Dissertation

On automorphism groups of p-groups

Submitted by

Joshua Maglione

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Summer 2017

Doctoral Committee:

Advisor: James B. Wilson

Alexander Hulpke
Tim Penttila
Kate Ross

Abstract

On automorphism groups of p-groups

We provide the necessary framework to use filters in computational settings, in particular for finitely generated nilpotent groups. The main motivation for this is to construct automorphisms of the group from derivations and Lie automorphisms of an associated Lie algebra. The main application of our work is a parallelizable algorithm to compute $\mathrm{Aut}(G)$, for finite p-groups G of exponent p. This algorithm comes as a consequence of several structure theorems on filters; one, which allows for parallelism, is a theorem about general decompositions of groups (e.g. central decompositions) and their automorphisms.

Acknowledgements

I want to thank the people, both faculty and graduate students, in the mathematics department at Colorado State University for their friendship and for creating a fun academic atmosphere. I am grateful to Daniel Bates, Alexander Hulpke, Eamonn O'Brien, and Tim Penttila for your wisdom, advice, and support. I am also thankful for my committee: for your questions, comments, and ultimately improving the quality of this work.

I am grateful to Peter Brooksbank for his generous support, guidance, and encouragement. My deepest debt of gratitude is owed to my advisor James Wilson for his endless patience, advice, and encouragement. I thank him for always challenging me: for expecting more of me than I thought possible. Not only have James and Peter been outstanding mentors, but they have become close friends for which I am enormously grateful.

Of course this work would not have been possible without the help and support from my friends and family, and I continually thank God for them. I want to specifically thank my parents Linda and Edward Maglione for encouraging me to pursue my PhD and for all of the love and support along the way. Finally and most importantly, I want to thank my gracious wife Erin for her unending love, support, and encouragement. I am especially grateful for her contagious joy and her adventurous spirit.

This research was supported in part by NSF grant DMS 1620454.

Dedication

To my wonderful wife Erin.

Table of Contents

Chapter 1

INTRODUCTION

The study of symmetries arises throughout the sciences to capture structure, compress information, and extrapolate patterns. Highly symmetric objects, such as those coming from systems of equations, are often recorded by small amounts of information making it difficult to recognize the groups of symmetries. For example a high-dimensional grid of numbers, known as a tensor, can be altered by an unknown change of coordinates. The resulting grid seems to give no clear method to retrieve the hidden transformation. Finding that unknown transformation is known as the *tensor equivalence problem*, and through a correspondence of Baer it is also a problem of group isomorphism. The work of Pultr and Herdrlin, c.f. [22], connects graph isomorphism to group isomorphism. A recent breakthrough in graph isomorphism by Babai suggests that improvements to graph isomorphism may have to come from improvements to group isomorphism [1].

The isomorphism problem for groups is closely tied with the automorphism problem which requires an efficient construction of the automorphism group: the group of isomorphisms from the group to itself. There are classes of groups for which we have highly efficient algorithms [2, 3, 8, 19] and even complete classifications [15, 12, 24, 27]. Unfortunately, the complexity of current algorithms for computing automorphism groups from arbitrary groups is not much better than naively testing all functions from one generating set to another. In particular, nilpotent groups are the largest thorn. This is not an insult to current algorithms—they are quite powerful and are the culmination of our best ideas [11, 13, 26]. This is instead a testament to how little we know about the automorphism groups of arbitrary nilpotent groups.

Algorithms to compute automorphism groups of nilpotent groups rely on induction and characteristic subgroups (i.e. subgroups fixed by every automorphism), see [13, 25] for more details. The algorithm constructs characteristic subgroups N_i in a series

$$G = N_1 \geq N_2 \geq \cdots \geq N_c \geq N_{c+1} = 1,$$

such that each N_k/N_{k+1} is a finite vector space. For the base case of the induction, we have the automorphism group of the vector space N_1/N_2: $\mathrm{GL}(d,p)$. The induction step then is to construct the automorphism group of the next layer, say N_1/N_{k+1}, by finding all automorphisms of N_1/N_k that lift to automorphisms of N_1/N_{k+1}. Of course even for modest-sized d and p, $|\,\mathrm{GL}(d,p)| \approx p^{d^2}$ becomes intractable to search through.

One way to combat this issue is to find additional characteristic subgroups, which constrain the number of possible automorphisms and hence decreases the complexity. However, the p-groups of class 2 (i.e. where $[G,G] \leq Z(G)$), the groups notorious for being the hardest class to compute automorphism groups, have few known characteristic subgroups. Indeed, the only classically known characteristic subgroups generally arise as verbal or marginal subgroups. Wilson [32] provides new ways to find and construct characteristic subgroups, and he organizes these subgroups into filters, generalizing Lazard's N-series [18].

Definition 1.0.1. *A* filter *is a function $\phi : M \to 2^G$ from a commutative pre-ordered monoid M into the normal subgroups of G satisfying, for all $s,t \in M$,*

$$[\phi_s, \phi_t] \leq \phi_{s+t} \qquad\qquad s \preceq t \implies \phi_s \geq \phi_t.$$

An important side of filters is their associated M-graded Lie ring $L(\phi)$. Because filters are not limited to the monoid $\mathbb{N}$, this allows filters to be refined, and hence keep the connection to Lie theory. At the inception of filters, few examples were known that were not just standard characteristic series. In [20], we recursively refine filters using the adjoint algebra associated to the graded product on $L(\phi)$. We apply this to the maximal unipotent subgroups of the classical groups over finite fields of odd charactersitic. If the initial length of the exponent-p filter is d, then the fully-refined filters have length $\Theta(d^2)$ In the resulting M-graded Lie algebra, the homogeneous components are at most 2-dimensional—compared to the the initial $\mathbb{N}$-graded Lie algebra with homogeneous components of dimension $O(d)$, see Section 7.1 for an extended example.

The quadratic growth of filters for maximal unipotent subgroups is not restricted just to these groups. In [21], we construct 2,000 sections (i.e. subgroups of quotients) of these unipotent subgroups, and we found that most of these filters grew quadratically as well. With J.B. Wilson, we surveyed 500,000,000 groups of order 2^{10} whose exponent-p series has exactly two nontrivial subgroups, see [4]. For about 40% of the groups surveyed, we were able to construct a characteristic composition series, so the associated Lie algebra has only 1-dimensional homogeneous components. In 97% of the groups surveyed, we were able to come up with at least one characteristic refinement, and in about 80%, the associated Lie algebra had homogeneous components of dimension no larger than 2.

These surveys were only recently possible because of [21], where we provide an efficient algorithm to refine filters whose monoids are totally-ordered. In the majority of examples we encounter, we are finding a wealth of characteristic subgroups due to an analysis of the graded product on $L(\phi)$. New ideas have immerged recently, and building off of work in [8], Brooksbank, O'Brien, and Wilson apply geometric and combinatorial methods to construct more characteristic subgroups and constrain the possible automorphisms. All of these new findings decrease the complexity of the search space in the algorithm of [13], but the other side of the filter, the associated Lie algebra $L(\phi)$, is not being used. We propose a different approach to compute the automorphisms of a p-group, which requires a detailed and technical study of filters.

1.1. Main results

The main goal is to create a new algorithm to construct automorphisms of a finite p-group. Because the monoid of a filter records only the commutation structure in the group, we produce algorithms for groups of exponent p. We will say an algorithm is naively parallel[1] if an increase in processors has a proportional decrease in the running time. We prove the following theorem.

THEOREM A. *If G is a finite p-group of exponent p, then there exists a parallelizable algorithm that returns* $\mathrm{Aut}(G)$ *and is naively parallelizable in the lenth of a filter.*

We accomplish Theorem A by constructing a characteristic filter $\phi : M \to 2^G$. That is, every $H \in \mathrm{im}(\phi)$ is a charactersitic subgroup of G, and these always exist. When we are able to refine the filter, we decrease the runtime both by decreasing the potential automorphisms that arise and by increasing the number of processors.

