ON THE THEORY AND EXAMPLES OF GROUP EXTENSIONS

by

Bernardo Gabriel Rodrigues

Submitted in fulfillment of the academic
requirements for the degree of
Master of Science
in the

School of Mathematics, Statistics and Information Technology
Faculty of Science and Agriculture
University of Natal
Pietermaritzburg.

July 1999

To Verónica and Dulce
and to the memory of my parents

Abstract

The work described in this dissertation was largely motivated by the aim of producing a survey on the theory of group extensions. From the broad scope of the theory of group extensions we single out two aspects to discuss, namely the study of the split and the non-split cases and give examples of both.

A great part of this dissertation is dedicated to the study of split extensions. After setting the background theory for the study of the split extensions we proceed in exploring the ramifications of this concept within the development of the group structure and consequently investigate well known products which are its derived namely the holomorph, and the wreath product. The theory of group presentations provides in principle the necessary tools that permit the description of a group by means of its generators and relators. Through this knowledge we give presentations for the groups of order pq, p^2q and p^3. Subsequently using a classical result of Gaschutz we investigate the split extensions of non-abelian groups in which the normal subgroup is either a non-abelian normal nilpotent group or a non-abelian normal solvable group. We also study other cases of split extensions such as the affine subgroups of the general linear and the symplectic groups. It is expected that some of the results obtained will provide a theoretical algorithm to describe these affine subgroups. A particular case of the non-split extensions is discussed as the Frattini extensions. In fact a simplest example of a Frattini extension is a non-split extension in which the kernel of an epimorphism ϵ is an irreducible G-module.

Preface

The work described in this dissertation was carried out under the supervision and direction of Professor Jamshid Moori, School of Mathematics, Statistics and Information Technology, University of Natal, Pietermaritzburg, from August 1997 to May 1999.

The dissertation represents original work by the author and has not otherwise been submitted in any form for any degree or diploma to any other University. Where use has been made of the work of others it is duly acknowledged in the text.

Acknowledgements

I wish to thank my supervisor, Professor Jamshid Moori, for the advises, encouragement and guidance he has given me during my studies which led to the compilation of this dissertation. I am uncertain as to what extent words like thankfulness and gratitude could express in great detail the relevance of his dedication and devoted attention to me. In the absence of a word or words which could convey my sense of humble gratitude I would like to say it in the way I know best : muito obrigado.

I am grateful for the facilities made available to me by the School of Mathematics, Statistics and Information Systems of the University of Natal, Pietermartizburg. I also wish to express my sincere gratitude to the Department of Mathematics at the University Agostinho Neto in Luanda for making all the contacts with the sponsors of my studies. I gratefully acknowledge the German Embassy in Angola and Professor Otto Berg who have made possible my first encounter with the Deutscher Akademischer Austauschdienst (DAAD) from which I have had my scholarship. Special thanks are also due to the Ministry of Petroleum of the Republic of Angola(bursary), the University of Natal (graduate assistantship). My special thanks go to my fiance Verónica Patricia L. d'Ornelas Sebastião for her unfailing support and enormous patience during my studies. Special thanks are also due to both our families, for enduring me at almost any time but as up to them I would wish to express my thankfulness personally. Finally I would like to thank my roommates Eugene, Faryad, Jan, Petrovious, for creating a pleasant working environment and to all my non mathematics friends Mr Gastão Lukangu and family whose help and comfort I will always keep in mind. Last, but not least my thanks are due to Mrs Meryl Savage whose valuable help and encouragement have paved the way for my understanding of the English language.

Notation and conventions

$\mathbb{N}$	natural numbers
$\mathbb{Z}$	integers
$\mathbb{Q}$	rational numbers
$\mathbb{R}$	real numbers
$\mathbb{C}$	complex numbers
G, N, H, K	groups
1_G	the identity element of G
$H \leq G$	H is a subgroup of G
$N \trianglelefteq G$	N is a normal subgroup of G
$H \cong G$	H is isomorphic to G
$\mathbb{F}$	a field
$\mathbb{F}^*$	$\mathbb{F} - \{0\}$
$\langle x, y \rangle$	the subgroup generated by x and y
$Aut(G)$	the automorphism group of G
$N{\cdot}H$	an extension of N by H
$N{:}H$	a split extension of N by H
h^g	conjugation of h by g
$o(g)$	order of $g \in G$
$C_G(g)$	the centralizer of g in G
$C_G(H)$	the centralizer of the subgroup H in G
$[g]$	a conjugacy class of G with representative g
$N_G(H)$	the normalizer of the subgroup H in G
$\Phi(G)$	the Frattini subgroup of G
$[G, G], G'$	the commutator subgroup of G
gH	the left coset of H in G
X, Y	sets
$\emptyset$	empty set
$\|X\|$	the cardinality of the set X
$GL(n, q)$	general linear group of dimension n over $GF(q)$
$dim(V)$	the dimension of a vector space V

D_{2n}	dihedral group of order $2n$
V_4	the Klein 4 - group
C_p	cyclic group of order p
S_n	the symmetric group on n symbols
$GF(q)$	the Galois field of q elements
$V(n,q)$	a vector space of dimension n over $GF(q)$
$SP(2n,q)$	symplectic group of dimension $2n$ over $GF(q)$
2^n	an elementary abelian group of order 2^n

Contents

Chapter 1

Introduction

The subject matter of this dissertation concerns with the study of the theory of group extensions and the examples for the split and non-split cases. In considering possible programmes to classify groups, two related general problems may be distinguished. On the one hand, there is the problem of *construction*: from a given collection of groups, we build up other groups from them by explicit procedures. On the other hand, there is the problem of *decomposition*: we intend to find out how any given group is built up by procedures from 'simpler' components. The easiest procedure is the direct product construction. The extension problem may be viewed as defining a construction procedure, though unlike the direct product construction, in general this does not lead to a unique type of group.

The fundamental notion underlying the theory of group presentations is that of a free group. From the broad scope of the theory of group presentations we single out two aspects to discuss, namely the study of the presentation of a group extension in general and the presentation of split extension in particular.

It is not immediately clear from the above that the theory of group extensions and the theory of group presentations are closely related. Often both these aspects are treated as distant and unrelated components. An early indication of a unified treatment of these aspects is found in [23]. In this dissertation we offer a perspective from which these relations and certain other classical results emerge naturally as a concatenated whole. It is easy to describe the coverage of this thesis by first referring to chapter 6, in which this perspective first emerges and undergoes considerable development.

Although drawing on results and definitions from a broad spectrum of mathematical fields, this dissertation is concerned principally with the study of the split and the non-split extensions. A general methodological aim of this dissertation has been to illustrate the theory presented as richly as possible with examples.

The preliminary chapter (chapter 2) presents general group theoretical results that will be required in the sequel.

In Chapter 3 we give a generic overview of the theory of group extensions. This chapter constitutes the backbone of the dissertation as a whole. A normal subgroup N of a group G determines a factor group G/N. We write $H = G/N$ and call G extension of N by H. Extension theory concerns with the problem of studying the structure of G using the knowledge about the properties of the two given groups N and H. Thus, the main problem is to find all possible extensions of N by H. Since every group extension is a short exact sequence of groups and homomorphisms, we discuss the background theory of exact sequences and build up to short exact sequences.

Chapter 4 is devoted primarily to an investigation of the structure of a semidirect product. The main result (Theorem 4.1.5) asserts that a semidirect product is equivalent to a split extension. Thus the notions of semidirect product and split extension are used interchangeably to allude to the same entity. We show that the semidirect product may be constructed from groups N and H by taking a homomorphism φ from H into $Aut(N)$ and defining multiplication for G. An important illustration of the semidirect product occur when H equals to $Aut(N)$, and $Aut(N)$ acts naturally on N, giving the holomorph of N. Other important examples of the semidirect product occur in the construction of the wreath products. The wreath product is explicitly represented as a semidirect product in which one group acts on another simply by permuting its factors. Some splitting properties of group extensions are investigated.

In chapter 5 we study the theory of group presentations. Along with the study of the notion of a free group we investigate thoroughly the concepts of presentations, presentations of group extensions and presentations of split extensions, with view of applications in chapter 6.

In chapter 6 we study the non-abelian groups of order pq, p^2q and p^3 respectively. Applying the theory of group presentations we give presentations for these groups and at the same time present some examples of groups of order pq in terms of matrices and permutations.

Chapter 7 concerns with a special type of group extensions. The extensions G for which the Kernel of the epimorphism ϵ is a subgroup of the Frattini subgroup of G. These extensions are known as the Frattini extensions. We derive some new properties from known results of the theory of Frattini extensions.

Yet another special type of extensions occur when the normal subgroup N is the commutator subgroup G' of the group G. These extensions are called commutator extensions and are studied in chapter 8. By reducing the study to the case in which N is an elementary abelian p-group we set the necessary tools to investigate this type of extensions.

Furthermore conditions under which a commutator extension splits are presented.

In chapter 9 we study yet another case of extensions of non-abelian groups. In this extensions the normal subgroup is either a non-abelian nilpotent group or a non-abelian solvable group. We observe that in general if a group G splits over a normal subgroup N the subgroups of G may not necessarily split over their intersections with N. Furthermore a characterization of normal subgroups of G with the property that every subgroup H of G splits over $H \cap N$ is presented. Such subgroups are known as hereditarily non-Frattini subgroups.

Chapter 10 is devoted to the study of the affine subgroups of both the general linear group and the symplectic groups. We start by discussing the general theory of the general linear group. A characterization of the general linear group as split extension is given and at the same time we draw in some results which indicate that the general linear group can be written as a direct product of $SL(n, \mathbb{F})$ and $\mathbb{F}^*$. We describe the affine subgroup of the general linear group as the holomorph of the vector space $\mathbb{F}^n$ over a field $\mathbb{F}$ and provide some examples of isomorphisms between the affine subgroup of the general linear group and the symmetric groups. Further we concentrate on symplectic groups. We discuss the general theory of symplectic groups and their affine subgroups. In the study of the affine subgroups of the general and symplectic linear groups we analyze the results of R. Gow [13] and prove various stated results in that article. One particular affine subgroup $2^3{:}SP(2,2)$ of the symplectic group $SP(4,2)$ has been studied. The symplectic groups are constructed by defining some bilinear form on the underlying vector space and then taking all the form-preserving automorphisms of the space. For further reading and information on symplectic groups, readers are encouraged to consult [9], [13], [14],[18], [19], [24],[26],[27] and [31].

Chapter 2

Preliminaries

The aim of this chapter is to assemble in readily usable form a selection of mostly standard results from the theory of groups which will be required in the sequel. We will not give proofs of every result. Most of the results could be found in standard texts such as [10], [19], [29], [30] and [31].

2.1 Automorphism Groups

Definition 2.1.1 *The* **automorphism group** *of a group G, denoted by $Aut(G)$, is the set of all automorphisms of G, under the binary operation of composition.*

Note 2.1.2 *This operation gives a group structure on $Aut(G)$.*

Definition 2.1.3 *Let g be any element of G. Define a map $\phi_g : G \longrightarrow G$ by $\phi_g(x) = gxg^{-1}$ for all $x \in G$. Then ϕ_g is an automorphism of G, known as an* **inner automorphism** *of G.*

Remark 2.1.4 *We can see that*

(i) $\phi_g(xy) = g(xy)g^{-1} = gxg^{-1}gyg^{-1} = \phi_g(x)\phi_g(y)$,

(ii) $\phi_g(x^{-1}) = gx^{-1}g^{-1}$,

(iii) $[\phi_g(x)]^{-1} = (gxg^{-1})^{-1} = gx^{-1}g^{-1} = \phi_g(x^{-1})$.

Each such a map ϕ_g is actually an automorphism of G. For given $x \in G$ we have that $x = \phi_g(g^{-1}xg)$ and if $\phi_g(x) = \phi_g(y)$ then $gxg^{-1} = gyg^{-1}$ and so $x = y$. We also have that $\phi_{gh}(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = g\phi_h(x)g^{-1} = \phi_g\phi_h(x)$, so $\phi_{gh} = \phi_g\phi_h$ for any $x \in G$ and $g, h \in G$.

Theorem 2.1.5 *(1) If H is a subgroup of G, then $C_G(H) \trianglelefteq N_G(H)$ and $N_G(H)/C_G(H)$ can be embedded in $Aut(H)$, that is, $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$.*

(2) The set of all inner automorphisms of G, denoted by $Inn(G)$ is a normal subgroup of $Aut(G)$ and $G/Z(G) \cong Inn(G)$.

Proof. (1) For each $x \in N_G(H)$, define a map ϕ_x on H by $\phi_x(h) = xhx^{-1}$.

(i) If $\phi_x(h) = \phi_x(g)$ then $xhx^{-1} = xgx^{-1}$, so $h = g$ and hence ϕ_x is injective.

(ii) Since for any $h \in H$ we have that $x^{-1}hx \in H$, because x^{-1} normalizes H and also $\phi_x(x^{-1}hx) = x(x^{-1}hx)x^{-1} = h$. Thus ϕ_x is surjective.

Now it only remains to show that ϕ_x is a homomorphism. But for all g and h in H we have $\phi_x(gh) = xghx^{-1} = xgx^{-1}xhx^{-1} = \phi_x(g)\phi_x(h)$, which implies that ϕ_x is a homomorphism.

The map $\phi : N_G(H) \longrightarrow Aut(H)$ given by $\phi(x) = \phi_x$ is a homomorphism. Since

$$(\phi(x)\phi(y))(h) = \phi(x)(\phi(y)(h)) = \phi(x)(yhy^{-1}) = x(yhy^{-1})x^{-1} = (xy)h(xy)^{-1} = \phi(xy)(h),$$

we have $\phi(x)\phi(y) = \phi(xy)$.

$$\begin{aligned} Ker(\phi) &= \{x \in N_G(H) \mid \phi(x) = 1_H\} \\ &= \{x \in N_G(H) \mid \phi(x)(h) = 1_H(h), \text{ for all } h \in H\} \\ &= \{x \in N_G(H) \mid xhx^{-1} = h, \text{ for all } h \in H\} \\ &= \{x \in N_G(H) \mid xh = hx, \text{ for all } h \in H\} \\ &= C_G(H). \end{aligned}$$

Therefore $C_G(H) \trianglelefteq N_G(H)$ and by the first isomorphism theorem we have that $N_G(H)/C_G(H) \cong Im(\phi)$. Hence $N_G(H)/C_G(H) \cong Im(\phi) \leq Aut(H)$.

(2) If $H = G$, then $N_G(H) = G$ and so $C_G(H) = Z(G)$ and the map ϕ given in part (1) has $Inn(G)$ as its image. Therefore the isomorphism established in (1) is now $G/Z(G) \cong Inn(G)$. To show that $Inn(G) \trianglelefteq Aut(G)$ we must show that if $\rho \in Aut(G)$ and $\phi_g \in Inn(G)$ then $\rho\phi_g\rho^{-1} \in Inn(G)$. We can see that $(\rho\phi_g\rho^{-1})(x) = \rho(\phi_g(\rho^{-1}(x))) = \rho(g\rho^{-1}(x)g^{-1}) = \rho(g)\rho(\rho^{-1}(x))\rho(g^{-1}) = \rho(g)x\rho(g^{-1}) = \phi_{\rho(g)}(x)$ for all $x \in G$. Hence $\rho\phi_g\rho^{-1} = \phi_{\rho(g)}$ for all $x \in G$ and $Inn(G) \trianglelefteq Aut(G)$. □

2.2 Commutator Subgroup

Definition 2.2.1 *Let x and y be elements of a group G. The* **commutator** *of x and y is the element $[x, y] = xyx^{-1}y^{-1}$.*

Definition 2.2.2 *The* **commutator subgroup** *or* **derived subgroup** *of G, denoted by $[G,G]$ or G', is the subgroup of G generated by all commutators.*

So $G' = [G,G] =< [x,y] \mid x,y \in G >$. By recursion, we define $G^{(i+1)}$ as the derived subgroup of $G^{(i)}$ with $G^{(0)} = G$ and $G^{(i+1)} := (G^{(i)})'$. We also write $G^{(2)} = G''$ and $G^{(3)} = G'''$.

Theorem 2.2.3 *Let G be a group. Then*

(i) $G' \trianglelefteq G$.

(ii) G/G' is abelian.

(iii) G is abelian if and only if $G' = \{1_G\}$.

(iv) If N is a normal subgroup of G. Then G/N is abelian if and only if $G' \leq N$.

(v) If $N \leq G$, then $N' \leq G'$.

Proof. See [30]. □

Lemma 2.2.4 *Let $N \trianglelefteq G$. Then $(G/N)' = G'N/N$.*

Proof. Since $(G/N)' =< [gN, hN] \mid g,h \in G >$ and $[gN,hN] = ghg^{-1}h^{-1}N = [g,h]N$, it follows that $(G/N)' = G'N/N$. □

2.3 Solvable and Nilpotent Groups

Definition 2.3.1 *A group G is said to be* **solvable** *if it has a series*

$$\{1_G\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

in which each factor G_{i+1}/G_i is abelian.

Remark 2.3.2 A subgroup H of a group G is called **characteristic** if $\phi(H) = H$ for every automorphism ϕ of G. Solvability can also be characterized by using a particular series which we introduce now. Evidently, $G \geq G' \geq G'' \geq G''' \geq \ldots$, and all $G^{(i)}$ are characteristic subgroups of G. The series of subgroups $G = G^{(0)}, G', G'', \cdots, G^{(i)}, \cdots$ is called the **derived series** of G. Each factor $G^{(i)}/G^{(i+1)}$ is abelian. A group G is solvable if and only if $G^{(k)} = \{1_G\}$ for some k.

Proposition 2.3.3 *[35] Let G be a solvable group. Then*

(i) for any subgroup H of G, H is a solvable group,

(ii) for any normal subgroup N of G, the quotient G/N is solvable.

Proof. See [35]. □

Definition 2.3.4 *A group G is called* **nilpotent** *if it has a series*

$$\{1_G\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

in which each $G_i \lhd G$ and such that G_{i+1}/G_i is contained in the centre of G/G_i for all i.

Remark 2.3.5 Note that by definition a nilpotent group G has a non-trivial centre. Also, every nilpotent group is solvable. There are several group theoretical properties which are equivalent to nilpotency for finite groups. Clearly all abelian groups are nilpotent. All finite p-groups are also nilpotent. The group S_3 is solvable but it is not nilpotent. We can also show that all subgroups and all quotient groups of a nilpotent group are nilpotent. (See [30].)

2.4 Frattini subgroup

Definition 2.4.1 *Let $\mathcal{M}$ be the collection of all maximal subgroups of a group G. The intersection of all elements of $\mathcal{M}$ is called the* **Frattini subgroup** *of G, and is denoted by $\Phi(G)$, that is,*

$$\Phi(G) = \bigcap_{M \in \mathcal{M}} M = \bigcap_{\substack{M \leq G \\ \max}} M.$$

Note 2.4.2 If $G \neq \{1_G\}$ and G is finite, then G certainly has at least one maximal subgroup. Every proper subgroup of G lies in a maximal subgroup of G. If G is infinite, it may have no maximal subgroups. If an infinite group G has no maximal subgroups, then we define $\Phi(G) = G$. If $G = \{1_G\}$, then we define $\Phi(G) = \{1_G\}$.

Remark 2.4.3 Since any automorphism of G, sends a maximal subgroup into a maximal subgroup, the set $\mathcal{M}$ is invariant by any automorphism, and so is $\Phi(G)$. This shows that $\Phi(G)$ is a characteristic subgroup and since characteristic subgroups are normal, we have that $\Phi(G) \trianglelefteq G$.

Lemma 2.4.4 *Let $\alpha : G \longrightarrow \overline{G}$ be an epimorphism. Then $g \in \Phi(G)$ implies that $\alpha(g) \in \Phi(\overline{G})$.*

Proof. Suppose that $g \in \Phi(G)$. Let $\overline{M}$ be an arbitrary maximal subgroup of $\overline{G}$. Then there exists a maximal subgroup M of G such that $\alpha(M) = \overline{M}$. But, then $g \in M$ implies that $\alpha(g) \in \overline{M}$. Since $\overline{M}$ is arbitrary we have that $\alpha(g) \in \Phi(\overline{G})$. □

Remark 2.4.5 For any homomorphism $\alpha : G \longrightarrow \overline{G}$, $\alpha(\Phi(G)) = \Phi(\alpha(G))$.

Definition 2.4.6 *An element x of G is said to be a* **non-generator** *of G if for every subset S of G such that $< S, x >= G$, then $< S >= G$.*

Note 2.4.7 The set of all non-generators of a group G is a subgroup. In Theorem 2.4.8 we will show that the Frattini subgroup of G is the set of all non-generators of G.

Theorem 2.4.8 *[12] For every finite group G the Frattini subgroup of G is the set of all non-generators of G.*

Proof. Let x be a non-generator of G, such that $x \notin \Phi(G)$. Then there exists a maximal subgroup M of G such that $x \notin M$. Then $M \neq < x, M >$ and so $G =< x, M >$. But this implies that $G =< M >= M$, since x is a non-generator of G, which is a contradiction. Therefore $x \in \Phi(G)$.

Conversely, let $x \in \Phi(G)$ and suppose that $G =< x, S >$ with $G \neq < S >$ for some subset S of G. Then there exists a maximal subgroup M of G such that $< S > \leq M$. Since $x \in \Phi(G)$, $x \in M$ and hence $G =< x, S > \leq M$, which is a contradiction. Thus x is a non-generator. □

Corollary 2.4.9 *If $G = \Phi(G)H$ for some subgroup H of G, then $G = H$.*

Proof. If $G = \Phi(G)H$, we have that $G =< \Phi(G), H >$. Now by the Theorem 2.4.8 we obtain that $G =< H >= H$. □

Note 2.4.10 Applying Theorem 2.4.8 we deduce that $G =< x_i \mid 1 \leq i \leq n >$ if and only if $G =< \Phi(G), x_i \mid 1 \leq i \leq n >$.

Corollary 2.4.11 *If $G/\Phi(G)$ is cyclic, then G is cyclic.*

Proof. Choose $x \in G$, such that $x\Phi(G)$ generates $G/\Phi(G)$. Then we have that $G =< x, \Phi(G) >$ and so by the Theorem 2.4.8 we deduce that $G =< x >$. Hence G is cyclic. □

Lemma 2.4.12 *The Frattini subgroup of G has no proper supplement. That is for all proper subgroups M of G we have that $\Phi(G)M \neq G$.*

Proof. If M is a maximal subgroup of G, then $\Phi(G) \leq M$. Hence $\Phi(G)M = M \neq G$. If M is not a maximal subgroup of G then there exists $N \leq G$ a maximal subgroup of G such that $M \leq N$, and so $\Phi(G) \leq N$. So we have that $\Phi(G)N = N$. Now $\Phi(G)M \leq N < G$. Thus $\Phi(G)$ has no proper supplement in G. □

Lemma 2.4.13 *If G is finite, then $\Phi(G)$ is nilpotent.*

Proof. See [30]. □

Lemma 2.4.14 *Let $N \trianglelefteq G$. Then*

(i) $\Phi(G)N/N \leq \Phi(G/N)$.

(ii) If $N \leq \Phi(G)$ then $\Phi(G/N) = \Phi(G)/N$.

Proof. (i) Let K be a maximal subgroup of G/N then $K = M/N$ where M is a maximal subgroup of G and $N \leq M \leq G$. Now $\Phi(G/N) = \bigcap M/N$ with M maximal in G. Since $\Phi(G) \leq M$, we have that $MN \supseteq \Phi(G)N$ and so $\Phi(G)N \leq M$ since $N \leq M$. Hence $\Phi(G)N/N \leq M/N$, for all M maximal in G. Therefore $\Phi(G)N/N \leq \Phi(G/N)$.

(ii) Let π be the natural homomorphism from G onto G/N. Under this homomorphism, there is a one-to-one correspondence between the subgroups of G/N and those subgroups of G containing N. Now $N \leq \Phi(G)$ implies that the maximal subgroups of G containing N correspond to the maximal subgroups of G/N. Hence

$$\begin{aligned}\Phi(G/N) &= \bigcap(M/N), \quad \text{where } M \text{ runs over all maximal subgroups of } G\\ &= (\bigcap M)/N = \Phi(G)/N.\end{aligned}$$

□

Lemma 2.4.15 $\Phi(G/\Phi(G)) = \Phi(G)/\Phi(G) = \{1_G\}$.

Proof. Since $\Phi(G) \trianglelefteq G$, by Lemma 2.4.14 part *(ii)* we have that $\Phi(G/\Phi(G)) = \Phi(G)/\Phi(G) = \{1_G\}$. □

Lemma 2.4.16 *Let $N \trianglelefteq G$ with G finite. Then $N \leq \Phi(G)$ if and only if there is no proper subgroup H of G such that $HN = G$.*

Proof. Assume that $N \leq \Phi(G)$, we need to show that there exists no proper subgroup H of G such that $HN = G$. Let $H < G$. Then there exists a maximal subgroup M of G such that $H \leq M < G$. Since $N \leq \Phi(G)$ then $N \leq M$. Hence $HN \leq M < G$. Thus there is no proper subgroup H of G such that $HN = G$.

Conversely if there is no proper subgroup H of G such that $HN = G$, we want to show that $N \leq \Phi(G)$. Suppose that $N \not\leq \Phi(G)$, then $G \neq \{1_G\}$ and by the definition of Frattini subgroup there exists a maximal subgroup M of G such that $N \not\leq M$. Now $M < MN \leq G$ and maximality of M imply that $MN = G$, which is a contradiction. □

Lemma 2.4.17 (Dedekind's Lemma) *[30] Let H, K, L be subgroups of a group G with $K \subseteq L$. Then $(HK) \cap L = (H \cap L)K$.*

Proof. Since $H \cap L \subseteq H$, then $(H \cap L)K \subseteq HK$. Also $H \cap L \subseteq L$ implies $(H \cap L)K \subseteq LK = L$. Hence $(H \cap L)K \subseteq HK \cap L$. (1)
Now let $x \in (HK) \cap L$. Then $x = hk$ and $x \in L$, for some $k \in K$ and $h \in H$. So $h = xk^{-1} \in LK = L$. Since $H \cap L \subseteq L$, we have that $h \in H \cap L$. Hence $x \in (H \cap L)K$. Thus $(HK) \cap L \subseteq (H \cap L)K$. (2) By (1) and (2) we have that $(HK) \cap L = (H \cap L)K$. □

Lemma 2.4.18 *[3] Let $N \trianglelefteq G$. Then $N \leq \Phi(G)$ if and only if $N/\Phi(N) \leq \Phi(G/\Phi(N))$.*

Proof. We know that $\Phi(N) \trianglelefteq N$, so $N/\Phi(N)$ is a group. Also, if $N \leq \Phi(G)$, then $\Phi(N) \leq \Phi(G)$. Therefore $N/\Phi(N) \leq \Phi(G)/\Phi(N) = \Phi(G/\Phi(N))$, by Lemma 2.4.14. Conversely assume that $N/\Phi(N) \leq \Phi(G/\Phi(N))$. Then since $\Phi(G/\Phi(N)) = \Phi(G)/\Phi(N)$ by Lemma 2.4.14, we must have $N/\Phi(N) \leq \Phi(G)/\Phi(N)$. Thus $N \leq \Phi(G)$. □

Lemma 2.4.19 *Let $H \leq G$ and $N \trianglelefteq G$.*

(i) If $N \leq \Phi(H)$ then $N \leq \Phi(G)$.

(ii) $\Phi(N) \leq \Phi(G)$.

Proof. (i) If $N \nleq \Phi(G)$, then there exists M a maximal subgroup of G such that $N \nleq M$. Now $M < MN \leq G$ and M a maximal subgroup imply that $MN = G$. Since $N \leq \Phi(H)$ we have that $N \leq H \leq MN = G$. By Lemma 2.4.17, since $N \leq MN$ we have that $MN \cap (NH) = N(H \cap MN)$. But $MN \cap (NH) = MN \cap H = H$ and $N(H \cap MN) = N(H \cap M)$ so we have $H = N(H \cap M)$. Now since $N \leq \Phi(H)$, application of Lemma 2.4.16 yields $H = H \cap M$ and so $H \leq M$. Hence $N \leq H \leq M$ implies that $N \leq M$ which is a contradiction.

(ii) Since $\Phi(N)$ is a characteristic subgroup of N and $N \trianglelefteq G$ we have that $\Phi(N)$ is normal in G. Let M be a maximal subgroup of G and suppose that $\Phi(N) \nleq M$. Since $M \leq \Phi(N)M \leq G$, maximality of M implies that $\Phi(N)M = G$. By Lemma 2.4.17 we have that $N = (\Phi(N)M) \cap N = \Phi(N)(M \cap N)$. By Corollary 2.4.9 we have $M \cap N = N$, hence $N \leq M$ and so $\Phi(N) \leq M$. But this is a contradiction with the assumption that $\Phi(N) \nleq M$. Hence $\Phi(N) \leq M$ for any maximal subgroup M of G, therefore $\Phi(N) \leq \Phi(G)$.

□

Lemma 2.4.20 *Let $N_1, N_2, \cdots, N_r$ be normal subgroups of a group G. Then the map*

$$\alpha \; : \; G \longrightarrow (G/N_1) \times \cdots \times (G/N_r)$$

defined by $\alpha(g) = (gN_1, gN_2, \cdots, gN_r)$ is a homomorphism, and its kernel is $\bigcap_{i=1}^{n} N_i$.

Proof. By the definitions of quotient groups and direct products we have that

$$\begin{aligned}\alpha(gg') &= (gg'N_1, gg'N_2, \cdots, gg'N_r)\\ &= (gN_1, gN_2, \cdots, gN_r)(g'N_1, g'N_2, \cdots, g'N_r) = \alpha(g)\alpha(g')\end{aligned}$$

and so α is a homomorphism. Furthermore $\alpha(g) = (N_1, N_2, \cdots, N_r)$, is the identity of $G/N_1 \times G/N_2 \times \cdots \times G/N_r$ if and only if $g \in N_i$ for all $i = 1, 2, \cdots, r$ and therefore $Ker(\alpha) = \bigcap_{i=1}^{n} N_i$. □

Lemma 2.4.21 *[10] Let $G_1, G_2, \cdots, G_r$ be finite groups. Then $\Phi(G_1 \times G_2 \cdots \times G_r) = \Phi(G_1) \times \Phi(G_2) \times \cdots \times \Phi(G_r)$.*

Proof. Let $D = G_1 \times G_2 \times \cdots \times G_r$ and identify G_i with the subgroup $1 \times 1 \times \cdots \times G_i \times \cdots \times 1$ of D. Since $G_i \trianglelefteq D$, by Lemma 2.4.19 part (ii) we have that $\Phi(G_i) \leq \Phi(D)$, and so $\Phi(G_1) \times \Phi(G_2) \times \cdots \times \Phi(G_r) \subseteq \Phi(D)$. (1)

Let $K_i = G_1 \times G_2 \times \cdots \times G_{i-1} \times 1 \times G_{i+1} \times \cdots \times G_r$. Since $K_i \trianglelefteq D$, we have that $\Phi(D)K_i/K_i \leq \Phi(D/K_i)$, $i = 1, 2, \cdots, r$. Since $D/K_i = G_iK_i/K_i \cong G_i$ and $\Phi(D)K_i/K_i \cong \Phi(D)/\Phi(D) \cap K_i$, we have that $\Phi(D)/\Phi(D) \cap K_i$ is isomorphic to a subgroup of $\Phi(G_i)$. Thus $|\Phi(D)/\Phi(D) \cap K_i| \leq |\Phi(G_i)|$. Since $\bigcap_{i=1}^{r} K_i = 1$, then by Lemma 2.4.20 we have that $\Phi(D)$ is isomorphic to a subgroup of the direct product of r groups $\Phi(D)/(\Phi(D) \cap K_i)$. Hence $|\Phi(D)| \leq \Pi_{i=1}^{r}|\Phi(G_i)| = |\Phi(G_1) \times \Phi(G_2) \times \cdots \times \Phi(G_r)|$. (2) Now (1) and (2) imply that $\Phi(G_1 \times G_2 \times \cdots \times G_r) = \Phi(G_1) \times \Phi(G_2) \times \cdots \times \Phi(G_r)$. □

Theorem 2.4.22 *The Frattini factor group $G/\Phi(G)$ of a finite p-group G is an elementary abelian p-group. Furthermore, $G/\Phi(G)$ is a vector space over $\mathbf{Z}_p$.*

Proof. Let $\mathcal{M}$ denote the set of all maximal subgroups of G. Since G is a p-group, $\forall M \in \mathcal{M}$ we have that $M \trianglelefteq G$ and G/M is a cyclic p-group of order p. Furthermore $G' \leq M$ for all $M \in \mathcal{M}$. Thus $G' \leq \Phi(G)$. Since G/M is a cyclic group of order p for all $M \in \mathcal{M}$, we have $x^p \in M$ for all $M \in \mathcal{M}$. Thus we deduce that $x^p \in \Phi(G)$ for all $x \in G$. Hence $(x\Phi(G))^p = \Phi(G)$ $\forall x \in G$. So $G/\Phi(G)$ is an elementary abelian p-group. Thus $G/\Phi(G)$ can be regarded as a vector space over $\mathbf{Z}_p$. □

Lemma 2.4.23 *Let G be a finite p-group. Then $\Phi(G) = \{1_G\}$ if and only if G is elementary abelian.*

Proof. We may assume that $G \neq \{1_G\}$. Suppose first that G is elementary abelian. Since $G \neq \{1_G\}$, then $\Phi(G) < G$ by the definition of $\Phi(G)$. Moreover, since $G \neq \{1_G\}$ and G is elementary abelian then G is characteristically simple by Theorem 7.41 of page 143 in [30]. Now, since $\Phi(G)$ is a proper characteristic subgroup of G we have that $\Phi(G) = \{1_G\}$. Conversely suppose that $\Phi(G) = \{1_G\}$. Since G is a finite p-group, by Theorem 2.4.22

$G/\Phi(G)$ is an elementary abelian p-group. Since $G/\Phi(G) = G/\{1_G\} \cong G$, the proof follows. □

Theorem 2.4.24 *Let G be a finite p-group and let $G^p =< x^p : x \in G >$. Then*

(i) $\Phi(G) = G'G^p$,

(ii) if $p = 2$, *then* $\Phi(G) = G^2$,

(iii) if $N \leq G$, *then* $\Phi(N) \leq \Phi(G)$, *in particular, if* $N \trianglelefteq G$, *then* $\Phi(G)N/N = \Phi(G/N)$.

Proof. (i) By Theorem 2.4.22 we have that every maximal subgroup of G contains all p-th powers and all commutators. Thus $G'G^p \subseteq \Phi(G)$. Obviously $G'G^p \trianglelefteq G$ and since $G/G'G^p$ is an abelian group of exponent p, $G/G'G^p$ is an elementary abelian p-group. By Lemma 2.4.23 we have that $\Phi(G/G'G^p) = \{1_G\}$. Now since $G'G^p \leq \Phi(G)$ we have that $\{1_G\} = \Phi(G/G'G^p) = \Phi(G)/G'G^p$ by Lemma 2.4.14 part (ii). Hence $\Phi(G) = G'G^p$.

(ii) By part (i) it suffices to show that $G' \leq G^2$. Let $x, y \in G$. Then $[x,y] = x^{-1}y^{-1}xy = x^{-1}y^{-2}xx^{-2}xyxy = x^{-1}y^{-2}xx^{-2}(xy)^2 = (x^{-1}y^{-1}x)^2x^{-2}(xy)^2 \in G^2$. Therefore $G' \leq G^2$, and hence $\Phi(G) = G'G^2 = G^2$.

(iii) Let $N \leq G$ then N is a p-group. By (i) we have that $\Phi(N) = N'N^p \leq G'G^p = \Phi(G)$. Now, let $N \trianglelefteq G$. Since G is a p-group we have that G/N is also a p-group. By applying part (i) and Lemma 2.4.14 we get $\Phi(G/N) = (G/N)'(G/N)^p = (G'N/N)(G^p/N) = G'NG^p/N = G'G^pN/N = \Phi(G)N/N$.

□

Theorem 2.4.25 *For every (possibly infinite) group G we have $G' \cap Z(G) \leq \Phi(G)$.*

Proof. Let $F = G' \cap Z(G)$. If $F \nleq \Phi(G)$ then there exists a maximal subgroup M of G, with $F \nleq M$. Therefore $M < MF < G$ and so maximality of M implies that $MF = G$. Then each $g \in G$ has a factorization $g = mf$ where $m \in M$ and $f \in F$. Since $f \in Z(G)$, $gMg^{-1} = (mf)M(mf)^{-1} = mfMf^{-1}m^{-1} = mMm^{-1} = M$, and hence $M \trianglelefteq G$. Since M is maximal, G/M has prime power order and hence is abelian. Thus $G' \leq M$. But $F \leq G' \leq M$ implies that $F \leq M$ which is a contradiction. □

Theorem 2.4.26 *Let N be a finite group. If there exists a group G with $N \trianglelefteq G$ and $N \leq \Phi(G)$, then $Inn(N) \leq \Phi(Aut(N))$.*

Proof. See Theorem 2.2.6 of page 404 in [8]. □

The converse of Theorem 2.4.26 has been an open problem for many years. It has been proved recently by Bettina Eick in [11].

Theorem 2.4.27 *[11] Let N be a finite group. If $Inn(N) \leq \Phi(Aut(N))$, then there exists a finite group G with $N \trianglelefteq G$ and $N \leq \Phi(G)$.*

Proof. See Theorem 5 of [11]. □

Chapter 3

Group Extensions: An overview

In this chapter we present all the basic definitions and results of group extensions which will be required later. If G is a finite group having a normal subgroup N, then we can factorize G into two groups, namely N and G/N. Extension theory concerns with the problem of studying the structure of an extension G of N by H using the knowledge about the properties of the groups N and $G/N \cong H$. Thus the main problem consists in finding all possible extensions of N by H.

