = \text{PSL}(3, p^a) \cong \text{PGL}(3, p^a)$. It then follows that the list given in the statement of the theorem is a list of subgroup types as claimed for $\text{SL}(3, p^a)$ and $\text{PGL}(3, p^a)$.

As a consequence of Theorem 6.3.4, Lemma 6.3.5 and the fact that $\text{SL}(3, p^a)$ has trivial centre, $\text{SL}(3, p^a)$ has exactly one subgroup of each type mentioned up to conjugacy in $\text{GL}(3, p^a)$. 

□

**The case $3 | (p^a - 1)$**

When associated with a linear group, $C_k$ shall denote the cyclic scalar subgroup of order $k$.

**Lemma 6.3.7.** For a group $G$, denote by $[G]$ the set of all subgroups $\langle H, Z \rangle$ of $\text{GL}(3, \mathbb{GF}(q))$ where $H \cong G$ and $Z$ is scalar. The complete list of possible central extensions by $\text{PGL}(2, q)$ in $\text{GL}(3, \mathbb{GF}(q))$ is as follows:

- i. $[\text{PGL}(2, q)]$,
- ii. $[\text{CSU}(2, q)]$,
- iii. $[\text{GL}(2, q)]$,
- iv. $[2^s.(\text{GL}(2, q)/C_k)]$ where $k \parallel (q - 1)$, $s \in \{0, 1, 2, \ldots\}$ and
- v. $[2^s.(\text{GU}(2, q)/C_k)]$ where $k \parallel (q + 1)$, $s \in \{0, 1, 2, \ldots\}$.

**Proof.** We have (up to isomorphism) that

$$\text{PSL}(2, q) \leq \text{PGL}(2, q) \leq \text{PSL}(2, q^2).$$

Recall from Lemma 6.2.8 that the unique Schur cover of $\text{PSL}(n, q)$ is $\text{SL}(n, q)$ (or it suffices to know that $\text{PSL}(n, q)$ is the derived subgroup of $\text{PGL}(n, q)$). Also $\text{PGL}(2, q) \cong \text{PGU}(2, q)$. The Schur multiplier for any $\text{PGL}(2, q)$ is 2. Hence the possible extensions of $\text{PGL}(2, p^b)$ are those listed in -i- to -v.- 

□
6.3. THE MODULAR LISTS FOR $\text{SL}(3, p^a)$ AND $\text{GL}(3, p^a)$

We now derive some results involving group isomorphisms which we need in order to avoid redundancies in the subsequent subgroup lists presented.

**Proposition 6.3.8.** Let $k$ be an odd positive integer. Then

$$\text{PGL}(2, q) \times C_k \cong \begin{cases} 
\text{GL}(2, q)/C_{\frac{q-1}{k}}, & \text{whenever } k \mid (q-1) \\
\text{GU}(2, q)/C_{\frac{q+1}{k}}, & \text{whenever } k \mid (q+1)
\end{cases}$$

Proof. Remember that $\text{PGL}(2, q) \cong \text{PGU}(2, q)$. Since $k$ is odd, if $k \mid (q-1)$ (respectively $k \mid (q+1)$) then $\text{GL}(2, q)/C_{\frac{q-1}{k}}$ (respectively $\text{GU}(2, q)/C_{\frac{q+1}{k}}$) has a subgroup isomorphic to $\text{PGL}(2, q)$ and a central cyclic subgroup of order $k$. The result then follows simply by comparing orders. □

**Proposition 6.3.9.** Let $r \mid (q-1)$. Then

$$\frac{\text{GL}(2, q)}{C_r} \odot_{C_{\alpha/\gcd(r, \frac{q-1}{r})}} \cong \frac{\text{GL}(2, q)}{C_k},$$

for each $k \mid r$ where $\hat{o}(r) = \hat{o}(k)$, $\alpha \mid \frac{q-1}{r}$ and $(\frac{r}{\alpha}; \frac{q-1}{r}) = 1$.

Proof. Denote $\frac{\text{GL}(2, q)}{C_r} \odot_{C_{\alpha/\gcd(r, \frac{q-1}{r})}}$ by $R$ and $\frac{\text{GL}(2, q)}{C_k}$ by $K$. Clearly $|R| = |K|$.

We have (up to isomorphism):

$$\frac{\text{SL}(2, q)}{\text{SL}(2, q) \cap C_r} \leq \frac{\text{GL}(2, q)}{C_r} \quad \text{and} \quad \frac{\text{SL}(2, q)}{\text{SL}(2, q) \cap C_k} \leq \frac{\text{GL}(2, q)}{C_k}.$$ 

Hence

$$\text{PSL}(2, q) \leq \frac{\text{GL}(2, q)}{C_r} \quad \text{and} \quad \frac{\text{GL}(2, q)}{C_k}, \quad \text{if } 2 \mid r \text{ and } 2 \mid k;$$

$$\text{SL}(2, q) \leq \frac{\text{GL}(2, q)}{C_r} \quad \text{and} \quad \frac{\text{GL}(2, q)}{C_k}, \quad \text{otherwise.}$$

Trivially $C_{\frac{q-1}{r}} \leq K$. Now $C_{\frac{q-1}{r}} = \langle C_{\frac{q-1}{k}}, C_{\alpha/\gcd(r, \frac{q-1}{r})} \rangle$ since $\alpha \mid \frac{q-1}{r}$ and $(\frac{r}{\alpha}; \frac{q-1}{r}) = 1$.

Hence $C_{\frac{q-1}{r}}$ is also a subgroup of $R$. If $r$ and $k$ are both odd, the result follows simply by orders. Let us now assume that $r$ and $k$ are even. Note that $|R| = |K| = 2^{\frac{q-1}{k}}|\text{SL}(n, q)| = 2^{\frac{q-1}{k}q}|\text{PSL}(n, q)|$. So, we get that

$$\frac{R}{\text{PSL}(2, q) \times C_{\frac{q-1}{r}}} \cong \frac{K}{\text{PSL}(2, q) \times C_{\frac{q-1}{r}}} \cong C_2.$$ 

Let $a = \hat{o}(2(q))$ and $b = \frac{q-1}{2^{a'}}$.

Since $\hat{o}(2(r)) = \hat{o}(2(k))$ and $\text{GL}(2, q) = \langle \text{SL}(2, q), \text{diag}(\zeta_b, \zeta_b), \text{diag}(1, \zeta_{2^a}) \rangle$, we have $R \cong K$. □
Corollary 6.3.10. Let \( r \mid (q - 1) \). Then
\[
\frac{\text{GL}(2, q)}{C_r} \times C_{r/k} \cong \frac{\text{GL}(2, q)}{C_k},
\]
for each \( k \mid r \) where \( \hat{o}_2(r) = \hat{o}_2(k) \) and \( (\frac{q-1}{r}, \frac{q-1}{k}) = 1 \).

Proposition 6.3.11. Let \( r \mid (q + 1) \). Then
\[
\frac{\text{GU}(2, q)}{C_r} \circ C_{\alpha r/k} \cong \frac{\text{GU}(2, q)}{C_k},
\]
for each \( k \mid r \) where \( \hat{o}_2(r) = \hat{o}_2(k) \), \( \alpha \mid \frac{q+1}{r} \) and \( (\frac{q+1}{r}, \frac{q+1}{k}) = 1 \).

Proof. The result follows similarly to the proof of Proposition 6.3.9 whereby SL is replaced by SU and \( (q - 1) \) is replaced by \( (q + 1) \). \( \square \)

Corollary 6.3.12. Let \( r \mid (q + 1) \). Then
\[
\frac{\text{GU}(2, q)}{C_r} \times C_{r/k} \cong \frac{\text{GU}(2, q)}{C_k},
\]
for each \( k \mid r \) where \( \hat{o}_2(r) = \hat{o}_2(k) \) and \( (\frac{q+1}{r}, \frac{q+1}{k}) = 1 \).

Theorem 6.3.13. Suppose that \( 3 \mid (p^a - 1) \). An insoluble irreducible modular subgroup of \( \text{SL}(3, p^a) \) is isomorphic to one and only one of the following groups.

<table>
<thead>
<tr>
<th>Sublist I:</th>
<th>Sublist III:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) ( \text{SL}(3, p^b) ), ( b \mid a ).</td>
<td>(a) ( \text{SL}(3, p^b)_3 ), ( 3 \mid (p^b - 1) ), ( 3b \mid a ).</td>
</tr>
<tr>
<td>( \text{SL}(3, p^b) \times C_3 ); ( 3 \nmid (p^b - 1) ), ( b \mid a ).</td>
<td></td>
</tr>
<tr>
<td>(b) ( \text{SU}(3, p^b) ), ( 2b \mid a ), ( p^b \neq 2 ).</td>
<td>(b) ( \text{SU}(3, p^b)_3 ), ( 3 \mid (p^b + 1) ), ( 6b \mid a ), ( p^b \neq 2 ).</td>
</tr>
<tr>
<td>( \text{SU}(3, p^b) \times C_3 ); ( 3 \nmid (p^b + 1) ), ( 2b \mid a ), ( p^b \neq 2 ).</td>
<td></td>
</tr>
<tr>
<td>(c) ( \text{PSL}(2, p^b) ), ( \text{PSL}(2, p^b) \times C_3 ); ( p \neq 2 ), ( b \mid a ), ( p^b \neq 3 ).</td>
<td></td>
</tr>
<tr>
<td>(c#) ( \text{PGL}(2, p^b)_3 ), ( \text{PGL}(2, p^b) \times C_3 ).</td>
<td></td>
</tr>
</tbody>
</table>

Moreover, for each of the groups \( H \) in Sublists I–V, \( \text{SL}(3, p^a) \) has exactly one subgroup \( G \) isomorphic to \( H \).
6.3. THE MODULAR LISTS FOR $\text{SL}(3, p^a)$ AND $\text{GL}(3, p^a)$

Proof. The collection of all central extensions in $\text{SL}(3, p^a)$ of groups given in Theorem 6.3.4 will produce a list which contains all insoluble irreducible subgroups of $\text{SL}(3, p^a)$. We will work through each of the families presented in Theorem 6.3.4 and find these central extensions for $3 \mid (p^a - 1)$ within each family. We determine which extensions are insoluble irreducible subgroups of $\text{SL}(3, p^a)$ and show that each of these is isomorphic to one of the groups given in Sublists I–V.

We divide the set of all possible $b$ dividing $a$ into those such that $3 \mid (p^b - 1)$ and those such that $3 \nmid (p^b - 1)$, where $b^{(3)}$ and $b'$ denote an element of the former and latter subsets respectively.

(a), (a$^+$) By Lemma 6.2.8, the unique Schur cover of $\text{PSL}(3, p^{b^{(3)}})$ is $\text{SL}(3, p^{b^{(3)}})$ and $\text{SL}(3, p^{b'}) = \text{PSL}(3, p^{b'})$. Hence $\text{SL}(3, p^b)$ is on our list. There is no faithful representation of $\text{PSL}(3, p^{b^{(3)}})$ in $\text{SL}(3, p^a)$, so $\text{PSL}(3, p^{b^{(3)}})$ or any split extension of it is irrelevant. The remaining possibilities are extensions of $\text{SL}(3, p^a)$. Let $Z_3 = \langle (\zeta_3, \zeta_3, \zeta_3) \rangle$. We have that $Z_3 \leq \text{SL}(3, p^a)$ but $Z_3 \not\leq \text{SL}(3, p^{b'})$. Hence $\langle \text{SL}(3, p^{b'}), Z_3 \rangle = \text{SL}(3, p^{b'}) \times C_3$ is on our list. On the other hand, $Z_3 \leq \text{SL}(3, p^{b^{(3)}}) \cap \text{SL}(3, p^a)$ so $\langle \text{SL}(3, p^{b^{(3)}}), Z_3 \rangle = \text{SL}(3, p^{b^{(3)}})$ and thus is irrelevant.

The remaining cases are possible extensions by $\text{PGL}(3, p^{b^{(3)}})$ in $\text{SL}(3, p^a)$ when $3b^{(3)} \mid a$. Note that 3-dimensional projective representations of subgroups of $\text{GL}(3, p^a)$ do not have faithful representations in $\text{SL}(3, p^a)$ as can be seen as a consequence of Lemma 6.2.2. Hence, the only possibility here is $\text{SL}(3, p^{b^{(3)}})$.

(b), (b$^+$) By [13, Theorem 2], $\text{SU}(3, p^b)$ has trivial Schur multiplier. Thus, by a similar argument to part (a), we get the list of corresponding groups.

(c), (c$^#$) $\text{SL}(3, p^a)$ contains $Z_3$ but neither the centreless $\text{PSL}(2, p^b)$ nor $\text{PGL}(2, p^b)$ has a subgroup isomorphic to $Z_3$. Hence we include $\text{PSL}(2, p^b) \times C_3$ and $\text{PGL}(2, p^b) \times C_3$.

By Lemma 6.3.7 and since $\frac{\text{GL}(2, p^{b^{(3)}})}{C_{(p^{b^{(3)}}-1)/3}}$ contains an isomorphic copy of $Z_3$, there must be a subgroup isomorphic to $\frac{\text{GL}(2, p^{b^{(3)}})}{C_{(p^{b^{(3)}}-1)/3}}$ in $\text{SL}(3, p^{b^{(3)}})$. However, by Corollary 6.3.10 that subgroup is isomorphic to $\text{PGL}(2, p^{b^{(3)}})$, so we can ignore it. When $3 \mid (p^b + 1)$, similarly, we have that $\text{PGL}(2, p^b) \cong \text{GU}(2, p^b)/C_{(p^b+1)/3}$.

(d) This case is clearly not relevant here.
6.3. THE MODULAR LISTS FOR $\text{SL}(3, p^a)$ AND $\text{GL}(3, p^a)$

(e), (f) Let $a$ be even. Since $|\text{Z}(\text{SL}(3, p^a))| = 3$, as well as the original groups, we need only consider central extensions of a group of order 3 by each of them. Since $\text{Alt}(5) \cong \text{PSL}(2, 5)$ and $\text{Alt}(6) \cong \text{PSL}(2, 9)$, we can appeal to Lemma 6.2.8 to find their covering groups.

In case (e), we have $p = 2$ and so we eliminate the possibilities $\text{Alt}(5)$, $\text{Alt}(6)$ and any possible split extensions in $\text{SL}(3, 2^a)$ for the following reasons:

$\text{Alt}(5) \cong \text{SL}(2, 4)$ and this is clearly reducible;

$\text{Alt}(6) \cong \text{Sp}(4, 2)$ and since $\text{Sp}(4, 2)$ is absolutely irreducible in $\text{GL}(4, 2)$ and $\text{GL}(4, 2)$ has a single conjugacy class of groups isomorphic to $\text{Sp}(4, 2)$, there is no faithful representation of $\text{Alt}(6)$ in $\text{GL}(3, 2^a)$.

This leaves us with $3.\text{Alt}(6)$ which is a triple cover of $\text{Alt}(6)$.

In case (f), we have $p = 5$ and so we eliminate the possibilities $\text{Alt}(6)$, $\text{Alt}(6).2$, $\text{Alt}(7)$ and any possible split extensions in $\text{SL}(3, 5^a)$ since:

$\text{GL}(5, 5)$ and $\text{GL}(4, 5)$ have a single conjugacy class of groups isomorphic to $\text{SL}(5, 5) \cong \text{Alt}(6)$ and $\text{SL}(4, 5) \cong \text{Alt}(6).2$ respectively (see [36]); and

the inclusion of $\text{Alt}(7)$ would imply that there is an isomorphic (not necessarily irreducible) copy of $\text{Alt}(6)$ in $\text{SL}(3, 5^a)$ which there clearly is not due to the reason just stated.

Thus, we are left with the covering groups of $\text{Alt}(7)$, $\text{Alt}(6)$ and $\text{Alt}(6).2$ which are $3.\text{Alt}(7)$, $3.\text{Alt}(6)$ and $3.\text{Alt}(6).2$ respectively.

If two groups are in different families then their central quotients are non-isomorphic – as we saw in Lemma 6.3.5. Within a family, they are non-isomorphic by just considering group orders. Hence, no two groups on the list are isomorphic given any particular choice of $p$ and $a$. □
6.3. THE MODULAR LISTS FOR $\text{SL}(3, p^a)$ AND $\text{GL}(3, p^a)$

6.3.4 Subgroups of $\text{GL}(3, p^a)$

We shall include the trivial case $r = 1$ for a direct product with factor $C_r$ unless the constraints given for a variable $r$ explicitly state otherwise.

The case $3 \mid (p^a - 1)$

**Theorem 6.3.14.** Let $3 \mid (p^a - 1)$, and let $G$ be an irreducible insoluble modular subgroup of $\text{GL}(3, p^a)$. Then $G$ is isomorphic to one and only one of the following groups.

(a) For each $b$ s.t. $b \mid a$:  
    (i) $\text{SL}(3, p^b) \times C_r$, $r \mid (p^a - 1)$, $(r; (p^b - 1)^2) \neq (p^b - 1)$, $p^b \neq 2$;  
    (ii) $\text{GL}(3, p^b) \times C_r$, $r \mid \frac{p^b - 1}{p^b - 1}$, $(r; p^b - 1) = 1$.

(b) For each $b$ s.t. $2b \mid a$ where $p = 3$:
    (i) $\text{SU}(3, 3^b) \times C_r$, $r \mid (3^a - 1)$, $(r; (3^b + 1)^2) \neq (3^b + 1)$;  
    (ii) $\text{GU}(3, 3^b) \times C_r$, $r \mid \frac{3^b - 1}{3^b + 1}$, $(r; 3^b + 1) = 1$.

For each $b$ s.t. $b \mid a$, $p \neq 2$ and $p^b \neq 3$:

(c) $\text{PSL}(2, p^b) \times C_r$, $r \mid (p^a - 1)$;

(c#) (i) $\text{PGL}(2, p^b) \times C_r$, $r \mid (p^a - 1)$;

    Either  
    (L-ii) $\text{GL}(2, p^b) / C_{2^r} \times C_t$, $r \mid \frac{p^b - 1}{4}$, when $4 \mid (p^b - 1)$  
    (L-iii) $2^s \left( \text{GL}(2, p^b) / C_{2^r} \right) \times C_t$, $2 \mid r, s \in [1, \ldots, \varphi_2\left(\frac{p^b - 1}{p^b - 1}\right)]$  

Or  

(U-ii) $\text{GU}(2, p^b) / C_{2^r} \times C_t$, $r \mid \frac{p^b + 1}{4}$, when $4 \mid (p^b + 1)$, $2b \mid a$  

(U-iii) $2^s \left( \text{GU}(2, p^b) / C_{2^r} \right) \times C_t$, $2 \mid r, s \in [1, \ldots, \varphi_2\left(\frac{p^b - 1}{p^b + 1}\right)]$  

When $p = 3$:

(d) (i) $\text{Alt}(5) \times C_r$, $r \mid (p^a - 1)$.

(ii) $\text{PSL}(2, 7) \times C_r$, $r \mid (p^a - 1)$.

Moreover, $\text{GL}(3, p^a)$ contains exactly one of the mentioned groups (for each indicated value of $b$, $r$ and $t$) up to isomorphism.
Proof. We take a similar approach as in Theorem 6.3.13 but here consider the list of subgroups of PGL(3, p^a) as in Corollary 6.3.6. Again, we deal with each family in turn.

(a) By [19, p. 246, Theorem 7.1.1(i)], SL(3, p^b) has trivial Schur multiplier. Hence the only possible extensions are split. Since here GL(3, p^b) = ⟨SL(3, p^b), Z(p^b−1)⟩, we get the conditions as stated. Note we impose the condition p^b ≠ 2 since SL(3, 2) ∼ GL(3, 2).