The algorithm for Theorem A involves computing the graded derivation algebra of $L(\phi)$, the associated Lie algebra of the filter $\phi : M \to 2^G$. From a particular Lie ideal of derivations, we induce bijections of G and either correct them to automorphisms or decide that no such correction exists. In order for a derivation of $L(\phi)$ to induce a bijection of G requires significant work.

The definition for a filter is not restrictive enough, and, for example, it is possible that $\phi : M \to 2^G$ is nontrivial but $L(\phi) = 0$. In fact, this can be done for every filter if we change

[1] Naively parallel is a technical term and not a reflection of the difficulty of the task.

the monoid, and this is one of the first big hurdles to overcome. To construct $L(\phi)$, we define the *boundary filter* $\partial\phi : M \to 2^G$ where $\phi_s = \langle \phi_{s+t} \mid t \neq 0 \rangle$. Thus, we set $L_0(\phi) = 0$ and for $s \neq 0$, $L_s(\phi) = \phi_s/\partial\phi_s$. A subgroup $H \in \operatorname{im}(\phi)$ is *inert* if for all $s \in M$, there exists $t \in M - 0$ such that $H = \phi_s = \phi_{s+t}$. If $H \in \operatorname{im}(\phi)$ is inert, then for all $s \in M$, where $\phi_s = H$, $\partial\phi_s = \phi_s$. In this case, H makes no contribution to the Lie algebra. If every subgroup in $\operatorname{im}(\phi)$ is inert, then $L(\phi) = 0$. Therefore, there is no structure we can abstract from $\operatorname{Der}(L(\phi))$. Although this is an extreme example, it illustrates a problem inert subgroups pose.

The first step, then, to constructing an algorithm for Theorem A requires us to deal with inert subgroups. In the following theorem, we can always refresh filters so that they contain no inert subgroups. If the filter is defined in a compatible way with the monoid, then we can redefine the filter over the given monoid. Otherwise, we refine the filter over $\mathbb{N}^d$.

THEOREM B. *If $\phi : M \to 2^G$ is a filter of a nilpotent group G, then there exists a filter $\widehat{\phi} : M' \to 2^G$ such that $\operatorname{im}(\phi) \subseteq \operatorname{im}\left(\widehat{\phi}\right)$ where $\widehat{\phi}$ has no inert subgroups.*

The construction of such a filter with no inert subgroups is simple to describe, and it employs a two-step process. The first is similar to the process of generating filters, c.f. [32], and the second step is a closure operation to force the order-reversing property of filters. Removing all the inert subgroups of ϕ implies that $L(\phi)$ maps onto $\partial\phi_0$ (Theorem 5.0.5), provided every subgroup of G is finitely generated. Now there are essentially two properties we need to get automorphisms of G from derivations of $L(\phi)$. The first is a bijection between $L(\phi)$ and G. The second is that every basis of $L(\phi)$, respecting the graded direct sum decomposition, induces a generating set G with suitable properties for filters.

A common theme for using groups effectively in computational settings is to have a structured generating set for the group. Some examples include bases and strong generating sets for permutation groups [29, Chapter 4], (special) polycyclic generating sequences for solvable groups [10][30, Chapter 9], and power-commutator presentations for p-groups [17, 23]. These generating sets are all based on a series in the group, so, influenced by these generating sets, we define an appropriate generating set in the context of filters.

To do this, we use the lattice structure of $\mathrm{im}(\phi)$ to get combinatorial properties. However, the set $\mathrm{im}(\phi)$ might not be a lattice, so let $\mathrm{Lat}(\phi)$ denote the intersection and product closure of $\mathrm{im}(\phi)$.

Definition 1.1.1. *A generating set $X \subseteq G$ is* filtered *by ϕ if*

(1) *for all $s \in M$, $\langle \phi_s \cap X \rangle = \phi_s$ and*

(2) $\cap X : \mathrm{Lat}(\phi) \to \mathrm{Lat}(\phi) \cap X$ *is a lattice isomorphism with inverse* $\langle \cdot \rangle : \mathrm{Lat}(\phi) \cap X \to \mathrm{Lat}(\phi)$.

Moreover, X is *faithfully filtered* by ϕ if X is filtered by ϕ and if for each $x \in X$, there exists a unique $s \in M$ such that $x \in \phi_s - \partial\phi_s$. Essentially, there is exactly one homogeneous component $L_s(\phi)$ such that $\overline{x} \in L_s(\phi)$, which is critical to get a bijection between $L(\phi)$ and $\partial\phi_0$.

Theorem C. *If X is faithfully filtered by ϕ, then there exists a bijection between $L(\phi)$ and $\partial\phi_0$ that induces a bijection between the set of bases of $L(\phi)$, respecting the graded direct sum decomposition, and the set of polycyclic generating sequences of $\partial\phi_0$ that are filtered by ϕ.*

To each characteristic filter $\phi : M \to 2^G$ (i.e. every $H \in \mathrm{im}(\phi)$ is characteristic in G), we associate a new filter $\Delta\phi : M \to 2^{\mathrm{Aut}(G)}$ where

$$\Delta\phi_s = \{\alpha \in \mathrm{Aut}(G) \mid \forall t \in M, \forall x \in \phi_t, x^{-1}x^{\alpha} \in \phi_{s+t}\}.$$

This filter is first defined in [31]. When X is faithfully filtered by $\phi : M \to 2^G$ and there exists $U \subset M$ such that $\langle \phi_u \mid u \in U \rangle$ is a decomposition of ϕ_s, then

$$\phi_s / \langle \partial \phi_u \mid u \in U \rangle \cong \bigoplus_{u \in U} L_u(\phi). \tag{1}$$

Because of the direct decomposition in (1), this splitting gets transferred to $\Delta\phi$. The next theorem is an important component of the algorithm in Theorem A as it is one of the key ideas to obtaining a parallelizable algorithm.

Theorem D. *Suppose $\phi : M \to 2^G$ is a characteristic filter and $X \subseteq G$ is faithfully filtered by ϕ. If there exists $U \subset M$ such that for all $s \in U$, $\langle \phi_t \mid t \in U \rangle \neq \langle \phi_t \mid t \in U - s \rangle$, then*

$$\langle \Delta\phi_u \mid u \in U \rangle / \langle \partial \Delta\phi_u \mid u \in U \rangle \cong \bigoplus_{u \in U} L_u(\phi).$$

1.2. Overview

Section 2 details preliminary definitions and theorems needed for the rest of the paper. We discuss topics concerning lattices, polycyclic and nilpotent groups, and filters. We also include examples of fitlers, some of which illustrate justification for future definitions. In Section 3, we give a brief overview of the algorithms for deciding isomorphism of groups. We also discuss the current algorithms for filters and provide some evidence that multilinear algebra techniques and filters find more characteristic subgroups than we previously knew.

In Sections 4 and 5 we define properties necessary for filters to construct an algorithm for Theorem A. This involves defining when a generating set is filtered by $\phi : M \to 2^G$ and studying the structure this condition imposes on the filter. For example, the lattice generated by $\mathrm{im}(\phi)$ must be a distributive lattice if there exists a generating set that is filtered by ϕ. In Section 5, we also tackle the issue of inertia. We give alternate characterizations of inert subgroups that get used throughout the paper, and we provide a process to remove inert subgroups from a given filter. Thus, proving Theorem B.