3.1 Exact Sequences and Extensions

Definition 3.1.1 *If N and H are two groups, then an* **extension** *of the group N by the group H is a group G having a normal subgroup $K \cong N$ and $G/K \cong H$. We denote an extension G of N by H, by $G = N{\cdot}H$.*

Let ϕ and ψ be the isomorphisms described in Definition 3.1.1. Consider $N \xrightarrow{\phi} \mathrm{K} \xrightarrow{i} G$ and $G \xrightarrow{\pi} \mathrm{G/K} \xrightarrow{\psi} H$, where i is the inclusion map and π is the natural homomorphism. Let $\alpha = i \circ \phi$ and $\beta = \psi \circ \pi$. Then we have that $\{1_N\} \longrightarrow \mathrm{N} \xrightarrow{\alpha} \mathrm{G} \xrightarrow{\beta} \mathrm{H} \longrightarrow \{1_H\}$ where α and β satisfy:

$$\begin{aligned} Ker(\alpha) &= \{n \in N \mid \alpha(n) = 1_G\} = \{n \in N \mid (i \circ \phi)(n) = 1_G\} \\ &= \{n \in N \mid \phi(n) = 1_G\} = Ker(\phi) = \{1_N\}, \end{aligned}$$

$Im(\alpha) = \{(i \circ \phi)(n) \mid n \in N\} = \{\phi(n) \mid n \in N\} = Im(\phi) = K,$

$$\begin{aligned} Ker(\beta) &= \{g \in G \mid \beta(g) = 1_H\} = \{g \in G \mid (\psi \circ \pi)(g) = 1_H\} = \{g \in G \mid \psi[\pi(g)] = 1_H\} \\ &= \{g \in G \mid \psi(gK) = 1_H\} = \{g \in G \mid gK = K\} = K = Im(\alpha) \end{aligned}$$

and $Im(\beta) = \{\beta(g) \mid g \in G\} = \{\psi(gK) \mid g \in G\} = Im(\psi) = H.$

Definition 3.1.2 *Let $\{N_n\}$ be a sequence of groups and $\{\alpha_n\}$ a sequence of homomorphisms from N_{n-1} into N_n Then we call*

$$\cdots \xrightarrow{\alpha_{n-1}} N_{n-1} \xrightarrow{\alpha_n} N_n \xrightarrow{\alpha_{n+1}} N_{n+1} \rightarrow \cdots \quad (*)$$

a sequence of groups and homomorphisms. We say that the sequence $(*)$ is **exact** *if $ker(\alpha_n) = Im(\alpha_{n-1})$ for each successive pair (α_{n-1}, α_n).*

Definition 3.1.3 *A* **short exact sequence** *of groups and homomorphisms is an exact sequence of the form $\{1_N\} \rightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \rightarrow \{1_H\}$.*

Remark 3.1.4 The conditions of exactness at N, G and H respectively asserts that $Ker(\alpha) = \{1_N\}, Im(\alpha) = Ker(\beta)$ and $Im(\beta) = H$ which is a restatemet of what we have discussed above. Thus the notion of group extensions and short exact sequences are the same and so we can define an extension as follows:

Definition 3.1.5 *If $\{1_N\} \rightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \rightarrow \{1_H\}$ is a short exact sequence, then we say that G is an extension of N by H.*

Remark 3.1.6 If G is an extension of N by H given by the short exact sequence $\{1_N\} \rightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \rightarrow \{1_H\}$, then $G/\alpha(N) = G/Ker(\beta) \cong H$ and $\alpha(N) \cong N$.

Theorem 3.1.7 *Let A and B be groups, α_1, α_2 and α_3 be homomorphisms. Then*
(i) the homomorphism $A \xrightarrow{\alpha_2} B$ is one-to-one iff the sequence $\{1\} \xrightarrow{\alpha_1} A \xrightarrow{\alpha_2} B$ is exact,
(ii) the homomorphism $A \xrightarrow{\alpha_2} B$ is onto iff the sequence $A \xrightarrow{\alpha_2} B \xrightarrow{\alpha_3} \{1\}$ is exact,
(iii) the homomorphism $A \xrightarrow{\alpha_2} B$ is an isomorphism iff the sequence $\{1\} \xrightarrow{\alpha_1} A \xrightarrow{\alpha_2} B \xrightarrow{\alpha_3} \{1\}$ is exact.

Proof. (i) Suppose that the sequence $\{1\} \xrightarrow{\alpha_1} A \xrightarrow{\alpha_2} B$ is exact. Then $ker(\alpha_2) = Im(\alpha_1)$. However $Im(\alpha_1) = \{1\}$. Thus $ker(\alpha_2) = \{1\}$ and hence α_2 is one-to-one. Conversely suppose that $A \xrightarrow{\alpha_2} B$ is one-to-one. Then $ker(\alpha_2) = \{1\}$. However from the sequence $\{1\} \xrightarrow{\alpha_1} A \xrightarrow{\alpha_2} B$ we have that $Im(\alpha_1) = \{1\} = ker(\alpha_2)$ and hence the sequence is exact.

(ii) Suppose that $A \xrightarrow{\alpha_2} B \xrightarrow{\alpha_3} \{1\}$ is exact. Then $ker(\alpha_3) = Im(\alpha_2)$. However $ker(\alpha_3) = B$ and thus $Im(\alpha_2) = B$ and hence α_2 is onto. Conversely suppose that $A \xrightarrow{\alpha_2} B$ is onto. Then we have that $Im(\alpha_2) = B$. However from $A \xrightarrow{\alpha_2} B \xrightarrow{\alpha_3} \{1\}$, we obtain that $ker(\alpha_3) = B = Im(\alpha_2)$. Hence the sequence is exact.

(iii) Suppose that $\{1\} \xrightarrow{\alpha_1} A \xrightarrow{\alpha_2} B \xrightarrow{\alpha_3} \{1\}$ is exact. Then $ker(\alpha_2) = Im(\alpha_1) = \{1\}$. Thus α_2 is one-to-one. Also from the exactness of sequence we have that $ker(\alpha_3) = B = Im(\alpha_2)$. Hence α_2 is onto and hence an isomorphism. Conversely suppose that α_2 is an isomorphism. Then we obtain that $ker(\alpha_2) = \{1\}$ and $Im(\alpha_2) = B$. Thus from the sequence $\{1\} \xrightarrow{\alpha_1} A \xrightarrow{\alpha_2} B \xrightarrow{\alpha_3} \{1\}$ we obtain that $ker(\alpha_2) = \{1\} = Im(\alpha_1)$ and $Im(\alpha_2) = B = Ker(\alpha_3)$ and hence the sequence is exact. □

Lemma 3.1.8 (Five Lemma) *[20]*

Let

$$\begin{tikzcd}
A_0 \arrow[r, "\alpha_0"] \arrow[d, "\phi_0"] & A_1 \arrow[r, "\alpha_1"] \arrow[d, "\phi_1"] & A_2 \arrow[r, "\alpha_2"] \arrow[d, "\phi_2"] & A_3 \arrow[r, "\alpha_3"] \arrow[d, "\phi_3"] & A_4 \arrow[d, "\phi_4"] \\
B_0 \arrow[r, "\beta_0"] & B_1 \arrow[r, "\beta_1"] & B_2 \arrow[r, "\beta_2"] & B_3 \arrow[r, "\beta_3"] & B_4
\end{tikzcd}$$

be a commutative diagram of groups and homomorphisms with exact rows. If ϕ_0, ϕ_1, ϕ_3 and ϕ_4 are isomorphisms, then so is ϕ_2.

Proof. We have to show that ϕ_2 is a one-to-one and onto homomorphism.

(i) ϕ_2 is one-to-one: Let $x \in Ker(\phi_2)$. Then $\phi_2(x) = 1_{B_2}$ and $\beta_2(\phi_2(x)) = 1_{B_3}$. Therefore we have that $\beta_2(\phi_2(x)) = \phi_3(\alpha_2(x)) = 1_{B_3}$ by commutativity. Hence $\alpha_2(x) = 1_{A_3}$, since ϕ_3 is one-to-one. Then $x \in Ker(\alpha_2)$. Hence there exists $y \in A_1$ such that $\alpha_1(y) = x$ (exactness at A_2) and $1_{B_3} = \phi_2(\alpha_1(y)) = \phi_2(x) = \beta_1(\phi_1(y))$ implies that $\phi_1(y) \in Ker(\beta_1)$. So $\phi_1(y) \in B_1$ and the exactness at B_1 implies that there exists $w \in B_0$ such that $\beta_0(w) = \phi_1(y)$. Since ϕ_0 is onto, there exists $j \in A_0$ such that $\phi_0(j) = w$. Then $\phi_1(y) = \beta_0(w) = \beta_0(\phi_0(j)) = \phi_1(\alpha_0(j))$ by commutativity. Since ϕ_1 is one-to-one then we have $\alpha_0(j) = y$. Now exactness at A_1 implies that $y \in Ker(\alpha_1)$, and so $\alpha_1(y) = 1_{A_2}$. Hence $x = 1_{A_2}$. Therefore $Ker(\phi_2) = \{1\}$ and hence ϕ_2 is one-to-one.

(ii) ϕ_2 is onto: Let $x \in B_2$, then there exists $y \in A_3$ such that $\phi_3(y) = \beta_2(x)$. Since $\beta_3(\beta_2(x)) = 1_{B_4}$ by exactness at B_4, $\beta_3[\phi_3(y)] = 1_{B_3}$. We get $\phi_4[\alpha_3(y)] = 1_{B_4}$ by commutativity and therefore $\alpha_3(y) = 1_{A_4}$, since ϕ_4 is an isomorphism. Thus $y \in Ker(\alpha_3)$ and there exists $z \in A_2$ such that $\alpha_2(z) = y$ by the exactness at A_3. Now we have $\beta_2(\phi_2(z)) = \phi_3(\alpha_2(z)) = \phi_3(y) = \beta_2(x)$. Therefore $\beta_2(\phi_2(z)(x^{-1})) = 1_{B_3}$ and hence $\phi_2(z)(x^{-1}) \in Ker(\beta_2)$. Now the exactness at B_2 implies that there exists $w \in B_1$ such that $\beta_1(w) = \phi_2(z)(x^{-1})$. Since ϕ_1 is onto, there exists $j \in A_1$ such that $\phi_1(j) = w$. Then we have $\phi_2(z)(x^{-1}) = \beta_1(w) = \beta_1(\phi_1(j)) = \phi_2(\alpha_2(j))$ by commutativity. Hence $x = [\phi_2(\alpha_2(j))]^{-1}.\phi_2(z) = \phi_2([\alpha_2(j)]^{-1}).\phi_2(z) = \phi_2(\alpha_2(j^{-1})z)$ and so ϕ_2 is onto, thus an isomorphism. □

Definition 3.1.9 *An extension $\{1_N\} \to N \xrightarrow{\alpha} G \xrightarrow{\beta} H \to \{1_H\}$ is said to be* **equivalent** *to an extension $\{1_N\} \to N \xrightarrow{\alpha_1} \overline{G} \xrightarrow{\beta_1} H \to \{1_H\}$ if there exists a homomorphism $\phi : G \longrightarrow \overline{G}$ such that the diagram*

$$\begin{tikzcd} N \arrow[r, "\alpha"] \arrow[dr, "\alpha_1"'] & G \arrow[r, "\beta"] \arrow[d, "\phi"] & H \\ & \overline{G} \arrow[ur, "\beta_1"'] & \end{tikzcd}$$

commutes.

Remark 3.1.10 If G and $\overline{G}$ are equivalent extensions, then by using the *five lemma* it can be shown that ϕ is an isomorphism between $\overline{G}$ and G. It is also very easy to prove that the equivalence of group extensions given in Definition 3.1.9 is an equivalence relation. We should also mention that equivalent extensions are isomorphic, but isomorphic extensions need not be equivalent. (See example 2 of page 221 of [35].)

Definition 3.1.11 *An extension* $\{1_N\} \to N \xrightarrow{\alpha} G \xrightarrow{\beta} H \to \{1_H\}$ *is called*

(i) abelian if G *is abelian,*

(ii) central if $Im(\alpha) = \alpha(N) \subset Z(G)$,

(iii) cyclic if H *is cyclic,*

(iv) split if there is a monomorphism $\lambda : H \longrightarrow G$ *such that* $\beta\lambda = I_H$.

Remark 3.1.12 If an extension is abelian, central or cyclic, then so is every equivalent extension. In Theorem 4.1.7 we prove that if an extension splits, then so does any equivalent extension.

Chapter 4

Semidirect Product

The focus of this chapter relates to the splitting extensions of finite groups which internally leads to the splitting of a group over a normal subgroup. For structural purposes, this appears to be the most natural approach for the decomposition of a group in that only the normal subgroup and a subgroup of its automorphism group is needed in order to effect the extension, the so-called *semidirect product.* We note that other well known products such as the holomorph and the wreath product derive from the semidirect product. So, we will explore the ramifications of this concept within the development of group structure.

4.1 Semidirect Product and Split Extensions

Definition 4.1.1 *A group G is a* **semidirect product** *of a subgroup N by a subgroup H, if the following conditions are satisfied:*

(i) $G = NH$,

(ii) $N \trianglelefteq G$,

(iii) $N \cap H = \{1_G\}$.

The subgroups N and H are said to be *complementary.* We use the notation $G = N{:}H$ for a semidirect product G of N by H. The notation $N{:}^{\varphi}H$ is also used to denote the semidirect product of N by H, this notation will be justified in the course of the discussion.

Remark 4.1.2 In contrast to a direct product, a semidirect product of N by H is not determined up to isomorphism by the two subgroups. However, the semidirect product depend on how N is normal in G.

Let $G = N : H$. Then we make the following observations.

(1) We have that $H = H/(N \cap H) \cong HN/N = G/N$ by the second isomorphism theorem. Consequently, if G is finite we have that $|G| = |N||G/N| = |N||H|$.

(2) Since $G = NH$, each $x \in G$ can be written as $x = nh$ for $n \in N$ and $h \in H$. Suppose that this could be done in two different ways, that is, suppose $x = n_1h_1$ and $x = n_2h_2$ for some $n_1, n_2 \in N$ and $h_1, h_2 \in H$, then we would have
$n_2^{-1}n_1 = h_2h_1{}^{-1} \in N \cap H = \{1_G\}$, forcing $n_1 = n_2$ and $h_1 = h_2$. Hence each $x \in G$ has a unique expression $x = nh$ where $n \in N$ and $h \in H$.

(3) Let $x, y \in G$ and write $x = n_1h_1$ and $y = n_2h_2$. We know that the element xy of G can be written as $n'h'$ for some unique $n' \in N$ and $h' \in H$, by (2), so explicitly we have $xy = n_1h_1n_2h_2 = n_1h_1n_2h_1{}^{-1}h_1h_2$ where $n' = n_1h_1n_2h_1{}^{-1} \in N$, since $N \trianglelefteq G$ and $h' = h_1h_2 \in H$.

(4) Let $h \in H$. Since $N \trianglelefteq G$, conjugation by h maps N to N. Consequently we can define a map $\varphi_h : N \longrightarrow N$ given by $\varphi_h(n) = hnh^{-1}$ for $n \in N$ and $h \in H$. The map φ_h is an automorphism of N.

φ_h is onto: For any $x \in N$, $x = \varphi_h(h^{-1}xh)$.
φ_h is one-to-one: If $\varphi_h(x) = \varphi_h(y)$, then $hxh^{-1} = hyh^{-1}$ so $x = y$
φ_h is a homomorphism: For any $x, y \in N$ and $h \in H$ we have

$$\varphi_h(xy) = h(xy)h^{-1} = hxh^{-1}hyh = (hxh^{-1})(hyh^{-1}) = \varphi_h(x)\varphi_h(y).$$

Also for any $g, h \in H$ we have

$$(\varphi_g\varphi_h)(x) = \varphi_g(\varphi_h(x)) = \varphi_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = ghx(gh)^{-1} = \varphi_{gh}(x).$$

Hence $\varphi_g\varphi_h = \varphi_{gh}$. In this way we have constructed a homomorphism $\varphi : H \longrightarrow Aut(N)$ where $\varphi(h) = \varphi_h$. The homomorphism φ is called the **conjugation homomorphism** of the semidirect product G. It can be seen from this that $(n_1h_1)(n_2h_2) = n_1\varphi_{h_1}(n_2)h_1h_2$ for any $n_1, n_2 \in N$ and $h_1, h_2 \in H$. Thus the group operation of G can be expressed in terms of the group operations of N and H and the homomorphism φ.

(5) If the homomorphism $\varphi : H \longrightarrow Aut(N)$ defined by $\varphi(h) = \varphi_h$ is the trivial homomorphism, then we have $nhn^{-1} = n\varphi_h(n^{-1})h = nn^{-1}h = h$ for any $n \in N$ and $h \in H$ and consequently $H \trianglelefteq G$, therefore $G = N \times H$. Conversely, if $G = N \times H$, then the elements of H commute with the elements of N and so the homomorphism φ must be trivial.

(6) If the conjugation homomorphism $\varphi : H \longrightarrow Aut(N)$ is non-trivial, then the group G must be non-abelian. Because there must be some $h \in H$ and $n \in N$ such that $hnh^{-1} = \varphi_h(n) \neq n$, in which case h and n do not commute.

Definition 4.1.3 *Given groups N and H and a homomorphism $\varphi : H \longrightarrow Aut(N)$, define $G = N{:}^{\varphi}H$ to be the set of all ordered pairs $(n,h) \in N \times H$ equipped with the operation*

$$(n,h)(n',h') := (n\varphi_h(n'), hh').$$

Lemma 4.1.4 *If $N \trianglelefteq G$, and $H \leq G$ then the following statements are equivalent:*

(i) G is a semidirect product of N by H,

(ii) every element $g \in G$ has a unique expression $g = nh$, where $n \in N$, and $h \in H$,

(iii) there exists a homomorphism $\lambda : H \longrightarrow G$, with $\phi\lambda = I_H$, where $\phi : G \longrightarrow H$ is the natural homomorphism,

(iv) there exists a homomorphism $\pi : G \longrightarrow G$, with $Ker(\pi) = N$ and $\pi(x) = x$ for all $x \in Im(\pi)$.

Proof. See Lemma 7.20 of [31]. □

Theorem 4.1.5 *A short exact sequence $\{1_N\} \rightarrow N \rightarrow G \xrightarrow{\pi} H \rightarrow \{1_H\}$ splits if and only if G is the semidirect product of N by H_1, where $H_1 \leq G$ and $H_1 \cong H$ with $\pi(H_1) = H$.*

Proof. Suppose that $\{1_N\} \rightarrow N \rightarrow G \xrightarrow{\pi} H \rightarrow \{1_H\}$ splits. Then there exists a homomorphism $\lambda : H \longrightarrow G$, such that $\pi\lambda = I_H$. Now

$$\begin{aligned} \lambda(x) = \lambda(y) &\Rightarrow \pi(\lambda(x)) = \pi(\lambda(y)) \\ &\Rightarrow (\pi\lambda)(x) = (\pi\lambda)(y) \\ &\Rightarrow x = y. \end{aligned}$$

So that λ is a monomorphism. Hence $H/Ker(\lambda) \cong Im(\lambda)$ which implies that $H \cong Im(\lambda)$. Thus $\lambda : H \longrightarrow Im(\lambda)$ is an isomorphism. Let $H_1 = Im(\lambda)$. Since $Ker(\pi) = N$ and $H_1 = Im(\lambda) \leq G$ we have that $N \cap H_1 = \{1_G\}$. We need to show that $NH_1 = G$. Since $N \trianglelefteq G$, $NH_1 \leq G$. Let $g \in G$. Then $\pi(g) \in H$ and $\lambda(\pi(g)) \in Im(\lambda) = H_1$. Since

$$\pi(\lambda(\pi(g))) = \pi\lambda(\pi(g)) = I_H(\pi(g)) = \pi(g),$$

we have $g.[\lambda\pi(g)]^{-1} \in Ker(\pi) = N$. Hence there exists $n \in N$ such that $g.[\lambda\pi(g)]^{-1} = n$. Then we get $g = n[\lambda\pi(g)] \in NH_1$. So $G \subseteq NH_1$ and hence $G = NH_1$. Hence G is a semidirect product of N by H_1.

Conversely, suppose that G is the semidirect product of N by H_1 a subgroup of G with $H_1 \cong H$. We need to show that $\{1\} \rightarrow N \rightarrow G \xrightarrow{\pi} H \rightarrow \{1\}$ splits. Since G is a semidirect product of N by H_1, then $G = NH_1$ and $N \cap H_1 = \{1\}$ and so the elements of H_1 form a right transversal (a complete set of coset representatives of N in G) of N in G. It follows that the restriction $\pi|_{H_1} : H_1 \longrightarrow H$, given by $(\pi|_{H_1})(h_1) = \pi(h_1)$, for all $h_1 \in H_1$ is an isomorphism. So there exists a homomorphism λ, from H to G given by

$$H \overset{(\pi|_{H_1})^{-1}}{\rightarrow} H_1 \overset{inc}{\rightarrow} G.$$

It is easily seen that

$$(\pi\lambda)(h) = \pi(\lambda(h)) = \pi[inc((\pi|_{H_1})^{-1}(h))] = \pi[(\pi|_{H_1})^{-1}(h)] = \pi(h_1) = h,$$

for all $h \in H$. Hence $\pi\lambda = I_H$. □

Note 4.1.6 From the above theorem, we have that every split extension G of N by H is equivalent to a semidirect product of N by H. Hence the terms split extension and semidirect product can be used interchangeably to mean one and the same entity.

Theorem 4.1.7 *[34] If an extension splits, then so does any equivalent extension.*

Proof. Let $\{1\} \rightarrow N \overset{\alpha}{\rightarrow} G \overset{\beta}{\rightarrow} H \rightarrow \{1\}$ be a split extension such that it is equivalent to the extension $\{1\} \rightarrow N \overset{\alpha_1}{\rightarrow} \overline{G} \overset{\beta_1}{\rightarrow} H \rightarrow \{1\}$. Let θ be the homomorphism that gives the equivalence. Then there is a monomorphism $\lambda : H \longrightarrow G$ such that $\beta\lambda = I_H$. Let $\lambda_1 = \theta\lambda$, then $\lambda_1 : H \longrightarrow \overline{G}$ is a monomorphism such that $\beta_1\lambda_1 = \beta_1\theta\lambda = \beta\lambda = I_H$. □

Remark 4.1.8 It is obvious that $NH = G$ implies that $HN = G$ so that N is a complement of H. An extension G of N by H is a semidirect product of N by H, if and only if $N \trianglelefteq G$ and N has a complement (necessarily isomorphic to H). A subgroup N of G, may not have a complement, and even if it does, a complement need not to be unique. If both subgroups N and H are normal in G, then G is a direct product of N and H.

Definition 4.1.9 *Let G, N and H be as in Definition 4.1.3 and $\varphi : H \longrightarrow Aut(N)$. Then the semidirect product G of N by H is said to* **realize** *φ if $\varphi_h(n) = n^h$ for all $n \in N$, $h \in H$.*

Theorem 4.1.10 *Let N and H be groups, $\varphi \in Hom(H, Aut(N))$. Then $G = N{:}^{\varphi}H$ is a semidirect product of N by H that realizes φ.*

Proof. See Theorem 7.22 of [31]. □

Theorem 4.1.11 *If G is a semidirect product of N by H, then $G \cong N{:}^{\varphi}H$ for some homomorphism $\varphi : H \longrightarrow Aut(N)$.*

Proof. Define $\varphi_h(n) = hnh^{-1}$. We know that each element $g \in G$ has a unique expression $g = nh$ with $n \in N$ and $h \in H$. Since multiplication in G satisfies $(nh)(n'h') = n(hn'h^{-1})hh' = nn'^{h}hh'$, it is easy to see that the map $\alpha : N{:}^{\varphi}H \longrightarrow G$, given by $\alpha(n,h) = nh$, is an isomorphism. For any $n, n' \in N$ and $h, h' \in H$ if $\alpha(n,h) = \alpha(n',h')$, then $nh = n'h'$. That is, $n'^{-1}n = h'h^{-1} \in N \cap H = \{1_G\}$. So $n'^{-1}n = 1_G$ and $h'h^{-1} = 1_G$. Hence $n = n'$ and $h' = h$, so that α is injective. Also, since $Im(\alpha) = \{\alpha(n,h) \mid n \in N \text{ and } h \in H\} = \{nh \mid n \in N \text{ and } h \in H\} = NH = G$ we have that α is onto. Finally we need to show that α is a homomorphism. For $n, n' \in N$ and h, h' we have that

$$\begin{aligned} \alpha[(n,h)(n',h')] &= \alpha(n\varphi_h(n'), hh') = \alpha(nhn'h^{-1}, hh') = nhn'h^{-1}hh' = nhn'h' \\ &= \alpha(n,h)\alpha(n',h'). \end{aligned}$$

Hence α is an isomorphism. □

As an illustration of the preceding discussion, we shall prove in the next example that, there exists only one non-abelian group of order 16 of the type $C_4 : C_4$.

Example 4.1.12 *There exists only one non-abelian group of order 16 of the type $C_4 : C_4$.*

Proof. Assume that $G = C_4 : C_4$. Then $C_4 \trianglelefteq G$ and $C_4 \cap C_4 = \{1_G\}$. Define $f_i : C_4 \longrightarrow C_4$ by $f_i(x) = x^i$, with $(i,4) = 1$. Also we have that

$$Aut(C_4) = \{f_i \mid f_i(x) = x^i,\ (i\ ,4) = 1\} = \{f_1, f_3\} \cong C_2.$$

Now define $\varphi : C_4 \longrightarrow Aut(C_4)$ by

$$\varphi_y = \begin{cases} f_1 & \text{if } y \text{ is not a generator} \\ f_3 & \text{if } y \text{ is a generator.} \end{cases}$$

Since φ is a homomorphism we have that ${\varphi_y}^4 = 1_{Aut(C_4)}$, so that ${\varphi_y}^4(x) = {f_i}^4 = x$. Therefore $x^{i^4} = x$ and so $i^4 \equiv 1(mod4)$.

If $i = 1$, then $i \equiv 1(mod4)$ and so $\varphi_y(x) = f_1(x) = x$. That is $yxy^{-1} = x$. Hence G is abelian. If $i = 3$, then we have $81 \equiv 1(mod4)$ so that $\varphi_y(x) = f_3(x) = x^{-1}$ and therefore G has the presentation

$$G =< x, y \mid x^4 = y^4 = 1,\ yxy^{-1} = x^{-1} > .$$

Hence there exists only one non-abelian group of order 16 of the type $C_4 : C_4$. In addition it can be easily shown that G has 12 elements of order 4 and 3 elements of order 2. □

Theorem 4.1.13 *Let G be an extension of N by H. If a subgroup K of G contains N, then K is an extension of N by K/N. If the extension G splits over N, then K also splits over N. If L is a complement to N in G, then $L \cap K$ is a complement to N in K.*

Proof. Since $N \leq K \leq G$ and $N \trianglelefteq G$, we have that $N \trianglelefteq K$. So K is an extension of N by K/N. Suppose that G splits over N and let L be a complement to N in G. So we have $NL = G$ and $N \cap L = \{1_G\}$. Then since $G = NL$, we get $K = NL \cap K$. Now N, L and K are subgroups of G such that $N \leq K$. So by Lemma 2.4.17 we have $K \cap NL = N(L \cap K)$ and hence $K = N(L \cap K)$. Since $N \cap (L \cap K) = (N \cap L) \cap K = \{1_G\}$, we get that $L \cap K$ is a complement of N in K. □

Definition 4.1.14 *Let G be a finite group. A subgroup K of G is said to be a* **Hall subgroup** *if* $(|K|, [G : K]) = 1$.

Theorem 4.1.15 *[31] If N is an abelian normal Hall subgroup of a finite group G, then N has a complement.*

Proof. See Theorem 7.39 of [31]. □

4.2 The Holomorph

Definition 4.2.1 *Let N be any group, and consider the natural action of $Aut(N)$ on N. Then the homomorphism $\varphi : Aut(N) \longrightarrow Aut(N)$ given by $\varphi(\alpha) = \alpha$ for every $\alpha \in Aut(N)$ defines a semidirect product $N{:}^{\varphi}Aut(N)$ which is called the* **holomorph** *of N and denoted by $Hol(N)$.*

Note 4.2.2 (i) $N \trianglelefteq Hol(N)$ by the definition of holomorph and for every $\alpha \in Aut(N)$ and $n \in N$ we have $\alpha n \alpha^{-1} = n^{\alpha}$, where the product on the left is defined in $Hol(N)$. Thus every automorphism of N is obtained by restriction from an inner automorphism of $Hol(N)$.

(ii) If $H \leq Aut(N)$ and we consider the natural action of H on N. Then the action is the inclusion map $i : H \longrightarrow Aut(N)$. The corresponding semidirect product $N{:}^{i}H$, is said to be a **relative holomorph** of N by H . Clearly by definition $N \leq N{:}^{i}H = NH \leq Hol(N)$.

Proposition 4.2.3 *If $G_1 \cong G_2$, then $Hol(G_1) \cong Hol(G_2)$.*

Proof. We first show that if $G_1 \cong G_2$ then $Aut(G_1) \cong Aut(G_2)$. Let $f : G_1 \longrightarrow G_2$, be an isomorphism. Now we define $\overline{f} : Aut(G_1) \longrightarrow Aut(G_2)$ by $\overline{f}(\alpha)(g_2) = f[\alpha(f^{-1}(g_2))]$, for all $g_2 \in G_2$. First notice that :

$$\begin{aligned} \overline{f}(\alpha)(g_2 g_2') &= f[\alpha(f^{-1}(g_2 g_2'))] = f[\alpha(f^{-1}(g_2) f^{-1}(g_2'))] = f[\alpha f^{-1}(g_2) \alpha f^{-1}(g_2')] \\ &= f[\alpha(f^{-1}(g_2))] f[\alpha(f^{-1}(g_2'))] = \overline{f}(\alpha)(g_2) \overline{f}(\alpha)(g_2'). \end{aligned}$$

It is not difficult to see that $\forall \alpha \in Aut(G_1)$ we have $\overline{f}(\alpha) \in Aut(G_2)$. We claim that $\overline{f}$ is an isomorphism.

$\overline{f}$ is well defined: Let $\alpha, \beta \in Aut(G_1)$ such that $\alpha = \beta$. Then $(\overline{f}(\alpha))(g_2) = f[\alpha(f^{-1}(g_2))]$ and $(\overline{f}(\beta))(g_2) = f[\beta(f^{-1}(g_2))]$. Now since $\alpha = \beta$ we have $f(\beta(f^{-1}(g_2))) = f(\alpha(f^{-1}(g_2)))$. So $\overline{f}(\alpha) = \overline{f}(\beta)$.

$$\begin{aligned} \overline{f} \text{ is one-to-one: } \overline{f}(\alpha) = \overline{f}(\beta) &\Rightarrow f(\alpha(f^{-1}(g_2))) = f(\beta(f^{-1}(g_2))), \quad \forall g_2 \in G_2 \\ &\Rightarrow \alpha(f^{-1}(g_2)) = \beta(f^{-1}(g_2)), \text{ since } f \text{ is one-to-one} \\ &\Rightarrow \alpha(g_1) = \beta(g_1), \quad \forall g_1 \in G_1, \text{ since } f \text{ is an isomorphism} \\ &\Rightarrow \alpha = \beta. \end{aligned}$$

$\overline{f}$ is onto: Let $\beta \in Aut(G_2)$. We need to find $\alpha \in Aut(G_1)$ such that $\overline{f}(\alpha) = \beta$. Let $\alpha = f^{-1}\beta f$. Then $f^{-1}\beta f \in Aut(G_1)$. Now we have

$$\overline{f}(\alpha)(g_2) = f(\alpha(f^{-1}(g_2))) = f[f^{-1}\beta f(f^{-1}(g_2))] = f(f^{-1}\beta(g_2)) = \beta(g_2), \forall g_2 \in G_2.$$

Thus $\overline{f}(\alpha) = \beta$.

$\overline{f}$ is a homomorphism: For all $\alpha, \beta \in Aut(G_1)$ and all $g_2 \in G_2$ we have

$$\overline{f}(\alpha\beta)(g_2) = f(\alpha\beta(f^{-1}(g_2))) = f(\alpha(\beta(f^{-1}(g_2))))$$

and

$$\begin{aligned} (\overline{f}(\alpha)\overline{f}(\beta))(g_2) &= \overline{f}(\alpha)(\overline{f}(\beta)(g_2)) = \overline{f}(\alpha)(f(\beta(f^{-1}(g_2)))) \\ &= f(\alpha(f^{-1}(f(\beta(f^{-1}(g_2)))))) = f(\alpha(\beta(f^{-1}(g_2)))). \end{aligned}$$

Thus $\overline{f}(\alpha\beta) = \overline{f}(\alpha)\overline{f}(\beta)$ and hence $\overline{f}$ is a homomorphism. So $\overline{f}$ is an isomorphism from $Aut(G_1)$ into $Aut(G_2)$. We have the following diagram

$$\begin{tikzcd} G_1 \arrow[r, "f"] & G_2 \arrow[d, "\beta"] \\ & G_2 \arrow[ul, "f^{-1}"] \end{tikzcd}$$

and the map $f^{-1}\beta f : G_1 \longrightarrow G_2$. Now we have to show that $Hol(G_1) \cong Hol(G_2)$. Define $\psi : Hol(G_1) \longrightarrow Hol(G_2)$ by $\psi(g_1, \alpha) = (f(g_1), \overline{f}(\alpha)), \quad \forall g_1 \in G_1$ and $\forall \alpha \in Hol(G_1)$.

ψ is well defined and one-to-one :

$$\begin{aligned}\psi(g_1,\alpha)=\psi(g_1',\alpha') &\Leftrightarrow (f(g_1),\overline{f}(\alpha))=(f(g_1'),\overline{f}(\alpha'))\\ &\Leftrightarrow f(g_1)=f(g_1') \quad \text{and} \quad \overline{f}(\alpha)=\overline{f}(\alpha')\\ &\Leftrightarrow g_1=g_1' \quad \text{and} \quad \alpha=\alpha' \quad \text{since } f \text{ and } \overline{f} \text{ are isomorphisms.}\end{aligned}$$

ψ is onto : Let $(g_2,\beta)\in Hol(G_2)$. There exists $g_1\in G_1$ such that $f(g_1)=g_2$ and there exists $\alpha\in Aut(G_1)$ such that $\overline{f}(\alpha)=\beta$. Now $\psi[(g_1,\alpha)]=(f(g_1),\overline{f}(\alpha))=(g_2,\beta)$ imply that ψ is onto.

ψ is a homomorphism :

$$\psi[(g_1,\alpha)(g_1',\alpha')]=\psi(g_1{g_1'}^{\alpha},\alpha\alpha')=(f(g_1{g_1'}^{\alpha}),\overline{f}(\alpha\alpha'))=(f(g_1)f({g_1'}^{\alpha}),\overline{f}(\alpha)\overline{f}(\alpha'))$$

and

$$\begin{aligned}\psi(g_1,\alpha)\psi(g_1',\alpha') &= (f(g_1),\overline{f}(\alpha))(f(g_1'),\overline{f}(\alpha'))=(f(g_1)[f(g_1')]^{\overline{f}(\alpha)},\overline{f}(\alpha)\overline{f}(\alpha'))\\ &= (f(g_1)\overline{f}(\alpha)[f(g_1')],\overline{f}(\alpha)\overline{f}(\alpha'))=(f(g_1)f(\alpha(g_1')),\overline{f}(\alpha)\overline{f}(\alpha'))\\ &= (f(g_1)f({g_1'}^{\alpha}),\overline{f}(\alpha)\overline{f}(\alpha'))\end{aligned}$$

imply that $\psi[(g_1,\alpha)(g_1',\alpha')]=\psi(g_1,\alpha)\psi(g_1',\alpha')$. □

Proposition 4.2.4 *If $\varphi : H \longrightarrow Aut(N)$ is a monomorphism, then $N{:}^{\varphi}H$ is isomorphic to the relative holomorph of N by $Im(\varphi)$.*

Proof. Let $G=N{:}^{\varphi}H$. Define $\varphi^* : G \longrightarrow Hol(N)$ by $\varphi^*(n,h)=(n,\varphi_h)$ for all $n\in N$ and $h\in H$. Then it is easy to see that φ^* is a homomorphism. Now

$$\begin{aligned}Ker(\varphi^*) &= \{(n,h)\mid (n,\varphi_h)=(1_N,I_N)\}\\ &= \{(n,h)\mid n=1_N,\varphi_h=I_N\}\\ &= \{(n,h)\mid n=1_N,h=1_H\}, \text{ since } \varphi \text{ is one-to-one}\\ &= (1_N,1_H)=1_G.\end{aligned}$$

Thus φ^* is a monomorphism. Hence $G\cong Im(\varphi^*)$ where

$$Im(\varphi^*)=\{(n,\varphi_h)\mid n\in N,h\in H\}= \text{ relative holomorph of } N \text{ by } Im(\varphi).$$

□

Corollary 4.2.5 *If $\varphi : Aut(N) \longrightarrow Aut(N)$ is an isomorphism, then $N{:}^{\varphi}Aut(N)\cong Hol(N)$.*

Proof. Follows immediately from Proposition 4.2.4.