(b) When 2b | a, we have that SU(3, 3^2) ≤ SL(3, 3^a) \ GU(3, 3^b). By [13, Theorem 2], SU(3, 3^b) has trivial Schur multiplier. Therefore the only possible extensions are split. Since here GU(3, p^b) = ⟨SU(3, p^b), Z(p^b+1)⟩, we get the conditions as stated.

(c) The unique Schur cover of PSL(2, p^b) is SL(2, p^b) by Lemma 6.2.8 but this is reducible in GL(3, p^a) so is irrelevant. Hence we are left with a split extension as given.

(c#) We examine each of the lists -i- to -v- in Lemma 6.3.7 with q = p^b in order to determine which central extensions of PGL(2, p^b) are relevant.

- i- These groups will occur with split extensions by C_k for k dividing \( \frac{p^b-1}{p^a-1} \).

- ii-, iii- We discard these entirely as all groups of these types are reducible in GL(3, p^a).

- iv- Since Z(SL(2, p^b)) = ⟨diag(−1, −1)⟩, we have for odd k, SL(2, p^b) ≤ GL(2, p^b)/C_k. By Corollary 6.2.10, these groups are reducible in GL(3, p^b) for odd k. Thus, only even k are relevant. Let k = 2r. Now the only possibilities for central extensions of GL(2, p^b)/C_{2r} are by those whose order divide \( \frac{2r(p^a-1)}{p^b-1} \) but not \( \frac{p^b-1}{2r} \). This is clear since GL(2, p^b)/C_{2r} contains a copy of C_{(p^b−1)/2r}. By Proposition 6.3.8, in order to avoid isomorphism with type -i- groups, we require \( \frac{p^b-1}{2r} \) to be even so relevant groups are only those in which 4 divides \( p^b−1 \). We impose further conditions on cases (L-ii), (L-iii), (U-ii), (U-iii) by taking into consideration Propositions 6.3.9 and 6.3.11 in order to avoid listing two groups which are isomorphic.

- v- A similar argument to case -iv- holds by applying Lemma 6.2.11 and noting that SU(2, p^b) ∼ SL(2, p^b). In this case, however, we require that 2b | a and replace \( p^b−1 \) by \( p^b+1 \).

(d) The split extensions arise as per arguments from the previous chapter (cf. Lemmas 5.2.1 and 5.2.4).

We have now exhausted all possibilities. It is trivial to see that groups with the same central quotient within each family, apart from (c#), are non-isomorphic by comparing orders. Groups in (c#) are pairwise non-isomorphic by Propositions 6.3.8, 6.3.9 and 6.3.11. This completes the proof. □
6.3. THE MODULAR LISTS FOR $\text{SL}(3, p^a)$ AND $\text{GL}(3, p^a)$

The case $3 \mid (p^a - 1)$.

The next theorem expands on Lemma 2.4.8.

**Theorem 6.3.15** ([11, Theorem 4.5]). Let $G$ be a subgroup of $\text{GL}(n, q)$. Then there exists $\tilde{G} \leq \text{SL}(n, \mathbb{F}_p)$ such that $G/Z(G) \cong \tilde{G}/Z(\tilde{G})$. In fact, $\tilde{G} \leq \text{SL}(n, q^m)$, where

(i) $m$ is a divisor of $n - 1$ if $n \neq p$ and $n$ does not divide $q - 1$,

(ii) $m = n$ if $n \neq p$ and $n$ divides $q - 1$.

(iii) $m = 1$ if $n = p$.

Further, $\tilde{G}$ has property $P$ if and only if $G$ has property $P$, where $P \in \{\text{irreducible, absolutely irreducible, }\mathbb{K}\text{-primitive}\}$, $\mathbb{K}$ a subfield of $\mathbb{F}_p$ containing $\text{GF}(q)$.

**Lemma 6.3.16.** Let $3 \mid (p^a - 1)$ and let $\tilde{G}$ be an insoluble modular subgroup of $\text{PGL}(3, p^a)$ which does not contain a normal elementary abelian subgroup. Then $\tilde{G}$ is isomorphic to one of the following groups.

<table>
<thead>
<tr>
<th>Sublist I:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) $\text{PSL}(3, p^b)$; $b \mid 3a$</td>
</tr>
<tr>
<td>(b) $\text{PSU}(3, p^b)$; $2b \mid 3a$</td>
</tr>
<tr>
<td>(c) $\text{PSL}(2, p^b)$, $p \neq 2$, $b \mid 3a$, $p^b \neq 3$.</td>
</tr>
<tr>
<td>(c#) $\text{PGL}(2, p^b)$; $p \neq 3$.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sublist III:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a+) $\text{PGL}(3, p^b)$; $3 \mid (p^b - 1)$, $b \mid a$.</td>
</tr>
<tr>
<td>(b+) $\text{PGU}(3, p^b)$; $3 \mid (p^b + 1)$, $2b \mid a$.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sublist IV [when $p = 2$ and $2 \mid a$]:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(e) $\text{Alt}(5)$, $\text{Alt}(6)$.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sublist V [when $p = 5$ and $2 \mid a$]:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(f) $\text{Alt}(6)$, $\text{Alt}(6).2$, $\text{Alt}(7)$.</td>
</tr>
</tbody>
</table>

**Proof.** Let $G \leq \text{GL}(3, p^a)$. By setting $n = 3$, $q = p^a$ with $3 \mid (q - 1)$ in Theorem 6.3.15, we find that there exists $\tilde{G} \leq \text{SL}(3, p^{3a})$ such that $\tilde{G} \cong G/Z(\tilde{G})$, where $\tilde{G} = G/Z(G)$. Hence for any $\tilde{G} \leq \text{PGL}(3, p^a)$, there exists a group isomorphic to $\tilde{G}$ in $\text{PSL}(3, p^{3a})$. Therefore, a complete list of isomorphism types of subgroups of $\text{PSL}(3, p^{3a})$ contains a complete list of isomorphism types of subgroups of $\text{PGL}(3, p^a)$. Since $\text{PSL}(3, p^{3a})$ and $\text{PGL}(3, p^a)$ are of the same dimension, the previous sentence remains valid if we replace “subgroups” by “insoluble modular subgroups”. By applying Theorem 6.3.4, the result then follows. □

Note that in Lemma 6.3.16, we have not stated that each subgroup given in the list is isomorphic to a subgroup of $\text{PGL}(3, p^a)$. We have merely stipulated that the list contains (as opposed to consists of) a complete list of insoluble modular subgroups of $\text{PGL}(3, p^a)$.
6.3. THE MODULAR LISTS FOR $\text{SL}(3,p^a)$ AND $\text{GL}(3,p^a)$

We shall refer to X-type groups to mean groups that are isomorphic to groups of the form $X(m,r)$ (for arbitrary parameters $m$ and $r$) where $X$ is one of the linear group types, e.g. $\text{PSL}$.

**Lemma 6.3.17.** Let $(n,q) \in S$. Then every PSL-type group which is a subgroup of $\text{PGL}(n,q)$ is also a subgroup of $\text{PSL}(n,q)$.

**Proof.** When $(n; q-1) = 1$ the result is clear. Now suppose that $(n; q-1) \neq 1$. Consider the homomorphism

$$\theta : \text{GL}(n,q) \to \text{PGL}(n,q)$$

where

$$\theta|_D : D(n,q) \to \text{PD}(n,q)$$

is defined by

$$\text{diag}(a_1, a_2, \ldots, a_n) \mapsto \text{diag}\left(\frac{a_1}{a_2}, \frac{a_2}{a_3}, \ldots, \frac{a_k}{a_{k+1}}, \ldots, \frac{a_n}{a_1}\right).$$

Note that $\ker(\theta|_D) = Z(\text{GL}(n,q))$. Define $\tau : S \to D(n,q)$ by

$$(n,q) \mapsto \begin{cases} (n-3)/2 \text{ times} & (n-1)/2 \text{ times} \\ \text{diag}(1, \ldots, 1, \zeta_{q-1}, 1, \ldots, 1), & \text{for } n \text{ odd;} \\ (n-4)/2 \text{ times} & (n-2)/2 \text{ times} \\ \text{diag}(1, \ldots, 1, \zeta_{q-1}, 1, \zeta_{q-1}, 1, \ldots, 1), & \text{for } n \text{ even.} \end{cases}$$

Then it is clear that

$$\text{PGL}(n,q) \cong \text{GL}(n,q)\theta = \langle \text{SL}(n,q)\theta, ((n,q))\tau \rangle.$$ 

Therefore, a subgroup in $\text{GL}(n,q)\theta$ corresponds to an isomorphic copy in $\text{PGL}(n,q)$ and vice-versa. Let $\bar{p}$ be a prime and $b$ a positive integer. We can see that there does not exist any subgroup $H$ which is an isomorphic copy of some $\text{PSL}(n,\bar{p}^b)$ in $\text{GL}(n,q)\theta$ not found in $\text{PSL}(n,q)$, since for any such $H$, we have $\langle((n,q))\tau \rangle \cap H = 1$. Hence a PSL-type subgroup of $\text{PGL}(n,q)$ is also a subgroup of $\text{PSL}(n,q)$.

**Corollary 6.3.18.** Let $(n,q) \in S$. Then the only PGL-type subgroups of $\text{PGL}(n,q)$ are those corresponding to PSL-type subgroups of $\text{PSL}(n,q)$ with the same parameters.

**Proof.** Consider $\theta$ and some $\bar{p}^b$ as in the proof of Lemma 6.3.17. We have that

$$\text{GL}(n,\bar{p}^b)\theta = \langle \text{SL}(n,\bar{p}^b)\theta, ((n,\bar{p}^b))\tau \rangle.$$ 

Thus, if $\text{PGL}(n,q)$ is to contain an isomorphic copy of a PGL-type then it would have to contain the corresponding PSL-type.

□
Corollary 6.3.19. Let \((n, q) \in S\). Then the only PSU or PGU-type subgroups of PGU\((n, q)\) are those which correspond to PSU-type subgroups of PSU\((n, q)\) with the same parameters.

Proof. Follows similarly to Lemma 6.3.17 and Corollary 6.3.18 after replacing SL with SU, GL with GU, \((n, q - 1)\) with \((n, q + 1)\) and \((n, \bar{p^b} - 1)\) with \((n, \bar{p^b} + 1)\). □

Lemma 6.3.20. Let \(3 \mid (p^a - 1)\) and \(\tilde{G}\) be an insoluble modular subgroup of PGL\((3, p^a)\) not containing a normal elementary abelian subgroup. Then \(\tilde{G}\) is isomorphic to one and only one of the following groups.

<table>
<thead>
<tr>
<th>Sublist I:</th>
<th>Sublist III:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) PSL((3, p^b)); (b \mid a)</td>
<td>(a) PGL((3, p^b)); (3 \mid (p^b - 1), b \mid a)</td>
</tr>
<tr>
<td>(b) PSU((3, p^b)); (2b \mid a)</td>
<td>(b) PGU((3, p^b)); (3 \mid (p^b + 1), 2b \mid a)</td>
</tr>
<tr>
<td>(c) PSL((2,p^b)), (p \neq 2, b \mid a)</td>
<td>Sublist IV ([\text{when } p = 2 \text{ and } 2 \mid a]):</td>
</tr>
<tr>
<td>(c#) PGL((2, p^b)); (p^b \neq 3)</td>
<td>(e) Alt((5)), Alt((6))</td>
</tr>
<tr>
<td></td>
<td>(f) Alt((6)), Alt((6,2)), Alt((7))</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Moreover, PGL\((3, p^a)\) contains exactly one of the mentioned groups (for each indicated value of \(b\)) up to isomorphism.

Proof. Apply Lemma 6.3.17 and Corollaries 6.3.18, 6.3.19 to Lemma 6.3.16. □

Before dealing with the case \(3 \mid (p^a - 1)\), we present a straightforward lemma in order to prevent redundancies in the list given in the subsequent theorem.

Lemma 6.3.21. Let \(r\) be prime and

\[
\left(\Omega, S\right) = \left(\operatorname{SL}(r, p^b), \delta_r(p^b - 1)\right) \text{ or } \left(\operatorname{SU}(r, p^b), \delta_r(p^b + 1)\right).
\]

Then \(\Omega \rtimes C_{r-1} \cong \Omega \circ_{C_r} C_{r^*}\).

Proof. Let \(A = \operatorname{diag}(\zeta_{r^*}, \ldots, \zeta_{r^*}, \zeta_{r^*}^{-1}, \ldots, \zeta_{r^*})\) and \(B = \operatorname{diag}(1, \ldots, 1, \zeta_{r^* - 1}, 1, \ldots, 1)\).

We have that \(\Omega \rtimes C_{r^* - 1} = \langle \Omega, B \rangle\) and \(\Omega \circ_{C_r} C_{r^*} = \langle \Omega, BA \rangle\). Since \(A \in \Omega\) and \(|\Omega \rtimes C_{r^* - 1}| = |\Omega \circ_{C_r} C_{r^*}|\), the groups are isomorphic. □

In the following theorem, we use parentheses [ ] to indicate a choice of inclusion or exclusion of a given part of a group name. For each part, there are associated conditions given in [ ]; these appear in the same respective order as the parts, e.g. \(A[xC_{r}] [\times C_{3s}]\) and conditions \([r][3^s] \mid q\) would indicate that the full list of corresponding subgroups are: \(A, A \times C_r \text{ for } r \mid q, A \times C_{3s} \text{ for } 3^s \mid q\) and \(A \times C_r \times C_{3s} \text{ for } r3^s \mid q\).
Theorem 6.3.22. Let $3 \mid (p^n - 1)$ and let $G$ be an insoluble irreducible modular subgroup of $\text{GL}(3, p^n)$. Then $G$ is isomorphic to one and only one of the groups in the following list. $\dagger$ indicates conditions are exactly the same as given in the corresponding family or subfamily (as a function of variables) in Theorem 6.3.14.

Sublist I:
(a) For each $b$ s.t. $b \mid a$:
(i) $\text{SL}(3, p^b) \times C_r$, $\dagger$
(ii) $\text{GL}(3, p^b) \times C_r$, $\dagger$
(iii) $\text{SL}(3, p^b) \times C_r$, $3 \mid r \mid (p^a - 1)$
(iv) $\text{SL}(3, p^b) \circ C_3 C_9 r$, $r \mid \frac{(p^a - 1)}{9}$

(b) For each $b$, s.t. $2b \mid a$, $p^b \neq 2$:
(i) $\text{SU}(3, p^b) \times C_r$, $r \mid (p^a - 1)$, $(r; (p^b + 1)^2) \neq (p^b + 1)$
(ii) $\text{GU}(3, p^b) \times C_r$, $r \mid (p^a - 1)/(p^b + 1)$, $(r; p^b + 1) = 1$
(iii) $\text{SU}(3, p^b) \times C_r$, $3 \mid r \mid (p^a - 1)$
(iv) $\text{SU}(3, p^b) \circ C_3 C_9 r$, $r \mid \frac{(p^a - 1)}{9}$

For each $b$, s.t. $b \mid a$, $p \neq 2$ and $p^b \neq 3$:
(c) $\text{PSL}(2, p^b) \times C_r$, $\dagger$
(d\#) (i) $\text{PGL}(2, p^b) \times C_r$, $\dagger$
(L-ii) $\text{GL}(2, p^b) \circ C_2 r$, $\dagger$
(L-iii) $2^a \left( \frac{\text{GU}(2, p^b)}{C_2 r} \right) \times C_t$, $\dagger$
(U-ii) $\text{GU}(2, p^b) \times C_t$, $\dagger$
(U-iii) $2^a \left( \frac{\text{GU}(2, p^b)}{C_2 r} \right) \times C_t$, $\dagger$

Sublist III:
(a\#) For each $b$ s.t. $b \mid a$, $3 \mid (p^b - 1)$:
(i) $\text{SL}(3, p^b) \times C_3 r [\circ C_3 C_9 r]$, $3^* [3'] \mid (p^a - 1)\{ (3^* [3'])^2 \mid (p^b - 1) \neq (p^b - 1)$
(ii) $\text{SU}(3, p^b) \circ C_3 r [\circ C_3 C_9 r]$, $3b \mid a$, $r \neq 1$, $[r][3'][3'] \mid (p^a - 1)$
(iii) $3\text{SL}(3, p^b) \times C_r$, $3b \mid a$, $r \mid (p^a - 1)$
(iv) $\text{GU}(3, p^b) \times C_r$, $r \mid \frac{p^a - 1}{p^b - 1}$, $(r; p^b - 1) = 1$

(b\#) For each $b$, s.t. $2b \mid a$, $3 \mid (p^b + 1)$, $p^b \neq 2$:
(i) $\text{SU}(3, p^b) \times C_3 r [\circ C_3 C_9 r]$, $3^* [3'] \mid (p^a - 1)$, $(3^* [3'])^2 \neq (p^b - 1)$
(ii) $\text{SU}(3, p^b) \circ C_3 r [\circ C_3 C_9 r]$, $3b \mid a$, $r \neq 1$, $[r][3'][3'] \mid (p^a - 1)$
(iii) $3\text{SU}(3, p^b) \times C_r$, $3b \mid a$, $r \mid (p^a - 1)$
(iv) $\text{GU}(3, p^b) \times C_r$, $r \mid \frac{p^a - 1}{p^b + 1}$, $(r; p^b - 1) = 1$

Sublist IV [when $p = 2$ and $2 \mid a$]:
(e) (i) $3\text{Alt}(6) \times C_r$, $3 \mid r \mid (p^a - 1)$
(ii) $3\text{Alt}(6) [\circ C_3 C_9 r]$, $r \mid \frac{p^a - 1}{9}$

Sublist V [when $p = 5$ and $2 \mid a$]:
(f) (i) $3\text{Alt}(k) \times C_r$, $3 \mid r \mid (p^a - 1)$
(ii) $3\text{Alt}(k) [\circ C_3 C_9 r]$, $r \mid \frac{p^a - 1}{9}$
(iii) $3\text{Alt}(6) / 2 \times C_r$, $3 \mid r \mid (p^a - 1)$
(iv) $3\text{Alt}(6) / 2 [\circ C_3 C_9 r]$, $r \mid \frac{p^a - 1}{9}$

Moreover, $\text{GL}(3, p^n)$ contains exactly one of the mentioned groups (for each indicated value of $p$ and $b$), up to isomorphism.
6.3. THE MODULAR LISTS FOR $\text{SL}(3, p^a)$ AND $\text{GL}(3, p^a)$

**Proof.** Our proof goes through the possibilities arising from Lemma 6.3.20 whereby we only consider families and subfamilies not covered in Theorem 6.3.14.

Subfamilies (a) (iii) and (iv) arise simply by recognising that $C_3 \leq \text{SL}(3, p^b)$. Similarly to Theorem 6.3.14, the fact that both $\text{SL}(3, p^b)$ and $\text{SU}(3, p^b)$ have trivial Schur multiplier verifies (b), (a$^+$) and (b$^+$). For family (a$^+$), we get the three possible covers of $\text{PGL}(3, p^b)$: $\text{SL}(3, p^b).3$ (by Corollary 6.2.19), $3.\text{SL}(3, p^b)$ (by Corollary 6.2.20) and $\text{SL}(3, p^b) \rtimes C_3$. In a similar fashion for (b$^+$), we get the three possible covers of $\text{PGU}(3, p^b)$: $\text{SU}(3, p^b).3$, $3.\text{SU}(3, p^b)$ and $\text{SU}(3, p^b) \rtimes C_3$. For families (b) and (b$^+$), we stipulate that $p^b \neq 2$, since both $\text{SU}(3, 2)$ and $\text{GU}(3, 2)$ are soluble.