Even with all the work from Sections 4 and 5, we still cannot construct automorphisms of G from derivations of $L(\phi)$—let alone bijections of G. In Section 6, we define what it means for a generating set to be faithfully filtered by ϕ, and we prove that such a generating set constrains the structure of ϕ. For example, if $x \in X$ and $x \in \phi_s - \partial\phi_s$, then $x \in \phi_t$ implies that $\partial\phi_t \geq \phi_s$. Moreover, the existence of such a generating set, one faithfully filtered by ϕ, implies that $L(\phi)$ and $\partial\phi_0$ are in bijection, provided every subgroup of G is finitely generated, which proves Theorem C.

In Section 7, we work through two extended examples: the upper unitriangular matrix group $UT(5, K)$ and a group from [13]. Finally in Section 8, we prove structure theorems related to the derivation algebra of $L(\phi)$. We provide a polynomial-time algorithm to construct a basis of an important subalgebra used to construct automorphisms of G. At the end, we prove Theorem A by developing a parallelizable algorithm to construct automorphisms of G from the derivation algebra of $L(\phi)$.

The algorithm for Theorem A is based off of a few technical theorems, but the basic idea of the algorithm is simple. Because we assume G has exponent p, all potential homomorphisms α need to satisfy $[g\alpha, h\alpha] = [g, h]\alpha$. Our algorithm is based on Noetherian induction and *corrects* a given bijection α to an automorphism, up to a certain tolerance. We then iterate the algorithm to either produce a homomorphism, and thus an automorphism, or we determine no such automorphism exists.

We end with questions that arose from this work in Section 9.

Chapter 2

PRELIMINARIES

We give a brief overview of definitions and theorems that will be used throughout. First, we state some assumptions used throughout the paper.

2.1. Notation and assumptions

We use notation from [28] for groups. We let 2^X denote the set of subsets of X. Furthermore, $\mathbb{N}$ will denote the set of nonnegative integers.

Throughout, G is a group. For $x, y \in G$, set

$$[x, y] = x^{-1}x^y = x^{-1}y^{-1}xy.$$

For subsets $X, Y \subseteq G$, set $[X, Y] = \langle [x, y] : x \in X, y \in Y \rangle$, and for $X_1, ..., X_n \subseteq G$, set $[X_1] = X_1$ and $[X_1, ..., X_n] = [[X_1, ..., X_{n-1}], X_n]$.

A commutative monoid $\langle M, +, 0\rangle$ is pre-ordered by a pre-order $\preceq$ if $s \preceq t$ and $s' \preceq t'$ imply that $s+s' \preceq t+t'$. Throughout, we will use $+$ for the (commutative) monoid operation, 0 for the additive identity in M, and $\preceq$ for the partial order on M. For $s, t \in M$, we let $s \parallel t$ denote the case when s and t are incomparable under $\preceq$. We assume that 0 is the minimal element of M. That is, for all $s \in M$, $0 \preceq s$. Thus, our monoids are *conical.*

Definition 2.1.1. *A commutative monoid M is* conical *if $s + t = 0$ implies $s = t = 0$, for all $s, t \in M$.*

Lemma 2.1.2. *Suppose M is a commutative, pre-ordered monoid. If 0 is the minimal element of M, then M is conical.*

Proof. Suppose $s + t = 0$. Since $0 \preceq s$, it follows that $t = 0 + t \preceq s + t = 0$. □

2.2. Partially-ordered sets and lattices

We draw notation and definitions from [6].

Definition 2.2.1. *A* partial order $\preceq$ *on a set M is reflexive, anti-symmetric, and transitive.*

Given partially-ordered sets $(S, \leq)$ and $(T, \preceq)$, a map $f : S \to T$ is *isotone* if for all $x, y \in S$,

$$x \leq y \implies f(x) \preceq f(y).$$

Definition 2.2.2. *An* order isomorphism $f : S \to T$ *is a isotone bijection whose inverse is also isotone.*

Lattices play an important role in our study of filters. All of our lattices are sublattices of either the power set of a pre-ordered monoid or the normal subgroups of a group. Both of these lattices are well-studied, so we do not state the general definition for a lattice on an arbitrary partially ordered set. Therefore, $\cap$ and $\cup$ are understood to be either set or subgroup intersection and union (join).

Definition 2.2.3. *A partially ordered set L is a* lattice *if for all $X, Y \in L$ both $X \cap Y \in L$ and $X \cup Y \in L$.*

Definition 2.2.4. *A partially ordered set L is a* complete lattice *if for all $X \subseteq L$ both $\bigcap_{x \in X} x \in L$ and $\bigcup_{x \in X} x \in L$.*

For lattices L and M, $f : L \to M$ is a *lattice homomorphism* if for all $X, Y \in L$

$$f(X \cap Y) = f(X) \cap f(Y) \qquad \text{and} \qquad f(X \cup Y) = f(X) \cup f(Y).$$

Similarly define a *complete lattice homomorphism* over arbitrary intersections and unions. Lattices L and M are *isomorphic* if they are isomorphic as partially-ordered sets.

THEOREM 2.2.5 ([6, Theorem 2.9]). *Lattices L and M are isomorphic if, and only if, there exists a bijection $f : L \to M$ such that for all $X, Y \in L$,*

$$f(X \cup Y) = f(X) \cup f(Y).$$

2.3. Nilpotent groups

For a group G, the *lower central series* of G is defined recursively with $\gamma_1 = G$ and $\gamma_{i+1} = [\gamma_i, G]$. This yields a descending series of normal subgroups

$$G = \gamma_1 \geq \gamma_2 \geq \cdots .$$

DEFINITION 2.3.1. *A group G is* nilpotent *if there exists $c \in \mathbb{N}$ such that $\gamma_{c+1} = 1$.*

If G is nilpotent, the *nilpotency class* of G is the smallest $c \in \mathbb{N}$ such that $\gamma_{c+1} = 1$. Equivalently, G is nilpotent class $\leq c$ if, and only if,

$$\underbrace{[G, \ldots, G]}_{c+1} = 1.$$

Groups of prime power order, *p-groups*, are prototypical examples of finite nilpotent groups.

THEOREM 2.3.2 ([28, Theorem 5.2.4]). *Suppose G is a finite group. Then G is nilpotent if, and only if, G is the direct product of its Sylow subgroups.*

Similar to the lower central series we define a more specialized central series for p-groups G: the *exponent p-central series* of G is defined by $\eta_1 = G$, and $\eta_{i+1} = [\eta_i, G]\eta_i^p$. If G is a p-group, the *p-class* of G is the smallest $c \in \mathbb{N}$ such that $\eta_{c+1} = 1$. For all finite p-groups, the p-class is no smaller than the nilpotency class.

The subgroups that consistent of the lower and exponent-p central series are invariant under automorphisms.

LEMMA 2.3.3. *If $N \leq G$ is invariant under automorphisms and $\varphi : G \to H$ is an isomorphism, then $N\varphi$ is independent of φ.*

PROOF. The coset of isomorphisms from G to H are given by $\mathrm{Aut}(G)\varphi$. If $\alpha \in \mathrm{Aut}(G)$, then $N\alpha = N$. Thus, the image of N under $\alpha\varphi$ is independent of choice of isomorphism. □

DEFINITION 2.3.4. *A subgroup $H \leq G$ is* characteristic *if for all $\alpha \in \mathrm{Aut}(G)$, $H\alpha = H$.*

2.4. Polycyclic groups

We state some definitions and theorems about polycyclic groups from [30, Chapter 9].

DEFINITION 2.4.1. *A G group is* polycyclic *if there exists subgroups*

$$G = G_1 \geq G_2 \geq \cdots G_n \geq G_{n+1} = 1, \tag{2}$$

where each G_i/G_{i+1} is cyclic.