Lemma 4.2.6 *If C_p is the cyclic group of order p (p prime),then $Aut(C_p) \cong C_{p-1}$.*

Proof. Let $C_p =< x >$. Each $\alpha \in Aut(C_p)$ is determined by $\alpha(x)$, so that $Aut(C_p) = \{\alpha_1, \alpha_2, \cdots, \alpha_{p-1}\}$ where α_i is defined by $\alpha_i(x) = x^i$ for some $i = 1, 2, \cdots, p-1$. Now let $\mathbb{Z}_p^*$ be the multiplicative group of non-zero elements of $\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ and define $\varphi : Aut(C_p) \longrightarrow \mathbb{Z}_p^*$ by $\varphi(\alpha_i) = \bar{i}$. Then φ is an isomorphism so that $Aut(C_p) \cong \mathbb{Z}_p^*$. But the group of non-zero elements of a finite field is cyclic, so $Aut(C_p) \cong C_{p-1}$. □

Example 4.2.7 $Hol(C_p)$.

We know that $Hol(C_p) = C_p{:}Aut(C_p) \cong C_p{:}C_{p-1}$. Let $C_p =< x >$ and $Aut(C_p) =< y >$ where $o(x) = p, o(y) = p-1$ and $y(x) = x^i$ with $1 \leq i \leq p-1$ and $i^k \not\equiv 1(modp)$ for all $k \in \{1, 2, \cdots, p-2\}$.

Let $\varphi : Aut(C_p) \longrightarrow Aut(C_p)$ be the isomorphism defined by $\varphi(y) = \varphi_y = y^j$ where $(j, p-1) = 1$ with $1 \leq j \leq p-1$. If $j = 1$, then $\varphi_y = y$ and $\varphi = I_{Aut(C_p)}$. Hence in this case we have

$$Hol(C_p) \cong C_p{:}^{\varphi}Aut(C_p) =< x, y \mid x^p = y^{p-1}, yxy^{-1} = x^i > .$$

If $j \neq 1$, then $\varphi \neq I_{Aut(C_p)}$. In this case we have $Hol(C_p) \cong C_p{:}^{\varphi}Aut(C_p)$, by Corollary 4.2.5, and

$$C_p{:}^{\varphi}Aut(C_p) =< x, y \mid x^p = y^{p-1}, yxy^{-1} = x^{ij} > .$$

For example if $p = 7$, then $y(x) = x^3$ and for $j = 1$ we get

$$Hol(C_7) =< x, y \mid x^7 = y^6 = 1, yxy^{-1} = x^3 > .$$

For $j = 5$ we have $\varphi_y = y^5$ and $i^j = 3^5 \equiv 5(mod7)$. Thus

$$Hol(C_7) \cong C_7{:}^{\varphi}C_6 =< x, y \mid x^7 = y^6 = 1, yxy^{-1} = x^5 > .$$

Next we show that the groups given by the above presentations are isomorphic. For this we identify the first presentation with G_1 and the second with G_2 and x and y with a and b respectively in G_2. Therefore we have

$$G_1 =< x, y \mid x^7 = y^6 = 1 \ , \ yxy^{-1} = x^3 >$$

and

$$G_2 =< a, b \mid a^7 = b^6 = 1 \ , \ bab^{-1} = a^5 > .$$

Define $\varphi : G_1 \longrightarrow G_2$ by $\varphi(x) = a$ and $\varphi(y) = b^{-1}$. Since $\varphi(yxy^{-1}) = \varphi(y)\varphi(x)[\varphi(y)]^{-1} = \varphi(x^3)$, we have $b^{-1}ab = a^3$. (1)

Now

$$\begin{aligned} bab^{-1} &= b^{-5}ab^5, \text{ since } b^6 = 1 \\ &= b^{-4}(b^{-1}ab)b^4 = b^{-4}a^3b^4, \text{ by (1)} \\ &= b^{-3}(b^{-1}a^3b)b^3 = b^{-3}(b^{-1}ab)^3b^3 = b^{-3}a^2b^3 = b^{-2}(b^{-1}a^2b)b^2 \\ &= b^{-2}(b^{-1}ab)^2b^2 = b^{-2}a^6b^2 = b^{-1}(b^{-1}ab)^6 = b^{-1}a^4b = (b^{-1}ab)^4 = a^5. \end{aligned}$$

Thus $G_1 \cong G_2$.

4.3 The Wreath Product

In this section we introduce the concept of wreath products. Subsequently we study the hyperoctahedral group as an example of the application of this concept.

Lemma 4.3.1 *Let X be a non-empty finite set and let G^X denote the set of all maps from X into the group G. For any $f, g \in G^X$ let fg be defined for all $x \in X$ by a pointwise multiplication $(fg)(x) = f(x)g(x)$. With respect with the operation of multiplication G^X is a group. Moreover G^X, is the direct product of $|X|$ isomorphic copies of G.*

Proof. See Lemma 8.21 of [30]. □

Lemma 4.3.2 *If G, H are groups and if H acts on a set X, then also H acts on G^X with action $f^h(x) = f(xh^{-1})$, for all $x \in X$, $h \in H$ and $f \in G^X$. Moreover, the action of H on G^X determines a homomorphism $\varphi : H \longrightarrow Aut(G^X)$ given by*

$$\varphi(h) = \varphi_h : f \quad \longmapsto \quad f^h$$

for all $h \in H$, and $f \in G^X$.

Proof. Let $h, h_1, h_2 \in H$, $x \in X$ and $f, g \in G^X$, then $f^{h_1h_2}(x) = f(x(h_1h_2)^{-1}) = f(xh_2{}^{-1}h_1{}^{-1}) = f((xh_2{}^{-1})h_1{}^{-1}) = f^{h_1}(xh_2{}^{-1}) = (f^{h_1})^{h_2}(x)$. So $f^{h_1h_2} = (f^{h_1})^{h_2}$. Also $f^1(x) = f(x1^{-1}) = f(x)$ and $(fg)^h(x) = (fg)(xh^{-1}) = f(xh^{-1})g(xh^{-1}) = f^h(x)g^h(x) = (f^hg^h)(x)$. Hence $(fg)^h = f^hg^h$.

Next, $Ker(\varphi_h)$ consists of all those functions $f \in G^X$ for which $f^h(x) = f(xh^{-1}) = 1 \in G$ for all $x \in X$, hence for all $xh^{-1} \in X$, so $f = 1 \in G^X$. Each φ_h is onto since $\varphi_h(f^{h^{-1}}) = (f^{h^{-1}})^h = f$ for any $f \in G^X$, so $\varphi_h \in Aut(G^X)$. Finally we have

$$\begin{aligned}\varphi_{hh'}(f)(x) &= f^{hh'}(x) = f(x(h'^{-1}h^{-1})) = f((xh'^{-1})h^{-1}) = f^h(xh'^{-1}) = (f^h)^{h'}(x) \\ &= (\varphi_h\varphi_h')(f)(x).\end{aligned}$$

Hence $\varphi_{hh'} = \varphi_h\varphi_{h'}$, for all $h, h' \in H$. □

Definition 4.3.3 *Let G and H be finite groups with H a subgroup of the symmetric group S_n. The* **permutation wreath product**, *$G \wr H$, is the semidirect product of a normal subgroup N by H, where N is the direct product of n copies of G. Thus, the elements of N are n-tuples $(g_1, g_2, \cdots, g_n)$ with each $g_i \in G$. The automorphism φ_h of G^n associated with a permutation h in H is defined by $\varphi_h(g_1, g_2, \cdots, g_n) = (g_{h(1)}, g_{h(2)}, \cdots, g_{h(n)})$.*

Now for $f, g \in G^n$ and $h, h' \in H$ we define $(f, h) \odot (g, h') = (f\varphi_h(g), hh')$.

Remark 4.3.4 In the above construction, H acts by conjugation on N, permuting the n direct factors. Also $|G| = |N| \times |H| = |G|^n \times |H|$.

4.3.1 The Hyperoctahedral Group

An important source of examples of permutation wreath product arises when the permutation group is taken to be the symmetric group S_n. In this section we study the group $C_2 \wr S_n$. We show that this group is the semidirect product of n copies of C_2 by the group S_n. The permutation wreath product $C_2 \wr S_n$ is also known as the hyperoctahedral group.

Definition 4.3.5 *A* **permutation matrix** *is a matrix in which every row and column has a unique non zero entry and all non zero entries are equal to 1.*

Remark 4.3.6 Every permutation matrix can be obtained from the identity matrix by permuting columns(rows). Every permutation matrix is orthogonal and thus has an inverse, that is again a permutation matrix, namely its transpose. The set of all permutation matrices is a group under the multiplication of matrices.

Proposition 4.3.7 *The set of all permutation matrices is a subgroup of $GL(n, \mathbb{F})$.*

Proof. Since the inverse of a permutation matrix is again a permutation matrix, it suffices to show that the product of two permutation matrices is a permutation matrix. Let

$A = (a_{ij})$ and $B = (b_{ij})$ be two permutation matrices and let $AB = C = (c_{ij})$. For any i and j we have that $c_{ij} = 1$ if there exists k, such that $a_{ik} = b_{kj} = 1$, and that $c_{ij} = 0$ otherwise. Now given i, there exists a unique k, such that $a_{ik} = 1$, and there exists a unique j such that $b_{kj} = 1$. Therefore, we have that $c_{ij} = 1$ for one and only one j. In a similar manner we have that for a given j, $c_{ij} = 1$ for exactly one i. Hence C is a permutation matrix. □

Proposition 4.3.8 *[1] The group of all permutation matrices is isomorphic to S_n.*

Proof. See Proposition 5 of page 42 of [1]. □

Note 4.3.9 Let X be a set of cardinality n. We may assume that $X = \{1, 2, \cdots, n\}$. The set of all subsets of X is denoted by $P(X)$, that is, $P(X) = \{A \mid A \subseteq X\}$.

Lemma 4.3.10 *The set $P(X)$ is an elementary abelian 2-group of order 2^n, under the operation of symmetric difference.*

Proof. It can be easily shown that $(P(X), \Delta)$ is an abelian group. Since for any $A \in P(X)$ we have that $A \ \Delta \ A = \emptyset = 1_{P(X)}$, we have that every non-identity element of $P(X)$ has order 2. Hence $P(X)$ is an elementary abelian 2-group.

For calculating the order of $P(X)$ we will consider those subsets X which have r elements each, where $0 \leq r \leq n$. It is known that the number of ways in which r elements can be selected out of n elements is $\left(\begin{array}{c} n \\ r \end{array}\right) = \frac{n!}{(n-r)!r!}$, which is therefore equal to the number of subsets of X having r elements each. Hence in total the number of subsets of X is $\sum_{r=0}^{n} \left(\begin{array}{c} n \\ r \end{array}\right)$. On substituting $a = 1$ in the binomial expansion $(1+a)^n = \sum_{r=0}^{n} \left(\begin{array}{c} n \\ r \end{array}\right) a^r$, we get $\sum_{r=0}^{n} \left(\begin{array}{c} n \\ r \end{array}\right) = 2^n$. This proves that X has exactly 2^n subsets. So $|P(X)| = 2^n = 2^{|X|}$. □

Remark 4.3.11 Let V be the vector space of dimension n over a field $\mathbb{F}$. Let $\{v_1, v_2, \cdots, v_{n-1}, v_n\}$ be an ordered basis for V. For each subset A of X we define an element f_A of $GL(n, \mathbb{F})$ as follows:

$$f_A(v_i) = \begin{cases} -v_i & if \ i \in A \\ v_i & if \ i \notin A \ . \end{cases}$$

We denote by D the set of all such mappings and in Proposition 4.3.12 we shall see that D is an elementary abelian 2-subgroup of $GL(n, \mathbb{F})$ which is isomorphic to $P(X)$.

Proposition 4.3.12 *[7] The group $D = \{f_A \mid A \subseteq X\}$ is an elementary abelian 2-subgroup of $GL(n, \mathbb{F})$ isomorphic to $P(X)$.*

Proof. It suffices to show that every non-identity element of D has order 2. Let $|A| = m < n$. By the observation made in Remark 4.3.11 we have that a non-identity element of D has the following representation in matrix form

$$f_A = \begin{pmatrix} -1 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix} = \begin{pmatrix} -I_m & 0 \\ 0 & I_{n-m} \end{pmatrix}.$$

However easy computation shows that ${f_A}^2 = I_n$ for all $A \subseteq X$. So D is an elementary abelian 2-subgroup of $GL(n, \mathbb{F})$ isomorphic to $P(X)$. □

Let G be the product of D and S_n in $GL(n, \mathbb{F})$. We show next that G is a split extension.

Theorem 4.3.13 *[7] The group $G = D.S_n$ is a split extension of the group D by S_n.*

Proof. We will show that (i) $D \trianglelefteq G$, (ii) $D \cap S_n = I_n$.

(i) For any $\pi \in S_n$ the action of π on the ordered basis $\{v_1 , v_2 , \cdots , v_n\}$ of V is given by $\pi(v_i) = v_{\pi(i)}$. Now if $\pi \in S_n$ and $A \subseteq X$ we show that $\pi f_A \pi^{-1} \in D$. But

$$\begin{aligned} (\pi f_A \pi^{-1})(v_i) = \pi f_A(\pi^{-1}(v_i)) &= \pi f_A(v_{\pi^{-1}(i)}) \\ &= \begin{cases} \pi(-v_{\pi^{-1}(i)}) & if\ \pi^{-1}(i) \in A \\ \pi(v_{\pi^{-1}(i)}) & if\ \pi^{-1}(i) \notin A \end{cases} \\ &= \begin{cases} -v_i & if\ i \in \pi(A) \\ v_i & if\ i \notin \pi(A) \end{cases} \\ &= f_{\pi(A)}(v_i). \end{aligned}$$

Hence $\pi f_A \pi^{-1} = f_{\pi(A)}$ and $f_{\pi(A)} \in D$, for any $A \subseteq X$. Therefore $D \trianglelefteq G$.

(ii) Since the only diagonal permutation matrix is I_n, we have $D \cap S_n = \{I_n\}$. □

Remark 4.3.14 From above we have that $|G| = |DS_n| = 2^n.n!$. The group G constructed in Theorem 4.3.13 is called the **hyperoctahedral** group and it is a special case of the generalised symmetric group.

Chapter 5

Presentations of Group Extensions

Due to its role in the description of a group, in this chapter we will study the theory of group presentations. Based on the theory of group presentation we study the presentation of a group extension as well as that of a split extension. For the study of presentations we have widely used [[20], [23], [29]].

5.1 Presentation of a Group

Definition 5.1.1 *A group F is said to be* **free** *on a subset $X \subseteq F$ if given any group G and any map $\alpha : X \longrightarrow G$ there is a unique homomorphism $\beta : F \longrightarrow G$ extending α, that is, having the property that $\beta(x) = \alpha(x), \forall x \in X$ or that the diagram*

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[d, "\alpha"'] & F \arrow[dl, "\exists\,!\,\beta"] \\ G & \end{tikzcd}$$

is commutative (that is $\alpha = \beta i$) where i is the inclusion map from X to F.

The set X is called a **basis** of F and $|X|$ is called the **rank** of F, denoted by $r(F)$.

Lemma 5.1.2 *If F is free on X, then X generates F.*

Proof. Let $H =< X >= \cap\{K \leq F, \quad X \subseteq K\}$. That is H is the smallest subgroup of F which contains the set X. Let $\phi : X \longrightarrow H$ denote the inclusion map with $\phi' : F \longrightarrow H$ the corresponding extension of ϕ. Then $\phi'(x) = \phi(x), \quad \forall x \in X$. Let $i' : H \longrightarrow F$, denote the inclusion map from H to F. It can be seen from the diagram below that $i'\phi'$ is an extension of $i'\phi$. But so does the identity map I_F. By uniqueness of the homomorphism $i'\phi'$, we have that $i'\phi' = I_F$. Thus $F = Im(I_F) = Im(i'\phi') = Im(\phi') \subseteq H$. Since H is a subgroup of F, we must have $F = H$ and hence X generates F.

$$\begin{tikzcd}
X \arrow[r, "i"] \arrow[d, "\phi"'] & F \arrow[dl, "\phi'"] \\
H \arrow[d, "i'"'] & \\
F &
\end{tikzcd}$$

□

Lemma 5.1.3 *Let G be a group generated by a subset Y and let X be any set in a bijective correspondence $\alpha : X \longrightarrow Y$, with Y. Then there exists a homomorphism β from the group F with basis X, onto G such that $\beta(x) = \alpha(x)$ for all $x \in X$.*

Proof. Since $< Y >= G$ and $\alpha : X \longrightarrow G$, there exists a unique homomorphism $\beta : F \longrightarrow G$ such that $\beta(x) = \alpha(x)$ for all $x \in X$. We need to show that $Im(\beta) = G$.

$$\begin{aligned}
Im(\beta) &= \{\ \beta(f) \mid f \in F\} \\
&\supseteq \{\beta(x) \mid x \in X\} \\
&\supseteq \{\alpha(x) \mid x \in X\} = Y, \text{ since } \alpha \text{ is a bijection.}
\end{aligned}$$

So $Im(\beta) \supseteq Y$ and hence $Im(\beta) \supseteq < Y >= G$. Since $Im(\beta) \subseteq G$, we must have $Im(\beta) = Y$. Hence β is onto. □

Proposition 5.1.4 *Every group is isomorphic to a factor group of some free group .*

Proof. Given a group G, let X be a set of generators of G. Let F be the free group generated by X. Let $\phi' : F \longrightarrow G$, be the extension of the inclusion $\phi : X \longrightarrow G$. Then

$$\begin{aligned}
Im(\phi') &= \{\ \phi'(f) \mid f \in F\} \\
&\supseteq \{\phi'(x) \mid x \in X\} \\
&\supseteq \{\phi(x) \mid x \in X\} = X.
\end{aligned}$$

Thus $Im(\phi') \supseteq < X >= G$ and since $Im(\phi') \subseteq G$ we have that $Im(\phi') = G$. Now if we let $Ker(\phi') = K$, then we have that $F/K \cong Im(\phi') = G$. □

Definition 5.1.5 *Let X be a set and F be a free group on X, that is, X generates F and we have no relations in the set $X^{\pm} = \{\, x, x^{-1} \mid x \in X\}$. Let $R \subseteq F$ and let Δ_R denote the normal closure of R in F (that is, Δ_R is the normal subgroup of F generated by R). We say that G is a group generated by X with relations $\{r_j = e \mid r_j \in R\}$ if $G \cong F/\Delta_R$. We denote this by $G = < X \mid R >$ and we say that $< X \mid R >$ is a* **presentation** *for G.*

Remark 5.1.6 If $|X| < \infty$ and $|R| < \infty$, then we say that G is *finitely presented* .

Theorem 5.1.7 *Let F, G and H be groups, $\beta : F \longrightarrow G$ and $\alpha : F \longrightarrow H$ be homomorphisms such that $Im(\beta) = G$ and $Ker(\beta) \subseteq Ker(\alpha)$. Then there exists a homomorphism $\sigma : G \longrightarrow H$ such that $\sigma\beta = \alpha$.*

Proof. We wish to prove the existence of $\sigma \in Hom(G, H)$, such that the diagram

$$\begin{tikzcd}
F \arrow[r, "\beta"] \arrow[d, "\alpha"'] & G \arrow[dl, "\sigma"] \\
H &
\end{tikzcd}$$

commutes.

Given $g \in G$, choose $f \in F$, such that $\beta(f) = g$ and define $\sigma(g) = \alpha(f)$. Such an f exists since $Im(\beta) = G$ and σ is well defined because $Ker(\beta) \subseteq Ker(\alpha)$.

$$\begin{aligned}
\beta(f') = \beta(f) \quad &\Leftrightarrow \quad \beta(f'f^{-1}) = 1_G \\
&\Leftrightarrow \quad f'f^{-1} \in Ker(\beta) \\
&\Rightarrow \quad f'f^{-1} \in Ker(\alpha), \text{ since } Ker(\beta) \subseteq Ker(\alpha) \\
&\Rightarrow \quad \alpha(f'f^{-1}) = 1_H \\
&\Rightarrow \quad \alpha(f') = \alpha(f).
\end{aligned}$$

Thus $\alpha(f)$ is independent of $f \in \beta^{-1}(g)$.

Now let $g, g' \in G$ and $f, f' \in F$, such that $\beta(f) = g$ and $\beta(f') = g'$. Since β is a homomorphism, we have $\beta(ff') = \beta(f)\beta(f') = gg'$ and

$$\begin{aligned}
\sigma(gg') &= \alpha(ff'), \text{ by the definition of } \sigma \\
&= \alpha(f)\alpha(f'), \text{ since } \alpha \text{ is a homomorphism} \\
&= \sigma(g)\sigma(g'), \text{ by the definition of } \sigma.
\end{aligned}$$

Proving that σ is a homomorphism. Finally, for each $f \in F$ we have $(\sigma\beta)(f) = \sigma(\beta(f)) = \alpha(f)$ by definition of σ. Hence $\sigma\beta = \alpha$. □

Proposition 5.1.8 (Substitution test) *[20] Suppose that we are given a presentation $G =< X \mid R >$, a group H and a mapping $\phi : X \longrightarrow H$. Then ϕ extends to a homomorphism $\phi'' : G \longrightarrow H$, if and only if for all $x \in X$ and $r \in R$ the result of substituting $\phi(x)$ for x in r yields the identity of H.*

Proof. Let $G =< X \mid R >$ and consider the commutative diagram

$$\begin{tikzcd}
& R \arrow[d, "\sigma"'] & \\
X \arrow[r, "i"] \arrow[dr, "\phi"'] & F \arrow[r, "\beta"] \arrow[d, "\phi'"] & G \arrow[dl, "\phi''"] \\
& H &
\end{tikzcd}$$

where σ and i are inclusions and β is the natural homomorphism with $Ker(\beta) = \Delta_R$ and $\beta(x) = x$ for all $x \in X$. Since F is free on X, we have that ϕ extends to a unique homomorphism $\phi' : F \longrightarrow H$.

Assume that for all $x \in X$ and $r \in R$, the result of substituting $\phi(x)$ for x in r yields the identity of H. Then for $r \in R$ with $r = x_i^m x_j^n \cdots x_k^l$ we have

$$\begin{aligned}
\phi'(r) &= \phi'(x_i^m x_j^n \cdots x_k^l) \\
&= [\phi'(x_i)]^m [\phi'(x_j)]^n \cdots [\phi'(x_k)]^l \\
&= [\phi(x_i)]^m [\phi(x_j)]^n \cdots [\phi(x_k)]^l \\
&= 1_H.
\end{aligned}$$

Thus $r \in Ker(\phi')$ and hence $R \subseteq Ker(\phi')$. Now $\Delta_R =< R >= Ker(\beta) \subseteq Ker(\phi')$, and then by Theorem 5.1.7 there exists ϕ'' such that $\phi''\beta = \phi'$. Since ϕ' is an extension of ϕ, for all $x \in X$ we have $\phi(x) = \phi'(x) = (\phi''\beta)(x) = \phi''(\beta(x)) = \phi''(x)$. So ϕ'' is an extension of ϕ on X.

Conversely assume that ϕ extends to a homomorphism $\phi'' : G \longrightarrow H$, we show that the result of substituting $\phi(x)$ for x in r yields the identity of H. Let $f \in Ker(\beta)$. Then $\beta(f) = 1_G$ and hence $\phi''(\beta(f)) = \phi''(1_G) = 1_H$. Then $f \in Ker(\phi''\beta)$ and hence $Ker(\beta) \subseteq Ker(\phi''\beta)$. Now, $Ker(\beta) \subseteq Ker(\phi''\beta)$ implies that $R \subseteq Ker(\phi')$ $(*)$. Let $r \in R$ then

$r = x_i^m \cdots x_j^n$ and by (*) we have that $\phi'(r) = 1_H$, so

$$\begin{aligned} 1_H &= \phi'(x_i^m \cdots x_j^n) = [\phi'(x_i)]^m \cdots [\phi'(x_j)]^n \\ &= [\phi(x_i)]^m \cdots [\phi(x_j)]^n, \text{ since } \phi'(x) = \phi(x)\ \forall x \in X. \end{aligned}$$

□

Note 5.1.9 In Proposition 5.1.8, if ϕ'' exists then it must be unique. Assume ϕ'' and ϕ_1'' are two homomorphisms such that $\phi''\beta = \phi'$ and $\phi_1''\beta = \phi'$. Then

$$\begin{aligned} (\phi''\beta)(x) = (\phi_1''\beta)(x) &\Rightarrow \phi''(\beta(x)) = \phi_1''(\beta(x)) \\ &\Rightarrow \phi''(x) = \phi_1''(x), \text{ for all } x \in X. \end{aligned}$$

Thus $\phi'' = \phi_1''$.

Remark 5.1.10 ϕ'' is an epimorphism if and only if $< \phi(X) >= H$.

Proof. Suppose that ϕ'' is an epimorphism. Then we have $\phi''(G) = H$. Hence $\phi''(< X >) = H$, so that $< \phi''(X) >= H$. Since ϕ'' is an extension of ϕ on X, we have $\phi''(X) = \phi(X)$. Thus $H =< \phi(X) >$. Conversely, assume that $H =< \phi(X) >$. We have $H =< \phi''(X) >= \phi''(< X >) = \phi''(G)$. This implies that ϕ'' is onto. □

Proposition 5.1.11 *If H and K are given by presentations $H =< X \mid R >$ and $K =< Y \mid S >$, then $H \times K =< X, Y \mid R, S, [X, Y] >$ $(*)$ where*

$$[X,Y] = \{[x,y] \mid x \in X, y \in Y\} = \{xyx^{-1}y^{-1} \mid x \in X, y \in Y\}.$$

Proof. Let G be the group presented by (*). By Proposition 5.1.8 the inclusions $i : X \longrightarrow G$ and $j : Y \longrightarrow G$ extend to homomorphisms $\alpha : H \longrightarrow G$ and $\beta : K \longrightarrow G$ respectively. Since $(h,e)(e,k)$ and $(e,k)(h,e)$ are both equal to (h,k), then the groups H and K centralize one another in G, and we have a homomorphism $\sigma : H \times K \longrightarrow G$ defined by $(h,k) \longmapsto \alpha(h)\beta(k)$ such that $\sigma(h,e) = \alpha(h)\beta(e) = \alpha(h)1_G = \alpha(h) = i(h) = h$ and $\sigma(e,k) = \alpha(e)\beta(k) = 1_G\beta(k) = \beta(k) = j(k) = k$ for all $h \in X$ and $k \in Y$.

On the other hand, the mapping $\phi : X \cup Y \longrightarrow H \times K$ sending x to (x,e) and y to (e,y), extends to a homomorphism $\rho : G \longrightarrow H \times K$. Since $\sigma\rho : G \longrightarrow G$ and $\rho\sigma : H \times K \longrightarrow H \times K$ both fix generating sets (in $H \times K$ and G respectively), it follows that σ and ρ are mutually inverse, hence σ is an isomorphism. □

5.2 Presentation of a group extension

Consider the extension $\{1_N\} \to N \overset{\alpha}{\to} G \overset{\beta}{\to} H \to \{1_H\}$. Assume that H and N are given by the presentations $H =< X \mid R >$ and $N =< Y \mid S >$ respectively. We need to find a presentation for G using these presentations. We introduce for this effect the following notations:
$\overline{Y} = \alpha(Y) = \{ \overline{y} \mid \overline{y} = \alpha(y),\ y \in Y\} \subseteq G$,
$\overline{S}$ = the set of all words in $\overline{Y}$ obtained from S by replacing each y by $\overline{y} = \{ \overline{s} \mid s \in S\}$,
$\overline{X} = \{ \overline{x} \mid x \in X\}$ to be a set of liftings of $\{ x \mid x \in X\}$ obtained by β, then $\overline{X}$ is a transversal for $Im(\alpha)$ in G. We can see that if $x \in H$ then there exists $\overline{x} \in G$, such that $\beta(\overline{x}) = x$. Also, let $\overline{R}$ be the set of all words in $\overline{X}$ obtained from R by replacing each x in R by $\overline{x}$.

Lemma 5.2.1 *(i) $\alpha(N)$ is generated by $\overline{Y}$,*

(ii) $\forall r \in R$ we have $\overline{r} \in Im(\alpha)$.

Proof. (i) N is generated by Y, implies that $\alpha(N)$ is generated by $\alpha(Y) = \overline{Y}$.

(ii) Let $r = w(x \mid x \in X)$ be a word in X. Then $\overline{r} = w(\overline{x} \mid \overline{x} \in \overline{X})$ is a word in $\overline{X}$. Since $\beta(\overline{r}) = 1_H$, by Proposition 5.1.8 we have that $\overline{r} \in Ker(\beta)$. Now $Im(\alpha) = Ker(\beta)$ implies that $\overline{r} \in Im(\alpha)$, $\forall r \in R$. □

Note 5.2.2 Lemma 5.2.1 implies that each $\overline{r} \in \overline{R}$ can be written as a word v_r in $\overline{Y}$, since $Im(\alpha) = \alpha(N)$ is generated by $\overline{Y}$. Let $\widetilde{R} =: \{\overline{r}(v_r)^{-1} \mid r \in R\}$. Since $Im(\alpha) \trianglelefteq G$ and $Im(\alpha)$ is generated by $\overline{Y}$, we have that $\forall \overline{x} \in \overline{X}$ and $\forall \overline{y} \in \overline{Y}$, $\overline{x}\ \overline{y}(\overline{x})^{-1} \in Im(\alpha)$. So $\overline{x}\ \overline{y}(\overline{x})^{-1}$ is a word in $\overline{Y}$, say $w_{x,y}$. Now let $\overline{T} = \{\overline{x}\ \overline{y}(\overline{x})^{-1}w_{x,y}^{-1} \mid x \in X, y \in Y\}$. Then we have the following result.

Theorem 5.2.3 *[20] If G is an extension of N by H, where $N =< Y \mid S >$ and $H =< X \mid R >$, then G has the presentation $G =< \overline{X}, \overline{Y} \mid \widetilde{R}, \overline{S}, \overline{T} >$. (*)*

Proof. Let F be the group given by the presentation (*). Since all the relations in (*) hold in G, by applying Proposition 5.1.8 to $\{F, G, i, i'\}$ where $i : \overline{X} \longrightarrow G$ and $i' : \overline{Y} \longrightarrow G$ are inclusions we deduce that there is a homomorphism

$$\begin{aligned} \phi \ : \ F &\longrightarrow G \\ \overline{x} &\longmapsto \overline{x} \\ \overline{y} &\longmapsto \overline{y}. \end{aligned}$$

The restriction of ϕ to the subgroup $<\overline{Y}>$ of F gives rise to a homomorphism

$$\begin{array}{rcccl} \phi' = \phi \mid_{<\overline{Y}>} & : & <\overline{Y}> & \longrightarrow & Im(\alpha) \cong N \\ & & \overline{y} & \longmapsto & y. \end{array}$$

Since the defining relations S of N (with each y replaced by $\overline{y}$) hold in $<\overline{Y}> \leq F$, we have $Ker(\phi') = \{\, \overline{y} \in <\overline{Y}> \mid y = 1_N\} = \{1_F\}$ and $Im(\phi') =< y \mid y \in N >= N$. Thus ϕ' is a bijection. Now the presence of the relations $\overline{T}$ in (*) means that $<\overline{Y}>$ is a normal subgroup of F. Since $\phi(<\overline{Y}>) \leq Im(\alpha)$, ϕ induces a homomorphism

$$\begin{array}{rcccl} \phi'' & : & F/<\overline{Y}> & \longrightarrow & G/Im(\alpha) \cong H \\ & & \overline{x}<\overline{Y}> & \longmapsto & x. \end{array}$$

The relations R defining H all hold (with x replaced by $\overline{x} < \overline{Y} >$) in $F/<\overline{Y}>$, so ϕ'' must be a bijection. Thus we have a commutative diagram

$$\begin{tikzcd}
1_N \arrow[r] & N \arrow[r, "\alpha"] \arrow[d, "\phi'"] & G \arrow[r, "\beta"] \arrow[d, "\phi"] & H \arrow[r] \arrow[d, "\phi''"] & 1_H \\
1_{<\overline{Y}>} \arrow[r] & <\overline{Y}> \arrow[r, "\text{inc}"] & F \arrow[r, "\text{nat}"] & F/<\overline{Y}> \arrow[r] & 1_{F/<\overline{Y}>}
\end{tikzcd}$$

with exact rows. Since ϕ' and ϕ'' are isomorphisms, it follows from Lemma 3.1.8 that ϕ is also an isomorphism. Hence the theorem is proved. □

The following is a very useful result in finding a presentation for a split extension.

Corollary 5.2.4 *[20] Let $N =< Y \mid S >$ and $H =< X \mid R >$ be groups. Let $\varphi : H \longrightarrow Aut(N)$ be a homomorphism such that $\varphi_x(y) = w_{x,y}$ is a word in $Y^{\pm}(\ x \in X,\ \ y \in Y)$. Then the semidirect product $N{:}^{\varphi}H$ of N by H has the following presentation*

$$G = N{:}^{\varphi}H =< X, Y \mid R,\ S,\ xyx^{-1}w_{x,y}^{-1},\ x \in X,\ y \in Y > .$$

Proof. Since $G = N{:}^{\varphi}H$ is an extension of $N =< Y \mid S >$, by $H =< X \mid R >$, by the Theorem 5.2.3 the group G has the presentation $G =< \overline{X}, \overline{Y} \mid \widetilde{R}, \overline{S}, \overline{T} >$ where $\overline{T} = \{\overline{x}\ \overline{y}(\overline{x})^{-1}\overline{w}_{x,y}^{-1} \mid x \in X, y \in Y\}$. Now since the extension splits, there exists a homomorphism $\sigma : H \longrightarrow G$ such that $\beta\sigma = I_H$. So we can choose the generators of $\overline{X}$ to be $\{\sigma(x) \mid x \in X\}$. Then for each $r \in R$ we have $\sigma(r) = \overline{r} = 1_G$, and since each $\overline{r} \in \overline{R}$ is a word in $\overline{Y}$ written as v_r, all the v_r are equal to e in $\widetilde{R}$. Identifying $\overline{X} = \{(x, e) \mid x \in X\}$ with X and $\overline{Y} = \{(e, x) \mid y \in Y\}$ with Y, we have the presentation

$$G =< X, Y \mid R, S, xyx^{-1}w_{x,y}^{-1}, \ \ x \in X, y \in Y > .$$

□

Example 5.2.5 (Metacyclic groups) Consider the group $G = N{:}H$ where $N \cong C_n$ and $H \cong C_m$ subject to the homomorphism φ. Let $N =< y \mid y^n = e >$ and $H =< x \mid x^m = e >$. We know that $Aut(N)$ is an abelian group with $|Aut(N)| = \phi(n)$ where ϕ is the *Euler totient* function. Assume that $\varphi_x(y) = y^k, \ 0 \leq k \leq n-1$. Then it can be shown that $k^m \equiv 1(modn)$. Now application of Corollary 5.2.4 yields that

$$\begin{aligned} G &= \ < x, y \mid x^m = y^n = e, \ xyx^{-1}(y^k)^{-1} = e > \\ &= \ < x, y \mid x^m = y^n = e, \ xyx^{-1} = y^k > . \end{aligned}$$

Remark 5.2.6 (i) In the above example if $k = 1$, then $G = N \times H$.
(ii) For $n = 3$ and $m = 2$, we have two different split extensions.
(1) $\varphi_x(y) = y$. So $k = 1$ and hence $G = C_3 \times C_2 = C_6$.
(2) $\varphi_x(y) = y^2 = y^{-1}$. So $k = 2$ and hence

$$G =< x, y \mid x^2 = y^3 = 1, \ xyx^{-1} = y^{-1} >\cong S_3.$$

Chapter 6

Groups of order pq, p^2q and p^3

The structure of a non-abelian group of order pq where p and q are distinct primes is well known. The existence of such groups is often demonstrated by constructing the group using group extensions. In this chapter we study the non-abelian groups of order pq, p^2q and p^3. We exhibit two examples of groups of order pq, one in terms of permutations and the other in terms of matrices. In this chapter p and q are distinct primes.

6.1 Groups of order pq

Proposition 6.1.1 *[1] Let H be a cyclic group and let N be an arbitrary group. If θ and ϑ are monomorphisms from H to $Aut(N)$ such that $\theta(H) = \vartheta(H)$, then we have $N{:}^{\theta}H \cong N{:}^{\vartheta}H$.*

Proof. Let $H =< x >$. Since $\theta(H) = \vartheta(H)$ by hypothesis, we have that $\theta(x)$ and $\vartheta(x)$ generate the same cyclic subgroup of $Aut(N)$. Hence we can find $a, b \in \mathbb{Z}$ such that $[\theta(x)]^a = \vartheta(x)$ and $[\vartheta(x)]^b = \theta(x)$. As H is cyclic we have that $\theta(h^a) = \vartheta(h)$ and $\vartheta(h^b) = \theta(h)$ for any $h \in H$. Now define $\rho : N{:}^{\vartheta}H \longrightarrow N{:}^{\theta}H$ by $\rho(nh) = nh^a$. Then we have

$$\begin{aligned}
\rho(n_1h_1n_2h_2) &= \rho(n_1\vartheta(h_1)(n_2)h_1h_2) \\
&= n_1\vartheta(h_1)(n_2)(h_1h_2)^a \\
&= n_1\theta(h_1^a)(n_2)h_1^ah_2^a, \text{since } H \text{ is abelian} \\
&= n_1{h_1}^a n_2{h_1}^{-a}{h_1}^a{h_2}^a = n_1h_1^an_2h_2^a \\
&= \rho(n_1h_1)\rho(n_2h_2)
\end{aligned}$$

which shows that ρ is homomorphism.