Again, groups in family (d) are not relevant here.

For (e), we can disregard the possibility of $3.\text{Alt}(6).2$ since we would require a scalar element of order precisely 2 which is impossible since here $p = 2$. We are left with the split extensions as presented.

For (f), all possible Schur covers of $\text{Alt}(6)$ and $\text{Alt}(7)$ are the same as in Theorem 6.3.13. The split extensions of these which we present follow trivially.

Within a family, apart from (a$^+$), (b$^+$) and (c$^\#$), orders of the individual groups prevent isomorphic copies. Pairwise distinct groups in (a$^+$) with the same order will contain subgroups $\text{GL}(3, p^b)$ and $\text{SL}(3, p^b).3$; hence they cannot be isomorphic as their centres are always different. A similar argument holds for (b$^+$). As already noted in the proof of Theorem 6.3.14, isomorphism among groups for given parameters $p$ and $a$ in (c$^\#$) does not occur. A careful examination of the groups listed reveals that possible redundancies discussed in Lemma 6.3.21 do not occur. \(\square\)

### 6.3.5 Generating sets

In this subsection, we list completely and irredundantly the matrix generating sets for the insoluble irreducible modular subgroups of $\text{GL}(3, p^a)$ up to conjugacy. We aim to provide generating sets which have the least number of generators possible. We elect not to include a corresponding list of such generating sets for subgroups of $\text{SL}(3, p^a)$ as it is a trivial exercise to derive these from those of $\text{GL}(3, p^a)$.

We first require a few results that enable us to achieve the above. The initial results deal with techniques to produce certain matrix generating sets and the later results tackle the issue of conjugacy.

**Lemma 6.3.23.** Let $E$ be any extension of $\text{GF}(q)$ and $q > 2$. If $G$ is a subgroup of $\text{GL}(n, E)$ isomorphic to $\text{SL}(n, q)$ then $G$ is irreducible over $E$, and is conjugate to $\text{SL}(n, q)$.

---

85
6.3. THE MODULAR LISTS FOR $\text{SL}(3,p^a)$ AND $\text{GL}(3,p^a)$

Proof. See [11, Theorem 5.16, pp. 482f.]. □

Lemma 6.3.24. Let $E$ be any extension of $\text{GF}(q^2)$ and $(n,q) \in S$. If $G$ is a subgroup of $\text{GL}(3,E)$ isomorphic to $\text{SU}(3,q)$ then $G$ is irreducible over $E$, and is conjugate to $\text{SU}(3,q)$.

Proof. Applying Theorem 2.3.6, we see that $\text{GF}(q^2)$ is a splitting field of $\text{SU}(3,q)$. The result then follows similar reasoning to that in the proof of [11, Theorem 5.16]. □

Lemma 6.3.25. Let $F$ be any field. For each $t \in \mathbb{Z}^+$, define

$$\phi_t : \text{GL}(2,F) \rightarrow \text{GL}(3,F)$$

where

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (ad - bc)^{t-1} \begin{pmatrix} a^2 & 2ab & 2b^2 \\ ac & ad + bc & 2bd \\ c^2/2 & cd & d^2 \end{pmatrix}$$

(6.2)

for any $a,b,c,d \in F$ such that $(ad - bc) \neq 0$.

(i) Each $\phi_t$ is a homomorphism.

(ii) $\ker(\phi_t) = \langle \text{diag}(\zeta_\delta, \zeta_\delta) \rangle$ where $\delta = \max \{ a \in \mathbb{Z}^+ | \zeta_a^2 \in F, \ zeta_a^{2t} = 1 \}$.

(iii) Let $G \subseteq \text{GL}(2,F)$. Then $\det \circ \phi_t(G) = \{ x^{3t} | x \in \det(G) \} \subseteq F^\times$.

Proof. Part (i) is straightforward to verify by direct calculation.

For (ii), note that in order to get the identity matrix on the right-hand side of (6.2), it is necessary that $b = c = 0$ and $a = d$. A quick calculation then verifies the conclusion.

For (iii), first note that

$$\begin{vmatrix} a^2 & 2ab & 2b^2 \\ ac & ad + bc & 2bd \\ c^2/2 & cd & d^2 \end{vmatrix} = (ad - bc)^3.$$

Take any $A \in \text{GL}(2,F)$ with entries $a,b,c,d$ as in (6.2). It then follows that $\det(A) = (ad - bc)$ and $\det(\phi_t(A)) = \det(A)^{3(t-1)} \cdot \det(A)^3 = \det(A)^{3t}$. This is true for all $A \in \text{GL}(2,F)$ and hence the result follows. □

Remark 6.3.26. We constructed the maps in (6.2) by generalising the special case of $t = 0$ which appears in Bloom [3].
6.3. THE MODULAR LISTS FOR $\text{SL}(3, p^a)$ AND $\text{GL}(3, p^a)$

**Lemma 6.3.27.** Let $q$ be an odd prime power and define $\mathcal{T}_q = \{1, \ldots, q-1\}$. Consider the collection of mappings $\{\phi_k\}_{k=1}^{q-1}$ arising from Equation (6.2). Let $G \leq \text{GL}(2, q)$ and write $\det(G) = \langle \zeta_r \rangle$ for some $r \mid (q-1)$. Then $i - iii$ below are equivalent for any $t, t' \in \mathcal{T}_q$.

i. $\ker \phi_t = \ker \phi_{t'}$ and $\det \circ \phi_t(G) \neq \det \circ \phi_{t'}(G)$,

ii. $(t; \frac{q-1}{2}) = (t'; \frac{q-1}{2})$ and $(3t; r) = (3t'; r)$,

iii. $2 \mid r$ and $\hat{o}_2(\{r, \frac{q}{2}\}) = \hat{o}_2(\{t, t'\})$

**Proof.** Note that when $F = \text{GF}(q)$ in Lemma 6.3.25, $\delta = 2(\frac{q-1}{2})$ in ii. It follows directly that $\ker \phi_t = \ker \phi_{t'}$ if and only if $(t; \frac{q-1}{2}) = (t'; \frac{q-1}{2})$. Since $\det(G)$ consists of all $r^{th}$ roots of unity, we have

$$\det(G) = \{x \mid x^r = 1\} \text{ and } \det \circ \phi_t(G) = \{y \mid y^{r/(3t; r)} = 1\}.$$

Hence $\det \circ \phi_t(G) = \det \circ \phi_{t'}(G)$ if and only if $(3t; r) = (3t'; r)$. Hence, we have $i \iff ii$.

Now, let $\alpha_s = (s; \frac{q-1}{2})$ and $\beta_{s,r} = (3s; r), s \in \mathcal{T}_q$.

Label the $k$ divisors of $q-1$ as $\{d_i\}_{i=1}^k$. Note that

$$\alpha_{d_i} = \begin{cases} \frac{d_i}{2}, & \text{if } \hat{o}_2(\frac{q-1}{d_i}) = 0; \\ d_i, & \text{otherwise.} \end{cases} \quad \text{and} \quad \beta_{d_i,q-1} = \begin{cases} 3d_i, & \text{if } 3 \mid \frac{q-1}{d_i}; \\ d_i, & \text{otherwise.} \end{cases}$$

Hence for each $d_j > d_i$,

$$\alpha_{d_j} = \alpha_{d_i} \iff d_j = 2d_i \text{ and } \hat{o}_2(\frac{q-1}{d_j}) = 0,$$

in which case, $\beta_{d_j,q-1} \neq \beta_{d_i,q-1}$. Now $\beta_{s,r} = (\beta_{s,q-1}; r)$ and so if $2 \mid r$ then $\beta_{d_j,r} \neq \beta_{d_i,r}$ and otherwise $\beta_{d_j,r} = \beta_{d_i,r}$.

Next consider the equivalence relation $\sim$ on $\mathcal{T}_q$ defined by $m_1 \sim m_2 \iff (m_1; q-1) = (m_2; q-1), \quad \forall m_1, m_2 \in \mathcal{T}_q$.

We can write our equivalence classes as precisely $[d_i]_{i=1}^k$. For any $s_i \in [d_i]$, we have $\alpha_{s_i} = \alpha_{d_i}$ and $\beta_{s_i,r} = \beta_{d_i,r}$. Combining with above, this gives $i \iff ii \iff iii$ and we are done. □

**Corollary 6.3.28.** Let $C_{2s} < G \leq \text{GL}(2, q)$ for some $s \mid (q-1)$. Then $G/C_{2s}$ has at least two non-conjugate isomorphic copies in $\text{GL}(3, q)$ when any of the conditions in Lemma 6.3.27 are satisfied with $s = (t; \frac{q-1}{2}) = (t'; \frac{q-1}{2})$ and $t \neq t'$.

**Proof.** It is clear that the groups $\phi_t(G)$ and $\phi_{t'}(G)$ are isomorphic since both $\phi_t$ and $\phi_{t'}$ are homomorphisms with the same domain and kernel. The images in $\text{GL}(3, q)$ have different determinant sets so they cannot be conjugate. □
Corollary 6.3.29. Suppose that $k$ is odd and $k \mid (p^b - 1)$. Then $\text{PGL}(2, p^b) \times C_k$ has at least two non-conjugate isomorphic copies in $\text{GL}(3, p^a)$ for each $b \mid a$.

Proof. By Proposition 6.3.8, $\text{PGL}(2, p^b) \times C_k \cong \text{GL}(2, p^b)/C_{(p^b - 1)/k}$ for each odd $k \mid (p^b - 1)$. Since $k$ is odd, $\tilde{\phi}_2\left(\frac{p^b - 1}{k}\right) = \tilde{\phi}_2(p^b - 1)$. Thus, taking $(t, t') = \left(\frac{p^b - 1}{2k}, \frac{p^b - 1}{k}\right)$ and $q = p^b$ in Corollary 6.3.28, it follows that there are at least two non-conjugate isomorphic copies of $\text{PGL}(2, p^b) \times C_k$ in $\text{GL}(3, p^b)$. Since $b \mid a$, we can rewrite the subgroups, obtained by the homomorphisms over $\text{GL}(3, p^b)$, over $\text{GL}(3, p^a)$. \hfill $\Box$

Corollary 6.3.30. Suppose that $\det(G) = \langle \zeta_r \rangle$ for some even $r$ where $r \mid (q - 1)$, and define $\alpha_s$ and $\beta_{s,r}$ as in Lemma 6.3.27. Then the pairs $(\alpha_d, \beta_{d,r})$ are distinct for each $d \mid r$.

Proof. Take distinct divisors $d$ and $d'$ of $r$. Without loss of generality, we can assume $d' > d$. It follows by Lemma 6.3.27 that, when $d' > d$,

$$\ker \phi_{d'} = \ker \phi_d \Leftrightarrow \alpha_{d'} = \alpha_d \Leftrightarrow d' = 2d$$

in which case $\beta_{d', r} \neq \beta_{d, r}$. In all other cases $\alpha_{d'} \neq \alpha_d$. Therefore the result stands. \hfill $\Box$

Corollary 6.3.31. Let $G \leq \text{GL}(2, q)$. Suppose $\det(G) = \langle \zeta_r \rangle$ where $r$ is even and $r \mid (q - 1)$. For any divisors $d \neq d'$ of $r$, groups $\phi_d(G)$ and $\phi_{d'}(G)$ are non-conjugate in $\text{GL}(3, q)$.

Theorem 6.3.32. Let $\mathbb{F}$ be any field where $\text{char } \mathbb{F} \neq 2$. Suppose $O$ is an orthogonal subgroup of dimension $n$ in $\text{GL}(n, \mathbb{F})$. Then there are $\left\lceil \frac{n + 1}{2} \right\rceil$ conjugacy classes of groups isomorphic to $O$ in $\text{GL}(n, \mathbb{F})$.

Proof. The result follows by [28, Theorem 7, p. 8]. \hfill $\Box$

Lemma 6.3.33. Suppose that $k$ is odd, $p \neq 2$ and $k \mid (p^b - 1)$. Then $\text{PGL}(2, p^b) \times C_k$ has exactly two non-conjugate isomorphic copies in $\text{GL}(3, p^a)$ for each $b \mid a$.

Proof. Note that $\text{PGL}(2, p^b) \cong \text{SO}(3, p^b)$. The result then follows by Theorem 6.3.29 and the fact that $C_k$ is not contained in either copy. \hfill $\Box$

Remark 6.3.34. It is interesting to note that the mappings defined in (6.2) could be applied to matrix generating sets for subgroups of $\text{GL}(2, q)$ given in Chapter 3 in order to produce matrix generating sets for subgroups of $\text{GL}(3, q)$. A group $G \leq \text{GL}(3, q)$ obtained in this way corresponds to some $H \leq \text{GL}(2, q)$ in that $G \cong H/C_{2r}$ for some $r \in \mathbb{Z}^+$. In fact, having information about subgroups of $\text{GL}(2, q)$ allows us to determine some of the subgroups of $\text{GL}(3, q)$, e.g. knowledge of the irreducible insoluble subgroup $A^*_5$ (Schur cover of $\text{Alt}(5)$) of $\text{GL}(2, q)$ as given in Theorem 3.0.6 guarantees the existence of the irreducible insoluble subgroup $\text{Alt}(5)$ of $\text{GL}(3, q)$ — a result shown independent of this remark.
The case $3 \nmid (p^a - 1)$

**Theorem 6.3.35.** Let $3 \nmid (p^a - 1)$. The following are explicit representatives for each conjugacy class of subgroups of $GL(3, p^a)$ satisfying the hypothesis of Theorem 6.3.14.

(a) 

$$(i), (ii) \left\{ \left\langle \begin{pmatrix} -1 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}, \zeta_r \begin{pmatrix} \zeta_{(p^a-1)} & 0 & 0 \\ 0 & \zeta_{(p^a-1)}^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle \bigg| \begin{array}{l} b \mid a, \\ r \mid (p^a - 1) \end{array} \right\}$$

(b) When $p = 3$. Define $\beta_u = -(1 + \zeta_{(3^a+1)})^{-1}$.

$$(i), (ii) \left\{ \left\langle \begin{pmatrix} \beta_b & -1 & 1 \\ -1 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \zeta_r \begin{pmatrix} \zeta_{(3^a+1)} & 0 & 0 \\ 0 & \zeta_{(3^b+1)} & 0 \\ 0 & 0 & \zeta_{(3^a+1)}^{-3^b} \end{pmatrix} \right\rangle \bigg| \begin{array}{l} 2b \mid a, \\ r \mid (3^a - 1) \end{array} \right\}$$

(c) When $p \neq 2$:

$$(i), (ii) \left\{ \left\langle \begin{pmatrix} 1 & -2 & 2 \\ 1 & -1 & 0 \\ 2^{-1} & 0 & 0 \end{pmatrix}, \zeta_r \begin{pmatrix} \zeta_{(p^a-1)}^2 & 0 & 0 \\ 0 & \zeta_{(p^a-1)} & 0 \\ 0 & 0 & \zeta_{(p^a-1)}^{-1} \end{pmatrix} \right\rangle \bigg| \begin{array}{l} b \mid a, \\ p^b \neq 3, \\ r \mid (p^a - 1) \end{array} \right\}$$

(c#) When $p \neq 2$:

$$(i) \left\{ \left\langle \zeta_r \begin{pmatrix} 1 & -2 & 2 \\ 1 & -1 & 0 \\ 2^{-1} & 0 & 0 \end{pmatrix}, \delta \begin{pmatrix} \zeta_{(p^a-1)} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \zeta_{(p^a-1)}^{-1} \end{pmatrix} \right\rangle \bigg| \begin{array}{l} b \mid a, p^b \neq 3, \\ r \mid (p^a - 1), \delta \in \langle (-1)^r \rangle \end{array} \right\}$$

When $4 \mid (p^b - 1)$:

$$(L-ii), (L-iii) \left\{ \zeta, \begin{pmatrix} 1 & -2 & 2 \\ 1 & -1 & 0 \\ 2^{-1} & 0 & 0 \end{pmatrix}, \zeta_2 \begin{pmatrix} \zeta_{(p^a-1)}^r & 0 & 0 \\ 0 & \zeta_{(p^a-1)} & 0 \\ 0 & 0 & \zeta_{(p^a-1)}^{-r} \end{pmatrix} \right\}, \text{ where } \mathcal{W}^- = \{ \hat{\delta}_2((p^b - 1) + 1, \ldots, \hat{\delta}_2((p^a - 1)) \}.$$

When $4 \mid (p^b + 1)$:

$$(U-ii), (U-iii) \left\{ \zeta, \begin{pmatrix} 1 & -2(\zeta_{(p^a-1)/2})^r & 2\zeta_{(p^a-1)} \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \zeta_2 \begin{pmatrix} \zeta_{(p^a-1)}^r & 0 & 0 \\ 0 & \zeta_{(p^a-1)} & 0 \\ 0 & 0 & \zeta_{(p^a-1)}^{-2^b} \end{pmatrix} \right\}, \text{ where } \mathcal{W}^+ = \{ \hat{\delta}_2((p^b + 1) + 1, \ldots, \hat{\delta}_2((p^a - 1)) \}.$$
6.3. THE MODULAR LISTS FOR $\text{SL}(3,p^a)$ AND $\text{GL}(3,p^a)$

(d) When $p = 3$ and $2 | a$:

\[
\begin{align*}
(i) & \left\{ \zeta_r \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \zeta_8 & \zeta_8^3 \\ \zeta_8 & \zeta_8^3 & 1 \\ \zeta_8^3 & 1 & \zeta_8 \end{pmatrix} \right\} & r & | (3^a - 1) \\
(ii) & \left\{ \zeta_r \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} -1 & \zeta_8^{-1} & 0 \\ 0 & 1 & 0 \\ 0 & \zeta_8^3 & -1 \end{pmatrix} \right\} & r & | (3^a - 1)
\end{align*}
\]

**Proof.** To prove that the lists of matrix generating sets are correct, the first step is to show that each matrix group (given by a set of matrix generators) is isomorphic to (or in some cases the same as) one and only one of the abstract groups as given in Theorem 6.3.14. (In this proof, “abstract group” refers to a group listed in Theorem 6.3.14.) The next step is to show that all conjugacy classes are represented and that distinct matrix generating sets are non-conjugate to each other.

For families (a) and (b), we use the known Steinberg generators, as outlined in Taylor’s article [34], of the groups $\text{SL}(3,p^b)$, $\text{GL}(3,p^b)$, $\text{SU}(3,p^b)$ and $\text{GU}(3,p^b)$. In each case, these are modified by multiplying the diagonal Steinberg generator by an appropriate scalar. The matrix groups so obtained are precisely the same as the abstract groups. Lemmas 6.3.23 and 6.3.24 ensure there is only one conjugacy class for families (a) and (b).

We derive matrix generators for (c) and (c') by first taking the Steinberg generators of the groups $\text{SL}(2,p^b)$, $\text{GL}(2,p^b)$ and $\text{GU}(2,p^b)$. Then we apply the mappings $\{\phi_k\}_{k=1}^{p^b-1}$ as in Lemma 6.3.25 for relevant values of $k$ in order to produce groups isomorphic to those of (c) and subfamilies (i), (L-ii) & (U-ii) in (c') of Theorem 6.3.14 which do not contain a split extension by a non-trivial cyclic group (i.e. $r = 1$ in (c),(c') (i) and $t = 1$ in (L-ii),(U-ii)). We adjoin the appropriate scalar to the non-diagonal matrix generator in order to form the split extensions by non-trivial cyclic groups. Due to Lemma 6.3.25(ii), these are isomorphisms of the relevant abstract groups.