The series in (2) is called a *polycyclic series.* Moreover, there exists $a_i \in G_i$ such that $\langle G_{i+1}a_i \rangle = G_i/G_{i+1}$.

Definition 2.4.2. *The sequence* $\mathcal{A} = (a_1, \ldots, a_n)$ *is a* polycyclic generating sequence (pcgs) *if the following is a polycyclic generating sequence*

$$G = \langle a_1, \ldots, a_n \rangle > \langle a_2, \ldots, a_n \rangle > \cdots > \langle a_n \rangle > 1.$$

Note that the order matters for a pcgs $\mathcal{A}$. We will call a set $\{a_1, \ldots, a_n\}$ a *polycyclic generating set* if, under some relabeling, it is a pcgs. We will not need to construct the composition series from a pcgs, so we will use pcgs to mean a polycyclic generating *set*.

Proposition 2.4.3 ([30, Chapter 9, Proposition 3.9]). *A group is polycyclic if, and only if, it is solvable and all subgroups are finitely generated.*

For each i where G_i/G_{i+1} is finite, let $m_i = [G_i : G_{i+1}]$. Define the set $E_i = \{0, \ldots, m_i - 1\}$, and if G_i/G_{i+1} is infinite, let $E_i = \mathbb{Z}$.

Proposition 2.4.4 ([30, p. 395]). *If* $\mathcal{A} = (a_1, \ldots, a_n)$ *is a pcgs for* G*, then for every* $g \in G$ *there exists unique* $e_i \in E_i$ *such that*

$$g = a_1^{e_1} \cdots a_n^{e_n}.$$

2.5. Filters

A classic approach to analyze p-group structure is to look at a descending central series like the exponent-p central series. For example, the group of 4×4 upper unitriangular matrices over a finite field K has the following series

$$G = \begin{bmatrix} 1 & * & * & * \\ & 1 & * & * \\ & & 1 & * \\ & & & 1 \end{bmatrix} \geq \begin{bmatrix} 1 & 0 & * & * \\ & 1 & 0 & * \\ & & 1 & 0 \\ & & & 1 \end{bmatrix} \geq \begin{bmatrix} 1 & 0 & 0 & * \\ & 1 & 0 & 0 \\ & & 1 & 0 \\ & & & 1 \end{bmatrix} \geq 1.$$

The lower central series satisfies the following relation for all $i, j \in \mathbb{Z}^+$, $[\gamma_i, \gamma_j] \leq \gamma_{i+j}$. Using this fact, we can define a product on the vector space $L = \gamma_1/\gamma_2 \oplus \gamma_2/\gamma_3 \oplus \gamma_3 \cong K^3 \oplus K^2 \oplus K$ given by commutation in the group, which makes L a Lie K-algebra. If we set $L_i = \gamma_i/\gamma_{i+1}$, then $[L_i, L_j] \leq L_{i+j}$. Hence, L is known as a graded Lie algebra.

Definition 2.5.1. *A ring R is* M-graded*, for some monoid M, if $R = \bigoplus_{s \in M} R_s$ and if for all $s, t \in R$, $R_s R_t \subseteq R_{s+t}$. Each R_s are called* homogeneous components *of R.*

Continuing with the above example, we know of another characteristic subgroup between G and G', so we want to update our series

$$G = \begin{bmatrix} 1 & * & * & * \\ & 1 & * & * \\ & & 1 & * \\ & & & 1 \end{bmatrix} \geq \begin{bmatrix} 1 & * & * & * \\ & 1 & 0 & * \\ & & 1 & * \\ & & & 1 \end{bmatrix} \geq \begin{bmatrix} 1 & 0 & * & * \\ & 1 & 0 & * \\ & & 1 & 0 \\ & & & 1 \end{bmatrix} \geq \begin{bmatrix} 1 & 0 & 0 & * \\ & 1 & 0 & 0 \\ & & 1 & 0 \\ & & & 1 \end{bmatrix} \geq 1.$$

Therefore this splits the first homogeneous component of the Lie algebra to $(K \oplus K^2) \oplus K^2 \oplus K$. The product, and hence the grading, is now lost because it is not $\mathbb{Z}^+$-graded. In [32], J.B. Wilson addresses this issue while generalizing Lazard's N-series from [18].

Definition 2.5.2. *A* filter *is a function $\phi : M \to 2^G$ from a commutative, pre-ordered monoid into the normal subgroups of G satisfying*

(1) *$\forall s, t \in M$, $[\phi_s, \phi_t] \leq \phi_{s+t}$, and*

(2) *$\forall s, t \in M$, $s \preceq t$ implies $\phi_t \leq \phi_s$.*

Associated to each filter is a boundary filter.

Definition 2.5.3. *Let $\phi : M \to 2^G$ be a filter. Define the* boundary filter *$\partial\phi : M \to 2^G$ where*

$$\partial\phi_s = \langle \phi_{s+t} : t \in M - 0 \rangle.$$

For each $s \in M - 0$, set $L_s(\phi) = \phi_s/\partial\phi_s$ and $L_0(\phi) = 0$. Define $L(\phi) = \bigoplus_{s \in M} L_s(\phi)$. The following theorem can be found in [32]. However, we include a proof for the sake of completeness.

Theorem 2.5.4 ([32, Theorem 3.1]). *If $\phi : M \to 2^G$ is a filter, then $L(\phi)$ is a $\mathbb{Z}[\phi_0/\partial\phi_0]$-module and an M-graded Lie ring with Lie bracket*

$$[\partial\phi_s x, \partial\phi_t y] = \partial\phi_{s+t}[x, y].$$

Proof. For all $s \in M$, $0 \preceq s$. Therefore, for all $s, t \in M$, $s \preceq s + t$. By the filter property, for all $s, t \in M$, $\phi_s \geq \phi_{s+t}$. Therefore, $\partial\phi_s \leq \phi_s$. Since $[\phi_0, \phi_s] \leq \phi_s$, it follows that each $\phi_s \trianglelefteq \phi_0$. Furthermore, when $s \in M - 0$, $[\phi_s, \phi_s] \leq \phi_{2s} \leq \partial\phi_s \leq \phi_s$, so $L_s = \phi_s/\partial\phi_s$ is abelian and $L(\phi)$ is an abelian group.

We define a product on the homogeneous components. For each $s, t \in M$, let $\circ_{st} : L_s \times L_t \to L_{s+t}$ such that $(\overline{x}, \overline{y}) \mapsto \overline{[x, y]}$. Since ϕ is a filter, if $x \in \phi_s$ and $y \in \phi_t$, $[x, y] \in \phi_{s+t}$. Moreover,

$$[\partial\phi_s, \phi_t] = \left[\prod_{u \in M-0} \phi_{s+u}, \phi_t\right] = \prod_{u \in M-0} [\phi_{s+u}, \phi_t] \leq \prod_{u \in M-0} \phi_{s+t+u} = \partial\phi_{s+t}.$$

Thus, $\circ$ is well-defined.

Let $\overline{x}, \overline{y} \in L_s$ and $\overline{z} \in L_t$. Then we apply commutator identities from [28, Chapter 5.1], and since $[x, z, y] \in \phi_{2s+t} \leq \partial\phi_{s+t}$, it follows that

$$[\overline{x} + \overline{y}, \overline{z}] = [\overline{xy}, \overline{z}] = \overline{[xy, z]} = \overline{[x, z][x, z, y][y, z]} = \overline{[x, z][y, z]} = \overline{[x, z]} + \overline{[y, z]}.$$

By a similar result for $[\overline{x}, \overline{y} + \overline{z}]$, it follows that $\circ_{st}$ is biadditive. Note that if $s = t$, then $\circ_{ss}$ is alternating.