Similarly it can be checked that the map $\sigma : N{:}^{\theta}H \longrightarrow N{:}^{\vartheta}H$ defined by $\sigma(nh) = nh^b$ is a homomorphism. Now it suffices to show that ρ and σ are mutually inverses. The map $\rho \circ \sigma$ sends $nh \in N{:}^{\theta}H$ to nh^{ab}. But $\theta(x) = [\vartheta(x)]^b = ([\theta(x)]^a)^b = \theta(x^{ab})$ and θ is a monomorphism, therefore $x^{ab} = x$ and hence $h^{ab} = h$, for all $h \in H$. Therefore $\rho \circ \sigma$ sends nh to nh, and so $\rho \circ \sigma$ is the identity map on $N{:}^{\theta}H$. In a similar way it can be checked that $\sigma \circ \rho$ is the identity map on $N{:}^{\vartheta}H$. Hence the result. □

Lemma 6.1.2 *Every group of order pq, has a normal subgroup .*

Proof. Let G be a group of order pq with p and q distinct primes. Without loss of generality, assume that $p > q$. Let $P \in Syl_p(G)$, then by Sylow's Theorem we have $n_p \equiv 1(modp)$ and $n_p \mid q$, where n_p is the number of Sylow p-subgroups of G. So $n_p = 1 + kp$ and $q = k'n_p$ for some $k, k' \in \mathbb{Z}$. Then $q = k'(1 + kp)$. Since q is a prime, we have $\{1 + kp = q$ and $k' = 1\}$ or $\{1 + kp = 1$ and $k' = q\}$. But $p > q$ implies that $1 + kp = q$ is not possible, so $1 + kp = 1$ and hence $k = 0$. Therefore $n_p = 1$, so that $P \trianglelefteq G$. □

Theorem 6.1.3 *If G is a finite group of order pq, where $p > q$. Then either G is cyclic or $G =< x, y >$ with relations $x^p = y^q = 1$ and $yxy^{-1} = x^i$, where $i \not\equiv 1(modp)$, $i^q \equiv 1(modp)$ and $q \mid p - 1$.*

Proof. Let G be a group of order pq. By Cauchy's Theorem there exist $x, y \in G$, such that $o(x) = p$ and $o(y) = q$. Let $P =< x >$, then $P \in Syl_p(G)$. By Lemma 6.1.2 we have that $P \trianglelefteq G$. Similarly if $Q =< y >$, then $Q \in Syl_q(G)$ and using the same argument as that of Lemma 6.1.2 we get $n_q = 1 + k'q$ where $k' = 0$ or $n_q = p$.

Case 1 : If $k' = 0$, then $n_q = 1$ and hence $Q \trianglelefteq G$. Since P and Q are normal subgroups of G and $P \cap Q = \{1_G\}$ and $PQ = G$, we have $G = P \times Q \cong C_{pq}$.

Case 2 : If $n_q = p \neq 1$, then $p \equiv 1(modq)$, and so $q \mid p - 1$. Then Q is not normal in G. Since $P \trianglelefteq G$, $yxy^{-1} = x^i$ for some i. If $i \equiv 1(modp)$, then we have that $x^i = x$ and so $yxy^{-1} = x$. Hence G is abelian and this shows that $Q \trianglelefteq G$ which is a contradiction. So $i \not\equiv 1(modp)$. Now $yxy^{-1} = x^i$ implies that $y^qxy^{-q} = x^{i^q}$, so that $x = x^{i^q}$. Thus $i^q \equiv 1(modp)$. Hence G is given by the presentation

$$G =< x, y \mid x^p = y^q = 1, yxy^{-1} = x^i >$$

where i and q satisfy relations $i^q \equiv 1(modp)$, $i \not\equiv 1(modp)$ and $q \mid p - 1$. □

Proposition 6.1.4 *There exists a non-abelian split extension of the form $C_p{:}C_q$ if and only if q divides $p - 1$; and when this is the case the extension is uniquely determined (up to isomorphism).*

Proof. If q divides $p-1$, the existence of the non-abelian split extension of the form $C_p{:}C_q$ has been dealt with in Theorem 6.1.3. We now show that if there exists a non-abelian split extension of order pq of the form $C_p{:}C_q$, then $q \mid p-1$. We also prove the uniqueness of such extensions. Consider the split extension $C_p{:}C_q$. If $p < q$, then C_q acts trivially on C_p and hence $C_p{:}C_q \cong C_p \times C_q$ contradicting the assumption that $C_p{:}C_q$ is non-abelian. Thus $p > q$.

Let $C_p =< x >= \{ 1, x, x^2, \cdots, x^{p-1}\} =< x^2 >= \cdots =< x^{p-1} >$ and $C_q =< y >= \{1, y, \cdots, y^{q-1}\}$. Then $C_p \cap C_q = \{1\}$. Define $f_i : C_p \longrightarrow C_p$ by $f_i(x) = x^i$ with $1 \leq i \leq p-1$. So that

$$Aut(C_p) = \{f_i \mid f_i(x) = x^i, \ 1 \leq i \leq p-1\} \cong \ C_{p-1}.$$

Let $\varphi : C_q \longrightarrow Aut(C_p) \cong C_{p-1}$ be given by $\varphi_y = f_i$. Then $\varphi_y = f_1$, or $\varphi_y = f_i$ and $2 \leq i \leq p-1$.

Suppose that $\varphi_y = f_1$. Then $\varphi_y(1) = f_1(1) = 1, \varphi_y(x) = x, \cdots, \varphi_y(x^{p-1}) = f_1(x^{p-1}) = x^{p-1}$ and multiplication is defined by $x_1y_1x_2y_2 = x_1y_1x_2y_1^{-1}y_1y_2 = x_1x_2^{y_1}y_1y_2 = x_1x_2y_1y_2$. Hence $C_p{:}C_q = C_p \times C_q \cong C_{pq}$. This contradicts the assumption that $C_p{:}C_q$ is non-abelian. Hence we must have $\varphi_y = f_i$ where $2 \leq i \leq p-1$.

Let $\varphi_y = f_i$ where $2 \leq i \leq p-1$. Then $\varphi_y(1) = f_i(1) = 1, \varphi_y(x) = x^i, \cdots, \varphi_y(x^{p-1}) = f_i(x^{p-1}) = (x^{p-1})^i$. Since φ is an automorphism, we have that $\varphi_{y^q} = f_i{}^q = 1_{Aut(C_p)}$. So $\varphi_{y^q}(x) = f_i^q(x) = x$ and $x^{i^q} = x$. Thus $x^{i^q-1} = 1$ and $i^q \equiv 1(\mathrm{mod}\, p)$. Now $2 \leq i \leq p-1$, implies that $x^i \neq x$, and so $i \not\equiv 1(\mathrm{modp}\ )$. Also, since φ is a homomorphism from C_q into $Aut(C_p)$, we have $Ker(\varphi) \trianglelefteq C_q$. Therefore $|Ker(\varphi)| \mid q$ and so $Ker(\varphi) = \{1\}$ or $Ker(\varphi) = C_q$. If $Ker(\varphi) = C_q$, then $\varphi = f_1$ which is a contradiction since $i > 1$. Therefore $Ker(\varphi) = \{1\}$. By the first isomorphism theorem, we have that $C_q/Ker(\varphi) \cong Im(\varphi) \leq Aut(C_p)$ and hence C_q is isomorphic to a subgroup of $Aut(C_p)$. Thus $q \mid p-1$ and we have that G is given by the presentation

$$G =< x, y \mid x^p = y^q = 1, yxy^{-1} = x^i, 1 < i \leq p-1 >$$

with i and q satisfying relations $i \not\equiv 1(\mathrm{mod}\, p)$, $i^q \equiv 1(modp)$ and $q \mid p-1$.

To show the uniqueness, assume that there exists another monomorphism from C_q to $Aut(C_p)$. Let ψ be such a monomorphism. Since $Aut(C_p)$ is a cyclic group of order $p-1$ and $q \mid p-1$ we have that $Aut(C_p)$ contains a unique subgroup of order q. Let K be such a subgroup. Then we must have that $\varphi(C_q) = K = \psi(C_q)$. Now by Theorem 6.1.1 we have $C_p{:}^{\varphi}C_q \cong C_p{:}^{\psi}C_q$ and hence the result. □

In the following we give two examples of non-abelian groups of order pq, one in term of permutations and the other in term of matrices.

Example 6.1.5 Let i, q and p satisfy relations $i \not\equiv 1(modp)$, $i^q \equiv 1(modp)$ and $q \mid p-1$. Let x be the cyclic permutation $(1\ 2\ 3\ \cdots\ p)$ and y be the permutation

$$y = \begin{pmatrix} 1 & 2 & \cdots & p-1 & p \\ i+1 & 2i+1 & \cdots & (p-1)i+1 & pi+1 \end{pmatrix}$$

where each of the integers $i+1, 2i+1, \cdots, pi+1$ is to be taken modulo p if it exceeds p. Then x and y generate a non-abelian group of order pq. For, it can be easily seen that $x^p = 1$ and

$$yx = x^i y = \begin{pmatrix} 1 & 2 & \cdots & p-1 & p \\ 2i+1 & 3i+1 & \cdots & pi+1 & i+1 \end{pmatrix}$$

so that $yxy^{-1} = x^i$. Now let $1 \leq k \leq p$. The permutation y^q maps k to the integer $ki^q + i^{q-1} + \cdots + i + 1$ modulo p if it exceeds p. But $i^q - 1 = (i-1)(i^{q-1} + \cdots + i + 1)$, and since $i^q \equiv 1(\text{mod}\, p)$ and $i \not\equiv 1(\text{mod}\, p)$, it follows that $i^{q-1} + \cdots + i + 1 \equiv 0(\text{ mod}\, p)$. Thus $y^q = 1$.

Example 6.1.6 Let $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $y = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}$ be 2×2 matrices over the field $\mathbb{F} = GF(q)$ of p elements, where i is to be taken modulo p if it exceeds p. We have that

$$x^p = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \text{ and } y^q = \begin{pmatrix} i^q & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

Let $G =< x, y >$. Then $yxy^{-1} = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} = x^i$, and hence G is a non-abelian group of order pq.

6.2 Groups of order p^2q

In this section we will study the non-abelian groups of order p^2q of type $C_{p^2}{:}C_q$ where p and q are primes and $p > q$. Before we embark into a more detailed discussion of the subject we need the following properties.

Remark 6.2.1 Similar to the argument used in Lemma 6.1.2 it can be shown that every group of order p^2q has a normal subgroup of order p^2.

Proposition 6.2.2 *Let p be a prime integer and let G be an elementary abelian p-group of order p^n, so that G is the direct product of n copies of C_p. The automorphism group of G is isomorphic to the group $GL(n,p)$ of invertible $n \times n$ matrices over the field $\mathbb{Z}_p$.*

Proof. See Proposition 22.4 of [18]. □

Theorem 6.2.3 *If p and q are two distinct prime integers such that $p > q$, then there are only two classes of non-isomorphic non-abelian groups of order p^2q namely $C_{p^2}{:}C_q$ and $(C_p \times C_p){:}C_q$.*

Proof. Let G be a group of order p^2q. Let N be a subgroup of order p^2 in G. Then $N \trianglelefteq G$. Let $H \in Syl_q(G)$, then $H \cong C_q$ and $H \cap N = \{1_G\}$ so $G = NH$ and hence $G = N{:}H$, a semidirect product of N by H. Since $|N| = p^2$, we have that N is either cyclic or isomorphic to $C_p \times C_p$.

Case 1 : Let N be a cyclic group of order p^2 generated by x. Define $f_i : C_{p^2} \longrightarrow C_{p^2}$ by $f_i(x) = x^i$ with $1 \leq i \leq p(p-1)$, then

$$Aut(C_{p^2}) = \{f_i \mid f_i(x) = x^i,\ 1 \leq i \leq p^2,\ (i,p^2) = 1\} \cong C^*_{p^2} \cong C_p \times C_{p-1}.$$

Let $H =< y >$ and let $\varphi : H \longrightarrow Aut(C_{p^2}) \cong C_p \times C_{p-1}$ given by $\varphi_y = f_i$. Since φ is a homomorphism, we have that $\varphi_{y^q} = f_i^q = 1_{Aut(C_{p^2})}$. $(*)$ Then $\varphi_{y^q}(x) = f_i^q(x) = x$. So $x^{i^q} = x$ so that $i^q \equiv 1 (\mathrm{mod}\, p^2)$. Now $(*)$ implies that $f_i = 1$ or $o(f_i) = q$. If $o(f_i) = q$ then we have that $q \mid p(p-1)$. Since q and p are primes, we deduce that $q \mid p-1$.

If $q = 2$, we have that $i^2 \equiv 1(\mathrm{mod}\, p^2)$, so $p^2 \mid i^2 - 1$, and hence $i \equiv 1(\mathrm{mod}\, p^2)$ (1) or $i \equiv -1(\mathrm{mod}\, p^2)$ (2) or $p \mid i+1$ and $p \mid i-1$. (3) Condition (3) implies that $p \mid 2$ so $p = 2$ which is a contradiction since $p > q$. From condition (1) we have that $yxy^{-1} = x$, so that G is an abelian group. However condition (2) implies that G is a non-abelian group given by

$$G =< x, y \mid x^{p^2} = y^q = 1, yxy^{-1} = x^{-1} > .$$

If $q \neq 2$, we have $G =< x, y \mid x^{p^2} = y^q = 1, yxy^{-1} = x^i \ 1 < i \leq p^2 >$ where i and q satisfy relations $i^q \equiv 1 mod p^2$ and $q \mid p-1$.

Now we will show that the split extension $C_{p^2}{:}C_q$ is unique up to isomorphism. Since $\varphi : H \longrightarrow Aut(C_{p^2})$, is a homomorphism we have that $Ker(\varphi) \trianglelefteq H$. So $Ker(\varphi) = \{1\}$ or $Ker(\varphi) = H$. The latter case implies that $\varphi_y = 1_{Aut(C_{p^2})}$, hence G is abelian and $G \cong C_{p^2} \times C_q$. If $Ker(\varphi) = \{1\}$ then φ is a monomorphism and we get that $H \cong Im(\varphi) \leq Aut(C_{p^2})$. Hence H is isomorphic to a subgroup of $Aut(C_{p^2})$. So, $q \mid p(p-1)$ and hence

$q \mid p-1$. Now assume that ψ is another monomorphism from $\psi : H \longrightarrow Aut(C_{p^2})$, given by $\psi_y = f_j$ for some $1 < j \leq p(p-1)$. Then since $C_q \cong H \cong \varphi(H) \leq Aut(C_{p^2})$ and $C_q \cong H \cong \psi(H) \leq Aut(C_{p^2})$, we have that $\psi(H) = H = \varphi(H)$. Now the Proposition 6.1.1 implies the uniqueness of the split extension in this case.

Case 2 : Let $N \cong C_p \times C_p =< x_1, x_2 >$ and let $H \cong C_q$, with $H =< y >$. Let $f : C_p \times C_p \longrightarrow C_p \times C_p$, be given by $f(x_1) = x_1^a x_2^c$ and $f(x_2) = x_1^b x_2^d$, where $a, b, c, d \in \mathbb{Z}_p$. Then it is not difficult to show that $f \in Aut(C_p \times C_p)$ if and only if $ad - bc \neq 0$. Hence

$$\begin{aligned} Aut(C_p \times C_p) &= \left\{ f \mid f(x_1) = x_1^a x_2^c, \;\; f(x_2) = x_1^b x_2^d, \; ad - bc \neq 0, \;\; a, b, c, d \in \mathbb{Z}_p \right\} \\ &\cong \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc \neq 0, \;\; a, b, c, d \in \mathbb{Z}_p \right\} = GL(2, p). \end{aligned}$$

Now consider the group $G = N{:}^{\varphi}H$ where $\varphi : H \longrightarrow Aut(C_p \times C_p)$ is given by $\varphi_y(x_1) = x_1^a x_2^c$ and $\varphi_y(x_2) = x_1^b x_2^d$ with $a, b, c, d \in \mathbb{Z}_p$ and $ad - bc \neq 0$. Then the group G has the following presentation

$$G =< x_1, x_2, y \mid x_1^p = x_2^p = y^q = 1, \; [y, \; x_1] = x_1^{a-1} x_2^c, \; [x_1, \; x_2] = 1, [y, \; x_2] = x_1^b x_2^{d-1} > .$$

Using the same argument as in case 1, it can be shown that the non-abelian split extension $(C_p \times C_p){:}C_q$ is unique up to isomorphism. □

Example 6.2.4 Let $G = (C_p \times C_p){:}^{\varphi}C_q$ where φ is given by $\varphi_y(x_1) = x_1 x_2$ and $\varphi_y(x_2) = x_2$. Then G has the following presentation

$$G =< x_1, x_2, y \mid x_1^p = x_2^p = y^q = 1, \; [y, \; x_1] = x_2, \; [x_1, \; x_2] = [y, \; x_2] = 1 > .$$

6.3 Groups of order p^3

We now study the non-abelian groups of order p^3 with p prime. We will assume the results mentioned in Lemma 6.3.2.

Lemma 6.3.1 *Let $|G| = p^n$, where p is a prime integer. If $0 \leq k \leq n$, then there exist $N \trianglelefteq G$ such that $|N| = p^k$.*

Proof. Let $|Z(G)| = p^m$ where $1 \leq m \leq n$. Let $x \in Z(G)$ such that $o(x) = p$. Let $H =< x >$. Then since $H \leq Z(G)$, we have that $H \trianglelefteq G$ and hence G/H is a group of order p^{n-1}. We use induction on n to prove the result. Let $1 \leq k \leq n$. Let $k' = k - 1$. Since $0 \leq k' \leq n - 1$, by induction hypothesis there exists $W \trianglelefteq G/H$ such that $|W| = p^{k'}$. Hence $W = N/H$ for some $N \trianglelefteq G$ such that $N \supseteq H$. Thus $|N| = |W|.|H| = p^{k'}.p = p^{k'+1} = p^k$. □

Lemma 6.3.2 *If G is a non-trivial p-group of order p^n and N is a non-trivial normal subgroup of G, then $N \cap Z(G) \neq \{1_G\}$.*

Proof. See Theorem 1, page 73 of [1]. □

Lemma 6.3.3 *If G is a non-abelian group of order p^3, then $|Z(G)| = p$.*

Proof. Since G is a non-abelian group, $G/Z(G)$ cannot be cyclic. Thus $|G/Z(G)| \neq p$ and hence $|Z(G)| = p$. □

Lemma 6.3.4 *Let G be a group and let $x, y \in G$. If $[x,y] \in Z(G)$, then $[x^n, y] = [x,y]^n$ and $x^n y^n = (xy)^n [x,y]^{\frac{n(n-1)}{2}}$ for any $n \in \mathbb{N}$.*

Proof. Consider the first statement. We use induction on n to prove the result. Assume that the statement is true for $n \in \mathbb{N}$, then we have

$$\begin{aligned}
[x^{n+1}, y] &= x^{n+1} y x^{-(n+1)} y^{-1} = x x^n (y^{-1} y) x^{-1} y^{-1} = x(x^n y x^{-n} y^{-1}) y x^{-1} y^{-1} \\
&= x[x^n, y] y x^{-1} y^{-1} = x[x, y]^n y x^{-1} y^{-1}, \text{ by induction hypothesis} \\
&= [x,y]^n x y x^{-1} y^{-1}, \text{ since } [x,y] \in Z(G) \\
&= [x,y]^n [x,y] = [x,y]^{n+1}.
\end{aligned}$$

Now we consider the second statement. Again we use induction on n. Assume that the statement is true for $n \in \mathbb{N}$. Then we have

$$\begin{aligned}
x^{n+1} y^{n+1} &= x x^n y (y x^n)^{-1} y x^n y^n = x(x^n y x^{-n} y^{-1}) y x^n y^n \\
&= x[x^n, y] y x^n y^n = x[x,y]^n y x^n y^n, \text{ by the previous statement} \\
&= [x,y]^n x y x^n y^n = [x,y]^n x y (xy)^n [x,y]^{\frac{n(n-1)}{2}}, \text{ by induction hypothesis} \\
&= [x,y]^n [x,y]^{\frac{n(n-1)}{2}} (xy)^{n+1} = (xy)^{n+1} [x,y]^{\frac{n(n+1)}{2}}.
\end{aligned}$$

□

Theorem 6.3.5 *Let p be an odd prime. Then there is exactly one isomorphism class of non-abelian groups of order p^3 having elements of order p^2.*

Proof. Assume that G is a non-abelian group of order p^3. Let $x \in G$ such that $o(x) = p^2$ and let $N =< x >$. Then N is a maximal subgroup of G and hence $N \trianglelefteq G$. Let $y \in G - N$. Then we have that $o(y) = p$ or $o(y) = p^2$.

Case 1 : Assume that $o(y) = p$. Let $H =< y >$. We claim that $N \cap H = \{1_G\}$. Suppose that $N \cap H \neq \{1_G\}$. Let $y^k \in N$ for some $1 \leq k \leq p-1$. Since $(k,p) = 1$, there exists $\alpha, \beta \in \mathbb{Z}$ such that $\alpha p + \beta k = 1$. This implies that $y = y^{\alpha p+\beta k} = (y^p)^\alpha.(y^k)^\beta = (y^k)^\beta \in N$ which is a contradiction . Thus $N \cap H = \{1_G\}$ and $G = N{:}H$. So $G \cong C_{p^2}{:}C_p$.

Case 2 : Assume that $o(y) = p^2$. Since N and $< y >$ are non-trivial normal subgroups of G, we must have $N \cap Z(G) \neq \{1_G\} \neq < y > \cap Z(G)$ by Lemma 6.3.2. Since $|Z(G)| = p$ by Lemma 6.3.3, we must have $Z(G) = N \cap Z(G) =< y > \cap Z(G)$ and hence $Z(G) =< x^p >=< y^p >$. So $y^p = x^{kp}$ for some $1 \leq k \leq p-1$. Let $x_1 = x^{-k}$. Then $y \notin < x_1 >$, $o(x_1) = p$ and $y^p = {x_1}^{-p}$. Since $G/Z(G)$ is an abelian group, we have $\{1_G\} \neq G' \subseteq Z(G)$ and hence $G' = Z(G)$. So, in particular, $[x_1, y] \in Z(G)$ and hence $[x_1, y]^p = 1_G$. Now by Lemma 6.3.4 we have

$$ {x_1}^p y^p = (x_1 y)^p.[x_1, y]^{\frac{p(p-1)}{2}} = (x_1 y)^p ([x_1, y]^p)^{\frac{p-1}{2}} = (x_1 y)^p, $$

since $\frac{p-1}{2} \in \mathbb{Z}$. Now ${x_1}^p y^p = {x_1}^p {x_1}^{-p} = 1_G$ implies that $o(x_1 y) \in \{1, p\}$. Since $y \notin < x_1 >$, $o(x_1 y) \neq 1$ and hence $o(x_1 y) = p$. Now let $H =< x_1 y >$. Then $H \cong C_p$ and we can easily see that $N \cap H = \{1_G\}$. Hence $G = N{:}H \cong C_{p^2}{:}C_p$.

In both the above cases the uniqueness of the group G, up to isomorphism follows from Proposition 6.1.1. □

Lemma 6.3.6 *[1] Let N and H be groups, let $\psi : H \longrightarrow Aut(N)$ be a homomorphism and let $f \in Aut(N)$. If $\overline{f}$ is the inner automorphism of $Aut(N)$ induced by f, then $N{:}^{\overline{f} \circ \psi} H \cong N{:}^{\psi} H$.*

Proof. Define $\theta : N{:}^{\psi} H \longrightarrow N{:}^{\overline{f} \circ \psi} H$ by $\theta(nh) = f(n)h$. We have

$$ \begin{aligned} \theta(n_1 h_1 n_2 h_2) &= \theta(n_1 \psi(h_1)(n_2) h_1 h_2) = f(n_1 \psi(h_1)(n_2) h_1 h_2) \\ &= f(n_1) f(\psi(h_1)(n_2)) h_1 h_2 = f(n_1)[f \circ \psi(h_1) \circ f^{-1} \circ f](n_2).h_1 h_2 \\ &= f(n_1)(\overline{f} \circ \psi)(h_1)(f(n_2)).h_1 h_2 = f(n_1) h_1 f(n_2) h_2 = \theta(n_1 h_1)\theta(n_2 h_2), \end{aligned} $$

which shows that θ is a homomorphism. But the homomorphism sending $nh \in N{:}^{\overline{f} \circ \psi} H$ to $f^{-1}(n)h \in N{:}^{\psi} H$ is the inverse of θ, and therefore θ is an isomorphism.

□

Theorem 6.3.7 *Let p be an odd prime. Then there is exactly one isomorphism class of non-abelian groups of order p^3 having no elements of order p^2.*

Proof. Let G be a non-abelian group of order p^3 with no elements of order p^2 by Lemma 6.3.1, there exists $N \trianglelefteq G$ such that $|N| = p^2$. Obviously $N \cong C_p \times C_p$. Let $x \in G - N$. Then we must have $o(x) = p$ and $H =< x >$ is a cyclic group of order p. It is easy to see that $N \cap H = \{1_G\}$ and $G = N{:}H$. Thus $G \cong (C_p \times C_p){:}C_p$. Let ψ and φ be monomorphisms from C_p to $Aut(C_p \times C_p) \cong GL(2,p)$. Then $\varphi(C_p)$ and $\psi(C_p)$ are subgroups of order p in $GL(2,p)$. Since $|GL(2,p)| = p(p-1)^2(p+1)$, $\varphi(C_p)$ and $\psi(C_p)$ are Sylow p-subgroups of $Aut(C_p \times C_p)$. Then $\varphi(C_p)$ and $\psi(C_p)$ are conjugate in $Aut(C_p \times C_p)$ and hence there exists $f \in Aut(C_p \times C_p)$ such that $\varphi(C_p) = f\psi(C_p)f^{-1}$.

Let $\overline{f}$ be the inner automorphism of $Aut(C_p \times C_p)$ induced by f. Then we have $\varphi(C_p) = (\overline{f} \circ \psi)(C_p)$ and hence $(C_p \times C_p){:}^{\psi}C_p \cong (C_p \times C_p){:}^{\overline{f}\circ\psi}C_p \cong (C_p \times C_p){:}^{\varphi}C_p$ by Proposition 6.1.1 and Lemma 6.3.6. □

Remark 6.3.8 Let $N =< x > \cong C_{p^2}$. As we have seen in the proof of Theorem 6.2.3 (case 1)

$$Aut(C_{p^2}) = \{f_i \mid f_i(x) = x^i, \ \ 1 \leq i \leq p^2, \ (i,p^2) = 1\ \} \cong \ \ C_p \times C_{p-1}.$$

Consider the non-abelian extension $N{:}^{\varphi}H$ where $H =< y > \cong C_p$ and $\varphi : H \longrightarrow Aut(N)$ is a homomorphism given by $\varphi_y = f_i$ with $1 \leq i \leq p(p-1)$. Then ${\varphi_y}^p = {f_i}^p = 1_{Aut(C_{p^2})}$ and hence we deduce that $x^{i^p} = x$ for all $x \in N$. So that $i^p \equiv 1(mod p^2)$. Now the group $N{:}^{\varphi}H$ has the following presentation :

$$N{:}^{\varphi}H =< x, y \mid x^{p^2} = y^p = 1\ , yxy^{-1} = x^i, \ 1 < i \leq p^2, \ (i,p^2) = 1, \ i^p \equiv 1(mod p^2) > \ .$$

If p is odd, then the above extension is unique, up to isomorphism by Theorem 6.3.5.

If $p = 2$, then $p^2 \mid i^p - 1$ implies that $4 \mid i^2 - 1$. Since $1 \leq i \leq 4$ and $(i,4) = 1$, we have $i \in \{1,3\}$. If $i = 1$ then $yxy^{-1} = x$, and $N{:}^{\varphi}H \cong C_{p^2} \times C_p$. If $i = 3$, then

$$N{:}^{\varphi}H =< x, y \mid x^4 = y^2 = 1, yxy^{-1} = x^3 = x^{-1} > \cong D_8.$$

Remark 6.3.9 Let $N =< x_1, x_2 > \cong C_p \times C_p$. As we have seen in the proof of Theorem 6.2.3 (case 2)

$$\begin{aligned} Aut(C_p \times C_p) &= \left\{ \ f \ \mid \ f(x_1) = x_1^a x_2^c, \ \ f(x_2) = x_1^b x_2^d \ \ ad - bc \neq 0, \ \ a,b,c,d \in \mathbb{Z}_p \right\} \\ &\cong \ GL(2,p). \end{aligned}$$

Consider the extension $N{:}^{\varphi}H$ where $H =< y > \cong C_p$ and $\varphi : H \longrightarrow Aut(N)$ is a homomorphism given by $\varphi_y(x_1) = x_1^a x_2^c$ and $\varphi_y(x_2) = x_1^b x_2^d$ with $a,b,c,d \in \mathbb{Z}_p$ and $ad - bc \neq 0,$. Then

$$N{:}^{\varphi}H =< x_1, x_2, y \mid x_1^p = x_2^p = y^p = 1, \ yx_1y^{-1} = x_1^a x_2^c, \ yx_2y^{-1} = x_1^b x_2^d, [x_1, x_2] = 1 > .$$

By Theorem 6.3.7, the non-abelian group of the above type is unique up to isomorphism.

For example, if $p = 2$, and we let $\varphi_y(x_1) = x_1$, $\varphi_y(x_2) = x_1x_2$ we get the following presentation

$$< x_1, x_2, y \mid x_1^2 = x_2^2 = y^2 = 1 \ , x_1x_2 = x_2x_1, \ \ yx_1y^{-1} = x_1, \ \ yx_2y^{-1} = x_1x_2 >$$

which produces a group isomorphic to D_8.

Note 6.3.10 From the above results we can deduce that unlike all other groups of order p^3 the quaternion group Q cannot be written non-trivially as a semidirect product.

Chapter 7

Frattini Extensions

7.1 Frattini Extensions

In this section we give an account of the study of the Frattini extensions. For the study of Frattini extensions we have extensively used [[2],[3],[6],[17]]. In order to accomplish our study we need the following definitions.

Definition 7.1.1 (G-Module) *Given a (multiplicativelly written) group G, a G-***module** *is an (additivelly written) abelian group A together with an action of G on A such that the following axioms hold for all $a, b \in A,\ g, h \in G$.*

(i) $(a+b)g = ag + bg$

(ii) $a(gh) = (ag)h$

(iii) $a1_G = a.$

Definition 7.1.2 (Submodule) *A subset B of a G-module A is said to be a* **submodule** *if B is a subgroup of A, and is closed under the action of G, that is, $bg \in B$ for all $b \in B$ and $g \in G$.*

Remark 7.1.3 Abelian groups can be regarded as $\mathbb{Z}$- modules. Elementary abelian p-groups can be regarded as modules over $GF(p) = \mathbb{Z}/p\,\mathbb{Z}$ (the naturally induced action is well defined as every element is annihilated by every multiple of p). Since $\mathbb{Z}_p$ is a field, elementary abelian groups are in fact vector spaces.

Definition 7.1.4 *Let G be a group. An extension (G,ϵ) is called a* **Frattini extension** *if the Kernel of ϵ is contained in the Frattini subgroup $\Phi(G)$ of G.*

Here we use (G,ϵ) as a shortened representation for $\{1_N\} \to N \to \mathrm{G} \xrightarrow{\epsilon} \mathrm{H} \to \{1_H\}$.

Theorem 7.1.5 gives a useful characterization of the Frattini extensions for finite groups.

Theorem 7.1.5 *Let G be an extension of N by H and assume that G is finite. Then G is a Frattini extension of N by H if and only if $G/\Phi(G) \cong H/\Phi(H)$.*

Proof. Assume that G is a Frattini extension of N by H. Since $N \leq \Phi(G)$and $G/N \cong H$, we have $\Phi(G)/N = \Phi(G/N) \cong \Phi(H)$. Thus $H/\Phi(H) \cong (G/N)/\Phi(G/N) \cong (G/N)/\Phi(G)/N \cong G/\Phi(G)$.

Conversely assume that $G/\Phi(G) \cong H/\Phi(H)$. Then $G/\Phi(G) \cong (G/N)/\Phi(G/N)$, since $H \cong G/N$. Since $\Phi(G/N) \supseteq \Phi(G)N/N \cong \Phi(G)/N \cap \Phi(G)$, we have

$$\begin{aligned}
\frac{|G|}{|\Phi(G)|} &= \frac{|G|}{|N|} \times \frac{1}{|\Phi(G/N)|} \leq \frac{|G|}{|N|} \times \frac{|N \cap \Phi(G)|}{|\Phi(G)|} \\
&\Rightarrow 1 \leq \frac{|N \cap \Phi(G)|}{|N|} \\
&\Rightarrow |N| \leq |N \cap \Phi(G)| \\
&\Rightarrow |N| = |N \cap \Phi(G)| \\
&\Rightarrow N = N \cap \Phi(G) \\
&\Rightarrow N \leq \Phi(G).
\end{aligned}$$

□

The following Lemma [Lemma 7.1.6] is a stated problem by D.Holt and W.Plesken in [17]. We give a detailed proof for this Lemma and derive some new properties of the Frattini extensions.

Lemma 7.1.6 *[17] Let (G,ϵ) be an extension in which $Ker(\epsilon)$ is a finite G-module. If L is a maximal subgroup of G which does not contain $Ker(\epsilon)$, then (L,α) is an extension with $\alpha = \epsilon|_L$ and $Ker(\alpha)$ a maximal G-submodule of $Ker(\epsilon)$.*

Proof. Let $\{1_N\} \to N \to \mathrm{G} \xrightarrow{\epsilon} \mathrm{H} \to \{1_H\}$ be the given extension where $N = Ker(\epsilon)$. We need to show that:

(i) (L,α) is an extension.

(ii) $Ker(\alpha)$ is a maximal G-submodule of $Ker(\epsilon)$.

(i) Since $N \not\leq L$ and L is a maximal subgroup of G, $L < LN \leq G$. But L is maximal in G implies that $LN = G$. Now, since (G, ϵ) is an extension we have that $G/N \cong H$, so $LN/N = G/N \cong H$. But $LN/N \cong L/N \cap L \cong H$ implies that L is an extension of $N \cap L$ by H. Also note that

$$\begin{aligned} Ker(\alpha) &= \{l \mid l \in L,\ \alpha(l) = 1_G\} = \{l \mid l \in L,\ \epsilon(l) = 1_G\} \\ &= \{l \mid l \in L,\ l \in Ker(\epsilon)\} = L \cap Ker(\epsilon) = L \cap N. \end{aligned}$$

(ii) Suppose to the contrary, that is, $Ker(\alpha) = N \cap L$ is not a maximal G-submodule of $Ker(\epsilon)$. Then there exists a G-submodule K of N such that $N \cap L < K < N$. Since $N \not\leq L$, we deduce that $L < LK < G$. This contradicts the maximality of L in G. Hence $N \cap L$ is a maximal G-submodule of $Ker(\epsilon)$. □

Now if $Ker(\epsilon)$ is an irreducible G-module we use Lemma 7.1.6 to prove the following result.

Theorem 7.1.7 *Let $Ker(\epsilon)$ be an irreducible G-module. Then (G, ϵ) is a Frattini extension if and only if it is non-split.*

Proof. Suppose that $\{1_N\} \to N \to G \xrightarrow{\epsilon} H \to \{1_H\}$ (*) is a non-split extension. We need to show that $N = Ker(\epsilon)$ is a subgroup of $\Phi(G)$. If $N \not\leq \Phi(G)$, then there exists L a maximal subgroup of G such that $N \not\leq L$ and so by Lemma 7.1.6 we have that (L, α) is an extension, with $\alpha = \epsilon|_L$. Moreover, $Ker(\alpha)$ is a maximal G-submodule of $Ker(\epsilon)$ and since $Ker(\epsilon)$ is irreducible as a G-module we have that $Ker(\alpha) = N \cap L = \{1_G\}$ or $Ker(\alpha) = N$. If $Ker(\alpha) = N$ we have that $N \leq L$ which is a contradiction. Hence $Ker(\epsilon) = \{1_G\}$ and therefore α is a monomorphism. But α is an epimorphism, since (L, α) is an extension. Hence α is an isomorphism, and so $\alpha^{-1} : H \longrightarrow L$ is also an isomorphism. Since $L \leq G$, we have that $\alpha^{-1} : H \longrightarrow G$ is a monomorphism. Now for all $h \in H$ we have

$$\begin{aligned} (\epsilon\alpha^{-1})(h) = \epsilon(\alpha^{-1}(h)) &= \epsilon(l) \quad \text{where } \alpha^{-1}(h) = l \text{ for some } l \in L \\ &= \alpha(l) = h. \end{aligned}$$

Hence $(\epsilon\alpha^{-1}) = I_H$, and so (*) splits, which is a contradiction.

Conversely, suppose that (G, ϵ) is a Frattini extension. We need to show that (*) is non-split. Suppose that (*) splits. Then there exists a homomorphism say ϕ from H into G such that $\epsilon\phi = I_H$, and so ϕ is a monomorphism and therefore $H \cong Im(\phi)$. Hence $\phi : H \longrightarrow Im(\phi)$ is an isomorphism. Also, we have that $Im(\phi) \leq G$ and $Ker(\epsilon) \leq G$. It is easy to show that $G = Ker(\epsilon).Im(\alpha)$ and $Ker(\epsilon) \cap Im(\alpha) = \{1_G\}$. Thus $G = Ker(\epsilon){:}Im(\phi)$ is a split extension. Since $Im(\phi) \not\supseteq Ker(\epsilon)$, $Im(\phi)$ is not a maximal subgroup of G. Thus there exists L a maximal subgroup of G such that $Im(\phi) < L < G$. But maximality of L implies that $L \supseteq \Phi(G) \supseteq Ker(\epsilon)$. Now, $Ker(\epsilon) \leq L$ and $Im(\phi) < L$ implies that $L \supseteq Ker(\epsilon)Im(\phi) = G$, which is contradiction. □

Remark 7.1.8 A simplest example of a Frattini extension is a non-split extension with $Ker(\epsilon)$ an irreducible G-module.