For the covering groups in (L-iii) and (U-iii), we take the generators from (L-ii) and (U-ii) respectively; then we adjoin an appropriate scalar to the diagonal matrix generator, and finally recombine the generators to form the matrix group. In a similar way to the previous paragraph, we have isomorphisms between these and the abstract groups given.

Each odd value of $r$ in (c') (i) gives rise to two options $\pm 1$ for $\delta$. These options for $\delta$ correspond to the two non-conjugate isomorphic copies as specified in Lemma 6.3.33.

For (d)(i), generators are lifted from equation (5.2.10). (d)(ii) is lifted directly from Lemma 5.2.12. As per Section 5.2.2, there is only one conjugacy class for groups in (d). □
6.3. THE MODULAR LISTS FOR $\text{SL}(3, p^a)$ AND $\text{GL}(3, p^a)$

The case $3 \mid (p^a - 1)$

**Theorem 6.3.36.** Let $3 \mid (p^a - 1)$. The following are explicit representatives for each conjugacy class of subgroups of $\text{GL}(3, p^a)$ satisfying the hypothesis of Theorem 6.3.22. The symbol $\downarrow$ indicates that the generating sets are exactly the same as the corresponding family or subfamily (as a function of variables $p$ and $a$) as in Theorem 6.3.35.

(a) 

(i), (ii),

$$(i),(ii), \left\{ \begin{pmatrix} -1 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}, \zeta_r \begin{pmatrix} \zeta_{(p^a-1)} & 0 & 0 \\ 0 & \zeta_{(p^a-1)}^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\} \mid b \mid a, \ r \mid (p^a - 1), \ \{\hat{d}_3(r) \neq 1 \text{ or } 3 \mid (p^b - 1)\}$$

(a) Define $\tilde{b} = \hat{d}_3((p^b - 1))$ and $\mathcal{T}_\tilde{b} = [(\tilde{b} + 1), \ldots, \hat{d}_3((p^a - 1))]$.

(i) 

$$(i) \left\{ \begin{pmatrix} -1 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}, \begin{pmatrix} \zeta_{(p^a-1)} & 0 & 0 \\ 0 & \zeta_{(p^a-1)}^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \zeta_r \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \zeta_r^{-1} \end{pmatrix}, \left[ \zeta_r I \right] \right\} \mid b \mid a, \ \{\hat{d}_3(r) \neq 1 \text{ or } 3 \mid (p^b - 1)\}$$

(b) Define $\beta_a = - (1 + \zeta_{(p^a+1)})^{-1}$.

(b) 

(i), (ii), 

$$(i), (ii), \left\{ \begin{pmatrix} \beta_b & -1 & 1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \zeta_r \begin{pmatrix} \zeta_{(p^b-1)} & 0 & 0 \\ 0 & \zeta_{(p^b-1)}^{-1} & 0 \\ 0 & 0 & \zeta_{(p^b-1)} \end{pmatrix} \right\} \mid 2b \mid a, \ r \mid (p^a - 1), \ \{\hat{d}_3(r) \neq 1 \text{ or } 3 \mid (p^b + 1)\}$$

(b) Define $\tilde{b} = \hat{d}_3((p^b + 1))$ and $\mathcal{T}_\tilde{b} = [(\tilde{b} + 1), \ldots, \hat{d}_3((p^a - 1))]$.

(i) 

$$(i) \left\{ \begin{pmatrix} \beta_b & -1 & 1 \\ -1 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \zeta_r \begin{pmatrix} \zeta_{(p^b-1)} & 0 & 0 \\ 0 & \zeta_{(p^b-1)}^{-1} & 0 \\ 0 & 0 & \zeta_{(p^b-1)} \end{pmatrix}, \zeta_r \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta_r^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \left[ \zeta_r I \right] \right\} \mid 2b \mid a, \ \{\hat{d}_3(r) \neq 1 \text{ or } 3 \mid (p^b + 1)\}$$

(b)
6.3. THE MODULAR LISTS FOR $\text{SL}(3, p^a)$ AND $\text{GL}(3, p^a)$

(ii) \[
\begin{cases}
\begin{pmatrix}
\beta_0 & -1 & 1 \\
-1 & -1 & 0 \\
1 & 0 & 0
\end{pmatrix}, \\
\begin{pmatrix}
\zeta_{(p^{2b-1})} & 0 & 0 \\
0 & \zeta_{(p^{b+1})} & 0 \\
0 & 0 & \zeta_{(p^{2b-1})}^{\beta_0}
\end{pmatrix}, \\
\begin{pmatrix}
\zeta_{(3^{b+1})} & 0 & 0 \\
0 & \zeta_{(3^{b+1})}^{-2} & 0 \\
0 & 0 & \zeta_{(3^{b+1})}^{-\beta_0}
\end{pmatrix}, \\
\begin{pmatrix}
1 & 0 & 0 \\
0 & \zeta_{(3^{b+1})}^{-1} & 0 \\
0 & 0 & 1
\end{pmatrix}, \\
\begin{pmatrix}
\beta_0 & -1 & 1 \\
-1 & -1 & 0 \\
1 & 0 & 0
\end{pmatrix},
\end{cases}
\]

(iii) \[
\begin{cases}
\begin{pmatrix}
\beta_0 & 1 & 1 \\
-1 & -1 & 1 \\
1 & 0 & 0
\end{pmatrix}, \\
\begin{pmatrix}
\zeta_{(p^{2b-1})} & 0 & 0 \\
0 & \zeta_{(p^{b+1})} & 0 \\
0 & 0 & \zeta_{(p^{2b-1})}^{\beta_0}
\end{pmatrix}, \\
\begin{pmatrix}
\zeta_{(3^{b+1})} & 0 & 0 \\
0 & \zeta_{(3^{b+1})}^{-1} & 0 \\
0 & 0 & \zeta_{(3^{b+1})}^{-\beta_0}
\end{pmatrix}, \\
\begin{pmatrix}
\zeta_{(3^{b+1})} & 0 & 0 \\
0 & \zeta_{(3^{b+1})}^{-1} & 0 \\
0 & 0 & \zeta_{(3^{b+1})}^{-\beta_0}
\end{pmatrix},
\end{cases}
\]

(iv) \[
\begin{cases}
\begin{pmatrix}
\beta_0 & -1 & 1 \\
-1 & -1 & 0 \\
1 & 0 & 0
\end{pmatrix}, \\
\begin{pmatrix}
\zeta_{(p^{2b-1})} & 0 & 0 \\
0 & 0 & \zeta_{(p^{2b-1})}^{-\beta_0}
\end{pmatrix}, \\
\begin{pmatrix}
\zeta_{(3^{b+1})} & 0 & 0 \\
0 & \zeta_{(3^{b+1})}^{-1} & 0 \\
0 & 0 & \zeta_{(3^{b+1})}^{-\beta_0}
\end{pmatrix},
\end{cases}
\]

\( r | (p^a - 1), \) \( \hat{\delta}_3(r) \neq 1 \)

Proof. A similar approach is required as in Theorem 6.3.35 and cases (a), (b), (c) & (c\#) are covered in the proof of that theorem.

The additional matrix generators in families \((a^+)^+\) and \((b^+)\) (not appearing in Theorem 6.3.35) follow by a combination of Corollaries 6.2.18 and 6.2.19 together with the equalities:

\[
\text{GL}(3, p^b) = \langle \text{SL}(3, p^b), (p^b - 1)I, \text{diag}(1, 1, \zeta_{3^b}) \rangle \text{ when } 3 | (p^b - 1); \text{ and }
\]

\[
\text{GU}(3, p^b) = \langle \text{SU}(3, p^b), (p^b + 1)I, \text{diag}(1, \zeta_{3^b}, 1) \rangle \text{ when } 3 | (p^b + 1), 2b | a;
\]
where \( \delta = \hat{o}_3(p^b - 1) \) and \( \hat{b} = \hat{o}_3(p^b + 1) \). There is only one conjugacy class as a result of Corollary 6.2.19 for these families.

It can be directly verified, that the groups of (e) and (f) in the case \( r = 1 \) are isomorphic to the corresponding abstract groups. (We used Magma to verify this direct correspondence for this finite set of groups.) The correspondence via isomorphism to the abstract groups for the infinite set of groups resulting from the addition of scalars follows trivially.

The generators in parts (e) and (f)(i) are lifted from Lemma 5.2.11. Those of (f)(ii) follow from those of (f)(i). Those of (f)(iii) and (iv) were suggested by a similar set of generators in Bloom [3, pp. 173f.]. The two options for \( \delta \) correspond to two non-conjugate isomorphic copies of the same group.
Chapter 7

Finite linear groups over integral domains of characteristic zero

For the entirety of this chapter, \( m \in \{2, 3\} \), \( n \in \mathbb{Z}^+ \) and \( \mathbb{K} \) is a real field (i.e. a subfield of \( \mathbb{R} \)). We denote by \( \mathbb{F}' \) some non-trivial extension of a given field \( \mathbb{F} \).

We are concerned with listing, completely and irredundantly, the irreducible subgroups of \( \text{GL}(m, \mathbb{F}) \) up to conjugacy for certain fields \( \mathbb{F} \subseteq \mathbb{C} \). In the case where \( \mathbb{F} \) is an algebraic number field, we also concern ourselves with such subgroups of \( \text{GL}(m, \mathbb{O}_\mathbb{F}) \) up to conjugacy; here \( \mathbb{O}_\mathbb{F} \) denotes the ring of integers of \( \mathbb{F} \).

Some of these classifications are already well-known (e.g. see [27, pp. 179-181], [33]). However, we present an independent derivation that applies some of the methods and classifications already explored in earlier chapters. Furthermore, we present some of the results in a more general form applicable to other degrees.

We emphasise the following two points:

- a group that is irreducible over \( \mathbb{F} \) may be reducible over \( \mathbb{C} \);
- a group that is primitive over \( \mathbb{F} \) may be monomial over \( \mathbb{F} \).

Also, we stress that there is a notable difference in the listing problem in degree 2 compared to that in larger degrees.

We use our lists of the finite non-abelian (irreducible) subgroups of \( \text{GL}(m, \mathbb{C}) \) as a starting point. Subsequently, we derive the subgroups of \( \text{GL}(m, \mathbb{K}) \) and then consider the subgroups of \( \text{GL}(m, \mathbb{O}_\mathbb{K}) \). Finally, we move on to listing matrix groups of degree 2 and 3 over cyclotomic and quadratic extensions of these fields and rings.
7.1 Preliminaries

Theorem 7.1.1. For each positive integer \( k \), GL\((2k, \mathbb{Q})\) has an element of order \( r \) if and only if GL\((2k + 1, \mathbb{Q})\) has.

Proof. See [22]. \( \square \)

By Theorem 7.1.1, given any odd \( n \), to determine the possible orders of finite subgroups of GL\((n, \mathbb{Q})\), it suffices to determine the orders of elements in GL\((n - 1, \mathbb{Q})\).

Theorem 7.1.2. Suppose \( g \in \text{GL}(n, \mathbb{Q}) \) has finite order \( t \) and let \( \mathcal{Y} \) be the set of prime powers \( \{p^r : p^r \mid t, p^r + 1 \notmid t\} \). Then \( \sum_{q \in \mathcal{Y} \setminus \{2\}} \varphi(q) \leq n. \)

Proof. Let the characteristic polynomial of \( g \) be
\[
\chi(\lambda) = \lambda^n + \alpha_{n-1}\lambda^{n-1} + \cdots + \alpha_0,
\]
where \( \alpha_0, \ldots, \alpha_{n-1} \in \mathbb{Z} \). We have that
\[
g^t - I_n = \prod_{d \mid t} \Phi_d(g) = 0_{n \times n},
\]
where \( \Phi_d(x) \) is the \( d \)th cyclotomic polynomial. Since \( \chi(g) = 0_{n \times n} \), there exist \( d_i \) dividing \( t \) such that \( \Phi_{d_i}(\lambda) \) is a factor of \( \chi(\lambda) \). So \( |g| = t \) implies all \( d_i \) divide \( t \) and \( \forall q \in \mathcal{Y}, \exists d_i \) such that \( q \mid d_i \). Given any \( \ell, a \in \mathbb{Z}^+ \), we have \( \varphi(\ell a) \geq \varphi(\ell)\varphi(a) \). Combining this with the restrictions found for the \( d_i \), means that \( n \geq \min \left( \{ \sum \varphi(\prod_{y \in \mathcal{Y}_i} y) : \bigcup_i \mathcal{Y}_i = \mathcal{Y}, \bigcap_i \mathcal{Y}_i = \emptyset \} \right) \).

Now, \( \varphi(\ell a) \geq \varphi(a) \) with equality \( \Leftrightarrow \ell = 1 \) or \((\ell = 2 \text{ and } 2 \nmid a) \). Since \( \varphi(1) = \varphi(2) = 1 \), then \( \varphi(\ell) + \varphi(a) > \varphi(\ell)\varphi(a) \Leftrightarrow \) at least one of \( \ell \) or \( a \leq 2 \). Incorporating these facts gives
\[
\min \left( \{ \sum \varphi(\prod_{y \in \mathcal{Y}_i} y) : \bigcup_i \mathcal{Y}_i = \mathcal{Y}, \bigcap_i \mathcal{Y}_i = \emptyset \} \right) = \sum_{q \in \mathcal{Y} \setminus \{2\}} \varphi(q) \leq n \text{ as required.} \quad \square
\]

Companion Matrix

Recall that the companion matrix of
\[
f(x) = x^k + \alpha_{k-1}x^{k-1} + \cdots + \alpha_1x + \alpha_0 \in \mathbb{F}[x]
\]
is
\[
\begin{pmatrix}
0 & 0 & 0 & \cdots & -\alpha_0 \\
1 & 0 & 0 & \cdots & -\alpha_1 \\
0 & 1 & 0 & \cdots & -\alpha_2 \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & \cdots & \cdots \\
0 & 0 & 0 & \cdots & -\alpha_{k-1}
\end{pmatrix}
\quad (7.2)
\]
7.2. SUBGROUPS OF THE GENERAL LINEAR GROUP OF DEGREES 2 AND 3 OVER A REAL FIELD

Frobenius-Schur Indicator Function

The Frobenius Schur (F-S) indicator function is usually defined on the set of complex irreducible characters of a given finite group. However, for our purposes, we restrict attention to the trace map ‘tr’ on a finite irreducible subgroup of $\text{GL}(n, \mathbb{C})$.

Let $G$ be the set of all finite irreducible subgroups of $\text{GL}(n, \mathbb{C})$. We define the F-S indicator function as:

$$\iota : G \to \{0, \pm 1\} \text{ where } G \mapsto \frac{1}{|G|} \sum_{g \in G} \text{tr}(g^2).$$  \hfill (7.3)

As is well-known (see e.g. [17, p. 58]):

- if $\iota(G) = 1$, then $\text{tr}(G) \subset \mathbb{R}$ and $G^x \leq \text{GL}(n, \mathbb{R})$ for some $x \in \text{GL}(n, \mathbb{C})$;
- if $\iota(G) = 0$, then $\text{tr}(G) \not\subset \mathbb{R}$;
- if $\iota(G) = -1$, then $\text{tr}(G) \subset \mathbb{R}$ but $\forall x \in \text{GL}(n, \mathbb{C}), G^x \not\leq \text{GL}(n, \mathbb{R})$.

We refer to $\iota(G)$ as the F-S indicator value of $G$.

7.2 Subgroups of the general linear group of degrees 2 and 3 over a real field

Let $E$ be a subfield of $F$. We say a subgroup or element of $\text{GL}(n, F)$ is realisable over $E$ if it can be conjugated over $\text{GL}(n, F)$ into $\text{GL}(n, E)$.

7.2.1 Subgroups of $\text{GL}(2, \mathbb{K})$

**Theorem 7.2.1.** Let $G$ be a finite irreducible subgroup of $\text{GL}(2, \mathbb{K})$. Then $G$ is monomial over $\mathbb{C}$. Moreover $G$ is soluble and either:

(i) cyclic of order $\geq 3$, or

(ii) dihedral.

**Proof.** We refer to the subgroups of $\text{GL}(2, \mathbb{C})$ given in Theorem 3.0.13 and determine which are relevant here.

Suppose $G \leq \text{GL}(2, \mathbb{C})$ is abelian and hence cyclic. If $|G| \leq 2$, then $G$ is clearly reducible in $\text{GL}(2, \mathbb{K})$. Hence, $G = \langle A \rangle$ has order $s \geq 3$ and at least one of the eigenvalues of $A$ is non-real. The characteristic polynomial of a matrix conjugate to $A$ is of the form

$$x^2 - (\alpha + \beta)x + \alpha\beta = 0,$$  \hfill (7.4)

*here we abuse standard notation and write $\iota(G)$ for the value of $\iota$ on tr
7.2. SUBGROUPS OF THE GENERAL LINEAR GROUP OF DEGREES 2 AND 3 OVER A REAL FIELD

for some indeterminate \( x \) with \( \alpha, \beta \) both \( s^{\text{th}} \) roots of unity. By Eq.(7.4), if \( A \) has real entries, then \( \beta = \bar{\alpha} \). We can thus take \( A \) to be the companion matrix in Eq.(7.2) of the characteristic polynomial in Eq.(7.4). Since both eigenvalues of \( A \) are non-real, \( G \) is irreducible over \( \mathbb{K} \).

Now suppose \( G \) is non-abelian, and hence absolutely irreducible. If \( G \) is primitive then it must be conjugate to one of the groups in Theorem 3.0.12. However, it is readily verified that the F-S indicator value is \(-1\) for each of these groups. Therefore \( G \) can only be monomial over \( \mathbb{C} \). \( \square \)

Theorem 7.2.2. Define \( S = \{ s \in \mathbb{Z} \mid s \geq 3, \cos(2\pi/s) \in \mathbb{K} \} \). The following is a complete and irredundant list of \( \text{GL}(2, \mathbb{K}) \)-conjugacy class representatives of the finite irreducible subgroups of \( \text{GL}(2, \mathbb{K}) \):

\[
(i) \quad \left\{ \begin{pmatrix} 0 & -1 \\ 1 & 2\cos(\frac{2\pi}{s}) \end{pmatrix} \right\} \cong C_s \quad s \in S
\]

\[
(ii) \quad \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 2\cos(\frac{2\pi}{s}) \end{pmatrix} \right\} \cong D_{2s} \quad s \in S
\]

Proof. We examine the possible subgroups arising from Theorem 7.2.1. Matrix generating sets in (i) follow by taking the relevant companion matrix (in this case also the rational canonical form) as the single matrix generator, as was described in the proof for (i) of Theorem 7.2.1.

For groups in (ii), we refer to Theorem 3.0.11 and, as usual, rely on Lemma 2.5.3. Excluding possibilities that return a F-S indicator value of 0 or \(-1\), we are left with just the groups in Theorem 3.0.11 (i) with \( r = 1 \). Conjugation of such a group by

\[
J = \begin{pmatrix} 1 & \zeta_s \\ \zeta_s & 1 \end{pmatrix}
\]

gives us the set of groups in (ii). \( \square \)

We state a few consequences of Theorem 7.2.2.

Corollary 7.2.3. A finite non-abelian irreducible subgroup of \( \text{GL}(2, \mathbb{K}) \) is primitive over \( \mathbb{K} \) if and only if its order does not divide 8.

Corollary 7.2.4. There always exist abelian finite irreducible monomial subgroups of \( \text{GL}(2, \mathbb{K}) \), and these form a single conjugacy class, of cyclic groups of order 4, in \( \text{GL}(2, \mathbb{K}) \).