Finally, let $s, t, u \in M$ and $\overline{x} \in L_s$, $\overline{y} \in L_t$, and $\overline{z} \in L_u$. Modulo $\partial\phi_{s+t+u}$,

$$\begin{aligned}[x, y^{-1}, z]^y \equiv [x, y^{-1}, z] = \left[\left([x,y]^{y^{-1}}\right)^{-1}, z\right] \\ \equiv \left[z, [x,y]^{y^{-1}}\right] = [z, [x,y][x,y,y^{-1}]] \equiv [z,[x,y]].\end{aligned}$$

A similar arugment is used to show that $[y, z^{-1}, x]^z \equiv [x, [y, z]]$ and $[z, x^{-1}, y]^x \equiv [y, [z, x]]$. Thus, by the Hall-Witt identity,

$$\begin{aligned}[\overline{x}, \overline{y}, \overline{z}] + [\overline{y}, \overline{z}, \overline{x}] + [\overline{z}, \overline{x}, \overline{y}] &= \overline{[x,y,z][y,z,x][z,x,y]} \\ &= -\overline{[z,[x,y]][x,[y,z]][y,[z,x]]} \\ &= -\overline{[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x} \\ &= 0.\end{aligned}$$

Therefore, extend these products $\circ_{st}$ linearly on $L(\phi)$ to make $L(\phi)$ a Lie ring.

Since $[\partial\phi_0, \phi_s] \leq \partial\phi_s$, it follows that $L_s = \phi_s/\partial\phi_s$ is a right $\mathbb{Z}[\phi_0/\partial\phi_0]$-module, where $\phi_0/\partial\phi_0$ acts via conjugation. □

One of the main uses of filters is to have an algorithmic process for refining known characteristic series. When inserting a new subgroup into a filter, the filter must be updated. This process of updating (or generating) a filter is made precise in [32], but we give necessary details here.

Definition 2.5.5. *A function $\pi : X \to 2^G$ is a* prefilter *if it satisfies the following conditions.*

(1) $0 \in X \subseteq M$ *and* $\langle X \rangle = M$;

(2) *if* $x \in X$ *and* $y \in M$ *with* $y \prec x$, *then* $y \in X$;

(3) *for all* $x \in X$*,* $\pi_x \trianglelefteq G$*;*

(4) *for all* $x, y \in X$*,* $x \preceq y$ *implies* $\pi_x \geq \pi_y$*.*

For $s \in \langle X \rangle$, a *partition* of s with respect to X is a sequence $(s_1, \ldots, s_k)$ where each $s_i \in X$ and $s = \sum_{i=1}^{k} s_i$. Let $\mathcal{P}_X(s)$ denote the set of partitions of $s \in \langle X \rangle$ with respect to X, and if $P = (s_1, \ldots, s_k) \in \mathcal{P}_X(s)$, then set

$$[\pi_P] = [\pi_{s_1}, \ldots, \pi_{s_k}].$$

For a function $\pi : X \to 2^G$, define a new function $\overline{\pi} : \langle X \rangle \to 2^G$ where

$$\overline{\pi}_s = \prod_{P \in \mathcal{P}_X(s)} [\pi_P]. \tag{3}$$

Because each $\pi_x \trianglelefteq G$, the subgroups $[\pi_P]$ are permutable and the order of the product in (3) runs through $\mathcal{P}_X(s)$ does not matter.

Theorem 2.5.6 ([32, Theorem 3.3]). *If* π *is a prefilter, then* $\overline{\pi}$ *is a filter.*

2.6. Examples of filters

The definition of a filter is not very restrictive, and in this section, we give some possibly surprising examples of what constitutes a filter. We also allude to important properties of filters for the coming sections.

Our first example is not too startling. Although $\mathbb{R}_{\geq 0} \cup \{\infty\}$ is usually totally-ordered, we apply a different ordering: one whose chains have length at most 3. However, the group we consider has chains of infinite length, so it is possible that the M and $\mathrm{im}(\phi)$ are not isomorphic as partially ordered sets.

EXAMPLE 2.6.1. Let $M = \mathbb{R}_{\geq 0} \cup \{\infty\}$, where for all $s, t \in M - 0$, $s + t = \infty$. Furthermore, let 0 and ∞ be the minimal and maximal elements, and if $s, t \in \mathbb{R}^+$, then $s \parallel t$. Set

$$G = \left\{ \begin{bmatrix} 1 & a & b \\ & 1 & a \\ & & 1 \end{bmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}.$$

Define a filter $\phi : M \to 2^G$ such that $\phi_0 = G$, $\phi_\infty = G'$, and

$$\phi_s = \left\langle \begin{bmatrix} 1 & s & t \\ & 1 & s \\ & & 1 \end{bmatrix} \;\middle|\; t \in \mathbb{R} \right\rangle.$$

Remarkably, ϕ is injective. In this example, the Hasse diagram yields no useful information. For example, we see that $\phi_1 \geq \phi_2 \geq \phi_4 \geq \phi_8 \geq \cdots$, but this cannot be deduced from the properties of the filter. Furthermore, the associated Lie ring is isomorphic to $\bigoplus_{s \in \mathbb{R}^+} \mathbb{Z}$. $\square$

In the next example, we show that the property

$$(\forall s, t \in M) \qquad\qquad [\phi_s, \phi_t] \leq \phi_{s+t}$$

does not need to be an equality. This is *not* the case for, say, the lower central series as $\gamma_{s+1} := [\gamma_s, \gamma_1]$. Furthermore, it should come as no surprise that a nilpotent group of finite class can have a filter containing a chain of infinite length.

EXAMPLE 2.6.2. We will use the same group G as Example 2.6.1, except over $\mathbb{Z}_p[x]$. Since $\mathbb{Z}_p[x]$ is a $\mathbb{Z}_p$-algebra, let $\mathcal{B} = \{1, x, x^2, \dots\}$ be an ordered basis. Let $M = \mathbb{N}^2$ with the lexicographical ordering, and define a filter $\phi : M \to 2^G$ where $\phi_0 = G$, $\phi_{(1,0)} = \gamma_2$,

$$\phi_{(0,s)} = \left\langle \begin{bmatrix} 1 & u & v \\ & 1 & u \\ & & 1 \end{bmatrix} \;\middle|\; u \in \mathcal{B} - \left\{1, \dots, x^{s-1}\right\},\ v \in \mathbb{Z}_p[x] \right\rangle,$$

$$\phi_{(1,s)} = \left\langle \begin{bmatrix} 1 & 0 & v \\ & 1 & 0 \\ & & 1 \end{bmatrix} \,\middle|\, v \in \mathcal{B} - \left\{1, \dots, x^{s-1}\right\}, \right\rangle,$$

and $\phi_t = 1$ otherwise. The condition $[\phi_s, \phi_t] \leq \phi_{s+t}$ is always satisfied, and provided $\phi_s \neq 1 \neq \phi_t$, it is always a strict containment. Even though G is class 2, the filter ϕ has infinite length and its associated Lie algebra is isomorphic to the abelian Lie algebra $\bigoplus_{s\in\mathbb{N}} \mathbb{F}_p$. □

In Section 2.1, we assert that 0 is the minimal element of M. In the following example, we provide some justification for this assumption. If, for example, that no element is a minimal element, then we cannot properly define an associated Lie ring. We provide a slight twist to Example 2.6.3 in Example 4.1.2.