Corollary 7.1.9 *If (G, ϵ) is a Frattini extension, then (G, ϵ) is non-split.*

Proof. The proof follows from the argument used in the second part of the proof of Theorem 7.1.7 or alternatively we can use Lemma 2.4.16. □

Theorem 7.1.10 *If (G, ϵ) is a Frattini extension, then $(\Phi(G), \epsilon)$ is also a Frattini extension.*

Proof. Since (G, ϵ) is an extension, we have $G/Ker(\epsilon) \cong H$, and so $\Phi(G/Ker(\epsilon)) \cong \Phi(H)$. By Lemma 2.4.14 (ii), we have that $\Phi(G/Ker(\epsilon)) = \Phi(G)/Ker(\epsilon)$ and hence $\Phi(G) = Ker(\epsilon)\Phi(H)$. □

Theorem 7.1.11 *[17] Let G be a finite group and let (G, ϵ) be a Frattini extension of N by H with H a perfect group. Then G is perfect.*

Proof. Suppose that G is not perfect. Since H is perfect we have that $H = H'$ and since G is an extension we have that $G/Ker(\epsilon) \cong H$. Set $N = Ker(\epsilon)$. Thus we have that $G/N \cong H$. Now $(G/N)' \cong H' = H$ imply that $(G/N)' \cong G/N$. $(*)$ Since $G'N \leq G$ and $G'N \supseteq N$, we have $(G/N)' = G'N/N \leq G/N$. So by (*) we have that $G'N/N = G/N$. Since G is finite and $G'N \leq G$, we have that $|G'N| = |G|$. Hence $G'N = G$. Since $N \leq \Phi(G)$, then by Lemma 2.4.16 we get a contradiction. Hence G is perfect. □

In [6] J.Cossey, O. Këgel and L. Kovács stated the following results (Theorem 7.1.12, Proposition 7.1.13 and Theorem 7.1.14) about Frattini extensions to which we give detailed proofs.

Theorem 7.1.12 *[6] If $\epsilon : L \longrightarrow M$ is an epimorphism of finite groups and G is minimal among the subgroups of L, with $\epsilon(G) = M$, then $(G, \epsilon|_G)$ is a Frattini extension.*

Proof. Let K be a maximal subgroup of G such that $Ker(\epsilon|_G) \nsubseteq K$ then we have $K < K.Ker(\epsilon|_G) \leq G$. Now maximality of K implies that $K.Ker(\epsilon|_G) = G$. Also we have that $Ker(\epsilon) \trianglelefteq L$, $Ker(\epsilon) \supseteq Ker(\epsilon|_G)$ and $K \leq L$. Thus $K \leq G = K.Ker(\epsilon|_G) \leq K.Ker(\epsilon) \leq L$. (1) Let $W = K.Ker(\epsilon)$, then

$$\begin{aligned} \epsilon(W) &= \{\epsilon(kx) \mid k \in K \quad \text{and} \quad x \in Ker(\epsilon)\} \\ &= \{\epsilon(k)\epsilon(x) \mid k \in K \quad \text{and} \quad x \in Ker(\epsilon)\} = \{\epsilon(k) \mid k \in K\} = \epsilon(K). \end{aligned}$$

Now by (1) we have that $\epsilon(G) \leq \epsilon(W) \leq \epsilon(L)$, that is $M \leq \epsilon(W) \leq M$. Thus $\epsilon(W) = M$ and hence $\epsilon(K) = M$. Since $K < G$ and $\epsilon(K) = M$, minimality of G produces a contradiction. It follows that $Ker(\epsilon|_G)$ is contained in every maximal subgroup of G and hence in the Frattini subgroup of G. Therefore $(G, \epsilon|_G)$ is a Frattini extension. □

Proposition 7.1.13 *[6] If (G, α) is a Frattini extension and $\beta : F \longrightarrow G$ is a homomorphism, such that $\alpha\beta$ is surjective, then β is surjective.*

Proof. Let $K = Im(\beta) = \beta(F)$. Since $\alpha\beta$ is surjective, we have that $G = (\alpha\beta)(F) = \alpha(\beta(F)) = \alpha(K)$. So for any $g \in G$, there exists $k \in K$ such that $\alpha(g) = \alpha(k)$. We have

$$\begin{aligned} \alpha(g) = \alpha(k) &\Rightarrow \alpha(gk^{-1}) = 1_G \\ &\Rightarrow gk^{-1} \in Ker(\alpha) \\ &\Rightarrow g \in Ker(\alpha)K, \forall g \in G \\ &\Rightarrow G \subseteq Ker(\alpha)K. \quad (1) \end{aligned}$$

Now $K \leq G$ and $Ker(\alpha) \trianglelefteq G$ implies that $Ker(\alpha)K \leq G$. Hence by (1) we have that $G = Ker(\alpha)K$. Since $Ker(\alpha) \leq \Phi(G)$, by Lemma 2.4.16 we deduce that $K = G$ and hence β is surjective. □

Theorem 7.1.14 *[6] Composites of Frattini extensions are Frattini extensions.*

Proof. Consider $\{1\} \rightarrow Ker(\alpha) \rightarrow \mathrm{G} \xrightarrow{\alpha} \mathrm{H} \rightarrow \{1\}$ with α an epimorphism and $Ker(\alpha) \leq \Phi(G)$ and let $\{1\} \rightarrow Ker(\beta) \rightarrow \mathrm{H} \xrightarrow{\beta} \mathrm{M} \rightarrow \{1\}$ with β an epimorphism and $Ker(\beta) \leq \Phi(H)$. We need to show that $\beta\alpha$ is an epimorphism and that $Ker(\beta\alpha) \leq \Phi(G)$.

(i) $\beta\alpha$ is an epimorphism: Since $h \in H$, then there exists $g \in G$ such that $\alpha(g) = h$. If $m \in M$, then there exists $h \in H$ such that $\beta(h) = m$. Hence $(\beta\alpha)(g) = \beta(\alpha(g)) = \beta(h) = m$.

(ii) $Ker(\beta\alpha) \leq \Phi(G)$: Since $\alpha(G) = H$ by Remark 2.4.5 we have that $\alpha(\Phi(G)) = \Phi(\alpha(G)) = \Phi(H)$. Thus $\Phi(G) = \alpha^{-1}(\Phi(H))$, the inverse image of $\Phi(H)$. But,

$$Ker(\beta\alpha) = \{g \mid (\beta\alpha)(g) = 1_M \ , \ g \in G\}$$

$$\begin{aligned} &= \{g \mid \beta(\alpha(g)) = 1_M \ , \ g \in G\} \\ &= \{g \mid \alpha(g) \in Ker(\beta) \ , \ g \in G\} \\ &= \{g \mid g \in \alpha^{-1}(Ker(\beta))\}. \end{aligned}$$

Since $Ker(\beta) \leq \Phi(H)$, we have that $\alpha^{-1}(Ker(\beta)) \leq \alpha^{-1}(\Phi(H)) = \Phi(G)$. Hence $Ker(\beta\alpha) \leq \Phi(G)$. □

The following theorem is a straightforward consequence of Theorem 2.4.27.

Theorem 7.1.15 *Let N be a finite abelian group. Then there exists a Frattini extension (G, ϵ) with $Ker(\epsilon) = N$.*

Proof. Since N is abelian, $Inn(N) = \{1_G\}$ and hence $Inn(N) \leq \Phi(Aut(N))$. Now by Theorem 2.4.27 we deduce that there exists a finite group G with $N \trianglelefteq G$ and $N \leq \Phi(G)$. If ϵ is the natural homomorphism from G into G/N, then $Ker(\epsilon) = N$. Hence (G, ϵ) is a Frattini extension with $Ker(\epsilon) = N$. □

Now if G is a p-group we will show that $\Phi(G)$ is an extension of G' by $\Phi(G/G')$.

Theorem 7.1.16 *If G is a p-group, then $\Phi(G)$ is an extension of G' by $\Phi(G/G')$.*

Proof. Since G is a p-group, G is nilpotent and hence $G' \leq \Phi(G)$. Also $G' \trianglelefteq G$ therefore $G' \trianglelefteq \Phi(G)$. Since $\Phi(G/G') = \Phi(G)/G'$ by Lemma 2.4.14, we deduce that $\Phi(G)$ is an extension of G' by $\Phi(G/G')$. □

Remark 7.1.17 The extension given in Theorem 7.1.16 is not a Frattini extension in general. For example take $G = Q$, the group of quaternions or $G = D_8$. It can be easily checked that $G' = \Phi(G) \cong C_2$ and $\Phi(\Phi(G)) = \{1_G\}$. Thus $G' \not\leq \Phi(\Phi(G))$ and hence the extension $\Phi(G)$ of G' by $\Phi(G/G')$ is not a Frattini extension.

In the following we determine all the non-abelian groups of order 16 and 32 for which $G' \leq \Phi(\Phi(G))$, respectively.

Example 7.1.18 From the library of small groups of GAP4 [33] we found that there are 14 non-isomorphic groups of order 16. Only 9 of these groups are non-abelian. We consider these non-abelian groups and label them as G_i with $1 \leq i \leq 9$ as listed in the first column of Table 1. The remaining columns of Table 1 have been computed by using GAP. It can be observed from Table 1 that the group G_3 is the only non-abelian group of order 16 for which $\Phi(G)$ is a Frattini extension of G' by $\Phi(G/G')$.

Table 1 : Non-abelian groups of order 16

G	$\Phi(G)$	G'	$\Phi(\Phi(G))$
G_1	V_4	C_2	$\{1_G\}$
G_2	V_4	C_2	$\{1_G\}$
G_3	C_4	C_2	C_2
G_4	C_4	C_4	C_2
G_5	C_4	C_4	C_2
G_6	C_4	C_4	C_2
G_7	C_2	C_2	$\{1_G\}$
G_8	C_2	C_2	$\{1_G\}$
G_9	C_2	C_2	$\{1_G\}$

Similarly there are 51 non-isomorphic groups of order 32. Only 44 of these are non-abelian and are labeled as G_i with $1 \leq i \leq 44$. These groups are listed in the first column of Table 2. As in Table 1, we completed the remaining columns of Table 2. We observe that there are 6 possible candidates among G_i, $1 \leq i \leq 44$ for which we may have $G' \leq \Phi(\Phi(G))$, namely $G_2, G_3, G_{10}, G_{14}, G_{32}$ and G_{33}. It is clear that G_{14}, G_{32} and G_{33} satisfy the condition $G' \leq \Phi(\Phi(G))$. Further investigation eliminates G_3 and G_{10}. Hence G_2, G_{14}, G_{32} and G_{33} are the only non-abelian groups of order 32 for which $\Phi(G)$ is a Frattini extension of G' by $\Phi(G/G')$.

Table 2 : Non-abelian groups of order 32

G	$\Phi(G)$	G'	$\Phi(\Phi(G))$
G_1	C_{2^3}	C_2	$\{1_G\}$
G_2	$C_4 \times C_2$	C_2	C_2
G_3	$C_4 \times C_2$	C_2	C_2
G_4	C_{2^3}	V_4	$\{1_G\}$
G_5	$C_4 \times C_2$	V_4	C_2
G_6	$C_4 \times C_2$	V_4	C_2
G_7	$C_4 \times C_2$	C_4	C_2
G_8	$C_4 \times C_2$	C_4	C_2
G_9	$C_4 \times C_2$	C_4	C_2
G_{10}	$C_4 \times C_2$	C_2	C_2
G_{11}	$C_4 \times C_2$	C_4	C_2
G_{12}	$C_4 \times C_2$	C_4	C_2
G_{13}	$C_4 \times C_2$	C_4	C_2
G_{14}	C_8	C_2	C_4
G_{15}	C_8	C_8	C_4
G_{16}	C_8	C_8	C_4
G_{17}	C_8	C_8	C_4
G_{18}	V_4	C_2	$\{1_G\}$
G_{19}	V_4	C_2	$\{1_G\}$
G_{20}	V_4	C_2	$\{1_G\}$
G_{21}	V_4	C_2	$\{1_G\}$
G_{22}	V_4	V_4	$\{1_G\}$
G_{23}	V_4	V_4	$\{1_G\}$
G_{24}	V_4	V_4	$\{1_G\}$
G_{25}	V_4	V_4	$\{1_G\}$
G_{26}	V_4	V_4	$\{1_G\}$
G_{27}	V_4	V_4	$\{1_G\}$
G_{28}	V_4	V_4	$\{1_G\}$
G_{29}	V_4	V_4	$\{1_G\}$
G_{30}	V_4	V_4	$\{1_G\}$
G_{31}	V_4	V_4	$\{1_G\}$
G_{32}	C_4	C_2	C_2
G_{33}	C_4	C_2	C_2
G_{34}	C_4	C_4	C_2

Table 2 : Non-abelian groups of order 32*(continued)*

G	$\Phi(G)$	G'	$\Phi(\Phi(G))$
G_{35}	C_4	C_4	C_2
G_{36}	C_4	C_4	C_2
G_{37}	C_4	C_4	C_2
G_{38}	C_4	C_4	C_2
G_{39}	C_4	C_4	C_2
G_{40}	C_2	C_2	$\{1_G\}$
G_{41}	C_2	C_2	$\{1_G\}$
G_{42}	C_2	C_2	$\{1_G\}$
G_{43}	C_2	C_2	$\{1_G\}$
G_{44}	C_2	C_2	$\{1_G\}$

Definition 7.1.19 *A group G is called a* **minimal Frattini extension** *of N by H, if it is a Frattini extension of N by H and N is a minimal normal subgroup of G.*

Lemma 7.1.20 *Let N be a minimal normal subgroup of G. If N has a complement in G, then $N \cap \Phi(G) = \{1_G\}$.*

Proof. If N is complemented in G then $G = NH$ and $N \cap H = \{1_G\}$ for some proper subgroup H of G. Since $N \trianglelefteq G$ and $\Phi(G) \leq G$, we have $N \cap \Phi(G) \trianglelefteq G$. Now $N \cap \Phi(G) \leq N$ and minimality of N implies that $N \cap \Phi(G) = \{1_G\}$ or $N \cap \Phi(G) = N$. If $N \cap \Phi(G) = N$ then $N \subseteq \Phi(G)$ and hence $NH \subseteq \Phi(G)H$, so that $G = \Phi(G)H$ and therefore $H = G$ by Corollary 2.4.9 which is not possible. Thus $N \cap \Phi(G) = \{1_G\}$ as required. □

We use Lemma 7.1.20 to give a full proof for the following theorem which was stated as Lemma 4.6 by Eick in [3].

Theorem 7.1.21 *[3] Let G be an extension of N by H. Then G is a minimal Frattini extension of N, if and only if N is a minimal non-complemented normal subgroup of G.*

Proof. Let N be a minimal normal subgroup of G. Suppose that N does not have a complement in G. Then $N \leq \Phi(G)$ by Lemma 2.4.16 and therefore G is a minimal Frattini extension. Conversely, if N is a complemented minimal normal subgroup of G, then by Lemma 7.1.20 we have that $N \cap \Phi(G) = \{1_G\}$ and hence N is not a subgroup of $\Phi(G)$. Hence G is not a Frattini extension. □

Remark 7.1.22 The minimal Frattini extensions of H are exactly the non-split extensions of H by an irreducible H-module M. See [3].

To construct the minimal Frattini extensions of H we have to consider all suitable irreducible H-modules M. Based on the theory of Frattini extensions, in [3] Bettina Eick and Hans Besche described a method to compute the minimal Frattini extensions. This method together with other related methods has been implemented in GAP4 [33] in order to classify the groups of order at most 1000, except the groups of order 512 and 768.

Chapter 8

Commutator extensions

8.1 Commutator extensions

In this chapter we intend to give an account on the study of the commutator extensions. By first reducing the study to the case in which N is an elementary abelian p-group we then build up to the necessary and sufficient conditions for the existence of a split commutator extension.

Definition 8.1.1 *Let N and H be groups. An extension G of N by H is said to be a* **commutator extension** *if N is the commutator subgroup G' of G.*

Remark 8.1.2 (i) Since G is an extension we have $G/N \cong H$. But $G/N = G/G'$ is abelian, so in order that there exists a commutator extension of N by H, H must be abelian. On the other hand, if N' is the commutator subgroup of N then N/N' is abelian. We may assume that N/N' is also finite. Henceforth, we may assume that H is abelian and finite.

(ii) The commutator subgroup N' of N is normal not only in N, but also in every extension of N. Since N' is a characteristic subgroup of N and $N \trianglelefteq G$, we have that $N' \trianglelefteq G$.

Theorem 8.1.3 *[28] G is a commutator extension of N by H if and only if G/N' is a commutator extension of N/N' by H.*

Proof. From the isomorphism $G/N \cong (G/N')/(N/N')$, it follows that G is an extension of N by H if and only if G/N' is an extension of N/N' by H. Now if $N = G'$, we have

$(G/N')' = G'N'/N' = NN'/N' = N/N'$. Thus G/N' is a commutator extension of N/N' by H.

Conversely if G/N' is a commutator extension of N/N' by H, then $N/N' = (G/N')'$. Now $N/N' = G'N'/N'$ and since $N' \leq G'$, we have that $N/N' = G'/N'$. Therefore $N = G'$. Hence G is a commutator extension of N by H. □

Remark 8.1.4 Theorem 8.1.3 reduces the discussion to the case in which N is finite abelian. If N is trivial, then every extension of N by H is a commutator extension. For if $N = \{1_G\}$ then $N = G' = \{1_G\}$. So $G/\{1_G\} = G \cong H$ is abelian. We may assume that N is a non-trivial finite abelian group. This lead us to the study of extensions of N by H where N and H are both finite abelian groups.

In order for us to elaborate in the study of other properties of the commutator extensions we need some concepts from the theory of extensions of N by H where N and H are both finite abelian groups .

Definition 8.1.5 *Let G be an extension of N by H, so that $G/N \cong H$. Let $\varphi : G \longrightarrow H$ be the epimorphism whose kernel is N. An element $\overline{u} \in G$ is called a* **representative** *of $u \in H$ if $\varphi(\overline{u}) = u$.*

Definition 8.1.6 *Let $(z_1,\ z_2,\ \cdots,\ z_s)$ be a basis of H, and let n_i be the order of z_i. An s-tuple $S = (\overline{z_1}\ ,\overline{z_2},\ \cdots,\ \overline{z_s})$ is called a* **set representative** *of the basis if each $\overline{z_i}$ is a representative of z_i.*

Definition 8.1.7 *Given a pair $(G,\ S)$ we define a triple $(X,\ B,\ M)$ where $X = (x_1,\ x_2,\ \cdots,\ x_s)$, $B = (b_1,\ b_2,\ \cdots,\ b_s)$, $M = (b_{ij})$ $(1 \leq i \leq s\ 1 \leq j \leq s)$ by the conditions*
(1) $a^{x_i} = \overline{z_i} a \overline{z_i}^{-1}$, for all $a \in N$,
(2) $z_i{}^{m_i} = b_i \in N$,
(3) $\overline{z_i}\ \overline{z_j}\ \overline{z_i}^{-1} \overline{z_j}^{-1} = b_{ij} \in N$,
the mappings $a \longmapsto a^{x_i}$ of N onto itself are automorphisms of N. Since $N \trianglelefteq G$, we have that $a^{x_i} = \overline{z_i} a \overline{z_i}^{-1} \in N$.

Lemma 8.1.8 *Let G be a commutator extension of N by H. A subgroup K of N is normal in G if and only if K is invariant under X.*

Proof. Assume that $K \trianglelefteq G$. Then $gkg^{-1} \in K$ for all $g \in G$ and $k \in K$. Now let $x_i \in X$ and $k \in K$. Then $k^{x_i} = \overline{z_i} k \overline{z_i}^{-1} \in K$, for all i, since $z_i \in G$. Hence K is invariant under X.

Conversely if $k^{x_i} \in K$ for all $x_i \in X$ we have that $\overline{z_i}k\overline{z_i}^{-1} \in K$ for all i. We show that $gkg^{-1} \in K$ for all $g \in G$ and $k \in K$. Since G is a commutator extension we have that $G/N = G/G' = H$ is a finite abelian group. So $gn \in H =< z_1, z_2, \cdots, z_s >$ and $gn = {z_1}^{\alpha_1}.{z_2}^{\alpha_2}\cdots {z_s}^{\alpha_s}$. On the other hand

$$(\overline{z_1})^{\alpha_1}.(\overline{z_2})^{\alpha_2}\cdots(\overline{z_s})^{\alpha_s}N = (\overline{z_1})^{\alpha_1}n \odot (\overline{z_2})^{\alpha_2}n \odot \cdots \odot (\overline{z_s})^{\alpha_s}n = {z_1}^{\alpha_1}.{z_2}^{\alpha_2}\cdots{z_s}^{\alpha_s} = gn.$$

Hence $g = (\overline{z_1})^{\alpha_1}(\overline{z_2})^{\alpha_2}\cdots(\overline{z_s})^{\alpha_s}n$. Now

$$\begin{aligned} gkg^{-1} &= (\overline{z_1})^{\alpha_1}(\overline{z_2})^{\alpha_2}\cdots(\overline{z_s})^{\alpha_s}nk[(\overline{z_1})^{\alpha_1}(\overline{z_2})^{\alpha_2}\cdots(\overline{z_s})^{\alpha_s}n]^{-1} \\ &= (\overline{z_1})^{\alpha_1}(\overline{z_2})^{\alpha_2}\cdots(\overline{z_s})^{\alpha_s}nkn^{-1}(\overline{z_s})^{-\alpha_s}\cdots(\overline{z_2})^{-\alpha_2}(\overline{z_1})^{-\alpha_1} \\ &= (\overline{z_1})^{\alpha_1}(\overline{z_2})^{\alpha_2}\cdots(\overline{z_s})^{\alpha_s}k'(\overline{z_s})^{-\alpha_s}\cdots(\overline{z_2})^{-\alpha_2}(\overline{z_1})^{-\alpha_1}, \text{ since } K \trianglelefteq N. \end{aligned}$$

Since K is invariant under X we have that $gkg^{-1} \in K$ for all $z_i \in G$ so that $K \trianglelefteq G$. □

Lemma 8.1.9 *If G is a commutator extension of N by H, then for each subgroup K of N invariant under X, G/K is a commutator extension of N/K by H.*

Proof. Assume that G is a commutator extension of N by H. Then $N = G'$. Also, let K be an X-invariant subgroup of N. Then by the Lemma 8.1.8 we have that $K \trianglelefteq G$. We need to show that $(G/K)' = N/K$. But

$$\begin{aligned} (G/K)' = G'K/K &= NK/K, \text{ since } G \text{ is a commutator extension} \\ &= N/K, \text{ since } K \leq N. \end{aligned}$$

Hence G/K is a commutator extension of N/K by H. □

Lemma 8.1.10 *Suppose that $N = N_1 \times N_2$ and that $\gcd(n_1, n_2) = 1$, where n_1 and n_2 are the orders of N_1 and N_2 respectively. If there exists commutator extensions of N_1 and N_2 by H, then there exists a commutator extension of N by H.*

Proof. See Lemma 2 of [28]. □

Lemma 8.1.11 *Let N and H be finite abelian groups. There exists a commutator extension of N by H if and only if for each Sylow subgroup N_p of N, there exists a commutator extension of N_p by H.*

Proof. Since N is a finite abelian group, we have that N is the direct product of its Sylow subgroups. Let $N = N_1 \times N_2 \times \cdots \times N_r$, where the N_i are Sylow p-subgroups of N. If

$n_1, n_2, \cdots, n_r$ are respectively the orders of the $N_i's$, then $\gcd(n_i, n_j) = 1$, for all $i \neq j$. Now if for each Sylow p-subgroup N_i of N there exists a commutator extension of N_i by H, then by Lemma 8.1.10 we have that there exists a commutator extension of N by H.

Conversely assume that G is a commuator extension of N by H. Since N is a finite abelian group we have $N = N_1 \times N_2 \times \cdots \times N_r$ with each N_i a Sylow p-subgroup of N. Thus use of Lemma 8.1.9 yields that for each such a Sylow p-subgroup N_i, G/N_i is a commutator extension of N/N_i by H and the proof follows by the Theorem 8.1.3. □

Theorem 8.1.12 *Let N be a finite abelian p-group, and let H be a finite abelian group. G is a commutator extension of N by H if and only if G/N^p is a commutator extension of N/N^p by H.*

Proof. Since $N^p = \{x^p \mid x \in N\}$, it can be easily checked that N^p is a characteristic subgroup of N. Hence N^p is a normal subgroup of G. So G/N^p is a group. Now, since G is a commutator extension of N by H and $N^p \trianglelefteq G$, by the Lemma 8.1.9 we obtain that G/N^p is a commutator extension of N/N^p by H.

Conversely assume that G/N^p is a commutator extension of N/N^p by H. Since G/N^p a commutator extension of N/N^p by H, we have that $N/N^p = (G/N^p)'$. So $N/N^p = G'N^p/N^p$ and hence we have $N = G'N^p$. Since N is a finite p-group we have that $\Phi(N) = N'N^p$. But N abelian implies that $N' = \{1_G\}$ so $\Phi(N) = N^p$. Now $\Phi(N) = N^p$ and $N = G'N^p$ imply that $N = G'$. Thus G is a commutator extension of N by H. □

Remark 8.1.13 (i) If N is a finite abelian p-group, then N/N^p is an elementary abelian p-group. For if $x \in N/N^p$ we have $x = nN^p$ for some $n \in N$, and

$$\begin{aligned} x^p = (nN^p)^p &= n^pN^p \\ &= N^p, \text{ since } n^p \in N^p \\ &= 1_{N/N^p} . \end{aligned}$$

(ii) N/N^p is an elementary abelian p group of the same rank as N.

Note 8.1.14 Theorem 8.1.12 and Remark 8.1.13 reduce the study to the case in which N is an elementary abelian p-group.

Theorem 8.1.15 establishes the conditions under which a commutator extension splits.

Theorem 8.1.15 *[28] Let N be an elementary abelian p-group of order p^n, and let H be a finite abelian group of order m. Let $q_1, q_2, \cdots, q_h$ be the distinct prime divisor of m different from p, and let $\gamma_1, \gamma_2, \cdots, \gamma_h$ be the orders of p mod q_1, $\cdots$, q_h, respectively. Then an extension of N by H is a split commutator extension if and only if*

$$n = r_1\gamma_1 + r_2\gamma_2 + \cdots + r_h\gamma_h \ (r_i \text{ nonnegative integers})$$

is solvable for r_i. In particular, $h \geq 1$.

Proof.

See Theorem 4 of [28]. □

Remark 8.1.16 If $\gcd(m, p) = 1$, then by Theorem 4.1.15 every extension of N by H splits over N and so the solvability of the equation given in the Theorem 8.1.15 is a necessary and sufficient condition for the existence of a commutator extension of N by H. Furthermore, Theorem 8.1.15 asserts that if H is also a p-group then there is no split commutator extension of N by H.

Chapter 9

Extensions of non-abelian groups

In the Theorem 9.1.1 we prove that a finite group G splits over an abelian normal subgroup N if its Frattini subgroup $\Phi(G)$ intersects N trivially. However when N is a non-abelian nilpotent normal subgroup of G the condition $\Phi(G) \cap N = \{1_G\}$ cannot be satisfied and hence it has to be modified. We study some similar type of conditions for G to split over N when the restriction of N being an abelian normal subgroup is removed. Also, we study a characterization of the split extensions of N in which every subgroup splits over its intersection with N.

9.1 Extensions of non-abelian groups

Although our aim is the study of extensions of non-abelian groups, the following result which is related to abelian groups is the key point for our discussion.

Theorem 9.1.1 (Gaschutz) *[30] Let G be a finite group and N be an abelian normal subgroup of G. Then G splits over N if $\Phi(G) \cap N = \{1_G\}$.*

Proof. Let $H \leq G$ be minimal subject to $G = HN$. Since $N \trianglelefteq G$, we have that $H \cap N \trianglelefteq H$. Also, since N is abelian we have that $H \cap N \trianglelefteq N$. Therefore $H \cap N \trianglelefteq HN = G$. If $H \cap N \leq \Phi(H)$, then by part (i) of Lemma 2.4.19 we have that $H \cap N \leq \Phi(G) \cap N = \{1_G\}$. Thus, we may assume that $H \cap N \nleq \Phi(H)$. So there is a maximal subgroup M of H such that $H \cap N \nleq M$. Now since $M < M(H \cap N) \leq H$, we get $M(H \cap N) = H$. But $G = HN$ implies $G = M(H \cap N)N = MN$. Hence we obtain a contradiction, since H is minimal by the assumption. □

Lemma 9.1.2 *If N is an abelian minimal normal subgroup of a finite group G, then either $N \leq \Phi(G)$ or G splits over N.*

Proof. Suppose that $N \not\leq \Phi(G)$. Then there exists a maximal subgroup say M of G such that $N \not\leq M$. Now $N \trianglelefteq G$ and $M \leq G$, implies that $NM \leq G$. Since $M < NM \leq G$ and M is maximal in G, we have $NM = G$. Now $M \cap N = \{1_G\}$ follows immediately from the fact that $N \not\leq M$ with M maximal in G and the minimality of N in G. Thus M is a complement of N in G. Hence G splits over N. □

In the Theorem 9.1.1 we have that a finite group G splits over an abelian normal subgroup N if its Frattini subgroup $\Phi(G)$ intersects N trivially. In the following we study the cases when N is either a non-abelian normal nilpotent subgroup or a non-abelian normal solvable subgroup of G.

Remark 9.1.3 If N is a non-abelian nilpotent subgroup of G, we have that $\Phi(G) \cap N \neq \{1_G\}$.

Proof. Since N is non-abelian, we have that $N' \neq \{1_G\}$. Since N is nilpotent, we have $N' \leq \Phi(G)$. Therefore $\{1_G\} \neq N' \leq \Phi(G)$. Now since $N' \leq N$ and $N' \leq \Phi(G)$, we have that $\{1_G\} \neq N' \leq \Phi(G) \cap N$. Hence $\Phi(G) \cap N \neq \{1_G\}$. □

Lemma 9.1.4 *Let N be a nilpotent normal subgroup of G and L be any subgroup of G. If $\Phi(L) \cap N = \{1_G\}$, then $L \cap N$ is abelian.*

Proof. Assume that $\Phi(L) \cap N = \{1_G\}$. Let $M = L \cap N$. Since N is nilpotent and $M \leq N$, then M is nilpotent. Hence M is a nilpotent subgroup of L. Now $\Phi(L) \cap M = \Phi(L) \cap (L \cap N) = \Phi(L) \cap N = \{1_G\}$. Thus M is abelian by the Remark 9.1.3. □

Theorem 9.1.5 *[36] Let N be a nilpotent normal subgroup of G. Then G splits over N if and only if G contains a subgroup L such that $G = LN$ and $\Phi(L) \cap N = \{1_G\}$.*

Proof. Assume that G splits over N. Then we need to show that there exists a subgroup L of G such that $G = LN$ and $\Phi(L) \cap N = \{1_G\}$. Since G splits over N, N has a complement in G. Let L be such a complement. Then $G = LN$ and $L \cap N = \{1_G\}$. Now $\Phi(L) \leq L$ implies that $\Phi(L) \cap N \leq L \cap N = \{1_G\}$. Thus $\Phi(L) \cap N = \{1_G\}$.

Conversely if $G = LN$ and $\Phi(L) \cap N = \{1_G\}$, we need to show that G splits over N. Since $\Phi(L) \cap N = \{1_G\}$ by Lemma 9.1.4 we have that $L \cap N$ is abelian. So by Theorem

9.1.1 we deduce that G splits over $L \cap N$. Now if M is a complement of $L \cap N$ in L, we will show that M is also a complement of N in G. That is $M \cap N = \{1_G\}$ and $MN = G$. Since $M \cap (L \cap N) = \{1_G\}$ and $M(L \cap N) = L$, we have $G = LN = M(L \cap N)N = MN$ and $\{1_G\} = M \cap (L \cap N) = (M \cap L) \cap N = M \cap N$, since $M \leq L$. So M is a complement of N in G and hence G splits over N. □

Lemma 9.1.6 *[35] If a non-trivial group G is solvable, then G contains a characteristic subgroup which is abelian and different from $\{1_G\}$.*

Proof. We may take the last term of the derived series which is different from $\{1_G\}$. □

Theorem 9.1.7 *Let N be a solvable normal subgroup of G. Then G splits over N if and only if G contains a subgroup L, minimal with respect to $G = LN$ such that $\Phi(L) \cap N = \{1_G\}$.*

Proof. Assume that G splits over N. Then N has a complement L in G. Then we have that $G = LN$ and $L \cap N = \{1_G\}$. We need to show that L is minimal with respect to $G = LN$ and that $\Phi(L) \cap N = \{1_G\}$. But L is a complement of N in G implies that L is minimal with respect to $G = LN$. Now since $\Phi(L) \leq L$, we have $\Phi(L) \cap N \leq L \cap N = \{1_G\}$. So that $\Phi(L) \cap N = \{1_G\}$.

Conversely let $M = L \cap N$. Since $N \trianglelefteq G$, we have that $M \trianglelefteq L$. Also since N is solvable, M is a solvable subgroup of L. Therefore M is a normal solvable subgroup of L. Assume that M is a solvable group of length $r \geq 1$. Then by Lemma 9.1.6 we have that the $(r-1)$th derived subgroup $M^{(r-1)}$ is abelian and non-trivial. Also $M^{(r-1)}$ is a characteristic subgroup of M, hence normal in M. So we have that $M^{(r-1)}$ is an abelian normal subgroup of M. Since $M^{(r-1)}$ is abelian, by the Remark 9.1.3 we have that $\Phi(L) \cap M^{(r-1)} = \{1_G\}$. Now by the Theorem 9.1.1 we have that L splits over $M^{(r-1)}$. Hence there exists $H \leq L$ with $L = HM^{(r-1)}$ and $H \cap M^{(r-1)} = \{1_G\}$. Since $G = LN = HM^{(r-1)}N = HN$ and since L is minimal with respect to $G = LN$, we must have that $\{1_G\} = H \cap M^{(r-1)} = L \cap M^{(r-1)} = M^{(r-1)}$ which is a contradiction. Thus $r = 0$ so that $M = L \cap N = \{1_G\}$. Hence G splits over N. □

Using a similar argument to that in the proof of Theorem 9.1.7, with convenient changes, the following result can be proved.

Theorem 9.1.8 *[36] If N is a normal subgroup of G such that there exists a solvable subgroup L of G minimal with respect to $G = LN$, and $\Phi(L) \cap N = \{1_G\}$, then G splits over N.*

Theorem 9.1.9 *[16] A subgroup H of a finite group G is a complement for the extension G over N if and only if H is minimal with respect to the property $G = NH$ and there exists for each prime p a p-Sylow subgroup S of G, and a complement of $N \cap S$ in S which is part of H.*

Proof. See Theorem 1 of [16]. □

Theorem 9.1.10 *G splits over a normal subgroup N if and only if G contains a subgroup L, minimal with respect to $G = LN$ such that for each prime p there exists a Sylow p-subgroup P of L such that $\Phi(P) \cap N = \{1_G\}$.*

Proof. Assume that G splits over N. Since G splits over N, N has a complement in G. Let L be such a complement of N. Then $LN = G$, and $L \cap N = \{1_G\}$. Since L is a complement of N, L is minimal with respect to $G = LN$. Now let $P \in Syl_p(L)$. Then we have that $\Phi(P) \leq L$ and that $\Phi(P) \cap N \leq L \cap N = \{1_G\}$. Hence $\Phi(P) \cap N = \{1_G\}$.

Conversely let L be minimal with respect to $G = LN$ and let $M = L \cap N$. Let $P \in Syl_p(M)$ and $Q \in Syl_p(L)$ such that $P \subseteq Q$. Since for each p there exists a Sylow p-subgroup S of L such that $\Phi(S) \cap N = \{1_G\}$ and since Sylow p-subgroups of L are conjugate, it follows that $\Phi(Q) \cap N = \{1_G\}$. Since $Q \cap N$ is a p-subgroup of M and $Q \cap N \supseteq P$, we have $Q \cap N = P$. Thus P is a nilpotent normal subgroup of Q. Now $\Phi(Q) \cap P \leq \Phi(Q) \cap N = \{1_G\}$ implies that $\Phi(Q) \cap P = \{1_G\}$. Hence by the Theorem 9.1.5 we have that Q splits over P, that is $Q = TP$ for some T complement of P in Q. Now let $R \in Syl_p(N)$ containing P. It can be seen that Q and R generate a Sylow p-subgroup V of G and that $V \cap N = R$. Moreover $V = TR$ and $T \cap R = \{1_G\}$. Thus T is a complement of $V \cap N$ in V. Now $T \subseteq Q \subseteq L$ and L is minimal with respect to $G = LN$. By the Theorem 9.1.9 we have that G splits over N. Therefore L is a complement of N in G. □

Remark 9.1.11 In general the minimality of L with respect to $G = LN$, does not necessarily mean that L is a complement of N, even in the case when N is abelian. In Theorem 9.1.12 we will see that if N is a nilpotent normal subgroup of G, then the minimality of L with respect to $G = LN$ is characterized by $L \cap N \subseteq \Phi(L)$.