Corollary 7.2.5. (i) Two finite irreducible subgroups of \( \text{GL}(2, \mathbb{K}) \) are isomorphic if and only if they are conjugate. (ii) A finite subgroup of \( \text{SL}(2, \mathbb{K}) \) is cyclic.
Corollary 7.2.6. For each \( s \geq 3 \), \( C_s \) and \( D_{2s} \) have faithful irreducible representations in \( \text{GL}(2, \mathbb{R}) \).

Corollary 7.2.7. The six groups arising from \( s \in \{3, 4, 6\} \) in Theorem 7.2.2 constitute a complete and irredundant list of \( \text{GL}(2, \mathbb{Q}) \)-conjugacy class representatives of the finite irreducible subgroups of \( \text{GL}(2, \mathbb{Q}) \).

Proof. The only \( s \geq 3 \) such that \( \cos(2\pi/s) \) is rational are \( s = 3, 4 \) or 6. \( \square \)

7.2.2 Subgroups of \( \text{GL}(3, \mathbb{K}) \)

Lemma 7.2.8. Let \( G \) be a finite irreducible subgroup of \( \text{GL}(2, \mathbb{C}) \) such that \( \det(G) \subseteq \{\pm 1\} \), \( \iota(G) \neq 0 \) and \( Z := Z(G) \) is non-trivial. Then there is a finite subgroup of \( \text{GL}(3, \mathbb{R}) \) isomorphic to \( G/Z \).

Proof. Recall the mapping \( \phi_1 : \text{GL}(2, \mathbb{F}) \rightarrow \text{GL}(3, \mathbb{F}) \) as in (6.2) given for any field \( \mathbb{F} \). For \( G \leq \text{GL}(2, \mathbb{C}) \), we have that \( \phi_1(G) \cong G/Z \). For all \( g \in G \),

\[
\text{tr} (\phi_1(g)) = \text{tr}^2(g) - \det(g). \tag{7.5}
\]

Since \( \det(g^2) = 1 \ \forall g \in G \), it then follows by Eqs. (7.3) and (7.5) that

\[
\iota(G) = \frac{1}{|G|} \sum_{g \in G} \left( \text{tr}^2(g^2) - 1 \right) = \left[ \frac{1}{|G|} \sum_{g \in G} \text{tr}^2(g^2) \right] - 1.
\]

Clearly, any finite subgroup of \( G \leq \text{GL}(2, \mathbb{C}) \) is completely reducible and so its elements are diagonalisable. Thus \( g \) can be conjugated to \( \text{diag}(\alpha, \pm \alpha^{-1}) \) where \( \alpha \) is some root of unity. Now, take any \( g \neq 1_G \). We find that

\[
\sum_{k=1}^{\lfloor |g|/2 \rfloor} \text{tr}(g^{2k}) = \begin{cases} 2, & \text{if } |g| = 2, \\ -2, & \text{otherwise}. \end{cases}
\]

Since \( (\alpha^2 \pm \alpha^{-2})^2 = \alpha^4 + \alpha^{-4} + 2 \), we get that

\[
\sum_{k=1}^{\lfloor |g|/2 \rfloor} \text{tr}^2(g^{2k}) = \begin{cases} 4, & \text{if } |g| = 2, \\ 12, & \text{if } |g| = 4 \text{ or } 8, \\ 2(|g| - 2), & \text{otherwise}. \end{cases}
\]

Let \( t = \frac{1}{|G|} \sum_{g \in G} \text{tr}^2(g^2) \). The fact \( \iota(G) \in \{0, \pm 1\} \) means that \( t \in \{0, 1, 2\} \). For all \( g \), we have \( \sum_{k=1}^{\lfloor |g|/2 \rfloor} \text{tr}^2(g^{2k}) \geq \sum_{k=1}^{\lfloor |g|/2 \rfloor} \text{tr}(g^{2k}) \). Also \( \text{tr}^2(1_G) = 4 \). It follows that \( t > |\iota(G)| \). Hence \( t \neq 0 \) and if \( \iota(G) = \pm 1 \) then \( t = 2 \). The latter case implies \( \iota(G) = 1 \) and therefore there is an isomorphic copy of \( G/Z \) realisable over \( \mathbb{R} \) as claimed. \( \square \)

\[\text{Here, we use } \text{tr}^2(g) \text{ synonymously with } (\text{tr}(g))^2.\]
7.2. SUBGROUPS OF THE GENERAL LINEAR GROUP OF DEGREES 2 AND 3
OVER A REAL FIELD

Soluble subgroups

This case has been studied previously by several authors. The following description of the
groups was provided separately by Dixon and Suprunenko.

**Theorem 7.2.9** ([6, Theorem 1],[31]). Let \( G \) be a finite soluble irreducible subgroup of
\( \text{GL}(n, \mathbb{K}) \) where \( n \) is an odd integer. Then \( G \) is absolutely irreducible and \( G \) is conjugate
in \( \text{GL}(n, \mathbb{K}) \) to a group of monomial matrices all of whose non-zero entries are \( \pm 1 \).

Theorem 7.2.9 is a powerful result in that it simplifies our task in this section. We point
out that [6] contains an error but this is unrelated to the validity of Theorem 7.2.9.

**Theorem 7.2.10.** Let \( G \) be a finite irreducible soluble subgroup of \( \text{GL}(3, \mathbb{K}) \). Then \( G \) is
isomorphic to one and only one of: \( \text{Alt}(4) \), \( \text{Alt}(4) \times C_2 \), \( \text{Sym}(4) \) or \( \text{Sym}(4) \times C_2 \).

**Proof.** By Theorem 7.2.9, we need only take monomial groups into account. Hence, it
suffices to consider only subgroups of \( C_3^2 \rtimes \text{Sym}(3) \) for \( \text{GL}(3, \mathbb{K}) \). For \( \text{SL}(3, \mathbb{K}) \) only subgroups
of \( C_3^2 \rtimes \text{Sym}(3) \) apply. The order of such a subgroup is thus at most 48.

Due to Lemma 2.6.3 (i), the irreducible finite subgroups of \( \text{GL}(3, \mathbb{K}) \) are also irreducible
in \( \text{GL}(3, \mathbb{C}) \). Let \( H \) be any reducible finite monomial subgroup of \( \text{GL}(3, \mathbb{C}) \). Then we have
a faithful representation \( \hat{H} \) in \( \text{GL}(2, \mathbb{C}) \). By Theorem 7.2.1, \( \hat{H} \) can be conjugated into a
irreducible subgroup of \( \text{GL}(2, \mathbb{R}) \). It follows that any finite monomial reducible subgroup
of \( \text{GL}(3, \mathbb{C}) \) is also reducible in \( \text{GL}(3, \mathbb{K}) \). In conjunction with Theorem 7.2.9, this means
that we do not need to consider any finite reducible subgroups of \( \text{GL}(3, \mathbb{C}) \) as possibilities.

By applying the map \( \phi_1 \) as in (6.2) to the relevant groups in Theorems 3.0.11 and 3.0.12,
we can determine a list of finite soluble subgroups of \( \text{SL}(3, \mathbb{K}) \). We first examine Theorem
3.0.6 which is a precursor to Theorems 3.0.11 and 3.0.12. Subgroups of (i) are abelian
so clearly reducible. The set of core groups \( \{ \text{Alt}(4), \text{Sym}(4) \} \) occur due to cases (iii) and
(iv) and are clearly relevant by Lemma 7.2.8. The only possible double covers of these in
\( \text{GL}(3, \mathbb{K}) \) are split.

All cases from Theorem 3.0.11 are irrelevant because we would require \( r, s \in \{1, 2, 4\} \).
Even when these conditions are satisfied, none of the resultant groups from the map \( \phi_1 \) has
3 dividing its order and so are all reducible in \( \text{GL}(3, \mathbb{K}) \).

A careful examination of [11, Theorem 6.15] (taking Theorem 7.2.9 into account) ensures
that there are no other subgroups of \( \text{GL}(3, \mathbb{K}) \) apart from those already stated. □
Insoluble subgroups

Theorem 7.2.11. If $\sqrt{5} \in \mathbb{K}$, then the complete set of irreducible insoluble finite subgroups of $\text{GL}(3, \mathbb{K})$ is $\{A_5, A_5 \times C_2\}$ where $A_5 \cong \text{Alt}(5)$; otherwise, $\text{GL}(3, \mathbb{K})$ has no irreducible insoluble subgroups.

Proof. By application of the F-S indicator function to the core matrix generating sets presented in Lemmas 5.2.10–5.2.12, we see that there is an isomorphic copy of $\text{Alt}(5)$ in $\text{GL}(3, \mathbb{R})$ but $\text{GL}(3, \mathbb{R})$ has no subgroups isomorphic to either $3\text{Alt}(6)$ or $\text{PSL}(2, 7)$. A simple character table argument shows that $\sqrt{5} \in \mathbb{K}$ in order that $A_5 \leq \text{GL}(3, \mathbb{K})$. Also $A_5 \times C_2$ appears. \[\square\]

Matrix generating sets of all irreducible subgroups of $\text{GL}(3, \mathbb{K})$

Theorem 7.2.12. Let $G$ be an irreducible finite subgroup of $\text{GL}(3, \mathbb{K})$. Then $G$ is conjugate in $\text{GL}(3, \mathbb{K})$ to one and only one of the following groups:

(i) $\{A_4, A_4 \times C_2\} : \left\{ \pm \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \right\}$

(ii) $\{S_4, S_4 \times C_2\} : \left\{ \begin{pmatrix} \delta & 0 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}, \delta^* \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \right\} | (\delta, \delta^*) \in \{(1, 1), (1, -1), (-1, 1)\}$

When $\sqrt{5} \in \mathbb{K}$:

(iii) $\{A_5, A_5 \times C_2\} : \left\{ \pm \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}, \frac{1}{2} \begin{pmatrix} \mu_2 & \mu_1 & -1 \\ \mu_1 & -1 & \mu_2 \\ -1 & \mu_2 & \mu_1 \end{pmatrix} \right\}$

where $\mu_1 = \frac{1}{2}(-1 + \sqrt{5})$ and $\mu_2 = -\frac{1}{2}(1 + \sqrt{5})$.

Proof. It is a straightforward exercise to verify that each generating set defines the appropriate group. However, we outline a derivation here of the generators using earlier results and in doing so prove the theorem. The matrix generators are found by first taking the matrix generators from Theorem 3.0.6 of $A_4^*$ in (iii), $S_4^*$ in (iv) and $A_5^*$ in (v). One then applies the map $\phi_1$ to these and proceeds by applying the conjugating matrix

$$
\begin{pmatrix}
1 & 0 & -i \\
0 & -1 & 0 \\
-\frac{1}{2} & 0 & -\frac{i}{2}
\end{pmatrix}
$$
to the individual generators. For $A_5^*$, we multiply the initial two resultant matrix generators to get a single generator; this results in a smaller number of generators while still representing the same group. The scalar $-1$ is multiplied by the non-trivial permutation matrix to provide generators for the corresponding split extension by $C_2$. For (ii), there is a non-conjugate copy of $S_4$, corresponding to $\delta^* = -1$. □

**Corollary 7.2.13.** Let $G$ be an irreducible finite subgroup of $\text{GL}(3, \mathbb{Q})$. Then $G$ is conjugate in $\text{GL}(3, \mathbb{Q})$ to one and only one of the groups in (i) or (ii) of Theorem 7.2.12.

### 7.2.3 Subgroups of $\text{GL}(m, \mathbb{Z})$

**Theorem 7.2.14** (Minkowski [22, Thm 1.4, p. 174]). If $G$ is a finite subgroup of $\text{GL}(n, \mathbb{Z})$, then $G$ is isomorphic to a subgroup of $\text{GL}(n, \mathbb{Z}_p)$ for all primes $p \neq 2$. In particular, $\text{GL}(n, \mathbb{Z})$ contains, up to isomorphism, only finitely many finite subgroups.

**Theorem 7.2.15** ([22, Thm 1.6, p. 175]). If $G$ is a finite subgroup of $\text{GL}(n, \mathbb{Q})$, then $G$ is conjugate to a subgroup of $\text{GL}(n, \mathbb{Z})$.

By Theorem 7.2.15, we see that the list of isomorphism types of finite subgroups of $\text{GL}(n, \mathbb{Z})$ and $\text{GL}(n, \mathbb{Q})$ are identical. However, it is important to bear in mind that two groups which are conjugate to each other in $\text{GL}(n, \mathbb{Q})$ are not necessarily conjugate in $\text{GL}(n, \mathbb{Z})$.

**Theorem 7.2.16.** Let $G$ be an irreducible finite subgroup of $\text{GL}(n, \mathbb{Q})$ and $n \geq 3$ be odd. Then, up to conjugacy in $\text{GL}(n, \mathbb{Z})$, there are exactly $\left\lceil \frac{n^2 + 2n - 4}{4} \right\rceil$ non-conjugate copies of $G$ realisable over $\mathbb{Z}$ which are all conjugate to each other in $\text{GL}(n, \mathbb{Q})$.

**Proof.** By Theorem 7.2.9 and Lemma 2.6.5, we can always choose a conjugation such that one of the original generators is invariant under this conjugating matrix. Hence, up to conjugacy and scalar multiplication in $\text{GL}(n, \mathbb{Q})$, we can restrict our search to consider only the set of all circulant matrices in $\text{GL}(n, \mathbb{Q})$ where each entry is in $\mathcal{K} = \{0, \pm 1\}$. Thus, our problem breaks down to determining, up to permutation and scalar multiplication, the number of possible combinations of elements in $\mathcal{K}$ in a row of length $n$ which give rise to a circulant matrix with non-zero determinant.

Let $n_k$ represent the number of $k$ amongst $n$ items, where $k \in \mathcal{K}$. By a well-known counting formula, the number of possible solutions to

\[ n_0 + n_1 + n_{-1} = n \quad \text{is} \quad \binom{n + 2}{2}. \quad (7.6) \]
Now, we exclude such combinations when \( n_1 = n_{-1} \) as these give rise to matrices of determinant zero. This is equivalent to finding the number of solutions to

\[
n_0 + 2n_{\pm 1} = n \quad \text{which is} \quad \left\lceil \frac{n + 2}{2} \right\rceil.
\]

(7.7)

If any \( n_k \) equals \( n \) this will also give rise to a singular matrix. One of these possibilities is covered by Eq.(7.7), leaving two additional possibilities.

Subtracting this and Eq.(7.7) from Eq.(7.6), and then multiplying by \( \frac{1}{2} \), in order to factor out scalar multiples, gives us the following number of pairwise non-conjugate copies:

\[
\frac{1}{2} \left( \binom{n+2}{2} - \left\lceil \frac{n+2}{2} \right\rceil - 2 \right) = \frac{1}{2} \left[ \frac{(n+2)(n+1) - (n+2) - 4}{2} \right]
\]

\[
= \left\lfloor \frac{n^2 + 2n - 4}{4} \right\rfloor.
\]

\[\square\]

**Corollary 7.2.17.** Let \( n \) be even and suppose \( G \) is an irreducible finite non-abelian subgroup of \( \text{GL}(n, \mathbb{Q}) \) containing an element of odd order. Then, up to conjugacy in \( \text{GL}(n, \mathbb{Z}) \), there are exactly \( 2 \left\lfloor \frac{n^2 + 2n - 4}{4} \right\rfloor \) non-conjugate copies of \( G \) realisable over \( \mathbb{Z} \) which are all conjugate to each other in \( \text{GL}(n, \mathbb{Q}) \).

**Proof.** Suppose \( g, x \in \text{GL}(n, \mathbb{C}) \) and \( kg = gx \). In the case where \( n \) is even, we have that either \( k = \pm 1 \). An irreducible subgroup of \( \text{GL}(n, \mathbb{Q}) \) must contain an element conjugate in \( \text{GL}(n, \mathbb{C}) \) to either \( A = \text{antidiag}(1, \ldots, 1) \) or \( A' = \text{antidiag}(-1, \ldots, -1) \). Let \( B \) be a matrix of odd order in \( \text{GL}(n, \mathbb{Q}) \). The groups (and hence groups containing) \( \langle A, B \rangle \) and \( \langle A', B \rangle \) will be non-conjugate in \( \text{GL}(n, \mathbb{Z}) \). \[\square\]

**Lemma 7.2.18.** Let \( G \) be an irreducible finite subgroup of \( \text{GL}(2, \mathbb{Z}) \). Then \( G \) is conjugate to either one and only one of the finite irreducible groups as referenced in Corollary 7.2.7 or the additional non-conjugate isomorphic copy of \( \text{Sym}(3) \) given below:

\[
\left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \right\rangle.
\]

**Corollary 7.2.19.** Let \( \mathcal{G} = \{A_4, A_4 \times C_2, S_4 \times C_2\} \). Up to conjugacy in \( \text{GL}(3, \mathbb{Z}) \), there are 3 non-conjugate copies of each \( G \in \mathcal{G} \) in \( \text{GL}(3, \mathbb{Z}) \). For \( S_4 \), there are 6 non-conjugate copies in \( \text{GL}(3, \mathbb{Z}) \).

**Proof.** By Corollary 7.2.13, up to conjugacy in \( \text{GL}(3, \mathbb{Q}) \), there is only one copy of each \( G \in \mathcal{G} \) and there are two non-conjugate copies of \( S_4 \). The result then clearly follows. \[\square\]
Corollary 7.2.20. When \( n = 3 \), there are three possibilities for \((n_0, n_1, n_{-1})\), up to permutation of \(n_1\) and \(n_{-1}\), namely \((n_0, n_1, n_{-1}) \in \{(1, 2, 0), (2, 1, 0), (0, 2, 1)\}\).

Corollary 7.2.21. Let \( G \) be a finite subgroup of \( \text{GL}(3, \mathbb{Z}) \) and
\[
\mathcal{M} = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & -1 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix} \right\}.
\]
Then the set \( \{G^M : M \in \mathcal{M}\} \) consists of non-conjugate copies of \( G \) over \( \text{GL}(3, \mathbb{Z}) \).

Theorem 7.2.22. Let \( G \) be an irreducible finite subgroup of \( \text{GL}(3, \mathbb{Z}) \). Then \( G \) is conjugate in \( \text{GL}(3, \mathbb{Z}) \) to one and only one of the following groups.

\[
(i) \quad \{A_4, A_4 \times C_2\}:
\]
\[
\left\{ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, A \right\} \mid A \in \left\{ \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ -1 & -1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 1 & 0 \end{pmatrix} \right\}
\]

\[
(ii) \quad \{S_4, S_4 \times C_2\}:
\]
\[
\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \delta^* A \right\} \mid A \in \left\{ \begin{pmatrix} 0 & 0 & -1 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & -1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\}, \quad (\delta, \delta^*) \in \{(1, 1), (1, -1), (-1, 1)\}
\]

Proof. Apply Corollary 7.2.21 to Corollary 7.2.13.

\( \square \)

7.3 Subgroups of degree 2 and 3 over a real number field

Let \( \mathbb{P} \) be either a real number field \( \mathbb{K} \) or its ring of integers \( \mathcal{O}_\mathbb{K} \). For the remainder of the chapter, we focus on cyclotomic and quadratic extensions of \( \mathbb{Q} \). It would not be much extra work to include the solution for polynomial extensions (given that we outline the necessary conditions below). However, we have opted not to include it here as it would be quite repetitive and does not require any extra special treatment of the material.