Example 2.6.3. Suppose $M = \mathbb{N}$, with the partial order $s \preceq t$ if, and only if, $s = t$. In other words, for distinct s, t, $s \parallel t$, and therefore 0 is not the minimal element of M. Let $G = \mathbb{Z}$, and define the filter $\phi : M \to 2^G$ such that

$$\phi_s = \begin{cases} s\mathbb{Z} & \text{if } s \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

Note that ϕ is a filter since G is abelian and all distinct $s, t \in M$ are incomparable. If p is a prime, then $\phi_p \not\geq \partial\phi_p$. If $s \in M$ is not prime, then $\phi_s = 0$, and because there exists a prime larger than s, $\phi_s < \partial\phi_s$. Therefore, the associated Lie ring, $\bigoplus_{s\in M-0} \phi_s/\partial\phi_s$, does not make sense as $\partial\phi_s$ is not necessarily contained in ϕ_s.

We need not limit ourselves to solvable groups. The next example is a filter of an almost quasi-simple group. The nonabelian simple composition factor makes no contribution to the associated Lie ring. These subgroups—subgroups not "seen" by the Lie ring—are studied in detail in Section 5.

Example 2.6.4. Let $G = \mathrm{GL}(2, 7)$ and $M = \mathbb{N}^2$ with the direct product ordering. Define a filter $\phi : M \to 2^G$ where

$$\phi_s = \begin{cases} \mathrm{GL}(2,7) & \text{if } s \in \{0, e_1, e_2\}, \\ \mathrm{SL}(2,7) & \text{otherwise.} \end{cases}$$

Therefore, $L(\phi) = \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

2.7. Graded derivations

Throughout this subsection, $L = \bigoplus_{s \in M} L_s$ is an M-graded Lie ring.

Definition 2.7.1. *A map $\delta \in \mathrm{End}_{\mathbb{Z}}(L)$ is a* derivation *if for all $x, y \in L$,*

$$[x\delta, y] + [x, y\delta] = [x, y]\delta.$$

The Lie ring of derivations is denoted $\mathrm{Der}(L)$*.*

In the context of graded rings, we want derivations to be compatible with the grading. A derivation $\delta \in \mathrm{Der}(L)$ is a *graded derivation* if for all $s \in M$,

$$x \in L_s \implies x\delta \in \bigoplus_{t \in M} L_{s+t}.$$

Because all of our derivations are graded, we refer to graded derivations just as derivations, and $\mathrm{Der}(L)$ denotes the ring of graded derivations.

2.8. Filters on operators

This section summarizes filters on operators associated to $\phi : M \to 2^G$, details of proofs are found in [31]. Let A be a group, and let G be an A-group with an A-invariant filter $\phi : M \to 2^G$, for example $A = \mathrm{Aut}(G)$. For $\alpha \in A$ and $g \in G$, set

$$[g, \alpha] := g^{-1} g^{\alpha}.$$

Let $\Delta\phi : M \to 2^A$ where for all $s \in M$,

$$\Delta\phi_s = \{\alpha \in A : \forall t \in M, [\phi_t, \alpha] \leq \phi_{s+t}\}. \tag{4}$$

Theorem 2.8.1 ([31]). *Assume $\phi : M \to 2^G$ is an A-invariant filter. The function $\Delta\phi : M \to 2^A$ given by the equation (4) is a filter and there is a natural graded Lie ring homomorphism $\mathcal{D} : L(\Delta\phi) \to \mathrm{Der}(L(\phi))$, given by*

$$\partial\Delta\phi_s\alpha \mapsto (\mathcal{D}_\alpha : \partial\phi_t x \mapsto \partial\phi_{s+t}[x, \alpha]).$$

We refer to [31] for the proof of Theorem 2.8.1. However, we will prove the following proposition.

Proposition 2.8.2. *Suppose $\phi : M \to 2^G$ is a filter where every $\circ : L_s(\phi) \times L_t(\phi) \rightarrowtail L_{s+t}(\phi)$ has trivial radicals, and suppose $\alpha \in \Delta\phi_0$. Then $\mathcal{D}_\alpha$ is a derivation if, and only if, $\alpha \in \partial\Delta\phi_0$.*

The proof of Proposition 2.8.2 comes down to the following technical lemma.

Lemma 2.8.3. *If $\alpha \in \Delta\phi_0$, $x \in L_s(\phi)$, and $y \in L_t(\phi)$, then*

$$[[x,\alpha],y]\ [x,[y,\alpha]] \equiv [[x,y],\alpha]\ [[y,\alpha],[x,\alpha]] \mod \partial\phi_{s+t}.$$

Proof. We employ several commutator identities and present a summary of the calculations, see [28, Chapter 5.1]. We let $x^{-\alpha}$ denote $(x^{-1})^{\alpha}$. Modulo $\partial\phi_{s+t}$,

$$\begin{aligned}
[[x,\alpha],y]\ [x,[y,\alpha]] &\equiv x^{-\alpha}xy^{-1}x^{-1}\ \underline{x^{\alpha}}\ \underline{yx^{-1}y^{-\alpha}yxy^{-1}}\ y^{\alpha} \\
&\equiv x^{-\alpha}[x^{-1},y]x^{-1}\ \underline{y^{-\alpha}}\ \underline{yxy^{-1}}\ x^{\alpha}y^{\alpha}\left[[y,\alpha]^{xy^{-1}},x^{\alpha}\right] \\
&\equiv [x^{-1},y][x,y^{-1}][x,y]^{\alpha}\left[y^{-\alpha},x^{y^{-1}}\right]\left[[y,\alpha],(x^{\alpha})^{yx^{-1}}\right] \\
&\equiv [x,y,\alpha]\ \left[[y,\alpha],x^{-1}\right]\left[[y,\alpha],(x^{\alpha})^{yx^{-1}}\right] \\
&\equiv [x,y,\alpha]\ \ [[y,\alpha],[x,\alpha]]\,.
\end{aligned}$$

□

Lemma 2.8.3 shows that if $\alpha \in \Delta\phi_0 - \partial\Delta\phi_0$ and $\mathcal{D}_\alpha$ is a derivation, then for all $x \in L_s(\phi)$ and $y \in L_t(\phi)$, $[[x,\alpha],[y,\alpha]] = 0$. In order words, $\mathcal{D}_\alpha$ maps every $x \in L_s(\phi)$ to the radical of $\circ : L_s(\phi) \times L_t(\phi) \rightarrowtail L_{s+t}(\phi)$. Because radicals of $\circ : L_s(\phi) \times L_t(\phi) \rightarrowtail L_{s+t}(\phi)$ yield characteristic subgroups of ϕ_s, ϕ_t, and ϕ_{s+t}, the filter ϕ can be updated to include these subgroups. Hence, we have proved Proposition 2.8.2.

The next lemma follows from the definition of the map $\mathcal{D}$.

Lemma 2.8.4. *The map $\mathcal{D} : L(\Delta\phi) \to \mathrm{Der}(L(\phi))$ is an injection.*

Proof. For $\alpha, \beta \in L_s(\Delta\phi)$, with $s \neq 0$, suppose $\mathcal{D}_\alpha = \mathcal{D}_\beta$. Thus, for all $x \in L_t(\phi)$,

$$[x,\alpha] \equiv [x,\beta] \mod \partial\phi_{s+t},$$

so $[x,\beta]^{-1}[x,\alpha] \in \partial\phi_{s+t}$. Observe that

$$[x,\beta]^{-1}[x,\alpha] = (x^{-1})^{\beta}x^{\alpha} = [x,\alpha\beta^{-1}]^{\beta} = [x,\alpha\beta^{-1}][[x,\alpha\beta^{-1}],\beta] \in \partial\phi_{s+t}.$$

However, $[[x,\alpha\beta^{-1}],\beta] \in \partial\phi_{2s+t} \leq \partial\phi_{s+t}$, so it follows that $[x,\alpha\beta^{-1}] \in \partial\phi_{s+t}$. Thus, $\alpha\beta^{-1} \in \partial\Delta\phi_s$. Hence, $\alpha \equiv \beta \mod \partial\Delta\phi_s$. □

Chapter 3

SUMMARY OF CURRENT ALGORITHMS

For a finite group G, the basic algorithm to compute $\mathrm{Aut}(G)$ relies on induction. The method we describe here is implemented in the computer algebra systems GAP [14] and Magma [7]. We summarize [11]; for details see [11, 13, 26]. The algorithm starts by computing the solvable radical of the group $R \leq G$, which is the largest solvable normal subgroup of G, and then constructing a series in R whose factors are elementary abelian groups, that is finite vector spaces. Thus we have the following series

$$G \geq R = R_1 \geq R_2 \geq \cdots \geq R_c \geq R_{c+1} = 1.$$

For groups where $G > R > 1$, the strategy is to construct $\mathrm{Aut}(G/R_{i+1})$ from $\mathrm{Aut}(G/R_i)$. The performance is given in [11, Table 1].