Theorem 9.1.12 *[36] Let N be a nilpotent normal subgroup of G. L is minimal with respect to $G = LN$ if and only if $L \cap N \subseteq \Phi(L)$.*

Proof. Let L be a minimal with respect to $G = LN$. Let $L \cap N = M$ and $K = \Phi(L) \cap M$, then $K = \Phi(L) \cap L \cap N = (\Phi(L) \cap L) \cap N = \Phi(L) \cap N$. Now $\Phi(L) \trianglelefteq L$ and $M = L \cap N \trianglelefteq L$, so $\Phi(L) \cap M \trianglelefteq L$. Hence $K \trianglelefteq L$. Also since $K = \Phi(L) \cap M$, with $\Phi(L) \trianglelefteq L$ and $M \leq L$, we have that $\Phi(L) \cap M \trianglelefteq M$. Thus $K \trianglelefteq M$. Let $\overline{L} = L/K$ and $\overline{M} = M/K$. Since $K \leq \Phi(L)$ we have that $\Phi(\overline{L}) = \Phi(L/K) = \Phi(L)/K$. Therefore $\Phi(\overline{L}) \cap \overline{M} = (\Phi(L)/K) \cap (M/K) = (\Phi(L) \cap M)/K = K/K = \{1_G\}$. However M is a nilpotent normal subgroup of L, (since N is a nilpotent normal subgroup of G) and we have that $M' \leq \Phi(M) \leq \Phi(L)$. Therefore $M' \leq \Phi(L) \cap N = K$. Since $M' \leq K$ and $K \trianglelefteq M$, we get $\overline{M} = M/K$ is abelian. Application of the Theorem 9.1.1 yields that $\overline{L}$ splits over $\overline{M}$. Let $\overline{A}$ be a complement of $\overline{M}$ in $\overline{L}$. Then $\overline{A} \cap \overline{M} = \{1\}$ and $\overline{L} = \overline{A}\ \overline{M}$. Let A be the set of all preimages of $\overline{A}$ in L. If $\overline{M} \neq \{1\}$, then A is a proper subgroup of L and $G = AN$ contradicting the minimality of L with respect to $G = LN$. Thus $\overline{M} = \{1\}$ and hence $M = N$. Thus $L \cap N = \Phi(L) \cap M$ so that $M = L \cap N \subseteq \Phi(L)$.

Conversely if $L \cap N \subseteq \Phi(L)$ we will show that L is minimal with respect to $G = LN$. Suppose that H is any subgroup of L such that $G = HN$. Let $K = \Phi(L) \cap N$ we have that $K \trianglelefteq G$. Let $\overline{G} = G/K$, $\overline{L} = L/K$ and $\overline{N} = N/K$. Then $\overline{G} = G/N = LN/K = (L/K)(N/K) = \overline{L}.\overline{N}$ with $\overline{L} \cap \overline{N} = \{1\}$. Since $G = HN$, we have $\overline{G} = HN/K = (HK/K).(N/K)$. Let $\overline{H} = HK/K$. Then $\overline{G} = \overline{H}.\ \overline{N} = \overline{HN}$. But $\overline{H} \subseteq \overline{L}$ implies that $\overline{H} \cap \overline{N} = \{1\}$. Hence $\overline{H} = \overline{L}$. Since $HK/K \cong H/H \cap K$, we deduce that $L = HK$. Now $K \subseteq \Phi(L)$ implies that $L = H$. This completes the proof. □

9.2 Hereditarily non-Frattini subgroups

Remark 9.2.1 In general if a group G splits over a normal subgroup N the subgroups of G may not necessarily split over their intersections with N. We will see next a characterization of normal subgroups of G with the property that every subgroup H of G splits over $H \cap N$.

Definition 9.2.2 *A subgroup N of G is said to be* **hereditarily non-Frattini** *in G if, for every non-trivial subgroups H of G, $N \cap H \not\subseteq \Phi(H)$ unless $N \cap H = \{1_G\}$.*

Lemma 9.2.3 *Let G be a finitely generated group and N be a normal subgroup of G such that $N \not\subseteq \Phi(G)$. Then G splits over N if every maximal subgroup M of G splits over $M \cap N$.*

Proof. See Lemma 2.2 of [36].

Theorem 9.2.4 *Let G be a finite group and N be a normal subgroup of G. Then every subgroup H of G splits over $H \cap N$ if and only if N is hereditarily non-Frattini in G.*

Proof. Suppose that every subgroup H of G splits over $N \cap H$. Then $N \cap H \nleq \Phi(H)$ unless $N \cap H = \{1_G\}$ (since otherwise, because $N \cap H \trianglelefteq H$ and $N \cap H \leq \Phi(H)$ imply that there exists no L a subgroup of H such that $(N \cap H)L = H$, which is a contradiction with the fact that H splits over $N \cap H$). Hence N is hereditarily non-Frattini in G.

Conversely if N is hereditarily non-Frattini in G, then we show that G splits over N. We apply induction on the order of G. Let H be any proper subgroup of G and let $N \cap H = M$. Moreover since N is hereditarily non-Frattini in G, it follows that M is hereditarily non-Frattini in H. Since H is a proper subgroup of G, by induction every subgroup K of H splits over $K \cap M$. In particular H splits over M. Thus every maximal subgroup of G splits over its intersection with N. Since $N \nleq \Phi(G)$, by the Lemma 9.2.3 we get that G splits over K. □

Chapter 10

Affine Subgroups

In this chapter we will discuss the general linear group $GL(n, \mathbb{F})$ and the symplectic group $SP(2n, \mathbb{F})$ as well as their corresponding affine subgroups. We construct the affine subgroups and prove that they are split extensions. Further properties of these subgroups will also be investigated. For further reading and information on the general linear and symplectic groups, readers are encouraged to consult [9], [13], [14],[18],[19],[24],[26], [27]and [31].

10.1 The General Linear Group

Definition 10.1.1 *Let $\mathbb{F}$ be a filed. For any positive integer n, the* **general linear group**, *denoted by $GL(n, \mathbb{F})$ is the set of all invertible $n \times n$ matrices over $\mathbb{F}$, under the matrix multiplication. If $\mathbb{F} = GF(q)$, the finite field of order q, then we denote $GL(n, \mathbb{F})$ by $GL(n, q)$.*

Proposition 10.1.2 *The order of the general linear group $GL(n, q)$ is $(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$.*

Proof. See Proposition 23.3 of [18]. □

Definition 10.1.3 *The* **special linear group**, *denoted by $SL(n, \mathbb{F})$ is the subgroup of the group $GL(n, \mathbb{F})$ consisting of those matrices whose determinant is 1.*

Proposition 10.1.4 *Let n be a positive integer and $\mathbb{F}$ a field. Then $GL(n, \mathbb{F})$ splits over $SL(n, \mathbb{F})$.*

Proof. We will show that $GL(n,\ \mathbb{F}) = SL(n,\ \mathbb{F})\colon \mathbb{F}^*$. Let $\varphi : GL(n,\ \mathbb{F}) \longrightarrow \mathbb{F}^*$ given by $\varphi(A) = det(A)$ for all $A \in GL(n,\ \mathbb{F})$. Then since $det(AB) = det(A).det(B)$ for all A and $B \in GL(n,\ \mathbb{F})$, we have that $\varphi(AB) = \varphi(A)\varphi(B)$. Hence φ is a homomorphism. If $a \in \mathbb{F}^*$, then $\varphi\begin{pmatrix} a & 0 \\ 0 & I_{n-1} \end{pmatrix} = a$. Hence φ is onto. Thus $Im(\varphi) = \mathbb{F}^*$. So $GL(n,\ \mathbb{F})/Ker(\varphi) \cong Im(\varphi) = \mathbb{F}^*$. But

$$Ker(\varphi) = \{A \mid A \in GL(n,\ \mathbb{F}), det(A) = 1_{\mathbb{F}}\} = SL(n,\ \mathbb{F}),$$

implies that $GL(n,\ \mathbb{F})/SL(n,\ \mathbb{F}) \cong \mathbb{F}^*$. Now let

$$H = \left\{\begin{pmatrix} a & 0 \\ 0 & I_{n-1} \end{pmatrix} \mid a \in \mathbb{F}^*\right\}.$$

Then $H \leq GL(n,\ \mathbb{F})$. Now

$$\begin{aligned} H \cap SL(n,\ \mathbb{F}) &= \left\{\begin{pmatrix} a & 0 \\ 0 & I_{n-1} \end{pmatrix} \mid a = 1_{\mathbb{F}}\right\} \\ &= \left\{\begin{pmatrix} 1 & 0 \\ 0 & I_{n-1} \end{pmatrix}\right\} = \{I_n\}. \end{aligned}$$

Since $SL(n,\ \mathbb{F}) \trianglelefteq GL(n,\ \mathbb{F})$, $SL(n,\ \mathbb{F}).H \leq GL(n,\ \mathbb{F})$. Let $A \in GL(n,\ \mathbb{F})$. Then $det(A) \neq 0_{\mathbb{F}}$ and hence $\begin{pmatrix} det(A) & 0 \\ 0 & I_{n-1} \end{pmatrix}$ is an element of H. If we let $B = A.\begin{pmatrix} 1/det(A) & 0 \\ 0 & I_{n-1} \end{pmatrix}$, then $B \in GL(n,\ \mathbb{F})$ with $det(B) = det(A)\frac{1}{det(A)} = 1$.

So $B \in SL(n,\ \mathbb{F})$. Now since $A = B.\begin{pmatrix} det(A) & 0 \\ 0 & I_{n-1} \end{pmatrix}$ we deduce that $GL(n,\ \mathbb{F}) = SL(n,\ \mathbb{F}).H$. Thus $GL(n,\ \mathbb{F})$ is a semidirect product of $SL(n,\ \mathbb{F})$ and H. □

Proposition 10.1.5 $|SL(n,q)| = (q^n - 1)(q^n - q)(q^n - q)(q^n - q^2)\cdots(q^n - q^{n-1})/(q-1)$.

Proof. By Proposition 10.1.4 we have $|GL(n,\ \mathbb{F})| = |SL(n,\ \mathbb{F})| \times |\ \mathbb{F}^*|$ where $\mathbb{F} = GF(q)$. Hence $|GL(n,q)| = |SL(n,q)| \times (q-1)$. Now the proof follows from Proposition 10.1.2. □

We shall see next in the Proposition 10.1.6 and its subsequent Corollary a characterization of the group $GL(n,\ \mathbb{F})$ as the direct product of $SL(n,\ \mathbb{F})$ and $\mathbb{F}^*$

Proposition 10.1.6 *Let $\mathbb{F}$ be a field and n be a positive integer. Suppose that for each $a \in \mathbb{F}$, there is a unique $b \in \mathbb{F}$, such that $b^n = a$. Then $GL(n,\ \mathbb{F}) \cong SL(n,\ \mathbb{F}) \times \mathbb{F}^*$. (In particular this is true when $\mathbb{F} = \mathbb{R}$ and n is odd).*

Proof. Let $K = \{aI_n \mid a \in \mathbb{F}^*\}$. Then $K = Z(GL(n,\ \mathbb{F}))$ and hence $K \trianglelefteq GL(n,\ \mathbb{F})$. Obviously $K.SL(n,\ \mathbb{F}) \leq GL(n,\ \mathbb{F})$. Now let $A \in GL(n,\ \mathbb{F})$. If $det(A) = a$, then $a \in \mathbb{F}^*$ and $a^{-1}A \in SL(n,\ \mathbb{F})$. Now since $A = (aI_n)(a^{-1}A)$, we deduce that $GL(n,\ \mathbb{F}) = K.SL(n,\ \mathbb{F})$. Now for $A = aI_n \in K$ we have

$$A \in K \cap SL(n,\ \mathbb{F}) \Leftrightarrow det(A) = 1 \Leftrightarrow a^n = 1_{\ \mathbb{F}}.$$

Since for $1_{\ \mathbb{F}} \in \ \mathbb{F}$, by the assumption there is only one element $a \in \ \mathbb{F}$ such that $a^n = 1_{\ \mathbb{F}}$. Since $(1_{\ \mathbb{F}})^n = 1_{\ \mathbb{F}}$, we must have $a = 1_{\ \mathbb{F}}$. Thus $K \cap SL(n,\ \mathbb{F}) = \{I_n\}$. Hence $GL(n,\ \mathbb{F})$ must be a direct product of K and $SL(n,\ \mathbb{F})$. Since $K \cong \ \mathbb{F}^*$, the proof follows. □

Lemma 10.1.7 *If $n = 2$ and $q = 2^m$, with $m \geq 1$ then $K \cap SL(2, 2^m) = I_2$. In general we have that $GL(2, 2^m) = SL(2, 2^m) \times K$ where $K \cong C_{2^m - 1}$.*

Proof. In this case it is easy to see that $K = \langle \alpha I_2 \rangle$ where $\mathbb{F}^* = \langle \alpha \rangle$ with $\alpha^{q-1} = 1_{\ \mathbb{F}}$. Now let $A \in K$. Then $A = \alpha^k I_2$ where $0 \leq k \leq q - 1$.

$$\begin{aligned} det(A) &= \alpha^{2k} = 1 \\ &\Leftrightarrow (q-1) \mid 2k \\ &\Leftrightarrow (q-1) \mid k, \text{ because } q-1 \text{ is odd} \\ &\Leftrightarrow k = 0, \text{ because } 0 \leq k \leq q-1 \\ &\Leftrightarrow A = I_2. \end{aligned}$$

Hence $K \cap SL(2, 2^m) = \{I_2\}$ and the proof follows.

□

Example 10.1.8 Using Lemma 10.1.7 we have $GL(2, 2^3) = SL(2, 2^3) \times C_7$. Also we know by Proposition 10.1.4 that $GL(2, 2^3) = SL(2, 2^3){:}H$, where $H \cong C_7$.
Let

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in F^* \right\},$$

where $\mathbb{F}^* = \{1, \alpha, \alpha^2, \cdots, \alpha^6\}$ and $\alpha^7 = 1$. Then if $y = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ we have $H =< y >\cong C_7$.

Now, if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, 2^3)$ then $ad - bc = 1$ and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^y = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha^6 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha a \alpha^{-1} & \alpha b \\ c\alpha^{-1} & d \end{pmatrix}.$$

Let $K =< \alpha I_2 >$. Then by Lemma 10.1.6 we have that $GL(2, 2^3) = SL(2, 2^3).K = SL(2, 2^3) \times K$ where $K \cong C_7$.

10.1.1 The Affine Subgroup of the General Linear Group

Let $\mathbb{F}$ be a field and let $\mathbb{F}^n$ be the n dimensional vector space consisting of row vectors over the field $\mathbb{F}$. The group $GL(n, \mathbb{F})$ of all $n \times n$ invertible matrices over $\mathbb{F}$ acts on $\mathbb{F}^n$ by left multiplication as follows: $(x, A) \longmapsto xA$ for $x \in \mathbb{F}^n$ and A$\in GL(n, \mathbb{F})$. We can see that
(i) $(x, I_n) \longmapsto xI_n = x$,
(ii) $(x, A_1A_2) \longmapsto x(A_1A_2) = (xA_1)A_2$, since matrix multiplication is associative.

Remark 10.1.9 We have seen that the elements of $GL(n, \mathbb{F})$ act on $\mathbb{F}^n$ as automorphisms (ie invertible linear transformations) as the equation $(\lambda x + \beta y)A = \lambda xA + \beta yA$ for all $(\lambda,\beta \in \mathbb{F}, x, y \in \mathbb{F}^n)$ says, and in fact all automorphisms of $\mathbb{F}^n$ are obtained in this way. Let V be any n-dimensional vector space over $\mathbb{F}$. Choose a basis $v_1, v_2, \ldots, v_n$ for V. Then with respect to this basis each element v of V has a unique expression as a linear combination $v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ for suitable $\alpha_i \in \mathbb{F}$, $1 \leq i \leq n$. Consequently the map $\phi : V \longrightarrow \mathbb{F}^n$ defined by $\phi(v) = (\alpha_1, \alpha_2, \cdots, \alpha_n)^t$ is well defined and obviously is a bijection. For if

$$\phi(v) = \phi(\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n) = (\alpha_1, \alpha_2, \cdots, \alpha_n)^t$$

and

$$\phi(v') = \phi(\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n) = (\beta_1, \beta_2, \cdots, \beta_n)^t$$

then

$$\begin{aligned} \phi(v) = \phi(v') \quad &\Leftrightarrow \quad (\alpha_1, \alpha_2, \cdots, \alpha_n)^t = (\beta_1, \beta_2, \cdots, \beta_n)^t \\ &\Leftrightarrow \quad \alpha_i = \beta_i, \ \forall i. \end{aligned}$$

For any $x \in F^n$, if $x = (x_1, x_2, \cdots, x_n)^t$, then let $v = (x_1, x_2, \cdots, x_n)$. Now $\phi(v) = (x_1, x_2, \cdots, x_n)^t = x$.

Moreover, if f is a linear transformation of V, then

$$f(v_i) = \sum_j a_{ij} v_j, \ 1 \leq i \leq n$$

for uniquely determinable scalars a_{ij}, and if f is invertible, then the matrix (a_{ij}) lies in $GL(n, \mathbb{F})$. The map $h : Aut(V) \longrightarrow GL(n, \mathbb{F})$ given by $f \longmapsto (a_{ij})$ is an isomorphism, and the pair (ϕ, h) is an equivalence between the permutation groups $(V, Aut(V))$ and $(\mathbb{F}^n, GL(n, \mathbb{F}))$. For if

$$v = \sum_i \alpha_i v_i \in V$$

and $f \in Aut(V)$ then

$$\begin{aligned}
\phi(f(v)) &= \phi(f(\sum_i \alpha_i v_i)) = \phi(\sum_i f(\alpha_i v_i)) \\
&= \phi(\sum_i \alpha_i(\sum_j f(v_i))) = \phi(\sum_i \alpha_i(\sum_j a_{ij} v_j)) \\
&= \phi(\sum_j (\sum_i \alpha_i a_{ij}) v_j) \\
&= \left(\sum_i \alpha_i a_{i1}, \sum_i \alpha_i a_{i2}, \cdots, \sum_i \alpha_i a_{in}\right)^t
\end{aligned}$$

whereas,

$$[h(f)](\phi(v)) = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & a_{ij} & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \left(\sum_i \alpha_i a_{i1}, \sum_i \alpha_i a_{i2}, \cdots, \sum_i \alpha_i a_{in}\right)^t.$$

Definition 10.1.10 *Let $\mathbb{F}$ be an arbitrary field, and let $V = \mathbb{F}^n$ be the n-dimensional vector space consisting of row vectors over the field $\mathbb{F}$. Given $A \in GL(n, \mathbb{F})$ and $b \in \mathbb{F}^n$, define $T_{A,b} : V \longrightarrow V$ by $x \longmapsto xA + b$. We can see that for $A, A' \in GL(n, \mathbb{F})$ we have*

$$\begin{aligned}
T_{A,b} = T_{A',b'} &\Leftrightarrow (x)(T_{A,b}) = (x)(T_{A',b'}),\ \forall x \in V \\
&\Leftrightarrow xA + b = xA' + b',\ \forall x \in V \\
&\Leftrightarrow xA - xA' = b' - b,\ \forall x \in V \\
&\Leftrightarrow (x)(A - A') = b' - b,\ \forall x \in V \\
&\Leftrightarrow (x)(A - A') + (b - b') = 0_V,\ \forall x \in V \\
&\Leftrightarrow (x)(A - A') = 0_V \text{ and } b - b' = 0_V,\ \forall x \in V \\
&\Leftrightarrow A - A' = 0_V \text{ and } b - b' = 0_V, \\
&\Leftrightarrow A = A' \text{ and } b = b'.
\end{aligned}$$

These mappings are known as the **affine transformations** *of V. They constitute the* **affine group***, to which we denote*

$$AGL(n, \mathbb{F}) = \{T_{A,b} \mid A \in GL(n, \mathbb{F}), b \in \mathbb{F}^n\}.$$

Note 10.1.11 $AGL(n, \mathbb{F}) \supseteq GL(n, \mathbb{F})$, since $T_{A,0} = A$.

Lemma 10.1.12 *$T_{A,b}$ is a bijection.*

Proof. For $x_1, x_2 \in \mathbb{F}^n$ we have

$$\begin{aligned}(x_1)(T_{A,b}) = (x_2)(T_{A,b}) &\Rightarrow x_1A + b = x_2A + b\\ &\Rightarrow x_1A_1 = x_2A\\ &\Rightarrow (x_1 - x_2)A\\ &\Rightarrow x_1 - x_2 = 0_V, \text{since } A \in GL(n, \mathbb{F})\\ &\Rightarrow x_1 = x_2.\end{aligned}$$

Therefore $T_{A,b}$ is one to one. We can easily check that $T_{A,b}$ is onto, since for any $x' \in V$ we can find $x \in V$, such that $(x)(T_{A,b}) = x'$. To find $x \in V$, notice that

$$\begin{aligned}(x)(T_{A,b}) = x' &\Rightarrow x' = xA + b\\ &\Rightarrow x' - b = xA\\ &\Rightarrow x = (x' - b)A^{-1}.\end{aligned}$$

Now $(x'A^{-1} - bA^{-1})(T_{A,b}) = (x'A^{-1} - bA^{-1})A + b = x' - b + b = x'$. □

Lemma 10.1.13 *The set $AGL(n, \mathbb{F})$ is a group under the composition of functions.*

Proof. (i) $AGL(n, \mathbb{F})$ is closed under the composition: For all $x \in V$ we have $(x)(T_{A,b}T_{C,d}) = (xA + b)(T_{C,d}) = (xA + b)C + d = xAC + bC + d$, thus $T_{A,b}T_{C,d} = T_{AC,\ bC + d}$.

(ii) $(x)(T_{I_n,0}) = x$, for all $x \in V$, implies that $T_{I_n,0} = 1_{AGL(n,F)}$.

(iii) By part (ii) we have $(T_{A,b})(T_{A',b'}) = T_{AA',bA'+b'}$. Now

$$\begin{aligned}(T_{A,b})(T_{A',b'}) = T_{I_n,0_{\mathbb{F}}} &\Leftrightarrow AA' = I_n \text{ and } bA' + b' = 0_{\mathbb{F}}\\ &\Leftrightarrow A' = A^{-1} \text{ and } b' = -bA^{-1},\end{aligned}$$

thus $(T_{A,b})^{-1} = T_{A',b'} = T_{A^{-1},-bA^{-1}}$. □

Note 10.1.14 Lemmas 10.1.12 and 10.1.13 show that $AGL(n, \mathbb{F}) \leq S_V$ where S_V is the Symmetric group on V.

Note 10.1.15 In general $(x + y)(T_{A,b}) \neq (x)(T_{A,b}) + (y)(T_{A,b})$ for $x, y \in V$.

Remark 10.1.16 The set $Tr(V) = \{\tau_b = T_{I_n,b} \mid b \in \mathbb{F}^n\}$ of all translations $\tau_b : V \longrightarrow V$ given by $(x)\tau_b = x + b$, is an abelian subgroup of $AGL(n, \mathbb{F})$. Note that if $|\mathbb{F}| < \infty$ then $|Tr(V)| = |\mathbb{F}^n|$.

Lemma 10.1.17 *The group $Tr(V)$ is isomorphic to the additive group of V.*

Proof. Define $\rho : V \longrightarrow S_V$ by $(b)\rho = \tau_b$ for all $b \in V$. We show that ρ is a monomorphism.

ρ is a homomorphism: We note that for all $x \in V$,

$$(x)(\tau_b \circ \tau_{b'}) = ((x)\tau_b)\tau_{b'} = (x+b)\tau_b' = (x+b)+b' = x+(b+b') = (x)\tau_{b+b'},$$

so $\tau_b \circ \tau_{b'} = \tau_{b+b'}$. The fact that ρ is a homomorphism, then follows since $(b)\rho \circ (b')\rho = \tau_b \circ \tau_{b'} = \tau_{b+b'} = (b+b')\rho$.

ρ is one to one:

$$\begin{aligned} Ker(\rho) &= \{b \in V \mid (b)\rho = 1_{S_V}\} = \{b \in V \mid \tau_b = 1_{S_V}\} \\ &= \{b \in V \mid (x)\tau_b = x, \text{ for all } x \in V\} \\ &= \{b \in V \mid x+b = x, \text{ for all } x \in V\} = \{0_V\}. \end{aligned}$$

So ρ is a monomorphism from V into S_V. Also

$$Im(\rho) = \{(b)\rho \mid b \in V\} = \{\tau_b \mid b \in V\} = Tr(V).$$

Since $V/Ker(\rho) \cong Im(\rho)$, we have $V \cong Tr(V)$. □

Remark 10.1.18 Let $\varphi = T_{A,b} \in AGL(n, \ \mathbb{F})$, then φ is of the form $\varphi = \tau \circ A$, where $A \in GL(n, \ \mathbb{F})$ and $\tau \in Tr(V)$. Hence $AGL(n, \ \mathbb{F}) = < GL(n, \ \mathbb{F}), Tr(V) > = Tr(V) \cdot GL(n, \ \mathbb{F})$. Also the stabilizer of the zero vector in $AGL(n, \ \mathbb{F})$ is

$$\begin{aligned} [AGL(n, \ \mathbb{F})]_{0_V} &= \{T_{A,b} \mid (T_{A,b})(0_V) = 0_V, A \in GL(n, \ \mathbb{F}), b \in \ \mathbb{F}^n\} \\ &= \{T_{A,b} \mid b = 0_{\ \mathbb{F}^n} \text{ and } A \in GL(n, \ \mathbb{F})\} \\ &= \{T_{A,0} \mid A \in GL(n, \ \mathbb{F})\} = GL(n, \ \mathbb{F}). \end{aligned}$$

Theorem 10.1.19 *The group $AGL(n, \ \mathbb{F})$ is the semidirect product of $Tr(V)$ by $GL(n, \ \mathbb{F})$.*

Proof. (i) $Tr(V) \trianglelefteq AGL(n, \ \mathbb{F})$: Let $A \in AGL(n, \ \mathbb{F})$ and $\tau = (T_{I_n,b'}) \in Tr(V)$. Then $(T_{A,b})^{-1} \circ T_{I_n,b'} \circ T_{A,b} = T_{I_n,A^{-1}b'} \in Tr(V)$. Hence $Tr(V) \trianglelefteq AGL(n, \ \mathbb{F})$.

(ii) $Tr(V) \cap GL(n, \ \mathbb{F}) = \{I_n\}$: Let $T_{I_n,b} \in Tr(V) \cap GL(n, \ \mathbb{F})$. Then $T_{I_n,b} = A = T_{A,0_V}$, for some $A \in GL(n, \ \mathbb{F})$. Hence $A = I_n$ and $b = 0_V$, so $T_{I_n,b} = T_{I_n,0} = I_n$. Therefore $Tr(V) \cap GL(n, \ \mathbb{F}) = \{I_n\}$. □

Remark 10.1.20 Since, $AGL(n,\ \mathbb{F}) = Tr(V) : GL(n,\ \mathbb{F})$, we have $AGL(n,\ \mathbb{F})/Tr(V) \cong GL(n,\ \mathbb{F})$. Since $V = \ \mathbb{F}^n$ and $Tr(V) \cong V$, we have that $AGL(n,\ \mathbb{F}) \cong F^n : GL(n,\ \mathbb{F}) \cong \ \mathbb{F}^n : Aut(\ \mathbb{F}^n) = Hol(\ \mathbb{F}^n)$, where $Hol(\ \mathbb{F}^n)$ is the holomorph of $\mathbb{F}^n$. The Theorem 10.1.19 shows that if $|\ \mathbb{F}| = q^n$, then $|AGL(n,\ \mathbb{F})| = q^n \times |GL(n,\ \mathbb{F})|$.

Theorem 10.1.21 *The affine group $AGL(n, F)$ is isomorphic to a subgroup of $GL(n+1,\ \mathbb{F})$.*

Proof. Define $\psi : AGL(n,\ \mathbb{F}) \longrightarrow GL(n+1,\ \mathbb{F})$ by

$$\psi(T_{A,b}) \ := \ \begin{pmatrix} A & 0 \\ b & 1 \end{pmatrix}.$$

We claim that ψ is an monomorphism.

(i) ψ is a homomorphism:

$$\begin{aligned} \psi(T_{A,b} \circ T_{A',b'}) &= \psi(T_{AA'},\ bA' + b') = \begin{pmatrix} AA' & 0 \\ bA' + b' & 1 \end{pmatrix} \\ &= \begin{pmatrix} A & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} A' & 0 \\ b' & 1 \end{pmatrix} = \psi(T_{A,b}) \circ \psi(T_{A',b'}). \end{aligned}$$

(ii) ψ is one to one:

$$\begin{aligned} Ker(\psi) &= \left\{ T_{A,b} \mid \begin{pmatrix} A & 0 \\ b & 1 \end{pmatrix} = \begin{pmatrix} I_n & 0 \\ 0 & 1 \end{pmatrix}, A \in GL(n,\ \mathbb{F}) \right\} \\ &= \{T_{A,b} \mid A = I_n, b = 0\} = \{T_{I_n,0}\} = \{1_{AGL(n,\ \mathbb{F})}\}. \end{aligned}$$

Hence ψ is monomorphism. Thus

$$AGL(n,\ \mathbb{F}) \cong Im(\psi) = \left\{ \begin{pmatrix} A & 0 \\ b & 1 \end{pmatrix} \mid A \in GL(n,\ \mathbb{F}), b \in \ \mathbb{F}^n \right\} \leq GL(n+1,\ \mathbb{F}).$$

□

Let $V =< e_1, e_2, \cdots, e_n >$ and $W =< e_1, e_2, \cdots, e_n, e_{n+1} >$. Then

$$\begin{pmatrix} A & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \Rightarrow \begin{pmatrix} A & 0 \\ b & 1 \end{pmatrix} e_{n+1} = e_{n+1}.$$

Thus

$$H = \left\{ \begin{pmatrix} A & 0 \\ b & 1 \end{pmatrix} \mid A \in GL(n, \mathbb{F}), b \in \mathbb{F}^n \right\} \leq [GL(n+1, \mathbb{F})]_{e_{n+1}}. \quad (1)$$

Now let $T \in [GL(n+1, \mathbb{F})]_{e_{n+1}}$, then $T(_{e_{n+1}}) = e_{n+1}$ and suppose that

$$\begin{aligned} T(_{e_1}) &= a_{11}e_1 + a_{21}e_2 + \cdots + a_{n1}e_n + b_1e_{n+1} \\ T(_{e_2}) &= a_{12}e_1 + a_{22}e_2 + \cdots + a_{n2}e_n + b_2e_{n+1} \\ &\vdots \\ T(_{e_i}) &= a_{1i}e_1 + a_{2i}e_2 + \cdots + a_{nn}e_n + b_ie_{n+1} \ . \end{aligned}$$

Then

$$T = \begin{pmatrix} A & 0 \\ b & 1 \end{pmatrix}_{(n+1)\times(n+1)} , where\ A = (a_{ij})_{n\times n} \ .$$

Therefore, $T \in H$ and hence $[GL(n+1, \mathbb{F})]_{e_{n+1}} \subseteq H$ (2). Now (1) and (2) imply that $H = [GL(n+1, \mathbb{F})]_{e_{n+1}}$.

We also deduce that $Hol(\mathbb{F}^n) \cong AGL(n, \mathbb{F}) \cong [GL(n+1, \mathbb{F})]_{e_{n+1}}$. In particular if $\mathbb{F} = GF(q)$, we have $|GL(n+1, \mathbb{F})_{e_{n+1}}| = |AGL(n, \mathbb{F})| = q^n \times |GL(n,q)|$.

In what follows we give some examples of isomorphisms between the affine group and the symmetric group.

Lemma 10.1.22 *The Affine group $AGL(n, \mathbb{F})$ which is defined as a subgroup of $S_{\mathbb{F}^n}$ produces the following isomorphisms*

(i) $AGL(1,2) \cong S_2$, (ii) $AGL(1,3) \cong S_3$

(iii) $AGL(1,4) \cong A_4$, (iv) $AGL(2,2) \cong S_4$.

Proof. Recall that $AGL(n, \mathbb{F})$ is defined to be the group of all transformations $T_{A,b}$ of the vector space $\mathbb{F}^n$ where $A \in GL(n, \mathbb{F})$, $b \in \mathbb{F}^n$, and $T_{A,b} : x \longmapsto xA + b$ for all $x \in \mathbb{F}^n$. We write $AGL(n,q)$ to denote $AGL(n, \mathbb{F})$ when $\mathbb{F} = GF(q)$. Note that $AGL(1,q)$ is the group of all transformations of the form $x \longmapsto xa + b$ with $a, b \in \mathbb{F}$ and $a \neq 0_{\mathbb{F}}$, and therefore $|AGL(1,q)| = q(q-1)$.

(i) $AGL(1,2)$ is a subgroup of S_2 of order 2. Therefore $AGL(1,2) \cong S_2$.

(ii)$AGL(1,3)$ is a subgroup of S_3 of order 6, and so $AGL(1,3) \cong S_3$.

(iii) Now $AGL(1,4)$ is a subgroup of S_4 of order 12. To see that $AGL(1,4) \cong A_4$ we either quote the fact that A_4 is the only subgroup of S_4 of order 12 or we examine each element of $AGL(1,4)$ and check that it is an even permutation.

(iv) The order of $GL(2,2)$ is 6. Thus there are 6 possibilities for A and 4 possibilities for b. Therefore we have 24 transformations $T_{A,b}$ in $AGL(2,2)$. Since $AGL(2,2) \leq S_4$ and $|S_4| = 24$, we have $AGL(2,2) \cong S_4$, as required. □

10.2 Symplectic Groups

In this section we will discuss the Symplectic Group and consequently its affine subgroup. We give a construction for the affine subgroup of $SP(4,2)$ and find its conjugacy classes.

10.2.1 Symplectic Forms

Definition 10.2.1 *Let V be a finite dimensional vector space over a field $\mathbb{F}$. A function f from the set $V \times V$ of ordered pairs in V to $\mathbb{F}$ is called a* **bilinear form** *on V if for each $v \in V$, the functions $f(v, \ )$ and $f(\ ,v)$ are linear functionals on V. In this case we say that (V,f) is an* **inner product space.**

If f is a bilinear form on V such that for each non-zero $x \in V$, there exists $y \in V$ for which $f(x,y) \neq 0$, then f is said to be **non-degenerate.**

Remark 10.2.2 A bilinear form f is called alternating (symplectic) on V if $f(x,x) = 0$ for all $x \in V$.

Let V be a vector space over a field $\mathbb{F}$ and f be a symplectic form on V. If $char(\mathbb{F}) \neq 2$ then we obtain that for all $x, y \in V$,

$$0 = f(x+y,x+y) = f(x+y,x) + f(x+y,y) = f(x,x) + f(y,x) + f(x,y) + f(y,y).$$

However, since $f(x+y,x+y) = f(x,x) = f(y,y) = 0$ we have that $f(x,y) = -f(y,x)$. Conversely if f is a bilinear form for which $f(x,y) = -f(y,x)$ for all $x,y \in V$, then in particular for $x \in V$ we have $f(x,x) = -f(x,x)$. This implies that $2f(x,x) = 0$ and so $f(x,x) = 0, \ \forall\, x \in V$.

10.2.2 Symplectic Spaces

Definition 10.2.3 *Let V be a vector space over a field $\mathbb{F}$. Let $f : V \times V \longrightarrow \mathbb{F}$ be a bilinear form on V such that*
(i) $f(x,x) = 0, \quad \forall\, x \in V$
(ii) $f(x,y) = -f(y,x), \quad \forall\, x,y \in V$.
Then we say that (V,f) is a **symplectic space** *over the field $\mathbb{F}$.*

Remark 10.2.4 If *char*($\mathbb{F}$) $\neq 2$, then the properties (i) and (ii) in the above definition are equivalent.

Let (V,f) and (U,g) be symplectic spaces over $\mathbb{F}$, then we say that $V \cong U$ if there exists an isomorphism $T \in L(V,U)$ such that $\forall\, x,y \in V$ we have $f(x,y) = g(T(x),T(y))$.

Definition 10.2.5 *Let (V,f) be a symplectic space. If $x,y \in W$, then x and y are* **orthogonal** *if $f(x,y) = 0$. If W is a subspace of V then the* **orthogonal complement** *of W is defined by*

$$W^{\perp} = \{y \in V \mid f(x,y) = 0, \ \forall\, x \in W\}.$$

Note that for all $x \in W$ we have $f(0,x) = f(x-x,x) = f(x,x) - f(x,x) = 0-0 = 0$, so that $0 \in W^{\perp}$. Now if $x,y \in W^{\perp}$, then for any $\alpha,\beta \in F$ and $z \in W$ we have

$$f(\alpha x + \beta y, z) = f(\alpha x, z) + f(\beta y, z) = \alpha f(x,z) + \beta f(y,z) = \alpha 0 + \beta 0 = 0,$$

therefore $\alpha x + \beta y \in W^{\perp}$, and hence $W^{\perp}$ is a subspace of V.

Let (V,f) be a symplectic space and define $R(V)$ by $R(V) = V^{\perp}$. Then we call $R(V)$ the **radical** of V. We can easily see that (V,f) is non-degenerate if and only if $R(V) = \{0_V\}$. (See [27].)

Definition 10.2.6 *Consider (V,f) with f bilinear . If $\{v_1, v_2, \cdots, v_n\}$ is an ordered basis of V, then the* **inner product matrix** *of f relative to this basis is given by an $n \times n$ matrix*

$$A = [f(v_i,v_j)]_{n \times n} \quad .$$

Remark 10.2.7 It is clear that f is completely determined by an inner product matrix, for if $u = \sum \alpha_i v_i$ and $v = \sum \beta_j v_j$ then $f(u,v) = \sum_{i,j} \alpha_i \beta_j f(v_i,v_j)$.