7.3.1 Requirements on roots of polynomials for existence of subgroups

In order for certain classes of finite irreducible subgroups of \( \text{GL}(m, \mathbb{C}) \) to exist over \( \mathbb{K}' \), we require that certain polynomials have roots in \( \mathbb{K}' \). This translates into the existence of certain non-integer values in \( \mathbb{K}' \). We outline these requirements below for both the degree 2 and 3 cases.
7.3. SUBGROUPS OF DEGREE 2 AND 3 OVER A REAL NUMBER FIELD

Degree 2:

<table>
<thead>
<tr>
<th>Group</th>
<th>Polynomials with roots</th>
<th>Values required</th>
</tr>
</thead>
<tbody>
<tr>
<td>(D_n)</td>
<td>(\Phi_{2n}(x))</td>
<td>(\zeta_{2n})</td>
</tr>
<tr>
<td>(A_4^*)</td>
<td>(x^2 - x + \frac{1}{2})</td>
<td>(i, 2^{-1})</td>
</tr>
<tr>
<td>(S_4^*)</td>
<td>(x^2 - x + \frac{1}{2}, \Phi_8(y))</td>
<td>(\zeta_8, 2^{-1})</td>
</tr>
<tr>
<td>(A_5^*)</td>
<td>(x^2 - x - 1,) (y^2 - xy + \frac{3}{4})</td>
<td>(i, \sqrt{5}, 2^{-1})</td>
</tr>
</tbody>
</table>

Degree 3:

<table>
<thead>
<tr>
<th>Group</th>
<th>Polynomials with roots</th>
<th>Values required</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\text{Alt}(5))</td>
<td>(x^2 - x - 1)</td>
<td>(2^{-1}, \sqrt{5})</td>
</tr>
<tr>
<td>3.(\text{Alt}(6))</td>
<td>(x^2 - x - 1,) (y + xy + x^2)</td>
<td>(2^{-1}, \zeta_3, \sqrt{5})</td>
</tr>
<tr>
<td>(\text{PSL}(2, 7))</td>
<td>(x^2 + x + 2)</td>
<td>(2^{-1}, \sqrt{-7})</td>
</tr>
</tbody>
</table>

The degree 2 requirements are consequences of Theorems 3.0.11 and 3.0.12 and those of degree 3 arise from Theorems 5.2.10 – 5.2.12. The soluble groups in degree 3 do not have any additional requirements due to Theorem 7.2.9. Also, the addition of inverses (i.e. \(2^{-1}\)) is relevant only when \(\mathbb{P}\) is not a field.

Whatever additional roots of unity occur may give rise to additional split and central extensions. Thus, for split extensions, we simply need to adjoin scalar matrices of the appropriate order to the subgroups in questions. We are not concerned by covering groups due to the following:

- The dihedral groups due to Theorem 7.2.1 do have covering groups but Theorem 3.0.6 (ii) deals with these cases.
- Schur covers of the soluble groups \(\text{Alt}(4)\) and \(\text{Sym}(4)\) in \(\text{GL}(3, \mathbb{P}')\) are all reducible (i.e. \(A_4^*\) and \(S_4^*\) appear as groups of degree 2 in Theorem 3.0.6).
- Earlier arguments deal with other cases connected with groups over \(\mathbb{C}\).

7.3.2 Relating extensions by roots of unity and surds

We now consider the following: if we extend \(\mathbb{P}\) by various roots of unity, what surds are present in \(\mathbb{P}'\)?
Theorem 7.3.1. Let \( p \) be an odd prime then
\[
\begin{align*}
\text{if } p &\equiv 1 \mod 4 \quad \text{then } \sqrt{p} \in \mathbb{Z}[\zeta_p] \quad \text{and} \\
\text{if } p &\equiv -1 \mod 4 \quad \text{then } \sqrt{-p} \in \mathbb{Z}[\zeta_p]
\end{align*}
\]

Proof. Let \( f(x) = 1 + x + \ldots + x^{p-1} = (x - \zeta_p)(x - \zeta_p^2)\ldots(x - \zeta_p^{p-1}). \)
We have that
\[ x^p - 1 = (x - 1)f(x). \quad (7.8) \]
Taking the derivative of (7.8) gives us that
\[
\begin{align*}
px^{p-1} &= f(x) + (x - 1)f'(x) \\
\implies f'(x) &= (px^{p-1} - f(x))/(x - 1) \\
\implies f'(\zeta_p^t) &= (p\zeta_p^{t(p-1)} - f(\zeta_p^t))/(\zeta_p^t - 1) = p\zeta_p^{t(p-1)}/(\zeta_p^t - 1), \quad \forall t \in \{1, \ldots, p - 1\}
\end{align*}
\]
\[
\implies \prod_{t=1}^{p-1} f'(\zeta_p^t) = p^{p-1} \frac{\prod_{t=1}^{p-1} \zeta_p^{t(p-1)}}{\prod_{t=1}^{p-1} (\zeta_p^t - 1)} = p^{p-1} \frac{\zeta_p^{(p-1)/2}}{p} = p^{p-1} \frac{1}{p} = p^{p-2}
\]
Using the fact that coefficients are all 1 in \( f(x) \), it is straightforward to work out the discriminant \( \Delta \) using the formula:
\[
\Delta = (-1)^{n(n-1)/2} \frac{1}{a_n} R(f, f'),
\]
where \( R(f, f') \) is the resultant determinant coming from the Sylvester Matrix. In our case, we get
\[
\Delta = (-1)^{(p(p-1))/2} p^{p-2}.
\]
Hence
\[
\Delta = \begin{cases} 
  p^{p-2}, & \text{when } p \equiv 1 \mod 4, \\
  -p^{p-2}, & \text{when } p \equiv -1 \mod 4.
\end{cases}
\]
Since \( p \) is a prime divisor of the discriminant and \( \Delta \) is necessarily a square in \( \mathbb{Z}[\zeta_p] \), the result follows. \( \square \)

Lemma 7.3.2. Define the sets \( \Gamma_s = \{\zeta_s, \ldots, \zeta_s^{s-1}\} \) for all \( s \in \mathbb{Z}_+^+ \). Suppose \( p \) and \( t \) are odd primes. Then \( \Gamma_p \cup \Gamma_t \setminus \{\kappa\} \) forms a linearly independent set over \( \mathbb{Q} \), where \( \kappa \) is any element of \( \Gamma_p \cup \Gamma_t \).
7.3. SUBGROUPS OF DEGREE 2 AND 3 OVER A REAL NUMBER FIELD

Proof. Assume without loss of generality that $\kappa \in \Gamma_t$. We have that $\Gamma_t$ is a $Q$-basis of $Q_t$. Since $Q(\zeta_p\zeta_t) = Q(\zeta_{pt})$ and $[Q(\zeta_{pt}) : Q] = \varphi(pt) = \varphi(p)\varphi(t)$, then $[Q(\zeta_t, \zeta_p) : Q(\zeta_p)] = \varphi(t)$. Thus, any $Q$-basis for $Q(\zeta_t)$ is also a $Q(\zeta_p)$-basis of $Q(\zeta_t, \zeta_p)$. In particular, $\Gamma_t$ is linearly independent over $Q(\zeta_p)$.

Now, the minimum polynomial of $\zeta_t$ over $Q(\zeta_p)$ is $1 + x + \ldots + x^{t-1}$. Hence, it follows that $\Gamma_t' = (\Gamma_t \setminus \{\kappa\}) \cup \{1\}$ is also a $Q(\zeta_p)$-basis of $Q(\zeta_t, \zeta_p)$. Any $Q$-linear combination of elements of $\Gamma_p \cup \Gamma_t \setminus \{\kappa\}$ may be regarded as a $Q(\zeta_p)$-combination of elements of $\Gamma_t'$. The result then holds since $\Gamma_p$ is independent over $Q$.

Corollary 7.3.3. Let $t$ now be any integer co-prime to $p$. If

$$\sum_{\rho \in \Gamma_p} d_{\rho} \rho = \sum_{\tau \in \Gamma_t} c_{\tau} \tau,$$

then $\exists a \in \mathbb{Z}$ such that $d_{\rho} = a$ and $c_{\tau} \in \{0, a\}$ for all $\rho \in \Gamma_p$ and $\tau \in \Gamma_t$.

Proof. We have that $\sum_{\rho \in \Gamma_p} \rho = \sum_{\nu \in \Gamma_q} \nu = -1$ for each prime $q$ dividing $t$. Thus, it follows that we cannot take any smaller linear combination of elements of $\Gamma_p$ or $\Gamma_q$ to get a linear combination of the other.

Theorem 7.3.4. Suppose $p$ is an odd prime and $t \in \mathbb{Z}^+$ such that $\gcd(p, t) = 1$. Then

$$\sqrt{\pm p} \notin \mathbb{Z}[\zeta_t].$$

Proof. As a direct consequence of Theorem 7.3.1, we have that $\sqrt{p}$ can be written as

$$\sum_{j=0}^{p-1} d_j \zeta_p^j \quad \text{when } p \equiv 1 \mod 4$$

and

$$i \sum_{j=0}^{p-1} d_j \zeta_p^j \quad \text{when } p \equiv -1 \mod 4,$$

for some $d_j \in \mathbb{Z}$. Now suppose $\sqrt{\pm p} \in \mathbb{Z}[\zeta_t]$. Then we would have

$$x := \sum_{k=0}^{t-1} c_k \zeta_t^k = i^a \sum_{j=0}^{p-1} d_j \zeta_p^j$$

for some $c_k \in \mathbb{Z}$ and $a \in \{0, 1, 2\}$. But, by Corollary 7.3.3, $x$ would have to be of the form $ib$ for some $b \in \mathbb{Z}$. Therefore we have a contradiction and so $\sqrt{\pm p} \notin \mathbb{Z}[\zeta_t]$.

Corollary 7.3.5. Let $t$ be any positive integer. Then

$$\sqrt{p} \in \mathbb{Z}[\zeta_t] \iff p \equiv 1 \mod 4 \text{ and } p \mid t,$$

$$\sqrt{-p} \in \mathbb{Z}[\zeta_t] \iff p \equiv -1 \mod 4 \text{ and } p \mid t.$$
7.3. SUBGROUPS OF DEGREE 2 AND 3 OVER A REAL NUMBER FIELD

7.3.3 Lists of subgroups over extensions

For the rest of this section, \( U \) shall refer to some arbitrary set of distinct square roots of integers such that \( \mathbb{Z}[i] \cap U = \emptyset \). We use \( \Gamma \) to refer to some set of primitive roots of unity with

\[
\Gamma^+ = \begin{cases} 
\Gamma \cup \{ \zeta_3 \}, & \text{if } \sqrt{-3} \in U \text{ or } (\sqrt{3} \in U \text{ and } i \in \Gamma) \\
\Gamma, & \text{otherwise}
\end{cases}
\]

\[
\mathcal{N}_r^\ast = \left\{ p_1^{\alpha_1} \ldots p_k^{\alpha_k} | \zeta_{p_i}^{\alpha_i} \in \Gamma^+; p_i \text{ prime}; \alpha_i, k, t \in \mathbb{Z}^+; p_i \neq p_j \text{ when } i \neq j; i, j \in \{1, \ldots, k\} \right\}
\]

and \( \Gamma^\ast = \{ \zeta_n | n \in \mathcal{N}_r^\ast \} \).

Note that we shall allow the empty sets in our definitions for \( U \) and \( \Gamma \). We defined \( \Gamma^+ \) due to the fact that \( \zeta_3 \) has a radical form in terms of \( \sqrt{3} \) and \( i \).

**Theorem 7.3.6.** Let \( G \) be a finite irreducible subgroup of \( \text{GL}(2, \mathbb{K}') \) where \( \mathbb{K}' \) is an extension of \( \mathbb{K} \) by elements of some \( U \cup \Gamma \). Then \( G \) is conjugate to one and only one of the following groups.

(i) \( \{ C_s, D_{2s} | s \in \mathbb{Z}^+ \setminus \{1, 2\}, \cos(2\pi/s) \in \mathbb{K}' \text{ and } s \notin \mathcal{N}_r^\ast \} \)

(ii) For each \( \zeta_r, \zeta_s \in \Gamma \) such that \( r, s \geq 3 \):

- \( \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \zeta_r & 0 \\ 0 & \zeta_r \end{pmatrix}, \begin{pmatrix} \zeta_s & 0 \\ 0 & \zeta_s^{-1} \end{pmatrix} \) 2 \( | \) \( r + s \),

- \( \begin{pmatrix} 0 & \zeta_r \\ \zeta_r & 0 \end{pmatrix}, \begin{pmatrix} \zeta_s & 0 \\ 0 & \zeta_s^{-1} \end{pmatrix} \) 4 \( | r, 2 | s \) and \( s \geq 4 \),

- \( \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \zeta_{s+r} & 0 \\ 0 & \zeta_{s+r} \end{pmatrix}, \begin{pmatrix} \zeta_s^2 & 0 \\ 0 & \zeta_s^{-2} \end{pmatrix} \) 4 \( | r, 4 | s \) and \( s \geq 8 \).

(iii) When \( \zeta_{2n} \in \Gamma \): \( \{ \hat{D}_n, \hat{D}_n \times C_r | r \in \mathcal{N}_r^\ast \} \cup \{ \hat{D}_n \times C_{2r} | r \in \mathcal{N}_r^\ast, 2 \nmid r \} \)

(iv) When \( i \in \Gamma \): \( \{ A_i^\ast, A_i^\ast \times C_r | r \in \mathcal{N}_r^\ast \} \cup \{ A_i^\ast \times C_{2r} | r \in \mathcal{N}_r^\ast, 2 \nmid r \} \)

(v) When \( \sqrt{2} \in U \) and \( i \in \Gamma \) or \( \zeta_8 \in \Gamma \): \( \{ S_i^\ast, S_i^\ast \times C_r | r \in \mathcal{N}_r^\ast \} \cup \{ S_i^\ast \times C_{2r} | r \in \mathcal{N}_r^\ast, 2 \nmid r \} \)

(vi) When \( \sqrt{\pm 5} \in U \) and \( i \in \Gamma \) or \( \zeta_5 \in \Gamma \): \( \{ A_5^\ast, A_5^\ast \times C_r | r \in \mathcal{N}_r^\ast \} \cup \{ A_5^\ast \times C_{2r} | r \in \mathcal{N}_r^\ast, 2 \nmid r \} \)

Generators for (iii)–(vi) are as per Theorem 3.0.6 with the addition of scalar matrices \( rI_{2 \times 2} \) for each \( r \in \mathcal{N}_r^\ast \), and \( -rI_{2 \times 2} \) when \( 2 \nmid r \) and \( 2r \notin \mathcal{N}_r^\ast \). Generators for (i) are as per Theorem 7.2.1.
Proof. The list of generating sets given is due to a combination of Theorems 7.2.1, 3.0.6, 3.0.11 and the “Degree 2” requirements as outlined in Section 7.3.1. Possible split extensions arise due to elements of the set $\Gamma^*$. \square

Next, we define

$$\hat{r} := \begin{cases} 2, & \text{if } 2r \in \mathcal{N}_r^* \text{ or } 2 \mid r, \\ 1, & \text{otherwise}. \end{cases}$$

**Theorem 7.3.7.** Let $G$ be a finite irreducible subgroup of $\text{GL}(3, \mathbb{K}')$ where $\mathbb{K}'$ is an extension of $\mathbb{K}$ by elements of some $\mathcal{U} \cup \Gamma$. Then $G$ is conjugate to one and only one of the following groups.

(i) $\{A_4, A_4 \times C_r \mid r \in \mathcal{N}_r^* \} \cup \{A_4 \times C_{2r} \mid r \in \mathcal{N}_r^* \cup \{1\}, 2 \mid r\}$:

$$\left\langle \delta_r \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \zeta_r \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \mid \zeta_r \in \Gamma^* \cup \{\pm 1\} \right. \right. \delta_r \in \langle (-1)^{\hat{r}} \rangle$$

(ii) $\{S_4, S_4 \times C_r \mid r \in \mathcal{N}_r^* \} \cup \{S_4 \times C_{2r} \mid r \in \mathcal{N}_r^* \cup \{1\}, 2 \mid r\}$:

$$\left\langle \delta_r \zeta_r \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \delta_r^* \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \mid \zeta_r \in \Gamma^* \cup \{\pm 1\} \right. \right. \delta_r \in \langle (-1)^{\hat{r}} \rangle \delta_r^* \in \langle (-1)^{\hat{r}+1} \rangle$$

When at least one of the following is true:

$\sqrt{5} \in \mathbb{K}$ or $\zeta_5 \in \Gamma^*$ or $\sqrt{5} \in \mathcal{U}$ or ($\sqrt{-5} \in \mathcal{U}$ and $i \in \Gamma^*$),

then:

(iii) $\{A_5, A_5 \times C_r \mid r \in \mathcal{N}_r^* \} \cup \{A_5 \times C_{2r} \mid r \in \mathcal{N}_r^* \cup \{1\}, 2 \mid r\}$:

$$\left\langle \delta_r \zeta_r \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}, \frac{1}{2} \begin{pmatrix} \mu_2 & \mu_1 & -1 \\ \mu_1 & -1 & \mu_2 \\ -1 & \mu_2 & \mu_1 \end{pmatrix} \mid \zeta_r \in \Gamma^* \cup \{\pm 1\} \right. \right. \delta_r \in \langle (-1)^{\hat{r}} \rangle$$

where $\mu_1 = \frac{1}{2}(-1 + \sqrt{5})$ and $\mu_2 = -\frac{1}{2}(1 + \sqrt{5})$.

When at least one of the following is true:

$\sqrt{5} \in \mathbb{K} \cup \mathcal{U}$ and $\zeta_3 \in \Gamma^*$ or $\zeta_{15} \in \Gamma^*$ or ($\sqrt{-5} \in \mathcal{U}$ and $i, \zeta_3 \in \Gamma^*$),

then:
When at least one of the following is true:

\[ \text{are a direct consequence of combining Theorems 7.2.22, 5.2.10, 5.2.11 and 5.2.12.} \]

Let \( \Gamma \) be conjugate to one and only one of the groups:

\[ \{3.A_6 \times C_r \mid r \in N^*_7, 3 \not| r \} \cup \{3.A_6 \times C_{2r} \mid r \in N^*_7, 2 \not| r \} \cup \{3.A_6 \circ C_r \mid r \in N^*_7, \delta_3(r) \geq 2 \} \cup \{3.A_6 \circ C_{2r} \mid r \in N^*_7, 2 \not| r, \delta_3(r) \geq 2 \} : \]

\[
\begin{pmatrix}
\delta_r \zeta_r \\
0 0 1 \\
0 1 0
\end{pmatrix},
\begin{pmatrix}
0 & 1 & 0 \\
-1 & 0 & 0 \\
-\zeta_1^7 - \zeta_1^3 & -\zeta_1^7 & -\zeta_1^5 & 1
\end{pmatrix}
\]

\[ \zeta_r \in \Gamma^* \cup \{\pm 1\}, \]

\[ \delta_3(r) \geq 2 \text{ or } 2 \not| r, \delta_r \in \langle(-1)^r \rangle \]

When at least one of the following is true:

\[ \sqrt{-7} \in \mathcal{U} \text{ or } \zeta_7 \in \Gamma^* \text{ or } (\sqrt{-7} \in \mathcal{U} \text{ and } i \in \Gamma^*), \]

then:

\[ \{L_2(7) \times C_r \mid r \in N^*_7 \} \cup \{L_2(7) \times C_{2r} \mid r \in N^*_7, 2 \not| r \} : \]

\[
\begin{pmatrix}
\delta_r \zeta_r \\
0 0 1 \\
0 1 0
\end{pmatrix},
\begin{pmatrix}
-1 & (-1 - \sqrt{-7})/2 & 0 \\
0 & 1 & 0 \\
0 & (-1 + \sqrt{-7})/2 & -1
\end{pmatrix}
\]

\[ \zeta_r \in \Gamma^* \cup \{\pm 1\}, \]

\[ \delta_r \in \langle(-1)^r \rangle \]

Proof. The proof follows easily by considering split extensions by the available roots of unity in \( \Gamma^* \) and given the “Degree 3” requirements outlined in Section 7.3.1. The generating sets are a direct consequence of combining Theorems 7.2.22, 5.2.10, 5.2.11 and 5.2.12. □

**Corollary 7.3.8.** Let \( G \) be a finite soluble irreducible subgroup of \( \text{GL}(3, \mathbb{K}') \). Then \( G \) is conjugate to one and only one of the groups in (i) or (ii).