There are two extreme cases with this strategy: $R = 1$ and $R = G$. The former has been carefully analyzed by Babai, Codenotti, Grochow, and Qiao [2, 3]. They prove the following theorem

Theorem 3.0.1 ([3, Theorem 1]). *Suppose G and H are groups with trivial solvable radical. Then we can decide if $G \cong H$ in $O(|G|^c)$ group operations.*

The focus of this proposal is the other extreme: $R = G$, in particular when G is a nilpotent group. A group is nilpotent if it is the direct product of its Sylow subgroups. Therefore, computing the automorphism group of a nilpotent group requires the computation of the automorphism groups of all of its Sylow subgroups. Hence, we need to compute automorphism groups of p-groups. The class of p-groups are a notoriously difficult obstacle in the automorphism problem which has its own specialized algorithm: first properly developed in [26] and then refined in [13].

Now we focus on p-groups where $|G| = p^n$. Similar to the generic algorithm described by Cannon and Holt, the nilpotent-quotient algorithm also computes $\mathrm{Aut}(G)$ by induction, a theme we continue with this work. Details on the basic algorithm and its refinements can be found in [13]. The algorithm starts by computing the exponent-p central series of G

$$G = \eta_1 \geq \eta_2 \geq \cdots \geq \eta_c \geq \eta_{c+1} = 1,$$

where $\eta_{i+1} = [\eta_i, G]\eta_i^p$. The factors of this series are elementary abelian p-groups, so for some $d \in \mathbb{Z}$, $\mathrm{Aut}(G/\eta_2) \cong \mathrm{GL}(d, p)$. The algorithm constructs generators for $\mathrm{Aut}(G/\eta_{i+1})$ based on $\mathrm{Aut}(G/\eta_i)$. The difficult part of the algorithm is to compute a stabilizer in $\mathrm{Aut}(G/\eta_i)$ because this group grows rapidly as $n = \log_p |G|$ increases.

Because the general problem is so difficult, the highly successful and efficient algorithms are specialized to specific subclasses of groups, and even these are few in the class of p-groups. For p-groups where $G' \cong \mathbb{Z}_p$ (so G is class 2), we have a complete classification by Blackburn [5]. Related to these groups are the epimorphic images of Heisenberg groups. That is, the group of 3×3 upper triangular matrices over a finite field, where every element has exactly one eigenvalue equal to 1. Lewis and Wilson proved the following.

Theorem 3.0.2 ([19, Theorem 1.3]). *There exists algorithms that determine*

(i) *if a group is a epimorphic image of an odd ordered Heisenberg group, and if so returns it, and*

(ii) *if two groups, that are epimorphic images of an odd ordered Heisenberg group, are isomorphic.*

These algorithms are deterministic polynomial-time in $\log|G|+p$ *and Las Vegas polynomial-time algorithms in* $\log|G|$.

For groups G of class 2 where $G' \cong \mathbb{Z}_p \times \mathbb{Z}_p$, we do not have a classification, but we have an efficient test to determine isomorphism.

THEOREM 3.0.3 ([8, Theorem 1.1]). *There are deterministic, polynomial-time algorithms that, given p-groups* G *and* H,

(1) *decides if* $G' \cong H' \cong \mathbb{Z}_p \times \mathbb{Z}_p$ *and if* $\exp(G) = \exp(H) = p$, *and*

(2) *if so, decides if* $G \cong H$.

It may seem surprising, given the slow pace of isomorphism testing, but this algorithm solves the isomorphism and automorphism problems even into size of 5^{256} in under an hour. All other algorithms require over an hour of CPU time and more than 500 GB of memory for groups of order 5^8.

3.1. An example of a bottleneck

At the beginning of the algorithm from [13], a stabilizer in $\mathrm{GL}(d,p)$ is computed; note that $|\,\mathrm{GL}(d,p)| \approx p^{d^2}$. To demonstrate how easily this becomes intractable, consider the group $G = UT(n,K)$ of $n \times n$ upper unitriangular matrices over the (finite) field K

$$G = \left\{ \begin{bmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \right\}.$$

Suppose $\gamma_3 < N < \gamma_2$, so that N is normal in G. Even for small dimensions and moderately sized fields (e.g. $n = 10$, $|K| = 25$), computing the automorphism group of G/N is not feasible in general.

3.2. Algorithms with filters

To address the bottleneck in Section 3.1, we can attempt to find characteristic subgroups to break apart the large vector space. Therefore, we can use the generation formula for filters in (3) on page 17. It is not computationally feasible to run through all the partitions of $s \in M$, but because characteristic subgroups can greatly reduce the complexity of computing automorphisms, there is desire to develop efficient algorithms to compute filters from prefilters.

In the case where M is finitely generated and totally-ordered, there exists an efficient algorithm to compute the closure of a prefilter and, hence, refine filters. Since M is totally ordered and finitely generated, there exists a congruence $\sim$ of $\mathbb{N}^d$ such that $\mathbb{N}^d/{\sim} \cong M$, where $\mathbb{N}^d$ is lexicographically ordered. To emphasis when we are assuming a total order, we will instead use $\mathbb{N}^d$

Theorem 3.2.1 ([21, Theorem 1]). *Suppose G is a finite group and $\phi : \mathbb{N}^d \to 2^G$ is a filter. There exists a polynomial-time algorithm that, given ϕ and $H \lhd G$ that refines ϕ, returns a refinement of ϕ containing H.*

Theorem 3.2.1 enables efficient refinements of filters over totally-ordered monoids. Therefore, if we find a new characteristic subgroup not contained in the image of $\phi : \mathbb{N}^d \to 2^G$ we can refine it and potentially find more.

In [32], Wilson gave potential locations for new characteristic subgroups. It seems likely that a "generic" p-group G does not have many verbal or marginal subgroups. Examples of this are exponent p, class 2 p-groups (groups where every element has order p and $G' \leq Z(G)$). This is certainly the trend for groups of order 512; while exponent 2 implies the group is abelian, there are still 8,785,772 groups of p-class 2 out of the total 10,494,213 [4].