Lemma 10.2.8 *Let V^* be the dual space of V. If (V,f) is a non-degenerate inner product space, then for every linear functional $g \in V^*$, there exists a unique $x \in V$, with $g = f(x,)$.*

Proof. We first prove that if $\{v_1, v_2, \cdots, v_n\}$ is a basis of V, then $\{f(v_1,), f(v_2,), \cdots, f(v_n,)\}$ is a basis of V^*. Since $dim\ V^* = n$, it suffices to show that these n linear functionals are linearly independent. If there are scalars, λ_i not all zero, with $\sum \lambda_i f(v_i,) = 0$ then $0 = \sum \lambda_i f(v_i,)(y) = f(\sum \lambda_i v_i, y)\ \forall y \in V$. Thus $\sum \lambda_i v_i = 0$, because f is non-degenerate, and this contradicts the independence of the v_i. Let $g \in V^*$. Then there exists $\mu_i \in \mathbb{F}$ with $g = \sum \mu_i f(v_i,)$. Now let $x = \sum \mu_i v_i$. Then for all $v \in V$ we have

$$\begin{aligned} g(v) &= [\sum \mu_i f(v_i,)](v) \\ &= \sum \mu_i f(v_i, v) \\ &= f(\sum \mu_i v_i, v) = f(x, v). \end{aligned}$$

Thus $g = f(x,)$. To prove the uniqueness of x, suppose that $f(x, v) = f(y, v)$ for all $v \in V$. Then $f(x - y, v) = 0\ \ \forall v \in V$. So non-degeneracy of f implies that $x - y = 0_V$ and hence $x = y$. □

Lemma 10.2.9 *Let (V, f) be an inner product space. Then (V, f) is non-degenerate if and only if the inner product matrices of f are non-singular.*

Proof. Let $\{v_1, v_2, \cdots, v_n\}$ be a basis for V. If an inner product matrix A of f is singular, then there is a non-zero column vector Y with $AY = 0$. Therefore if $Y = (\mu_1, \mu_2, \cdots, \mu_n)$ where $\mu_i \in \mathbb{F}$ then $u = \sum \mu_i v_i$ is a non-zero vector with $f(v, u) = X^t AY = 0$, for all $v = \sum \lambda_i v_i$, where $X = (\lambda_1, \lambda_2, \cdots, \lambda_n)$. Conversely if u is a non-zero vector satisfying $f(u, v) = 0$ for all $v \in V$, then $f(u, v_i) = 0$ for all v_i. This implies that if $u = \sum \mu_j v_j$, then $\sum_j \mu_j f(v_j, v_i) = 0$. Let $Y = (\mu_1, \mu_2, \cdots, \mu_n)^t$ be the column vector of u. Then $Y \neq 0$ and $AY = 0$, hence A is singular. □

Remark 10.2.10 Let (V, f) be a non-degenerate inner product space. If W is a subspace of V then it is possible that the restriction $f \downarrow (W \times W)$ is degenerate. For example let $V = < x, y >$ be a two dimensional space over a field $\mathbb{F}$ and let f be a bilinear form having the following inner product matrix relative to the basis $\{x, y\}$

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then f is symmetric and non-degenerate. However, if $W = < x >$, then the restriction $f \downarrow (W \times W)$ is zero and hence degenerate.

Lemma 10.2.11 *[31] Let (V, f) be a symplectic space and let W be a subspace of V.*
(i) If $f \downarrow (W \times W)$ is non-degenerate, then $V = W \oplus W^{\perp}$.
(ii) If (V, f) is a non-degenerate space and $V = W \oplus W^{\perp}$, then $f \downarrow (W^{\perp} \times W^{\perp})$ is non-degenerate.

Proof. (i) If $x \in W \cap W^{\perp}$, then $f(x, w) = 0$ for all $w \in W$ and so by the non-degeneracy of f we have $x = 0_V$. If $v \in V$, then the restriction $g = f(v,) \downarrow W$ is a linear functional on W and so by Lemma 10.2.8 there is a unique $w_0 \in W$ such that $g = f(w_0,)$. Now for all $w \in W$ we obtain that $g(w) = f(v, w) = f(w_0, w)$. But $v = w_0 + (v - w_0)$ and $f(v - w_0, w) = f(v, w) - f(w_0, w) = 0\ _{\mathbb{F}}$ imply $v - w_0 \in W^{\perp}$.

(ii) If $\{v_1, v_2, \cdots, v_r\}$ is a basis of W and $\{v_{r+1}, v_{r+2}, \cdots, v_n\}$ is a basis of $W^{\perp}$, then the inner product matrix of f relative to the basis $\{v_1, v_2, \cdots, v_n\}$ has the form

$$A = \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix},$$

so that $detA = det(B)det(C)$. Since A is non-singular by Lemma 10.2.9, C is also non-singular. Hence the restriction of f to $W^{\perp} \times W^{\perp}$ is non-degenerate by Lemma 10.2.9. □

Definition 10.2.12 *An* **isometry** *of a non-degenerate space* (V, f) *is a linear transformation* $T : V \longrightarrow V$*, such that* $f(T(x), T(y)) = f(x, y)$ *for all* $x, y \in V$*.*

Lemma 10.2.13 *If* (V, f) *is a non-degenerate space, then every isometry is non-singular, and so the set of all isometries denoted by* $\mathbf{Isom}(V, f)$ *form a subgroup of* $GL(V)$*.*

Proof. If T is an isometry and $T(x) = 0_V$, for some $x \in V$ then $f(x, y) = f(T(x), T(y)) = f(0_V, T(y)) = 0_V$, for all $y \in V$. Since f is non-degenerate, it follows that $x = 0_V$ and T is injective. Since V is finite dimensional, T is non-singular and so $\mathbf{Isom}(V, f) \leq GL(V)$. □

Remark 10.2.14 (i) The product of isometries is also an isometry: For if T_1 and T_2 are two isometries, we have $f(T_1(x), T_1(y)) = f(x, y) \quad \forall x, y \in V$ and $f(T_2(x), T_2(y)) = f(x, y) \quad \forall x, y \in V$. Then

$$f(T_1T_2(x), T_1T_2(y)) = f(T_1[T_2(x)], T_1[T_2(y)]) = f(T_2(x), T_2(y)) = f(x, y).$$

Hence T_1T_2 is an isometry.

(ii) The identity map is an isometry: Because $f(I_V(x), I_V(y)) = f(x, y) \quad \forall x, y \in V$.

(iii) An isometry T has an inverse T^{-1} and T^{-1} is also an isometry: Because $f(T^{-1}(x), T^{-1}(y)) = f(TT^{-1}(x), TT^{-1}(y)) = f(I_V(x), I_V(y)) = f(x, y)$.

Lemma 10.2.15 *Let* (V, f) *be a non-degenerate space. Let* A *be the inner product matrix of* f *relative to an ordered basis* $B = \{v_1, v_2, \cdots, v_n\}$ *of* V*, and let* T *be a linear transformation on* V*. Then* T *is an isometry if and only if its matrix* $M = (m_{ij})$ *relative to* B *satisfies* $M^tAM = A$*. If* T *is an isometry, then* $det(M) = \pm 1$*.*

Proof. Since $f(T(v_i),T(v_j)) = f(\sum_k m_{ki}v_k, \sum_r m_{rj}v_r) = \sum_{k,r} m_{ki}f(v_k,v_r)m_{rj}$, we have that $f(T(v_i),T(v_j)) = f(v_i,v_j)$ if and only if $M^tAM = A$. If T is an isometry, then $M^tAM = A$ and we have

$$det(A) = det(M^tAM) = det(M^t)det(A)det(M) = (det(M))^t det(M)det(A) = (detM)^2 detA.$$

Non-degeneracy of (V, f) gives non-singularity of A and so $\det(M) = \pm 1$. □

Remark 10.2.16 The group $GL(V)$ acts on $\mathcal{F}(V)$, the set of all functions $V \times V \longrightarrow \mathbb{F}$ in the following way. If f is a function and $P \in GL(V)$, define

$$f^P(x,y) = f(P^{-1}(x), P^{-1}(y)).$$

If $Q \in GL(V)$, then $f^{PQ} = (f^Q)^P$, since

$$\begin{aligned} f^{PQ}(x,y) &= f((PQ)^{-1}(x),(PQ)^{-1}(y)) = f(Q^{-1}P^{-1}(x),Q^{-1}P^{-1}(y)) \\ &= f(Q^{-1}(P^{-1}(x)),Q^{-1}(P^{-1}(y))) = f^Q(P^{-1}(x),P^{-1}(y)) = (f^Q)^P(x,y). \end{aligned}$$

If f is symplectic, then so is f^P. Because

$$f^P(x,y) = f(P^{-1}(x),P^{-1}(y)) = -f(P^{-1}(y),P^{-1}(x)) = -f^P(y,x) \quad \forall x,y \in V$$

and $f^P(x,x) = f(P^{-1}(x),P^{-1}(x)) = 0 \ \ \forall x \in V$.

Theorem 10.2.17 *[31] Let V be a vector space over a field $\mathbb{F}$. Let f be a bilinear form on V. If f is symplectic, then the stabilizer of f in $GL(V)$, under the action of $GL(V)$ on $\mathcal{F}(V)$, is* **Isom**(V,f). *Moreover, if g is in the orbit of f, then* **Isom**(V,g) *is isomorphic to* **Isom**(V,f).

Proof. The stabilizer $GL(V)_f$ of f is $GL(V)_f = \{P \in GL(V), \mid f^P = f\}$. Hence

$$\begin{aligned} P \in GL(V)_f &\Leftrightarrow f^P(x,y) = f(x,y) \quad \forall x,y \in V \\ &\Leftrightarrow f(P^{-1}(x),P^{-1}(y)) = f(x,y) \quad \forall x,y \in V \\ &\Leftrightarrow P^{-1} \in \mathbf{Isom}(V,f) \\ &\Leftrightarrow P \in \mathbf{Isom}(V,f). \end{aligned}$$

Hence $GL(V)_f = \mathbf{Isom}(V,f)$.

If $g = f^P$ for some $P \in GL(V)$, then

$$\begin{aligned} \mathbf{Isom}(V,g) = GL(V)_{f^P} &= \{Q \in GL(V) \mid (f^P)^Q = f^P\} = \{Q \in GL(V) \mid f^{PQ} = f^P\} \\ &= \{Q \in GL(V) \mid (f^{QP})^{P^{-1}} = f\} = \{Q \in GL(V) \mid f^{P^{-1}QP} = f\} \\ &= \{Q \in GL(V) \mid P^{-1}QP \in GL(V)_f\} \\ &= \{Q \in GL(V) \mid Q \in P\, GL(V)_f\, P^{-1}\} \\ &= P\, GL(V)_f\, P^{-1} = P\, \mathbf{Isom}(V,f)\, P^{-1}. \end{aligned}$$

□

Definition 10.2.18 *Two elements $f, g \in \mathcal{F}(V)$ are called* **equivalent** *if $g = f^P$ for some $P \in GL(V)$.*

Remark 10.2.19 From Theorem 10.2.17 we deduce that equivalent symplectic forms determine isomorphic groups of isometries.

Definition 10.2.20 *Let (V, f) be a symplectic space and $\{V_1, V_2, \ldots, V_n\}$ be a set of subspaces of V such that*

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$$

and $f(y_i, y_j) = 0$ for all $y_i \in V_i$, $y_j \in V_j$ for which $i \neq j$. Then we say that V is an **orthogonal sum** *of the subspaces $\{V_1, V_2, \ldots, V_n\}$ and we denote this by writing*

$$V = V_1 \perp V_2 \perp \ldots \perp V_n.$$

Remark 10.2.21 Let (V, f) be a symplectic space and W be a subspace of V. Then it can be shown that (see [19]):
(1) $dim(W^{\perp}) \geq dim(V) - dim(W)$.
(2) If V is finite dimensional non-degenerate, then $dim(W^{\perp}) = dim(V) - dim(W)$.
(3) If V is non-degenerate, then there exists a linear isomorphism $\theta : V \longrightarrow V^*$ given by $u^{\theta}(v) = f(u, v)$.
(4) If W is non-degenerate, then $V = W \perp W^{\perp}$.

Note 10.2.22 Assume that (V, f) is a non-degenerate symplectic space. If f is not identically zero, there are vectors x and y with $f(x, y) = \alpha \neq 0$. Replacing x by $\alpha^{-1}x$ if necessary, we may assume that $f(x, y) = 1$. If $dim\ V = 2$, then its inner product matrix is thus

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

Definition 10.2.23 *Let (V, f) be a symplectic space and $x, y \in V$ such that $f(x, y) = 1$. Then the vectors $x, y \in V$ are called a* **hyperbolic pair** *and the 2-dimensional subspace of V generated by $\{x, y\}$ is called a* **hyperbolic plane**.

Remark 10.2.24 We can easily show that every hyperbolic plane is non-degenerate. If $H =< x, y >$ is an hyperbolic plane in V, then $f \downarrow (H \times H)$ is a bilinear form on H. Let

$u = \lambda_0 x + \mu_0 y \in H$. We need to show that if $f(u, v) = 0, \forall v \in H$ then $u = 0$. Consider an arbitrary element $v = ax + by$ of H. Then $0 = f(u, v) = f(\lambda_0 x + \mu_0 y, ax + by) = \lambda_0 a + \mu_0 b$, $\forall a, b \in \mathbb{F}$ imply that $\lambda_0 = \mu_0 = 0$. Hence $u = 0$.

Theorem 10.2.25 *[9] Let (V, f) be a non-degenerate finite dimensional symplectic space over a field $\mathbb{F}$. If W is a subspace of V such that $W \cap W^{\perp} = 0$, then $V = W \oplus W^{\perp}$.*

Proof. Since V is finite dimensional, then W is finite dimensional. Let $\{x_1, x_2, \ldots, x_k\}$ be a basis for W. Then $W^{\perp}$ will be the collection of all vectors $y \in V$ for which $f(x_i, y) = 0$, $1 \leq i \leq k$. Since V is non-degenerate, then $dim(W^{\perp}) = dim(V) - dim(W)$ and thus we obtain that $dim(V) = dim(W^{\perp}) + dim(W)$. Since $W \cap W^{\perp} = 0$, then we obtain that $V = W \oplus W^{\perp}$. □

Theorem 10.2.26 *Let (V, f) be a symplectic space over a field $\mathbb{F}$ such that $dim(V) = n$ and $dim(R(V)) = r$. Then we have*

$$V = H_1 \perp H_2 \perp \ldots \perp H_m \perp R(V),$$

where $H_i, 1 \leq i \leq m$ are hyperbolic planes. Furthermore $n - r = 2m$.

Proof. We have that $R(V)$ is a subspace of V. However if $R(V) = V$, then $m = 0$ and thus $n - r = 0 = 2 \times 0$ and the proof is complete. Thus, without loss of generality, suppose that $R(V) \neq V$. Let $x \in V - R(V)$. Since $x \notin R(V)$, there $\exists$ $z \in V$ such that $f(x, z) \neq 0$. Thus we can choose $y \in V$ such that $f(x, y) = 1$ and hence $\{x, y\}$ is a hyperbolic pair. This is true, since if $f(x, z) = \alpha \neq 0$, then for $y = \frac{1}{\alpha} z$ we have $f(x, y) = 1$. Now suppose that H_1 is the hyperbolic plane generated by $\{x, y\}$ and that $H_1^{\perp} = V_1$. Since H_1 is a hyperbolic plane, then it is non-degenerate and thus we have that $V = H_1 \perp V_1$ and we also have that $R(H_1) = 0$. Hence $R(V) = R(H_1) \perp R(V_1) = R(V_1)$.

We now apply induction on $dim(V) = n$. Since $H_1 = \langle x, y \rangle$, then $dim(H_1) = 2$ and so we have that $dim(V) = n = dim(H_1) + dim(V_1)$. Thus, $dim(V_1) = n - 2 < dim(V)$ and so by induction hypothesis we obtain

$$V_1 = H_2 \perp H_3 \perp \ldots \perp H_m \perp R(V_1),$$

where H_i, $2 \leq i \leq m$ are hyperbolic planes and that $2(m - 1) = n - 2 - r$. So we get $2m = n - r$. Since $R(V_1) = R(V)$ and $V = H_1 \perp V_1$, then we also obtain that

$$V = H_1 \perp H_2 \perp H_3 \perp \ldots \perp H_m \perp R(V).$$

□

The result that follows shows that the dimension of a non-degenerate symplectic space must be even.

Corollary 10.2.27 *Let (V, f) be a non-degenerate symplectic space of dimension n over a field $\mathbb{F}$. Then*

$$V = H_1 \perp H_2 \perp \ldots \perp H_m,$$

where H_i, $1 \leq i \leq m$ are hyperbolic planes and $n = 2m$.

Proof. By the above theorem, we obtain that $V = H_1 \perp H_2 \perp \ldots \perp H_m \perp R(V)$. However V is non-degenerate and thus $R(V) = 0$.
Hence we obtain that $V = H_1 \perp H_2 \perp \ldots \perp H_m$ and $dim(V) = n = 2m$. □

Theorem 10.2.28 *Let (V, f) be a non-degenerate symplectic space and $\{u_1, \ldots, u_r\}$ be a linearly independent set of elements of V such that $f(u_i, u_j) = 0 \; \forall \; i, j$. Then there is a linearly independent set $\{v_1, v_2, \ldots, v_r\}$ of elements of V such that*

$$V = H_1 \perp H_2 \perp \ldots \perp H_r \perp V_1,$$

where V_1 is a subspace of V and H_i, $1 \leq i \leq r$ are hyperbolic planes and $2r \leq dim(V)$.

Proof. Since V is non-degenerate, $R(V) = 0$. Hence $u_1 \notin R(V)$ and there is $v_1 \in V$ such that $f(u_1, v_1) = 1$. Let $H_1 = \langle u_1, v_1 \rangle$. Then H_1 is a hyperbolic plane. Since H_1 is non-degenerate, $V = H_1 \perp H_1^{\perp}$. Now $0 = R(V) = R(H_1) \perp R(H_1^{\perp})$ implies that $R(H_1^{\perp}) = 0$. Hence $H_1^{\perp}$ is non-degenerate. Since $f(u_1, u_i) = 0$ for $2 \leq i \leq r$, $u_i \in H_1^{\perp}$. Hence $\{u_2, u_3, \ldots, u_r\} \subseteq H_1^{\perp}$. Since $dim(H_1^{\perp}) = dim(V) - 2 \leq dim(V)$, by induction there exists $\{v_2, v_3, \ldots, v_r\} \subseteq H_1^{\perp}$ such that

$$H_1^{\perp} = H_2 \perp H_3 \perp \ldots \perp H_r \perp V_1 \quad ,$$

where $H_i = \langle u_i, v_i \rangle, 2 \leq i \leq r$. Since $V = H_1 \perp H_1^{\perp}$, we have

$$V = H_1 \perp H_2 \perp H_3 \perp \ldots \perp H_r \perp V_1.$$

Also $dim(V) = 2r + dim(V_1)$ and hence $2r \leq dim(V)$. □

Theorem 10.2.29 *[19] Let (V, f) be a non-degenerate symplectic space and W_1, W_2 be two subspaces of V and $T : W_1 \longrightarrow W_2$ be an isometry. Then there exists an isometry $S : V \longrightarrow V$ such that $S \downarrow_{W_1} = T$.*

Proof. We have that $W_1 = H_1 \perp H_2 \perp \ldots \perp H_m \perp R(W_1)$, where H_i, $1 \leq i \leq m$ are hyperbolic planes. Thus we obtain that

$$W_2 = T(W_1) = T(H_1) \perp T(H_2) \perp \ldots \perp T(H_m) \perp T(R(W_1)) \quad .$$

If $H_i = \langle x_i, y_i \rangle$, then we obtain that

$$T(H_i) = T(\langle x_i, y_i \rangle) = \langle T(x_i), T(y_i) \rangle = H_i',$$

and H_i' is a hyperbolic plane in W_2. Since $T(R(W_1)) = R(T(W_1)) = R(W_2)$, we have

$$W_2 = H_1' \perp H_2' \perp \ldots \perp H_m' \perp R(W_2) \quad .$$

Now let

$$H = H_1 \perp H_2 \perp \ldots \perp H_m \quad \text{and} \quad H' = H_1' \perp H_2' \perp \ldots \perp H_m'.$$

Then we get

$$W_1 = H \perp R(W_1) \quad \text{and} \quad W_2 = H' \perp R(W_2).$$

Since H_i and H_i', $1 \leq i \leq m$, are hyperbolic planes, they are non-degenerate and hence $R(H_i) = R(H_i') = 0$, $1 \leq i \leq m$. Thus we obtain that $R(H) = R(H') = 0$ and hence H, H' are non-degenerate. Therefore $V = H \perp H^{\perp} = H' \perp (H')^{\perp}$. However since V is non-degenerate, then $R(V) = 0$. Thus

$$0 = R(V) = R(H) \perp R(H^{\perp}) = R(H') \perp R((H')^{\perp})$$

and hence we obtain that $R(H^{\perp}) = R((H')^{\perp}) = 0$. Therefore $H^{\perp}$, $(H')^{\perp}$ are non-degenerate. Since $H \subseteq W_1$ and $H' \subseteq W_2$, $R(W_1) \subseteq H^{\perp}$ and $R(W_2) \subseteq (H')^{\perp}$. Let $\{u_1, u_2, \ldots, u_k\}$ be a basis for $R(W_1)$. Then $f(u_i, u_j) = 0 \ \forall\ i, j$. Thus by Theorem 10.2.28, there exists a linearly independent set $\{v_1, v_2, \ldots, v_k\}$ such that

$$H^{\perp} = K_1 \perp K_2 \perp \ldots \perp K_k \perp L \quad ,$$

where L is a subspace of $H^{\perp}$ and $K_i = \langle u_i, v_i \rangle$ such that $f(u_i, v_i) = 1$. Since T is an isometry, $\{T(u_1), T(u_2), \ldots, T(u_k)\}$ is a linearly independent set in $T(R(W_1)) = R(W_2)$. We also obtain that $0 = f(u_i, u_j) = f(T(u_i), T(u_j))$. Again by Theorem 10.2.28 there exists a linearly independent set $\{v_1', v_2' \ldots v_k'\}$ such that

$$(H')^{\perp} = K_1' \perp K_2' \perp \ldots \perp K_k' \perp L',$$

where $K_i' = \langle T(u_i), v_i' \rangle$ such that $f(T(u_i), v_i') = 1$. Now we have

$$\begin{aligned} V &= H_1 \perp H_2 \ldots \perp H_m \perp K_1 \perp K_2 \ldots \perp K_k \perp L \\ &= H_1' \perp H_2' \ldots \perp H_m' \perp K_1' \perp K_2' \ldots \perp K_k' \perp L' \end{aligned}$$

with $R(L) = R(L') = 0$ and $dim(V) = 2(m+k) + dim(L) = 2(m+k) + dim(L')$. Thus we obtain that $dim(L) = dim(L')$. Hence there exists an isometry $M : L \longrightarrow L'$. Define a linear transformation $S : V \longrightarrow V$ by

$$S(h) = T(h) \; \forall \; h \in H, S(u_i) = T(u_i) \;\; 1 \leq i \leq k$$

$$S(v_i) = v_i' \;\; 1 \leq i \leq k, S(\ell) = M(\ell) \; \forall \; \ell \in L.$$

Then S is an isometry on V and $S \downarrow_{W_1} = T$. □

10.2.3 Symplectic Groups

Definition 10.2.30 *Let (V, f) be a non-degenerate symplectic space of dimension $2n$ over a field $\mathbb{F}$. Then by Lemma 10.2.13* **Isom**(V, f) *is a subgroup of $GL(V)$. The group* **Isom**(V, f) *is denoted by $SP(2n, \mathbb{F})$, and is called the* **symplectic group** *of degree $2n$ over $\mathbb{F}$.*

Note 10.2.31 If $\mathbb{F} = GF(q)$ is a Galois field of q elements, where $q = p^k$ for some k with p a prime, we denote $SP(2n, \mathbb{F})$ by $SP(2n, q)$. We further obtain that **Isom**$(V, f) = SP(2n, \mathbb{F}) \leq GL(2n, \mathbb{F})$. We shall see in Theorem 10.2.33 that this group (within isomorphism) is independent of the choice of f.

Definition 10.2.32 *Let (V, f) be a non-degenerate symplectic space of dimension $2m$. Let $B = \{x_1, y_1, x_2, y_2, \ldots, x_m, y_m\}$ be a basis for V such that $\{x_i, y_i\}$ is a hyperbolic pair for all $1 \leq i \leq m$ with $f(x_i, x_j) = 0 = f(y_i, y_j)$ for all i, j* and *$f(x_i, y_j) = \delta_{ij} = -f(y_j, x_i)$, where $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$. Then we say that the set B is a* **hyperbolic basis** *for V.*

Thus all inner product are 0 except $f(x_i, y_i) = 1 = -f(y_i, x_i)$ for all i.

Theorem 10.2.33 *[31] Let (V, f) be a non-degenerate symplectic space of dimension $2m$.*
(i) V has a hyperbolic basis $\{x_1, y_1, x_2, y_2, \cdots, x_m, y_m\}$.
(ii) The inner product matrix A of f relative to this ordered basis is the matrix J which is the direct sum of 2×2 blocks $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.
(iii) If $u = \sum_i(\alpha_i x_i + \beta_i y_i)$ and $v = \sum_i(\lambda_i x_i + \mu_i y_i)$, then $f(u, v) = \sum_i(\alpha_i \mu_i - \beta_i \lambda_i)$.
(iv) All non-degenerate symplectic forms on V are equivalent and the symplectic group **Isom**(V, f)*, up to isomorphism, do not depend on the choice of f.*

Proof. (i) Since V is the orthogonal direct sum of hyperbolic planes H_i by Corollary 10.2.27, the union of the bases of H_i, $1 \leq i \leq m$ produces hyperbolic basis of V.

(ii) By simple calculations we can see that the matrix of f with respect to the above basis is

$$J = \begin{pmatrix} \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & & & 0 \\ & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & & \\ & & \cdot & & \\ & & & \cdot & \\ & 0 & & & \cdot \\ & & & & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} \end{pmatrix}$$

which is the direct sum of 2×2 blocks $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

(iii) Let $u = \sum_i(\alpha_i x_i + \beta_i y_i)$ and $v = \sum_i(\lambda_i x_i + \mu_i y_i)$, then

$$\begin{aligned} f(u,v) &= f(\sum_i(\alpha_i x_i + \beta_i y_i), \sum_i(\lambda_i x_i + \mu_i y_i)) \\ &= \sum_{i,j} \alpha_i\lambda_j f(x_i,x_j) + \sum_{i,j} \alpha_i\mu_j f(x_i,y_j) + \sum_{i,j} \beta_i\lambda_j f(y_i,x_j) + \sum_{i,j} \beta_i\mu_j f(y_i,y_j) \\ &= \sum_i \alpha_i\mu_i + \sum_i(-1)\beta_i\lambda_i = \sum_i(\alpha_i\mu_i - \beta_i\lambda_i). \end{aligned}$$

(iv) If g is a non-degenerate symplectic form, then there exists a hyperbolic basis of V relative to g, so that any inner product matrix of g is also congruent to J, and hence to any inner product matrix of f. Therefore, by Theorem 10.2.17 the isometry group **Isom**(V,f) does not depend on the choice of f. Thus up to isomorphism there is a unique class of symplectic groups on V. □

Note 10.2.34 The result of part *(iii)* in Theorem 10.2.33 implies that the symplectic forms are sums of 2×2 determinants. If a hyperbolic basis is reordered so that all the x_i precede all the y_i, then the matrix J is congruent to $\begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$. In this case we say that $\{x_1, x_2, \cdots, x_m, y_1, y_2, \cdots, y_m\}$ is a **reordered hyperbolic** basis of V.

Definition 10.2.35 *If (V,f) is a non-degenerate space, then the* **adjoint** *of a linear transformation T, denoted by T^*, is a linear transformation on V for which $f(T(x),y) = f(x,T^*(y))$ $\forall x,y \in V$.*

Lemma 10.2.36 *Let (V, f) be a non-degenerate symplectic space and let T be a linear transformation on V having an adjoint T^*. Then T is an isometry if and only if $T^*T = I_V$.*

Proof. If T has an adjoint with $T^*T = I_V$. Then for all $x, y \in V$ we have $f(T(x), T(y)) = f(x, T^*T(y)) = f(x, y)$, hence T is an isometry. Conversely assume that T is an isometry. Then for all $x, y \in V$ we have $f(x, T^*T(y) - y) = f(x, T^*T(y)) - f(x, y) = f(T(x), T(y)) - f(x, y) = 0$. Since f is non-degenerate, we must have $T^*T(y) - y = 0_V$ for all $y \in V$. That is $(T^*T - 1_V)(y) = 0_V$ for all $y \in V$. Hence $T^*T = I_V$. □

Theorem 10.2.37 *[31] Let (V, f) be a non-degenerate symplectic space. Let $T \in GL(V)$, and let $\{x_1, x_2, \cdots, x_m, y_1, y_2, \cdots, y_m\}$ be a reordered hyperbolic basis of V. If the matrix Q of T with respect to this basis is decomposed into $m \times m$ blocks $Q = \begin{pmatrix} A & C \\ B & D \end{pmatrix}$ then T^* exists and has a matrix*

$$Q^* = \begin{pmatrix} D^t & -C^t \\ -B^t & A^t \end{pmatrix},$$

moreover, $Q \in SP(2n, q)$ if and only if $Q^*Q = I_{2m}$.

Proof. Assume that T^* exists. If $T(x_i) = \sum_k(\alpha_{ki}x_k + \beta_{ki}y_k)$, then

$$\begin{aligned} f(x_i, T^*(x_j)) &= f(T(x_i), x_j) = f(\sum_k(\alpha_{ki}x_k + \beta_{ki}y_k), x_j) \\ &= f(\sum_k \alpha_{ki}x_k, x_j) + f(\sum_k \beta_{ki}y_k, x_j) = \sum_k \alpha_{ki}f(x_k, x_j) + \sum_k \beta_{ki}f(y_k, x_j) \\ &= -\beta_{ji}. \end{aligned}$$

On the other hand if $T^*(x_j) = \sum_r(\lambda_{rj}x_r + \mu_{rj}y_r)$, then

$$\begin{aligned} f(x_i, x_j) &= f(x_i, \sum_r \lambda_{rj}x_r + \mu_{rj}y_r) \\ &= f(x_i, \sum_r \lambda_{rj}x_r) + f(x_i, \sum_r \mu_{rj}y_r) = \sum_r \lambda_{rj}f(x_i, x_r) + \sum_r \mu_{rj}f(x_i, y_r) \\ &= \mu_{ij}. \end{aligned}$$

Hence $-\beta_{ji} = \mu_{ij}$, and so it follows that the matrix of T^* is $Q^* = \begin{pmatrix} M & X \\ N & Y \end{pmatrix}$ where $N = -B^t$. Similar calculations give the other three blocks, that is, $M = D^t, X = -C^t$ and $Y = A^t$. For the existence of T^* we can see that the matrix construction defines a linear transformation that behaves as the adjoint must. Now from Lemma 10.2.36 we deduce that T is an isometry if and only if $T^*T = I_V$. Hence $Q \in SP(2n, q)$ if and only if $Q^*Q = I_{2m}$.
□

Note 10.2.38 Notice that by Lemma 10.2.15, symplectic matrices have determinant ± 1. It can be shown, in fact that every symplectic matrix has determinant 1; that is $SP(2n,\ \mathbb{F}) \leq SL(2n,\ \mathbb{F})$.

Theorem 10.2.39 *$SP(2n,\ \mathbb{F})$ is a transitive permutation group on the set of all hyperbolic pairs.*

Proof. $SP(2n,\ \mathbb{F})$ has a permutation representation on the set of all hyperbolic pairs $\{x, y\}$ given by $T \mapsto T_1$, where $T \in SP(2n,\ \mathbb{F})$ and

$$T_1 = \left(\begin{array}{c} \{x, y\} \\ \{T(x), T(y)\} \end{array} \right) .$$

Let $\{x_1, y_1\}$,$\{x_2, y_2\}$ be two hyperbolic pairs. Then we have that $f(x_1, y_1) = f(x_2, y_2) = 1$. Thus there is a linear automorphism T such that $T(x_1) = x_2$ and $T(y_1) = y_2$. Let

$$H_1 = \langle x_1, y_1 \rangle \quad \text{and} \quad H_2 = \langle x_2, y_2 \rangle \ .$$

Then we observe that $T : H_1 \longrightarrow H_2$ is an isometry. By Theorem 10.2.29, there is an isometry $S \in SP(2n,\ \mathbb{F})$ such that $S \downarrow_{H_1} = T$. Hence $SP(2n,\ \mathbb{F})$ is transitive on the set of all hyperbolic pairs. □

Theorem 10.2.40 *[19] Let (V, f) be a non-degenerate symplectic space of dimension $2n$ over $GF(q)$. Then the number of hyperbolic pairs of V is $q^{2n-1}.(q^{2n} - 1)$.*

Proof. We observe that $|V| = q^{2n}$. Let $\{x, y\}$ be a hyperbolic pair. Then we have that $f(x, y) = 1$ and hence $x \neq 0_V$. Thus we have that $dim(\langle x \rangle) = 1$ and hence we obtain that $dim(\langle x \rangle^{\perp}) = 2n - 1$. Therefore the number of elements of V which are not in $\langle x \rangle^{\perp}$ is $q^{2n} - q^{2n-1}$. Since $|\ \mathbb{F}^*| = q - 1$, the number of elements $y \in V$ for which $f(x, y) = 1$ is given by $\frac{q^{2n} - q^{2n-1}}{q-1}$. Thus the number of hyperbolic pairs is given by

$$(q^{2n} - 1).(\frac{q^{2n} - q^{2n-1}}{q - 1}) = (q^{2n} - 1).q^{2n-1}(\frac{q - 1}{q - 1}) = q^{2n-1}.(q^{2n} - 1) \ .$$

□

Theorem 10.2.41 *[9] Let (V, f) be a non-degenerate symplectic space of dimension $2n$ over $GF(q)$. Then*

$$|SP(2n, q)| = q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1) \ .$$

Proof. Since V is non-degenerate, there is a hyperbolic basis for V. Let $\{x_1, y_1, x_2, y_2, \cdots, x_n, y_n\}$ be a fixed hyperbolic basis for V. Let $T \in SP(2n,q)$. Since T is an isometry, $\{T(x_1), T(y_1), T(x_2), T(y_2), \ldots, T(x_n), T(y_n)\}$ is a hyperbolic basis for V. Thus we obtain that $|SP(2n,q)|$ is the number of hyperbolic bases for V. We apply induction on n, to count the number of ways of choosing hyperbolic bases for V. There are $q^{2n-1}.(q^{2n}-1)$ ways of choosing a hyperbolic pair $x_1, y_1 \in V$. Let $H_1 = \langle x_1, y_1 \rangle$, then the restriction $\overline{f}$ of f to $H_1^\perp$ is non-degenerate and thus making $(H_1^\perp, \overline{f})$ into a non-degenerate symplectic space. Thus the remaining vectors of the hyperbolic basis for V may be chosen as a hyperbolic basis for $(H_1^\perp, \overline{f})$. Since $dim(H_1^\perp) = 2n-2$, the number of hyperbolic bases for $(H_1^\perp, \overline{f})$ is equal to $|SP(2n-2,q)|$. Hence we obtain that

$$\begin{aligned} |SP(2n,q)| &= q^{2n-1}.(q^{2n}-1).|SP(2n-2,q)| \\ &= q^{2n-1}.(q^{2n}-1).q^{(n-1)^2}\prod_{i=1}^{n-1}(q^{2i}-1) \\ &= q^{n^2}\prod_{i=1}^{n}(q^{2i}-1). \end{aligned}$$

□

Note 10.2.42 If V is a $2n$-dimensional non-degenerate symplectic space over a field $\mathbb{F}$, and $SP(2n, \mathbb{F})$ is the symplectic group of isometries of V, then the centre $Z(SP(2n, \mathbb{F})$ of $SP(2n, \mathbb{F})$ consists of the transformations $T = kI$, where $k = \pm 1$. The factor group $SP(2n, \mathbb{F})/Z(SP(2n, \mathbb{F}))$ is called the *projective symplectic group* and is denoted by $PSP(2n, \mathbb{F})$. The projective symplectic groups are simple except for $PSP(2,2) = PSL(2,2)$, $PSP(2,3) = PSL(2,3)$ and $PSP(4,2)$. If $\mathbb{F} = GF(q)$, is the Galois field of q elements, then $SP(2n, \mathbb{F})$ and $PSP(2n, \mathbb{F})$ are denoted by $SP(2n,q)$ and $PSP(2n,q)$ respectively, and we have

$$\begin{aligned} Z(SP(2n,q)) &= \{I\} \;\; if \;\; char(\mathbb{F}) = 2 \;\; and \\ Z(SP(2n,q)) &= \{I, -I\} \;\; if \;\; char(\mathbb{F}) \neq 2 \end{aligned}$$

We also have

$$\begin{aligned} |PSP(2n,q)| &= \frac{1}{(2,q-1)} \times |SP(2n,q)| \\ &= \frac{q^{n^2}}{(2,q-1)}\prod_{i=1}^{n}(q^{2i}-1) \;\; . \end{aligned}$$

Definition 10.2.43 *If V is a vector space of dimension n and H is a subspace of V of dimension $n-1$, then we say that H is a* **hyperplane** *of V. If $\mathbb{F} = GF(q)$ and H is a hyperplane in V, then H contains q^{n-1} points.*

Definition 10.2.44 *Let V be a non-degenerate symplectic space over a field $\mathbb{F}$ and $T \in SP(2n, \mathbb{F})$, $T \neq I$ such that for some hyperplane H of V, we have*
(i) $T(h) = h \ \ \forall\, h \in H$,
(ii) $T(u) - u \in H \ \ \forall\, u \in V - H$. Then T is called **symplectic transvection** *of V.*

Theorem 10.2.45 *[19] Let T be a symplectic transvection with hyperplane H. Then there is a non-zero $z \in V$ such that $H = \langle z\rangle^{\perp}$ and for all $y \in V$ we have $T(y) = y + kf(z, y)z$ for $k \in \mathbb{F}$. Conversely for $z \neq 0, z \in V$ and $0 \neq k \in \mathbb{F}$ define $T : V \longrightarrow V$ by $T(y) = y + kf(z, y)z$ for all $v \in V$. Then T is a symplectic transvection with hyperplane $\langle z\rangle^{\perp}$.*

Proof. Let $u \in V - H$. Since T is non-identity, $T(u) - u \neq 0$. Let $v \in H$ such that $v \neq 0$ and $T(u) - u = v$. Since H is a hyperplane and $u \notin H$, $V = \langle u\rangle \oplus H$. Then $dim(H^{\perp}) = 1$ and hence $H^{\perp} = \langle z\rangle$ for some $z \neq 0, z \in V$. Define $\phi : V \longrightarrow \mathbb{F}$ by $\phi(y) = \phi(\lambda u + h) = \lambda$ and it can be shown that ϕ is a linear functional, so there is $w \in V$ such that $w^{\theta} = \phi$, where $\theta : V \longrightarrow V^{*}$ is the linear isomorphism given in Remark 10.2.21 part 3. For all $y \in V$, $\phi(y) = w^{\theta}(y) = f(w, y)$,

$$\begin{aligned} T(y) &= T(\lambda u + h) = \lambda T(u) + T(h) = \lambda T(u) + h = \lambda(v + u) + h \\ &= \lambda v + \lambda u + h = y + \lambda v = y + \phi(y)v = y + f(w, y)v. \end{aligned}$$

Now, for all $h \in H$, $f(h, u) = f(T(h), T(u)) = f(h, u+v) = f(h, u)+f(h, v)$. So $f(h, v) = 0$ for all $h \in H$, that is $v \in H^{\perp}$. Since $H = \langle z\rangle^{\perp}$ then $v \in \langle z\rangle$, so that $v = k_1 z$ for some $k_1 \in \mathbb{F}$. Since $v \neq 0$, then $k_1 \neq 0$. Therefore $T(y) = y + k_1 f(w, y)z$. Since $0 = \phi(h) = f(w, h)$ for all $h \in H$, $w \in H^{\perp}$ and thus $w = k_2 z$ for some $k_2 \in \mathbb{F}$. Hence $T(y) = y + k_1 k_2 f(z, y)z$.