**Corollary 7.3.9.** Let \( G \) be a finite insoluble irreducible subgroup of \( \text{GL}(3, \mathbb{K}') \). Then \( G \) is conjugate to one and only one of the groups in (iii), (iv) or (v).

**Theorem 7.3.10.** Let \( G \) be a finite irreducible subgroup of \( \text{GL}(3, \mathbb{Z}') \) where \( \mathbb{Z}' \) is an extension of \( \mathbb{Z} \) by elements of some \( \mathcal{U} \cup \Gamma \cup \mathcal{Q} \) where \( \mathcal{Q} \) is a finite subset of \( \mathcal{Q} \). If \( 2^{-1} \in \mathcal{Q} \), then \( G \) is conjugate to one and only one of the groups in Theorem 7.3.7. Otherwise \( G \) is conjugate to one and only one of the following groups:

(i) \( \{A_4 \times C_r \mid r \in N^*_7 \} \cup \{A_4 \times C_{2r} \mid r \in N^*_7, 2 \not| r \} : \)

\[
\begin{pmatrix}
\delta_r \zeta_r \\
0 0 1 \\
1 0 0
\end{pmatrix},
\begin{pmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
1 & 0 & 0
\end{pmatrix}
\]

\[ \zeta_r \in \Gamma^* \cup \{\pm 1\}, \]

\[ \delta_r \in \langle(-1)^r \rangle \]

(ii) \( \{S_4 \times C_r \mid r \in N^*_7 \} \cup \{S_4 \times C_{2r} \mid r \in N^*_7, 2 \not| r \} : \)

\[
\begin{pmatrix}
\delta_r \zeta_r \\
0 0 1 \\
1 0 0
\end{pmatrix},
\begin{pmatrix}
0 & 1 & 0 \\
0 & 1 & 0 \\
1 & 0 & 0
\end{pmatrix}
\]

\[ \zeta_r \in \Gamma^* \cup \{\pm 1\}, \]

\[ \delta_r \in \langle(-1)^r \rangle \]

\[ \delta_r^* \in \langle(-1)^{r+1} \rangle \]
When \( \zeta_{15} \in \Gamma^* \) then:

(iii) \( \{3. A_6 \times C_r \mid r \in N_{\Gamma}^*, 3 \mid r\} \cup \{3. A_6 \times C_{2r} \mid r \in N_{\Gamma}^*, 2 \mid r\} \cup \{3. A_6 \circ_{c_3} C_r \mid r \in N_{\Gamma}^*, \delta(3, r) \geq 2\} \cup \{3. A_6 \circ_{c_3} C_{2r} \mid r \in N_{\Gamma}^*, 2 \mid r, \delta(3, r) \geq 2\} : \\
\begin{bmatrix}
\delta_r \zeta_r \\
0 1 0 \\
0 0 1 \\
0 1 0
\end{bmatrix}, \\
\begin{bmatrix}
0 & 1 & 0 \\
-1 & 0 & 0 \\
-\zeta_{15}^7 - \zeta_{15}^{13} & -\zeta_{15}^2 & -\zeta_{15}^8 & 1
\end{bmatrix} \\
\zeta_r \in \Gamma^* \cup \{\pm 1\}, \\
\delta(3, r) > 1 \text{ or } 3 \mid r, \\
\delta_r \in \langle (-1)^{\delta} \rangle
\}

When \( \zeta_7 \in \Gamma^* \) then:

(v) \( \{L_2(7) \times C_r \mid r \in N_{\Gamma}^*\} \cup \{L_2(7) \times C_{2r} \mid r \in N_{\Gamma}^*, 2 \mid r\} : \\
\begin{bmatrix}
\delta_r \zeta_r \\
0 1 0 \\
0 0 1 \\
1 0 0
\end{bmatrix}, \\
\begin{bmatrix}
0 & -\zeta_7 - \zeta_7^3 - \zeta_7^5 & 0 \\
0 & 1 & 0 \\
0 & -\zeta_7^2 - \zeta_7^4 - \zeta_7^6 & -1
\end{bmatrix} \\
\zeta_r \in \Gamma^* \cup \{\pm 1\}, \\
\delta_r \in \langle (-1)^{\delta} \rangle
\}

Proof. All the matrices in Corollary 7.2.21 are invertible when \( 2^{-1} \in \mathbb{Z}' \) – otherwise they are not. Thus, the additional non-conjugate groups given in Theorem 7.2.22 can be eliminated in the case when \( 2^{-1} \in \mathbb{Z}' \). Therefore it follows easily that the relevant groups are those of Theorem 7.3.7. On the other hand, if \( 2^{-1} \not\in \mathbb{Z}' \), we need to include conjugations over \( \mathbb{Q}' \) by matrices in Corollary 7.2.21. In the cases of 3.A_6 and L_2(7), we have the given generating sets which do not require \( 2^{-1} \). \( \square \)
Chapter 8

Computer implementation

8.1 Technical details

The computer implementation was designed for the computer package MAGMA. It is broken up over the files outlined below:

- attributes.m
- common.m
- deg2_abelian.m
- deg2_insoluble.m
- deg2_monomial.m
- deg2_primitive.m
- deg2_char_zero.m
- deg3_groups.m
- deg3_insoluble.m
- deg3_insoluble_modular.m
- deg3_insoluble_nonmodular.m
- deg3_monomial.m
- deg3_primitive.m
- deg3_char_zero.m
- mat_subgroups_of_small_degree.m

The files listed in *italics* indicate slightly modified versions of the files originally encoded by Flannery and O’Brien [11] for the degree 2 case and for the degree 3 soluble case over finite fields in MAGMA. The newly created files use some of the functions in the older files. All MAGMA computer code can be viewed and assessed at:

8.1. TECHNICAL DETAILS

8.1.1 Primary function: getMatrixSubgroupsOverSmallDegree

This allows the user to search for matrix subgroups of degree 2 or 3 for various inputs.

Inputs:

- \(d\) Degree of Matrix Group, user can enter either 2 or 3 or "both"

- \(fF\) Integral domain or a parameter list of integral domains.
  Can be the name of an integral domain (including extensions) or a prime power;
  in the case of a prime power, the unique Galois field of this size is used.

- \(L\) A comma-separated parameter list with each parameter closed by double quotes: "...", Possible parameters are:

  - irreducible, reducible, soluble, insoluble, imprimitive, primitive,
  - \(GL, SL, by\_iso, by\_conj\)

Most parameters are self-explanatory. We describe those that are not.

- \(by\_iso\): list is restricted to non-isomorphic matrix groups.
- \(by\_conj\): list distinguishes non-conjugate matrix groups as opposed to non-isomorphic.

Default settings are \(GL\) and \(by\_conj\).

Output:

A list of matrix groups (each given by a set of generating matrices) separated into logical sublists.

Attributes

The function also attaches some attributes to the matrix groups:

- Description
- BaseRing
- Properties
- \(CQ = CentralQuotient\)
- Family
8.1. TECHNICAL DETAILS

8.1.2 Other functions

Insoluble matrix groups over finite fields

getInsolubleMatrixGroupsOfDimThreeOverGL(Fpa,...),
getInsolubleMatrixGroupsOfDimThreeOverSL(Fpa,...)

Inputs:
Fpa either of p or p,a or a finite field F

Output:
list of irreducible insoluble subgroups of \(GL(3,F)\) and \(SL(3,F)\) respectively, where

\[
F = \begin{cases} 
GF(p), & \text{when user enters } p \\
GF(p^a), & \text{when user enters } p,a \\
F, & \text{when user enters finite field argument}
\end{cases}
\]

Subroutines:
getInsolubleMatrixGroupsOfDimThree

getInsolubleMatrixGroupsOfDimThreeOverGL(L, isGL)

Inputs:
L list of the form [* *] with arguments either p or p,a or a finite field F
isGL Boolean value, true indicates list over GL and false indicates list over SL

Output:
list of irreducible insoluble subgroups of \(GL(3,F)\) or \(SL(3,F)\) when parameter isGL is true or false respectively, where F is as previous entry.

Subroutines:
getInsolubleMatrixGroupsOfDimThreeOverGL
### 8.1. TECHNICAL DETAILS

**getInsolubleMatrixGroupsOfDimThreeFF**(*F*, **isGL**, **isByConj**)

This function combines the modular and non-modular matrix groups. Given an input field whose base field is GF(\(p^a\)), we initially run various checks on the values of \(p\) and \(a\) in order to determine which subgroups and scalar groups are applicable. In this way, computation is kept to a minimum.

**Inputs:**
- **F** a finite field
- **isGL** true/false indicates list over GL/SL resp.
- **isByConj** true indicates listing up to conjugacy in ambient general linear group
  - false indicates listing by isomorphism type

**Output:**
A list of the irreducible insoluble subgroups of GL(3, \(F\)) or SL(3, \(F\)) when parameter **isGL** is either true or false respectively.

**Subroutines:**
- getInsolubleModularMatrixGroupsOfDimThreeFF,
- getInsolubleNonmodularMatrixGroupsOfDimThreeFF

**getInsolubleModularMatrixGroupsOfDimThreeFF**(*F*, **isGL**, **isByConj**)

This function deals with the irreducible insoluble modular subgroups of Chapter 6. We use the generating sets as presented in Theorems 6.3.35 and 6.3.36.

**Inputs:**
- **F** a finite field
- **isGL** true/false indicates list over GL/SL resp.
- **isByConj** true indicates listing up to conjugacy in ambient general linear group
  - false indicates listing by isomorphism type

**Output:**
A list of the irreducible insoluble modular subgroups of GL(3, \(F\)) or SL(3, \(F\)) when parameter **isGL** is either true or false respectively.

A total of 9 sublists are produced corresponding respectively to the families of subgroups (a),(b),(c),(c\#), (d), (a\+), (b\+), (e) and (f) as outlined in Chapter 6.
8.1. TECHNICAL DETAILS

Subroutines:

getList_a_CQ_PSL3pb, getList_b_CQ_PSU3pb, getList_c_CQ_PSL2pb,
gList_ch_CQ_PGL2pb, getList apl_CQ_PGL3pb, getList_bpl_CQ_PGU3pb,
gList_e_CQ_A6peq2, getList_f_CQ_A6A7peq5,
gList d_CQ_A5PSL27peq3 (getAlt5AsMG, getPSL27AsMG).

gGetInsolubleNonmodularMatrixGroupsOfDimThreeFF(F, isGL)

This function deals with the irreducible insoluble non-modular subgroups of Chapter 5. We use the generators as presented in Section 5.2.3. We lift these groups from $\text{GL}(n, \mathbb{C})$ to $\text{GL}(n, F)$ and use the corresponding generating sets for these matrix groups. Originally we applied the algorithm of Glasby and Howlett [12] in order to produce the set of generators in the smallest field possible but the algorithm was improved to avoid this extra overhead.

Inputs:

- $F$ a finite field
- $isGL$ true/false indicates list over $\text{GL}/\text{SL}$ resp.

Output:

A list of the irreducible insoluble non-modular subgroups of $\text{GL}(3, F)$ or $\text{SL}(3, F)$ when parameter $isGL$ is either true or false respectively.

A total of 3 sublists are produced. Each sublist contains all subgroups having the same central quotient up to isomorphism. These central quotients are $\text{Alt}(5), \text{Alt}(6) \text{ or } \text{PSL}(2, 7)$ as per Chapter 6 and result in the 3 sublists.

Subroutines:

getAlt5AsMG, get3Alt6AsMG, getPSL27AsMG
8.1. TECHNICAL DETAILS

Finite matrix groups over integral domains of characteristic zero

The functions here compile the results and generating sets seen in Chapter 7. Generators for the extensions of base integral domain are found by first picking out the relevant generating sets of the base integral domain given in Chapter 7. Then, depending on various conditions, some or none of the generating sets of Theorem 3.0.6 (ii)–(v) and of Section 5.2.3 are included.

In order to produce the generating sets in 7.2.2, we made use of the following facts:

- for $n \in \mathbb{Z}^+$, the degree of the irreducible polynomial of $\cos(2\pi/n)$ is 1 when $n = 1$ or 2; otherwise it is $\varphi(n)/2$ (cf. [1]).

- $\varphi(n) \leq \sqrt{n}$ where $n \neq 2$ or 6 (cf. [29, p. 9]).

The helper method `getMaxPossibleCosArg` within `deg2_char_zero.m` applies this logic. The functions calling this method are responsible for producing all the possible cyclic and dihedral groups relevant to the inputted integral domain.

The issue of conjugacy in the general linear group over certain classes of rings is also addressed. This can depend on whether certain inverses exist or not in the particular ring. The number of conjugacy classes of subgroups of the general linear group over a given integral domain may be smaller than over the base ring of this integral domain. For example, the ring of dyadic rationals $\mathbb{Z}[\frac{1}{2}] = \{ \frac{n}{2^k} | n, k \in \mathbb{Z}, k \geq 0 \}$ contains $2^{-1}$ whereas $\mathbb{Z}$ does not. Hence some of the groups in Theorem 7.2.22 are conjugate in $\text{GL}(3, \mathbb{Z}[\frac{1}{2}])$ whereas they are pairwise non-conjugate over $\mathbb{Z}$.

`getFiniteMatrixGroupsOfDimTwoOverPIDOfCharZero(R, isGL, isByConj)`

**Inputs:**
- R \hspace{1cm} \text{integral domain of characteristic zero}
- isGL \hspace{1cm} \text{true/false indicates list over GL/SL resp.}
- isByConj \hspace{1cm} \text{true indicates listing up to conjugacy in ambient general linear group}
- false \hspace{1cm} \text{indicates listing by isomorphism type}

**Outputs:**
A list of all finite matrix groups of $\text{GL}(3, R)$.

**Subroutines:**
- `getFiniteSolubleMatrixGroupsOfDimTwoOverPIDOfCharZero`
- `getFiniteInsolubleMatrixGroupsOfDimTwoOverPIDOfCharZero`
getFiniteSolubleMatrixGroupsOfDimTwoOverPIDOfCharZero(R, isGL, isByConj)

Inputs:
R integral domain of characteristic zero
isGL true/false indicates list over GL/SL resp.
isByConj true indicates listing up to conjugacy in ambient general linear group
false indicates listing by isomorphism type

Outputs:
A list of all finite soluble matrix groups of GL(3, R).

Subroutines:
getMaxRootOfUnityToAddToCharZeroDeg2PID
cycAsMG
dihedralAsMG
A4starAsMG
S4starAsMG

generateFiniteInsolubleMatrixGroupsOfDimTwoOverPIDOfCharZero(R, isGL, isByConj)

Inputs:
R integral domain of characteristic zero
isGL true/false indicates list over GL/SL resp.
isByConj true indicates listing up to conjugacy in ambient general linear group
false indicates listing by isomorphism type

Outputs:
A list of all finite insoluble matrix groups of GL(3, R).

Subroutines:
getMaxRootOfUnityToAddToCharZeroDeg2PID
A5starAsMG
getFiniteMatrixGroupsOfDimThreeOverPIDOfCharZero(R, isGL, isByConj)

**Inputs:**
- R: integral domain of characteristic zero
- isGL: true/false indicates list over GL/SL resp.
- isByConj: true indicates listing up to conjugacy in ambient general linear group, false indicates listing by isomorphism type

**Outputs:**
A list of all finite matrix groups of GL(3, \(R\)).

**Subroutines:**
- getFiniteSolubleMatrixGroupsOfDimThreeOverPIDOfCharZero,
- getFiniteInsolubleMatrixGroupsOfDimThreeOverPIDOfCharZero

getFiniteSolubleMatrixGroupsOfDimThreeOverPIDOfCharZero(R, isGL, isByConj)

**Inputs:**
- R: integral domain of characteristic zero
- isGL: true/false indicates list over GL/SL resp.
- isByConj: true indicates listing up to conjugacy in ambient general linear group, false indicates listing by isomorphism type

**Outputs:**
A list of all finite soluble matrix groups of GL(3, \(R\)).

**Subroutines:**
- getMaxRootOfUnityToAddToCharZeroPID,
- getAlt4AsMG, getSym4AsMG, getA4CopyGroups, getS4CopyGroups.

getFiniteInsolubleMatrixGroupsOfDimThreeOverPIDOfCharZero(R, isGL, isByConj)

**Inputs:**
- R: integral domain of characteristic zero
- isGL: true/false indicates list over GL/SL resp.

**Outputs:**
A list of all finite insoluble matrix groups of GL(3, \(R\)).

**Subroutines:**
- getMaxRootOfUnityToAddToCharZeroPID,
- getAlt5AsMG, get3Alt6AsMG, getPSL27AsMG.
Routines for Matrix Groups

get\text{Description}(\text{MG or L})

This can take either one of two arguments:

- \text{MG: GrpMat} description of the matrix group
- \text{L: SeqEnum[GrpMat]} a list of descriptions of the matrix groups.

get\text{BaseRing}(\text{MG: GrpMat})

Outputs the field or ring associated with the matrix group \text{MG}.

get\text{Properties}(\text{MG: GrpMat})

Outputs string with properties of matrix group \text{MG}: \text{Irreducible, Imprimitive}, etc.

get\text{CentralQuotient}(\text{MG: GrpMat}), \text{getCQ}(\text{MG : GrpMat})

Outputs the central quotient of the matrix group \text{MG}.

8.2 Veracity and results of code

8.2.1 Confirming veracity of the implemented lists

We compiled a series of tests that ensured irredundancy and completeness of our lists. In addition, we ensured that an infinite matrix group is never included in these lists. Some test files used for this purpose are available at the URL given at the beginning of Section 8.1.

For sufficiently small finite fields, we were able to determine results directly from \textit{Magma} and compare these with our lists. For all prime powers up to 256, we established a complete correspondence between our lists and the results of direct computations.

For larger fields, we performed some successful tests with the help of the in-built \textit{Magma} function \textit{RandomSchreier}. This function constructs a probable base and strong generating set (BSGS) for a given group $G$. To effectively apply the algorithm, a carefully selected set of base points with sufficiently small orbits is required (cf. [26]). However, complete verification is not computationally possible and the case of insoluble groups over larger fields proved particularly difficult in most cases to verify completely.

We compared directly our lists of subgroups over the rationals and integers with those given in [27] and [33]. Due to Theorem 7.2.9, only a small number of tests was required to ensure veracity for the lists over any real field. Tests of verification were also successful for
various inputted integral domains of characteristic zero, e.g. Eisenstein integers, Gaussian
integers, some cyclotomic fields, and various extensions of the rationals and integers. We
chose the tests which involve rational and integer extensions, so that, all of the possible
core groups (as per the degree 2 and 3 requirements of Section 7.3.1) would feature as part
of the expected (combined) outputs.

8.2.2 Table of insoluble irreducible subgroups of $\text{GL}(3, q)$

In the table below, we report the time $t$ in CPU seconds (to the nearest millisecond)
to construct all $k$ conjugacy classes of insoluble irreducible subgroups of $\text{GL}(3, q)$ using
Magma:

<table>
<thead>
<tr>
<th>$q$</th>
<th>$k$</th>
<th>$t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>11</td>
<td>0.010</td>
</tr>
<tr>
<td>$5^4$</td>
<td>326</td>
<td>0.010</td>
</tr>
<tr>
<td>$5^{10}$</td>
<td>1,272</td>
<td>0.160</td>
</tr>
<tr>
<td>$5^{12}$</td>
<td>7,760</td>
<td>1.130</td>
</tr>
<tr>
<td>$17^6$</td>
<td>4,064</td>
<td>0.520</td>
</tr>
<tr>
<td>$97^6$</td>
<td>10,896</td>
<td>2.010</td>
</tr>
<tr>
<td>$131^{10}$</td>
<td>14,848</td>
<td>4.140</td>
</tr>
</tbody>
</table>

8.2.3 Sample results

For sections of code, we indicate user input by ‘$>$’ followed by the segment of code.
Output associated with this input will come on the line directly after it. In order to
facilitate ease of illustration, we consider a small example.

Suppose we want the full list of non-isomorphic irreducible insoluble subgroups of $\text{GL}(3, 5)$. Assume we have loaded the appropriate file, we can then enter the following
code into Magma:

```magma
> L:= getMatrixSubgroupsOverSmallDegree(3, 5, ["irreducible", "insoluble"]);
```

$L$ now contains a list of matrix groups separated into various sublists. The first 9 sublists
are the irreducible insoluble modular groups and the remaining 3 sublists correspond to the
irreducible insoluble non-modular groups. Some of the sublists may be empty.

Recall that the function `getDescription` can take a list argument, i.e. we can present
it with a list of matrix subgroups produced by the program. It sub-categorises these into
the sublists, e.g.
> getDescription(L);

produces the following output:

(1)
i. SL(3,5)
ii. SL(3,5)x_C_2
iii. GL(3,5)

(2)
<Empty>

(3)
i. PSL(2,5)
ii. PSL(2,5)x_C_2
iii. PSL(2,5)x_C_4

(4)
i. PGL(2,5)
ii. PGL(2,5) (NonConj Copy)
iii. PGL(2,5)x_C_2
iv. PGL(2,5)x_C_4
v. GL(2,5) mod _C_2

(5)
<Empty>

(6)
<Empty>

(7)
<Empty>

(8)
<Empty>

(9)
<Empty>

(10)
<Empty>

(11)
<Empty>

(12)
<Empty>
Hence, we have a description of all the non-isomorphic insoluble irreducible subgroups of $GL(3,5)$.

If we type `> L[4]` then all those groups relating to list 4 appear with generating sets. We shall not include that output here for space reasons. Instead, we first check how many there are and then pick an individual one of these matrix groups:

```plaintext
> #L[4];
5
```

We can access an individual group as follows:

```plaintext
> L[4][1];
MatrixGroup(3, GF(5)) of order $2^2 * 3 * 5$
Generators:
  [1 3 2]
  [1 4 0]
  [3 0 0]

  [2 0 0]
  [0 1 0]
  [0 0 3]
```

Other information of interest:

```plaintext
> getDescription(L[4][1]);
PGL(2,5)
```

```plaintext
> getBaseRing(L[4][1]);
Finite field of size 5
```

```plaintext
> getProperties(L[4][1]);
Modular, Irreducible, Insoluble
```

```plaintext
> getDescription(L[4][5]);
GL(2,5) mod C_2
```

```plaintext
> getCQ(L[4][5]);
PGL(2,5)
```
8.2. VERACITY AND RESULTS OF CODE

Since the example is quite small, it is fairly straightforward to check that $L[4][1]$ is indeed $\text{PGL}(2, 5)$:

```
> IsIsomorphic(L[4][1], PGL(2,5));
true
```

Homomorphism of $\text{MatrixGroup}(3, \text{GF}(5))$ of order $2^3 * 3 * 5$ into $\text{GrpPerm}$:
Degree 6, Order $2^3 * 3 * 5$ induced by

\[
\begin{bmatrix}
1 & 3 & 2 \\
1 & 4 & 0 \\
3 & 0 & 0 \\
2 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 3
\end{bmatrix} \rightarrow (1, 6, 5)(2, 3, 4)
\]

\[
\begin{bmatrix}
2 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 3
\end{bmatrix} \rightarrow (2, 6, 4, 3)
\]

We can also identify $L[4][2]$ as a copy of $\text{PGL}(2, 5)$:

```
> getDescription(L[4][2]);
PGL(2,5) (NonConj Copy)
```

Using the function $\text{IsIsomorphic}$ verifies an isomorphism between $L[4][1]$ and $L[4][2]$:

```
> IsIsomorphic(L[4][1], L[4][2]);
true
```

Homomorphism of $\text{MatrixGroup}(3, \text{GF}(5))$ of order $2^3 * 3 * 5$ into $\text{MatrixGroup}(3, \text{GF}(5))$ of order $2^3 * 3 * 5$ induced by

\[
\begin{bmatrix}
1 & 3 & 2 \\
1 & 4 & 0 \\
3 & 0 & 0 \\
4 & 0 & 3 \\
3 & 2 & 4 \\
2 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 3 \\
4 & 4 & 0 \\
4 & 3 & 3
\end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 3 \\ 2 & 0 & 0 \\ 2 & 0 & 0 \end{bmatrix}
\]

However, we can confirm they are not conjugate in $\text{GL}(3, 5)$:

```
> IsGLConjugate(L[4][1], L[4][2]);
false
```
Appendix A

Notation and terminology

A.1 Notation

Let $G$ be a group, $\mathbb{F}$ be any specified field and $x, y \in \mathbb{F}$.

Rings, fields and elements

1. $\mathbb{Z}$ ring of integers
2. $\mathbb{Z}^+$ set of positive integers
3. $\mathbb{Q}$ rational field
4. $\mathbb{R}$ real field
5. $\mathbb{C}$ complex field
6. $R[X]$ polynomial ring in indeterminate $X$ over a ring $R$.
7. s.t. such that
8. $\mathcal{O}_K$ ring of algebraic integers contained in $K$
9. $\overline{\mathbb{F}}$ algebraic closure of $\mathbb{F}$
10. $\zeta$ some primitive root of unity over $\mathbb{F}$
11. $\zeta_x$ primitive $x^{\text{th}}$ root of unity over $\mathbb{F}$, $x \neq 0$
12. $\varphi$ the Euler totient function
13. $\Phi_k(X)$ the $k^{\text{th}}$ cyclotomic polynomial
14. $[\ ]_p$ reduction modulo $p$ map on $\mathbb{Z}$ or group ring elements over $\mathbb{Z}$
15. $(a; b), \text{gcd}(a, b)$ greatest common divisor of $a, b \in \mathbb{Z}^+$
16. $\text{diag}(x_1, \ldots, x_n)$ $n \times n$ matrix with diagonal entries $x_1, \ldots, x_n$ and 0’s elsewhere
17. $\text{mon}(x_1, \ldots, x_n)$ any $n \times n$ monomial matrix with non-zero entries $x_1, \ldots, x_n$
18. $x \mid y; \ x \parallel y$ $x$ divides $y$; $x$ properly divides $y$
19. $\hat{\delta}_n(m)$ exponent of the largest power of $n$ dividing $m$ where $n, m \in \mathbb{Z}$
20. $\left( \frac{p}{q} \right)$ the Legendre symbol of $p$ and $q$
Matrices

Let $A$ be an arbitrary square matrix.

(21) $\text{tr}(A)$ trace of $A$ (sum of all diagonal entries of $A$)

(22) $\text{det}(A)$ determinant of $A$

Let $G$ and $H$ be groups and $C$ an abelian group.

Group Theory

(23) $\langle x, y, \ldots \rangle$ group generated by the elements $x, y, \ldots$

(24) $|G|$ order of $G$

(25) $|G : H|$ index of a subgroup $H$ in $G$

(26) $\text{soc}(G)$ socle of $G$ (group generated by all minimal normal subgroups of $G$)

(27) $\text{Aut}(G)$ automorphism group of $G$

(28) $C_G(\ )$ centraliser in $G$

(29) $N_G(\ )$ normaliser in $G$

(30) $Z(G)$ centre of $G$, i.e. $C_G(G)$

(31) $H \leq G$ ($H < G$) subgroup inclusion (proper inclusion)

(32) $H \trianglelefteq G$ ($H \vartriangleleft G$) $H$ is a normal subgroup of $G$ (proper)

(33) $G \cong H$ $H$ is isomorphic to a subgroup of $G$

(34) $G \times H$ direct product of $G$ and a group $H$

(35) $G \trianglerighttimes H$ semi-direct product of $G$ and a group $H$

(36) $G \circ_C H$ central product of $G$ and $H$ over their common central subgroup $C$

Formally, we have injections $\alpha : C \rightarrow G$, $\beta : C \rightarrow H$. Then $G \circ_C H$ is the quotient of $G \times H$ by sets of ordered pairs of the form $(\alpha(c), \beta(c))$ ($c \in C$)

(37) $n.G$ central non-split extension of cyclic group $C_n$ of order $n$ by $G$

(38) $G.n$ group containing a subgroup isomorphic to $G$ of index $n$

(39) $g^h$ $h^{-1}gh$ (conjugation of $g$ by $h$) where $g, h \in G$

Cohomology

(40) $\text{Hom}(G, C)$ group of homomorphisms from $G$ into $C$

(41) $Z^2(G, C)$ group of all cocycles $G \times G \rightarrow C$

(42) $B^2(G, C)$ group of all coboundaries $G \times G \rightarrow C$

(43) $H^2(G, C)$ 2nd cohomology group: $Z^2(G, C)/B^2(G, C)$
**Linear Groups**

Let $n$ be an integer, $\mathbb{F}$ be a field and $q$ a prime power.

1. **Notation**

   - **Mat**($n, \mathbb{F}$), **Mat**($n, q$) ring of all $n \times n$ matrices over $\mathbb{F}$ and over the field of $q$ elements respectively
   - **GL**($n, \mathbb{F}$), **GL**($n, q$) group of all invertible $n \times n$ matrices over $\mathbb{F}$ and over the field of $q$ elements respectively
   - **SL**($n, \mathbb{F}$), **SL**($n, q$) subgroup of **GL**($n, \mathbb{F}$), **GL**($n, q$) respectively consisting of all elements of determinant 1. In general, the prefix ‘S’ denotes the subgroup of all elements of determinant 1
   - **U**($n, q$) (or **GU**($n, q$)) subgroup of **GL**($n, q^2$) of all matrices $A$ such that $\overline{A}^\top JA = J$, for $J$ symmetric and non-singular. ($\overline{A}$ is obtained by replacing each entry $a_{ij}$ in $A$ by $a_{ij}^q$)
   - **CU**($n, q$) (CSU($n, q$)) conformal (special) unitary group. Subgroup of **GL**($n, q^2$) (resp. **SL**($n, q^2$)) of all matrices preserving the same Hermitian form as **GU**($n, q$) up to a scalar (see also: (80))
   - **O**($n, \mathbb{F}$) subgroup of **GL**($n, \mathbb{F}$) consisting of all $n \times n$ matrices preserving a non-singular quadratic form
   - **D**($n, \mathbb{F}$) subgroup of **GL**($n, \mathbb{F}$) consisting of all diagonal matrices
   - **Mon**($n, \mathbb{F}$) subgroup of **GL**($n, \mathbb{F}$) consisting of all monomial matrices
   - **PGL**($n, \mathbb{F}$), **PGL**($n, q$) **GL**($n, \mathbb{F}$)/$Z$ where $Z$ is the scalar subgroup. In general the prefix ‘P’ denotes the quotient by its scalar subgroup

Let $G \leq \text{GL}(n, \mathbb{F})$.  

- **tr**($G$) = \{**tr**($g$) | $g \in G$\}  
- **det**($G$) = \{**det**($g$) | $g \in G$\}

**Older notation**

Some of the older resources to which we refer use different names for the linear groups.

<table>
<thead>
<tr>
<th>Old</th>
<th>Modern</th>
<th>Alternative modern</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GLH</strong>($n, p^e$) (General Linear Homogeneous Group)</td>
<td><strong>GL</strong>($n, p^e$)</td>
<td><strong>GL</strong>$_n$($p^e$)</td>
</tr>
<tr>
<td><strong>SLH</strong>($n, p^e$) (Special Linear Homogeneous Group)</td>
<td><strong>SL</strong>($n, p^e$)</td>
<td><strong>SL</strong>$_n$($p^e$)</td>
</tr>
<tr>
<td><strong>LF</strong>($n, p^e$) (Linear Fractional Group)</td>
<td><strong>PSL</strong>($n, p^e$)</td>
<td><strong>PSL</strong>$_n$($p^e$), <strong>L</strong>$_n$($p^e$)</td>
</tr>
<tr>
<td><strong>HO</strong>($n, p^e$) (Hyperorthogonal Group)</td>
<td><strong>PSU</strong>($n, p^e$)</td>
<td><strong>PSU</strong>$_n$($p^e$)</td>
</tr>
</tbody>
</table>
A.2 Terminology

Cohomology

Let $G$ be a group and $C$ an abelian group.

(55) Exact sequence  
A sequence $\cdots \rightarrow G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} G_{i+2} \xrightarrow{f_{i+2}} \cdots$ where $G_i$ are groups and $f_i$ homomorphisms, s.t. $\forall i \ker(f_{i+1}) = \im(f_i)$

(56) Short exact sequence  
Exact sequence of length five: $1 \rightarrow G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \rightarrow 1$.

(57) (2-)Cocycle  
a map $\psi : G \times G \rightarrow C$ such that $\psi(g, h)\psi(gh, k) = \psi(g, hk)\psi(h, k)$ $\forall g, h, k \in G$

(58) (2-)Coboundary  
a cocycle $\tilde{\phi}$ defined from a (normalised) set map $\phi : G \rightarrow C$ by $\tilde{\phi}(g, h) = \phi(g)\phi(h)\phi(gh)^{-1}$

(59) Central extension  
a group $E$ with a specified subgroup $N$ in the centre of $E$; we say that $E$ is a (central) extension of $N$ by $G \cong E/N$

Group Theory

(60) Irredundant list  
List of subgroups of a group in which distinct elements are not conjugate in the containing group

(61) Hall subgroup  
Subgroup of a finite group whose order and index are relatively prime

(62) Torsion subgroup  
Subgroup of abelian group $A$ consisting of all finite order elements

(63) Projective order  
Order of $h\mathbb{Z}(H) \in H/\mathbb{Z}(H)$ where $h$ is an element of a finite group $H$

(64) Soluble  
Property of group with an abelian tower whose last element is the trivial group

(65) Insoluble  
Property said of group which is not soluble (see above)
A.2. TERMINOLOGY

Matrices

(66) Monomial matrix square matrix in which each column and each row has exactly one non-zero entry

(67) Unitriangular matrix square matrix with 1s on the main diagonal, and 0s everywhere above (or below) the main diagonal

Linear Groups and Actions

Let $G$ be a subgroup of $\text{GL}(n, \mathbb{F})$ acting on the $n$-dimensional $\mathbb{F}$-vector space $V$

(68) $G$ is reducible there exists a proper non-zero $G$-submodule of $V$

(69) $G$ is irreducible $G$ is not reducible

(70) $G$ is absolutely irreducible $G$ is irreducible over every extension $\mathbb{E}$ of $\mathbb{F}$

(71) $G$ is completely reducible $V = S_1 \oplus \cdots \oplus S_k$, where each $S_i$ is an irreducible $G$-submodule of $V$ (in particular, $G$ is completely reducible if it is irreducible)

(72) Imprimitivity system of $G$ set $\{S_1, \ldots, S_k\}$ of subspaces of $V$ such that $V = S_1 \oplus \cdots \oplus S_k$ and for all $g \in G$ and $1 \leq i \leq k$, $gS_i = S_j$ for some $j$

(73) $G$ is imprimitive there exists an imprimitivity system of $G$ of size at least 2

(74) $G$ is primitive $G$ is irreducible and not imprimitive

(75) $V$ is decomposable (as $G$-module) $V$ is a direct sum of proper $G$-submodules

(76) $V$ is indecomposable (as $G$-module) $V$ is not decomposable

(77) Non-/modular linear group finite subgroup of $\text{GL}(n, \mathbb{F})$ whose order is not divisible/is divisible by the characteristic of $\mathbb{F}$
A.2. TERMINOLOGY

Other

Let $V$ be a vector space and $F$ a field.

(78) Algebraic integer complex number which is a root of a monic polynomial over $\mathbb{Z}$
(note: sums and products of algebraic integers are algebraic integers)

(79) Bilinear form a bilinear mapping $B : V \times V \to F$, i.e.

$B(u_1 + u_2, u_3) = B(u_1, u_3) + B(u_2, u_3)$,
$B(u_1, u_2 + u_3) = B(u_1, u_2) + B(u_1, u_3)$ and
$B(\lambda u_1, u_2) = B(u, \lambda u_2) = \lambda B(u_1, u_2)$,

for all $u_1, u_2, u_3 \in V$ and $\lambda \in F$.

(80) Conformal map $f : U \to V$ s.t. for every two differentiable curves $\gamma_1, \gamma_2 \in U$
defined on an interval $(-\epsilon, \epsilon)$ which intersect at 0, the angle
formed by their tangents at $\gamma_1(0)$ is equal to the angle formed
by tangents to $f \circ \gamma_1$ and $f \circ \gamma_2$ at $f(\gamma_1(0))$

(81) Hermitian form a function $f : V \times V \to \mathbb{C}$ such that

$f(a u_1 + b u_2, u_3) = af(u_1, u_3) + bf(u_2, u_3)$ and
$f(u_1, u_2) = \overline{f(u_2, u_1)}$, $\forall u_1, u_2, u_3 \in V; a, b \in \mathbb{R}$

(82) Lifting (or lift) Let $f$ be a map from an object $X$ to $Y$, and $g$ be a map from
$Z$ to $Y$. Then, a map $h$ from $X$ to $Z$, whereby $g \circ h = f$, is
called a lifting (or lift) of $f$ to $Z$

(83) Quadratic form an homogeneous polynomial of degree two in a number of
variables
Acknowledgements

Firstly, I am indebted to my supervisor Dr. Dane Flannery for all his help, guidance and for sharing his mathematical expertise in the area. I greatly appreciate his contribution to the thesis, especially in the earlier chapters. I thank both the internal examiner Dr. Rachel Quinlan and the external examiner Prof. Eamonn O'Brien for thoroughly going through the thesis and offering helpful suggestions and corrections. In addition, I am grateful to Prof. O'Brien for his examination and testing of the Magma code, and also for his quick response to any coding queries I had. I am much obliged to Prof. Graham Ellis for overseeing the viva and to Dr. David O’Keeffe for helping out with my preparations for the viva presentation.

I owe a debt of gratitude to my parents Ted & Vi, wife Asia and all my friends who offered support during the thesis and withstood my mood swings and mathematical ramblings. It is befitting to also mention my son Liam who entered this world while I was working on the thesis. His addition to my life helped greatly as a distraction away from the work and kept me somewhat sane. Also, I acknowledge my daughter Nadia whose recent birth signals the close of the thesis corrections. Finally, I thank God that I could finally reach the end of this thesis.
Bibliography

[1] S. Beslin and V. de Angelis, *The minimal polynomials of* \( \sin((2\pi)/p) \) *and* \( \cos((2\pi)/p) \), *Math. Mag.* 77 (2004), 146–149.