Conversely for $0 \neq k \in \mathbb{F}$ and $0 \neq z \in V$, define $T : V \longrightarrow V$ by $T(y) = y + kf(z, y)z$ for all $y \in V$. It can be shown that $T \in SP(2n, \mathbb{F})$. Let $H = \langle z\rangle^{\perp}$ then for $h \in H$, $T(h) = h + kf(z, h)z = h + 0 = h$ and if $y \in V$ then $T(y) - y = kf(z, y)z = az$ for some $a \in F$. Since $\langle z\rangle \subseteq \langle z\rangle^{\perp}$, then $T(y) - y \in \langle z\rangle^{\perp} = H$. Therefore T is a symplectic transvection with the hyperplane $H = \langle z\rangle^{\perp}$. □

If T is a transvection, then by Theorem 10.2.45 there exists $k \in F^{*}$ and $z \in V^{*}$ such that $T = T_{k,z}$. For $T = T_{k,z}$ we say that T is a transvection in the direction z. Let X be the set of all symplectic transvections of V. Then it can be shown that $\langle X\rangle$ is transitive on $V - \{0_V\}$ and on hyperbolic pairs.

Theorem 10.2.46 *[19] $SP(2n, \mathbb{F})$ is generated by the set of all symplectic transvections.*

Proof. For $n = 1$, we obtain that $SP(2,\ \mathbb{F}) \cong SL(2,\ \mathbb{F})$ and that $SL(V) = \langle X\rangle$ and the proof is complete. Suppose that $n > 1$ and let $\{u, v\}$ be a hyperbolic pair and $S \in SP(2n,\ \mathbb{F})$. Then $\{S(u), S(v)\}$ is also a hyperbolic pair. Since $\langle X\rangle$ is transitive on hyperbolic pairs, then there exists $T \in \langle X\rangle$ such that $T(u) = S(u)$ and $T(v) = S(v)$. Let $P = T^{-1}S : \{u,v\} \longrightarrow \{u,v\}$ and $H = \langle u,v\rangle$. Then $V = H \perp H^{\perp}$. Since P fixes H, then $P(H^{\perp}) = H^{\perp}$ and thus P also fixes $H^{\perp}$. Thus by Theorem 10.2.29 we obtain that $P\downarrow_{H^{\perp}}= P'$ is an isometry on $H^{\perp}$. Now suppose the result is true for all symplectic spaces whose dimensions are less than $2n$. Since $dim(H^{\perp}) = 2n-2$, then by the induction hypothesis

$$P' = \prod_i T_i' \quad ,$$

where T_i''s are symplectic transvections of $H^{\perp}$. Now we define $T_i : V \longrightarrow V$ by $T_i(h+h') = h + T_i'(h')\ \forall\ h \in H,\ h' \in H^{\perp}$ and all indices i. If T_i' is a transvection with hyperplane $\langle h_i'\rangle^{\perp} \cap H^{\perp}$, where $h_i' \in H^{\perp}$, then T_i will also be a transvection with hyperplane $H^{\perp}(\langle h_i'\rangle^{\perp} \cap H^{\perp})$. Since

$$P' = \prod_i T_i' \quad \text{and} \quad P = T^{-1}S \quad ,$$

then we obtain that

$$S = \prod_i TT_i$$

and thus $S \in \langle X\rangle$. □

Corollary 10.2.47 *$SP(2n,\ \mathbb{F})$ is transitive on $V - \{0_V\}$.*

Proof. The result follows immediately since $SP(2n,\ \mathbb{F})$ is generated by the set of all symplectic transvections of V. □

10.2.4 The Affine Subgroup of the Symplectic Group

Since $SP(2n, q)$ is transitive on the non-zero vectors of V, we consider the subgroup of $SP(2n, q)$ which is a stabilizer of a non-zero vector of V and study its structure.

Definition 10.2.48 *Let (V, f) be a non-degenerate symplectic space of dimension $2n$ over $\mathbb{F} = GF(q)$, where $q = p^k$ for some prime p. Let $B = \{e_1, e_2, \ldots, e_{2n}\}$ be a basis for V and $f : V \times V \longrightarrow \mathbb{F}$ defined by $f(e_i, e_j) = \delta(i, 2n+1-j)$, where $i \leq j$. Let T be an isometry of (V, f) and*

$$G(n) = SP(2n, q) = \{T \mid f(T(x), T(y)) = f(x, y)\ \ \forall x, y \in V\}.$$

Since $G(n)$ acts transitively on $V - \{0_V\}$, let $\alpha \in V - \{0_V\}$ and $A(n)$ be the stabilizer of α in $G(n)$ then we have that

$$A(n) = \{T \in G(n) \mid T(\alpha) = \alpha\}.$$

Thus $A(n) \leq G(n)$. The group $A(n)$ is called the **affine subgroup** *of $G(n)$.*

Remark 10.2.49 Since $A(n)$ is the stabilizer of $\alpha \in V - \{0_V\}$ in $G(n)$, we have that $[G(n){:}A(n)] = |V - \{0_V\}| = q^{2n} - 1$. Now since $G(n)$ acts transitively on $V - \{0_V\}$, then we let $A(n)$ to be the stabilizer of e_1 in $G(n)$. That is $A(n) = \{T \in G(n) \mid T(e_1) = e_1\}$.

Remark 10.2.50 If P is a p-group. Then $P' \leq \Phi(P)$. We say that P is a **special** p-group if we have that $Z(P) = P' = \Phi(P)$ is elementary abelian.

Lemma 10.2.51 *Let $a \in GF(q)$, with $char(GF(q)) = p$ and $(n,p) = 1$, $n \in \mathbb{N}$. Then there exists $b \in GF(q)$ such that $nb = a$.*

Proof. If $a = 0$, then let $b = 0$. Suppose $a \neq 0$. Let $(GF(q))^* =< x >$ where $o(x) = q - 1$. Then $a \in (GF(q))^*$ implies that $a = x^{m'}, 1 \leq m' \leq q - 1$. Since $(n,p) = 1, nx \neq 0$. Thus $nx \in (GF(q))^*$ and hence $nx = x^m$ where $1 \leq m \leq q - 1$. Let $b = x^{m'-m+1}$. Then $b \in (GF(q))^*$ and $nb = nx^{m'-m+1} = (nx)x^{m'-m} = x^m.x^{m'-m} = x^{m'} = a$. □

Definition 10.2.52 *We define $P(n)$ to be the subgroup of $A(n)$ consisting of elements $T \in G(n)$, such that*

$$T(e_1) = e_1$$

$$T(e_i) = \alpha_i e_1 + e_i, \quad 2 \leq i \leq 2n - 1$$

and

$$T(e_{2n}) = \sum_{i=1}^{2n} \beta_i e_i$$

with $\beta_{2n} = 1$ and

$$\alpha_j = \begin{cases} -\beta_{2n+1-j} & 2 \leq j \leq n \\ \beta_{2n+1-j} & n < j \leq 2n - 1. \end{cases}$$

If $x \in P(n)$, then x is represented by the following matrix, with respect to the basis B given in Definition 10.2.48:

$$\begin{pmatrix} 1 & -\beta_{2n-1} & -\beta_{2n-2} & \cdots & \beta_2 & \beta_1 \\ 0 & 1 & 0 & \cdots & 0 & \beta_2 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \beta_{2n-1} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

It is convenient to describe $P(n)$ as an abstract group P in the following manner: Let (V, f) be a non-degenerate symplectic space of dimension $2n-2$ over $GF(q)$ and consider the pairs $[v, a]$, where $v \in V$ and $a \in GF(q)$. Define a multiplication on such pairs by $[v, a][u, b] = [u+v, a+b+f(v, u)]$. It is clear that $|P| = q^{2n-2} \times q = q^{2n-1}$.

Lemma 10.2.53 *[13] If* char($\mathbb{F}$) $= p$ *where p is an odd prime, then the group P is a non-abelian special p-group of order q^{2n-1} isomorphic to $P(n)$.*

Proof. It is not difficult to see that P is a non-abelian group of order q^{2n-1} under the multiplication defined above, with $[0_V,\ 0] = 1_P$ and $[v,\ a]^{-1} = [-v\ , -a]$.

(i) P is non-abelian: Since

$$[v, a][u, b] = [u+v, a+b+f(v, u)] \text{ and } [u, b][v, a] = [u+v, a+b+f(u, v)],$$

it suffices to show that $f(u, v) \neq f(v, u)$. Now, since f is symplectic we have that $f(u, v) = -f(v, u) \neq f(v, u)$, thus P is non-abelian.

(ii) P is special: We need to show that $Z(P) = P' = \Phi(P)$. Now

$$\begin{aligned} [v, a] \in Z(P) &\Leftrightarrow [v, a][u, b] = [u, b][v, a] \quad \forall u \in V \textit{ and } \quad \forall a, b \in GF(q) \\ &\Leftrightarrow f(u, v) = f(v, u) \quad \forall u \in V \\ &\Leftrightarrow f(u, v) = f(v, u) = -f(u, v) \quad \forall u \in V \\ &\Leftrightarrow 2f(u, v) = 0 \quad \forall u \in V \\ &\Leftrightarrow f(u, v) = 0 \quad \forall u \in V \\ &\Leftrightarrow v = 0_V. \end{aligned}$$

Thus $Z(P) = \{[0_V, a] \mid a \in GF(q)\} \cong GF(q)$ and $|Z(P)| = |GF(q)| = q$. Now

$$\begin{aligned} P' &= < [v, a], [u, b] \mid u, v \in V,\ \ a, b \in GF(q) > \\ &= \{[v, a][u, b][v, a]^{-1}[u, b]^{-1} \mid u, v \in V,\ a, b \in GF(q)\} \\ &= \{[v, a][u, b]([u, b][v, a])^{-1} \mid u, v \in V, a, b \in GF(q)\} \\ &= \{[0_V,\ 2f(u, v)] \mid u, v \in V, a, b \in GF(q)\}. \end{aligned}$$

Hence $P' \subseteq Z(P)$. Conversely we need to show that $Z(P) \subseteq P'$. By Lemma 10.2.51, if $[0_V, a] \in Z(P)$, with $a \in GF(q)$ we can find $b \in GF(q)$ such that $2b = a$. Now let $v = e_1$ and $u = be_{2n}$, then $f(v, u) = f(e_1, be_{2n}) = b\delta_{11} = b$, so $2f(v, u) = 2b = a$. Hence $[0_V, a] = [0_V,\ 2f(v, u)] \in P'$, which implies that $Z(P) \subseteq P'$. Thus $P' = Z(P)$. Therefore $P' = \{[0_V, a] \mid a \in GF(q)\}$. Since $P = \{[v, a] \mid v \in V,\ a \in GF(q)\}$, we have

$$P^p \ = \ < \ x^p \mid x \in P \ > \ = \ < \ [v, a]^p \ \mid v \in V,\ \ a \in GF(q) \ > .$$

But

$$\begin{aligned}[v,a]^p &= [\ pv,\ pa + \underbrace{f(v,v) + \cdots + f(v,v)}_{(p-1)times}\ ] \\ &= [\ 0_V,\ \underbrace{f(v,v) + \cdots + f(v,v)}_{(p-1)times}\ ] = [0_V, c] \in P',\ \text{where } c = \underbrace{f(v,v) + \cdots + f(v,v)}_{(p-1)times},\end{aligned}$$

implies that $[v,a]^p \in P'$ and hence $P^p \subseteq P'$. Since $\Phi(P) = P'P^p$, we have that $\Phi(P) = P'P^p = P'$. Thus P is a special p-group.

(iii) $P(n)$ is isomorphic to P : Define $\phi : P(n) \longrightarrow P$ given by $\phi(x) = [v,a]$, where $x \in P(n)$ has the form

$$x = \begin{pmatrix} 1 & -\beta_{2n-1} & -\beta_{2n-2} & \cdots & \beta_2 & \beta_1 \\ 0 & 1 & 0 & \cdots & 0 & \beta_2 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \beta_{2n-1} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix},$$

and $v = (-\beta_{2n-1}, -\beta_{2n-2}, \cdots, \beta_3, \beta_2)$ with $a = \beta_1$ (see Definition 10.2.52). We need to show that ϕ is a one to one and onto homomorphism.

ϕ is a homomorphism: Let $x, y \in P(n)$ such that

$$x = \begin{pmatrix} 1 & -\beta_{2n-1} & -\beta_{2n-2} & \cdots & \beta_2 & \beta_1 \\ 0 & 1 & 0 & \cdots & 0 & \beta_2 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \beta_{2n-1} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

and

$$y = \begin{pmatrix} 1 & -\beta'_{2n-1} & -\beta'_{2n-2} & \cdots & \beta'_2 & \beta'_1 \\ 0 & 1 & 0 & \cdots & 0 & \beta'_2 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \beta'_{2n-1} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

If $v = (-\beta_{2n-1}, -\beta_{2n-2}, \cdots, \beta_3, \beta_2)$ and $v' = (-\beta'_{2n-1}, -\beta'_{2n-2}, \cdots, \beta'_3, \beta'_2)$ then we have that $\phi(xy) = [\ v + v',\ \beta_1 - \beta_{2n-1}\beta'_2 - \beta_{2n-2}\beta'_3 - \cdots + \beta_3\beta'_{2n-2} + \beta_2\beta'_{2n-1} + \beta'_1\ ]$. Since $\phi(x) = [v,\ \beta_1]$ and $\phi(y) = [v',\ \beta'_1]$, we have $\phi(x)\phi(y) = [v + v', \beta_1 + \beta'_1 + f(v,v')]$. So it suffices to show that $-\beta_{2n-1}\beta'_2 - \beta_{2n-2}\beta'_3 - \cdots + \beta_3\beta'_{2n-2} + \beta_2\beta'_{2n-1} = f(v,v')$. Now direct calculations show that $f(v,v') = -\beta_{2n-1}\beta'_2 - \beta_{2n-2}\beta'_3 - \cdots + \beta_3\beta'_{2n-2} + \beta_2\beta'_{2n-1}$, and hence we have that $\phi(xy) = \phi(x)\phi(y)$.

ϕ is one-to-one:

$$\begin{aligned}\phi(x) = \phi(y) &\Rightarrow [v,\ \beta_1] = [v',\ \beta'_1] \\ &\Rightarrow v = v' \ and\ \beta_1 = \beta'_1\end{aligned}$$

$$\begin{aligned}
&\Rightarrow \beta_i = \beta_i' \textit{ and } \beta_1 = \beta_1' \quad 2 \leq i \leq 2n-1 \\
&\Rightarrow \beta_i = \beta_i' \ \forall i \quad 1 \leq i \leq 2n-1 \\
&\Rightarrow x = y.
\end{aligned}$$

Now

$$\begin{aligned}
Im(\phi) = \{\phi(x) \mid x \in P(n)\} &= \{[v,\ \beta_1] \mid v \in V,\ \beta_1 = a \in GF(q)\} \\
&= \{[v,\ a] \mid v \in V,\ a \in GF(q)\} = P.
\end{aligned}$$

Hence ϕ is onto, so $P(n) \cong P$.

We know that

$$P(n) = \left\{ \begin{pmatrix} 1 & -\beta_{2n-1} & -\beta_{2n-2} & \cdots & \beta_2 & \beta_1 \\ 0 & 1 & 0 & \cdots & 0 & \beta_2 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \beta_{2n-1} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix},\ \beta_i \in GF(q),\ \ i = 1, 2 \cdots, 2n-1 \right\}.$$

Since the entries above the main diagonal are arbitrary elements of $GF(q)$ and there are exactly $2n-1$ places above the diagonal, we have that $|P(n)| = q^{2n-1}$. □

Remark 10.2.54 *If $p = 2$, then $P(n)$ is an elementary abelian 2-group.* Let $x \in P$, then $x = [v, a]$ where $v \in V$ and $a \in GF(q)$. Since $p = 2$ we have that $x^2 = [v, a]^2 = [2v, 2a] = [0_V, 0] = 1_P$. Thus P is an elementary abelian 2-group. Since $P(n) \cong P$, then $P(n)$ is also an elementary abelian 2-group.

Lemma 10.2.55 *[24] Let H be the subgroup of $A(n)$ which fixes e_{2n}. Then H fixes both e_1 and e_{2n} and acts on $W = \langle e_2, e_3, \ldots, e_{2n-1}\rangle$ as $G(n-1)$. Moreover $H \cong G(n-1) \cong SP(2n-2, q)$.*

Proof. Follows immediately from Theorem 10.2.41. □

Theorem 10.2.56 *[13] Let q be a power of an odd prime p. Then $A(n)$ is a split extension of $P(n)$ by H where $H \cong G(n-1) \cong SP(2n-2, q)$. That is*

$$A(n) = P(n){:}H = P(n){:}SP(2n-2, q) \quad .$$

Proof. We need to show that H is a complement of $P(n)$ in $A(n)$. This is equivalent to show the following:

(i) $P(n) \cap H = \{1_{A(n)}\}$

(ii) $P(n) \cdot H = A(n)$

(iii) $P(n) \trianglelefteq A(n)$.

(i) Let $T \in P(n)$ then $T(e_{2n}) = \beta_1 e_1 + \beta_2 e_2 + \cdots + \beta_{2n-1} e_{2n-1} + e_{2n}$. If $T \in H$, then $T(e_{2n}) = e_{2n}$ and hence we must have $\beta_i = 0 \quad 1 \leq i \leq 2n-1$ and $\beta_{2n} = 1$. Hence $\alpha_i = 0, \quad 2 \leq i \leq 2n-1$. Thus $T(e_i) = e_i \quad \forall i$, so that $T = I_{A(n)}$.

(ii) Since $G(n)$ acts transitively on $V - \{0_V\}$, we have that $|G(n)| = |V^*||A(n)|$.

So

$$\begin{aligned} |A(n)| &= \frac{q^{n^2}(q^{2n-2}-1)(q^{2n-4}-1)\cdots(q^4-1)(q^2-1)(q^{2n}-1)}{q^{2n}-1} \\ &= q^{n^2}(q^{2n-2}-1)(q^{2n-4}-1)\cdots(q^4-1)(q^2-1). \end{aligned}$$

Now

$$|P(n) \cdot H| = \frac{|P(n)||H|}{|P(n) \cap H|} = |P(n)||H|.$$

Since $H \cong SP(2n-2, q)$, we have that

$$|H| = q^{(n-1)^2}(q^{2n-2}-1)(q^{2n-4}-1)\cdots(q^4-1)(q^2-1).$$

Thus

$$\begin{aligned} |P(n)||H| &= q^{2n-1}q^{(n-1)^2}(q^{2n-2}-1)\cdots(q^4-1)(q^2-1) \\ &= q^{n^2}(q^{2n-2}-1)\cdots(q^4-1)(q^2-1) \\ &= |A(n)|. \end{aligned}$$

Since $P(n) \cdot H \subseteq A(n)$, we must have $P(n) \cdot H = A(n)$.

(iii) If $A \in A(n)$, then $A = p_0 T_0$ where $p_0 \in P(n)$ and $T_0 \in H$. To show that $P(n) \trianglelefteq A(n)$, let $p \in P(n)$. Then

$$p_0 T_0 p (p_0 T_0)^{-1} = p_0 T_0 p T_0^{-1} p_0^{-1} = p_0 (T_0 p T_0^{-1}) p_0{}^{-1}.$$

Hence it suffices to show that $TpT^{-1} \in P(n) \quad \forall T \in H, \forall p \in P(n)$. If $B' = \{e_1, e_2, \cdots, e_n, e_{2n}, e_{2n-1}, e_{2n-2}, \cdots, e_{n+2}, e_{n+1}\}$ is the ordered basis obtained from B, then the action of $T \in H$ on the vectors of B' is described by

$$T(e_1) = e_1, \quad T(e_{2n}) = e_{2n}$$

and

$$T(e_i) = \sum_{j=1}^{n} \lambda_{ji} e_j + \sum_{j=n+1}^{2n} \lambda_{ji} e_{3n+1-j}, \quad 2 \leq i \leq n,$$

$$T(e_i) = \sum_{j=1}^{n} \lambda_{j\ 3n+1-i} e_j + \sum_{j=n+1}^{2n} \lambda_{j\ 3n+1-i} e_{3n+1-j}, \quad n < i \leq 2n-1.$$

Hence T can be represented by the following matrix, with respect to B'

$$\begin{pmatrix} 1 & \lambda_{1\,2} & \cdots & \lambda_{1\,n} & 0 & \lambda_{1\,n+2} & \cdots & \lambda_{1\,2n} \\ 0 & \lambda_{2\,2} & \cdots & \lambda_{2\,n} & 0 & \lambda_{2\,n+2} & \cdots & \lambda_{2\,2n} \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \lambda_{n\,2} & \cdots & \lambda_{n\,n} & 0 & \lambda_{n\,n+2} & \cdots & \lambda_{n\,2n} \\ 0 & \lambda_{n+1\,2} & \cdots & \lambda_{n+1\,n} & 1 & \lambda_{n+1\,n+2} & \cdots & \lambda_{n+1\,2n} \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \lambda_{2n\,2} & \cdots & \lambda_{2n\,n} & 0 & \lambda_{2n\,n+2} & \cdots & \lambda_{2n\,2n} \end{pmatrix} = (\lambda_{ij})_{2n\times 2n}.$$

Since T is an isometry, then the adjoint of T exists and its action on the vectors of B' is given by

$$T^*(e_1) = e_1, \quad T^*(e_{2n}) = e_{2n}$$

and

$$T^*(e_i) = \sum_{j=1}^{n} \mu_{ji} e_j + \sum_{j=n+1}^{2n} \mu_{ji} e_{3n+1-j}, \quad 2 \leq i \leq n,$$

$$T^*(e_i) = \sum_{j=1}^{n} \mu_{j\,3n+1-i} e_j + \sum_{j=n+1}^{2n} \mu_{j\,3n+1-i} e_{3n+1-j}, \quad n < i \leq 2n-1.$$

Using the definition of adjoint of T, we find the entries of the first and the $(n+1)$-th rows of the matrix of T^* with respect to B'. For example, entries in the first row of the matrix of T^* are obtained as follows:

$$\begin{aligned} f(T(e_{2n}), e_1) &= f(e_{2n}, T^*(e_1)) = f(e_{2n}, e_1) = 1, \quad \text{so} \quad \mu_{1\,1} = \lambda_{n+1\,n+1} = 1 \\ f(T(e_{2n}), e_2) &= f(e_{2n}, T^*(e_2)), \quad \text{so} \quad \mu_{1\,2} = \lambda_{n+2\,n+1} = 0 \\ &\vdots \\ f(T(e_{2n}), e_n) &= f(e_{2n}, T^*(e_n)), \quad \text{so} \quad \mu_{1\,n} = \lambda_{2n\,n+1} = 0 \\ f(T(e_{2n}), e_{2n}) &= f(e_{2n}, T^*(e_{2n})) = f(e_{2n}, e_{2n}) = 0, \quad \text{so} \quad \mu_{1\,n+1} = \lambda_{1\,n+1} = 0 \\ &\vdots \\ f(T(e_{2n}), e_{n+1}) &= f(e_{2n}, T^*(e_{n+1})), \quad \text{so} \quad \mu_{1\,2n} = \lambda_{n\,n+1} = 0. \end{aligned}$$

Similar calculations give the entries of the $(n+1)$-th row of the matrix of T^*. Now by using the Theorem 10.2.37, we can easily see that T and T^* have the following matrix representations (with respect to B') respectively

$$\left(\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \lambda_{2\,2} & \cdots & \lambda_{2\,n} & 0 & \lambda_{2\,n+2} & \cdots & \lambda_{2\,2n} \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \lambda_{n\,2} & \cdots & \lambda_{n\,n} & 0 & \lambda_{n\,n+2} & \cdots & \lambda_{n\,2n} \\ \hline 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & \lambda_{n+2\,2} & \cdots & \lambda_{n+2\,n} & 0 & \lambda_{n+2\,n+2} & \cdots & \lambda_{n+2\,2n} \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & \lambda_{2n\,2} & \cdots & \lambda_{2n\,n} & 0 & \lambda_{2n\,n+2} & \cdots & \lambda_{2n\,2n} \end{array}\right) = \begin{pmatrix} A & C \\ B & D \end{pmatrix}$$

and

$$\left(\begin{array}{cccc|cccc}
1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
0 & \lambda_{n+2\;n+2} & \cdots & \lambda_{2n\;n+2} & 0 & -\lambda_{2\;n+2} & \cdots & -\lambda_{n\;n+2} \\
\vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
0 & \lambda_{n+2\;2n} & \cdots & \lambda_{2n\;2n} & 0 & -\lambda_{2\;2n} & \cdots & -\lambda_{n\;2n} \\
\hline
0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\
0 & -\lambda_{n+2\;2} & \cdots & -\lambda_{2n\;2} & 0 & \lambda_{2\;2} & \cdots & \lambda_{n\;2} \\
\vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
0 & -\lambda_{n+2\;n} & \cdots & -\lambda_{2n\;n} & 0 & \lambda_{2\;n} & \cdots & \lambda_{n\;n}
\end{array}\right) = \begin{pmatrix} D^t & -C^t \\ -B^t & A^t \end{pmatrix} .$$

Since $T \in P(n) \subseteq SP(2n,q)$, by Theorem 10.2.37 we have that $T^*T = I_{2n}$. Using this fact we obtain the following relations

$$\sum_{k=2}^{n} (\lambda_{n+k\;n+i}\lambda_{kj} - \lambda_{k\;n+i}\lambda_{n+k\;j}), \quad 2 \le i \le n, \quad 2 \le j \le 2n,$$

and

$$\sum_{k=0}^{n-2} (-\lambda_{i+k\;i-n}\lambda_{lj} + \lambda_{l\;i-n}\lambda_{i+k\;j}), \quad n+2 \le i \le 2n, \quad 2 \le j \le 2n, \quad 2 \le l \le n.$$

Now if $p \in P(n)$, then p can be represented (with respect to B') by the following matrix

$$\begin{pmatrix}
1 & -\beta_{2n-1} & -\beta_{2n-2} & \cdots & -\beta_{n+1} & \beta_1 & \cdots & \beta_n \\
0 & 1 & 0 & \cdots & 0 & \beta_2 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 & \beta_3 & \cdots & 0 \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & \beta_n & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 & 1 & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 & \beta_{2n-1} & \cdots & 0 \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\
0 & 0 & 0 & \cdots & 0 & \beta_{n+1} & \cdots & 1
\end{pmatrix} .$$

Using the above relations obtained for the entries of T we deduce that $T^{-1}pT$ has the following matrix representation

$$\begin{pmatrix}
1 & -\beta'_{2n-1} & -\beta'_{2n-2} & \cdots & -\beta'_{n+1} & \beta'_1 & \cdots & \beta'_n \\
0 & 1 & 0 & \cdots & 0 & \beta'_2 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 & \beta'_3 & \cdots & 0 \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & \beta'_n & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 & 1 & \cdots & 0 \\
0 & 0 & 0 & \cdots & 0 & \beta'_{2n-1} & \cdots & 0 \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\
0 & 0 & 0 & \cdots & 0 & \beta'_{n+1} & \cdots & 1
\end{pmatrix} .$$

Thus $T^{-1}pT \in P(n)$, so that $P(n) \trianglelefteq A(n)$. □

10.2.5 The group $A(2) = 2^3{:}SP(2,2)$

Here $P(2)$ is an elementary abelian group of order 8, so $P(2) \cong V_3(2)$, the vector space of dimension three over the field of two elements. Let $H \cong SP(2,2)$, we determine the conjugacy classes of the group $A(2) = P(2){:}H \cong 2^3{:}SP(2,2)$, where H acts naturally on $P(2)$.

Let $P(2)$ be generated by $\{\epsilon_1, \epsilon_2, \epsilon_3\}$, according to the Definition 10.2.52, where

$$\epsilon_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \epsilon_2 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \epsilon_3 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

and $\epsilon_i^2 = 1$, for $1 \leq i \leq 3$. Hence $P(2) = \{1, \epsilon_1, \epsilon_2, \epsilon_3, \epsilon_1\epsilon_2, \epsilon_1\epsilon_3, \epsilon_2\epsilon_3, \epsilon_1\epsilon_2\epsilon_3\}$. Let $H =< \alpha, \beta >$, where

$$\alpha = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

with $o(\alpha) = 2$ and $o(\beta) = 3$. Then the group $A(2)$ is generated by two 4×4 matrices over $GF(2)$, namely

$$x = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where $o(x) = 6$ and $o(y) = 2$.

10.2.6 The conjugacy classes of $A(2) = 2^3{:}SP(2,2)$

We have used GAP3 [32] to compute the conjugacy classes of the group $A(2)$, and we found that $A(2)$ has 10 conjugacy classes. We use Atlas [5] notation to list the conjugacy classes of $A(2)$. We also give class representatives in terms of 4×4 matrices over $GF(2)$. The information is given in the Table 9.1.

Table 9.1: The conjugacy classes of elements of $2^3{:}SP(2,2)$

$[g]_G$	M	$\vert[g]_G\vert$	$[g]_G$	M	$\vert[g]_G\vert$
$1A$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	1	$2A$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	6
$2B$	$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	3	$2C$	$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	6
$2D$	$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	1	$2E$	$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	3
$3A$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	8	$4A$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	6
$4B$	$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	6	$6B$	$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	8

Lemma 10.2.57 *The group $A(2)$ is isomorphic to the generalised symmetric group $2^3{:}S_3$.*

Proof. In the generalized symmetric group $2^3{:}S_3$, S_3 acts on 2^3 naturally producing four orbits of lengths 1, 1, 3 and 3 respectively. Using Table 9.1 we can see that for the group $A(2) = P(2){:}SP(2,2)$ we have $P(2) = \{1A\} \bigcup [2B] \bigcup [2E] \bigcup [2D]\}$, where $|[1A]| = 1$, $|[2B]| = |[2E]| = 3$ and $|[2D]| = 1$. Hence $SP(2,2)$ has 4 orbits of lengths 1, 1, 3 and 3 on $P(2) = 2^3$. Since $SP(2,2) \cong S_3$, the proof follows. □

Remark 10.2.58 Using the technique of the Fischer-Clifford matrices, Mpono in [27] has determined the conjugacy classes and constructed the character table of the affine group $A(3) = 2^5{:}S_6 \cong 2^5{:}SP(4,2)$ which is maximal in the group $SP(6,2)$ of index 63. For a more detailed and thorough account on the subject the reader is submitted to a reading of [26] and [27].

Bibliography

[1] J. L. Alperin and R. B. Bell, *Groups and Representations*, Springer-Verlag, New York, Inc., 1995.

[2] H. U. Besche and B. Eick, *The groups of order at most 1000, except 512 and 768*, J. Symb. Comput. **27**(4) (1999), 405 - 413.

[3] H. U. Besche and B. Eick, *Construction of finite groups*, J. Symb. Comput. **27**(4) (1999), 387 - 404.

[4] N. Biggs, *Finite Groups of Automorphisms*, London Mathematical Society Lecture Note Series **6**, Cambridge University Press, London, 1971.

[5] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups*, Oxford University Press, Oxford, 1985.

[6] J. Cossey, O. H. Këgel and L. G. Kovács, *Maximal Frattini extensions*, Archiv Der Mathematik **35** (1980), 210 - 217.

[7] M. R. Darafsheh and A. Iranmanesh, *Construction of the character table of the hyperoctahedral group*, Riv. Mat. Pura Appl. **17** (1996), 71 - 82.

[8] M. Deaconescu, *Frattini-like Subgroups of Finite Groups*, Mathematical Reports, Harward Academic publishers GmbH, London, 1986, Vol 2, 385 - 498.

[9] J. D. Dixon, *The Structure of Linear Groups*, Van Nostrand Reinhold Company, New York, 1971.

[10] K. Doerk and T. Hawkes, *Finite Soluble Groups*, Walter de Gruyter, Berlin, 1992.

[11] B. Eick, *The converse of a theorem of W. Gaschutz on Frattini subgroups*, Math Z. **224** (1997), 103 - 111.

[12] D. Gorenstein, *Finite Groups*, Harper and Row Publishers, New York, 1968.

[13] R. Gow, *Some characters of affine subgroups of classical groups*, J. London Math. Soc. **2** (1976), 231 - 238.

[14] L. C. Grove, *Groups and Characters*, John Willey and Sons, Inc., 1997.

[15] M. Hall, Jr., *The Theory of Groups*, The Macmillan Company, New York, 1959.

[16] D. G. Higman, *Remarks on splitting extensions*, Pacific J. Math. **4** (1954), 545 - 555.

[17] D. F. Holt and W. Plesken, *Perfect Groups*, Oxford University Press, New York, 1989.

[18] J. F. Humphreys, *A Course in Group Theory*, Oxford University Press, Oxford, 1996.

[19] B. Huppert, *Eindliche Gruppen I*, Springer-Verlag, Berlin, Heidelberg, 1967.

[20] D. L. Johnson, *Presentations of Groups*, Cambridge University Press, Second Edition, 1997.

[21] Y. K. Leong and T. A. Peng, *On non-abelian groups of order pq*, Bull. Singapore Math. Soc. (1973), 19 - 23.

[22] J. Moori, *Representation Theory*, Lecture Notes, University of Natal, Pietermaritzburg.

[23] J. Moori, *Presentations of group extensions*, Article presented at the 8th Kwazulu Natal Conference, University of Natal, Pietermaritzburg, 1996.

[24] J. Moori, *On the affine subgroups of the symplectic groups*, Article presented at the 9th Kwazulu Natal Conference, University of Durban-Westville , 1997.

[25] J. Moori, *Generalized symmetric groups*, Article presented at the 11th Kwazulu Natal Conference, University of Natal, Durban, 1999.

[26] J. Moori and Z. E. Mpono, *The Fischer-Clifford matrices of the group* $2^6 : SP(6,\ 2)$, Quaestiones Mathematicae, to appear.

[27] Z. E. Mpono, *Fischer Clifford Theory and Character Tables of Group Extensions*, PhD Thesis, University of Natal, Pietermaritzburg, 1998.

[28] H. Onishi, *Commutator extensions of finite groups*, Illinois Math. Journal **4** (1968) 119 - 126.

[29] D. J. S. Robinson, *A Course in Group Theory* , Springer-Verlag, New York, Inc., 1982.

[30] J. S. Rose, *A Course on Group Theory*, Dover Publications, Inc., New York, 1978.

[31] J.J. Rotman, *An Introduction to the Theory of Groups* , 4th Edition, Springer-Verlag, New York, Inc., 1995.

[32] M. Schönert et al., *GAP – Groups, Algorithms, and Programming.* Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, 5th edition, 1995.

[33] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.1*, Aachen, St Andrews, 1999 (`http://www-gap.dcs.st-and.ac.uk/~gap`).

[34] W. R. Scott, *Group Theory*, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1964.

[35] M. Suzuky, *Group Theory I*, Springer-Verlag, New York, 1982.

[36] C. Y. Tang, *Notes on splitting extensions of groups*, Canadian Math. Bull. **11** no. 3, (1968).

[37] N. S. Whitley, *Fischer Matrices and Character Tables of Group Extensions*, MSc Thesis, University of Natal, Pietermaritzburg, 1994.

[38] H. J. Zassenhaus, *The Theory of Groups*, Chelsea Publishing Company, New York, Second Edition, 1958.

Index