In cases where we lack characteristic structure, we use the associated Lie ring to find more characteristic structure. Let $\phi : M \to 2^G$ be a filter and $L = L(\phi)$ its associated Lie ring. The graded product of L gives rise to biadditive maps $[,]_{st} : L_s \times L_t \rightarrowtail L_{s+t}$. We construct associated rings for each $[,]_{st}$ and use ring theory to deduce structure in G. For a biadditive map $\circ : U \times V \rightarrowtail W$ of abelian groups, define the adjoint ring, centroid, derivation ring, left scalars, and right scalars as follows

$$\begin{aligned}
\mathrm{Adj}(\circ) &= \{(f,g) \in \mathrm{End}(U) \times \mathrm{End}(V)^{\mathrm{op}} : \forall u \in U, \forall v \in V, uf \circ v = u \circ gv\},\\
\mathrm{Cent}(\circ) &= \{(f,g,h) \in \mathrm{End}(U) \times \mathrm{End}(V) \times \mathrm{End}(W) : \forall u \in U, \forall v \in V, \forall w \in W,\\
&\qquad uf \circ v = u \circ vg = (u \circ v)h\},\\
\mathrm{Der}(\circ) &= \{(f,g,h) \in \mathfrak{gl}(U) \times \mathfrak{gl}(V) \times \mathfrak{gl}(W) : \forall u \in U, \forall v \in V, \forall w \in W,\\
&\qquad uf \circ v + u \circ vg = (u \circ v)h\},\\
\mathcal{L}(\circ) &= \{(f,g) \in \mathrm{End}(U)^{\mathrm{op}} \times \mathrm{End}(W)^{\mathrm{op}} : \forall u \in U, \forall v \in V, fu \circ v = g(u \circ v)\},\\
\mathcal{R}(\circ) &= \{(f,g) \in \mathrm{End}(V) \times \mathrm{End}(W) : \forall u \in U, \forall v \in V, u \circ vf = (u \circ v)g\}.
\end{aligned}$$

The first three rings appear in [32], and the last two appear in [31]. In these rings, we exploit the characteristic structure of the Jacobson radical. Indeed, the Jacobson radical acts on the homogeneous components and yields characteristic subgroups (for $\mathrm{Der}(\circ)$ this is done in the associative enveloping algebra). In a vast majority of the groups we surveyed, we found characteristic structure, previously unknown by classical methods.

In [21], we looked at a random sample of 2,000 quotients of subgroups (i.e. sections) of the Sylow 3-subgroups of classical groups with Lie rank 15. We record how many new subgroups were found, relative to how many we started with. Some groups required as many

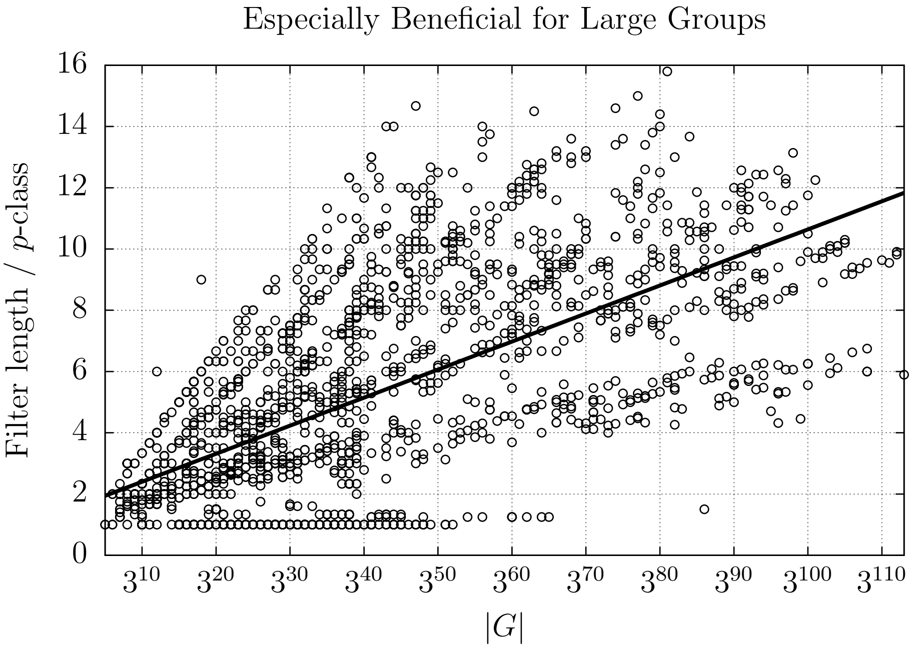


FIGURE 3.1. We sample 2,000 sections of the Sylow 3-subgroups of groups of Lie type. We refine filters until all the algebras in Section 3.2 are semisimple.

as 20 iterations of refinement: an intractable task without an efficient algorithm. All these filter were constructed in under three minutes, and a scatter plot of this data is seen in Figure 3.1.

In [20], we applied this to the maximal unipotent subgroups of the classical groups of Lie rank d and found that the length of the filter went from $\Theta(d)$ to $\Theta(d^2)$ in length.

THEOREM 3.2.2 ([20, Theorem 1.1]). *If U is a maximal unipotent subgroup of a classical Chevalley group of Lie rank d, then there exists a computable characteristic series of U with length $\Theta(d^2)$.*

This is exhibited in Figure 3.2 where the extended class of a group is defined to be the number of nontrivial subgroups in a filter whose rings associated to its bilinear maps are semisimple. Therefore, the extended class of a group might be defined as the length of the fully refined filter using the rings described above.

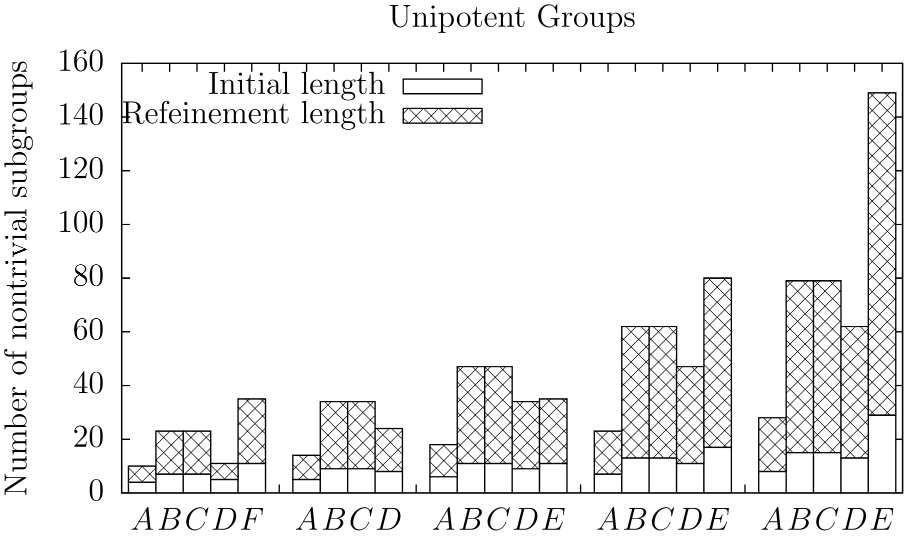


FIGURE 3.2. We refine the lower central series of the maximal unipotent subgroups of the classical and exceptional Chevalley groups. We compare the initial length and the length after refining the filter, using the rings described above. We surveyed groups with Lie rank between 4 and 10.

3.3. Survey of 500,000,000 groups

The perspective of considering tensors led to the discovery of new characteristic subgroups invariant under isomorphisms. To determine how this affects filters, J.B. Wilson and the author constructed 500,000,000 groups of order 1024 where few characteristic subgroups were known a priori. All the groups constructed were 6-generated, exponent 4, and p-class 2. We surveyed groups of order 2^{10} by constructing central extensions of $\mathbb{Z}_2^6$ by $\mathbb{Z}_2^4$.

We found that our methods elucidated previously unknown structure in all but 3% of the cases. In about 40% of the groups surveyed, we were able to construct a *maximal* characteristic series of length 10. It is highly unlikely we constructed the same central extension (as $|\operatorname{Hom}_{\mathbb{Z}_2}(\mathbb{Z}_2^6 \wedge \mathbb{Z}_2^6, \mathbb{Z}_2^4)| = 2^{144}$), but it is certainly possible we constructed *isomorphic* central extensions. Note that there are approximately 50 billion non-isomorphic groups of order 2^{10} of p-class 2 [4]. Although our construction probably favors groups with small automorphism groups, this still demonstrates that filters are finding new characteristic subgroups, hidden to classical methods.

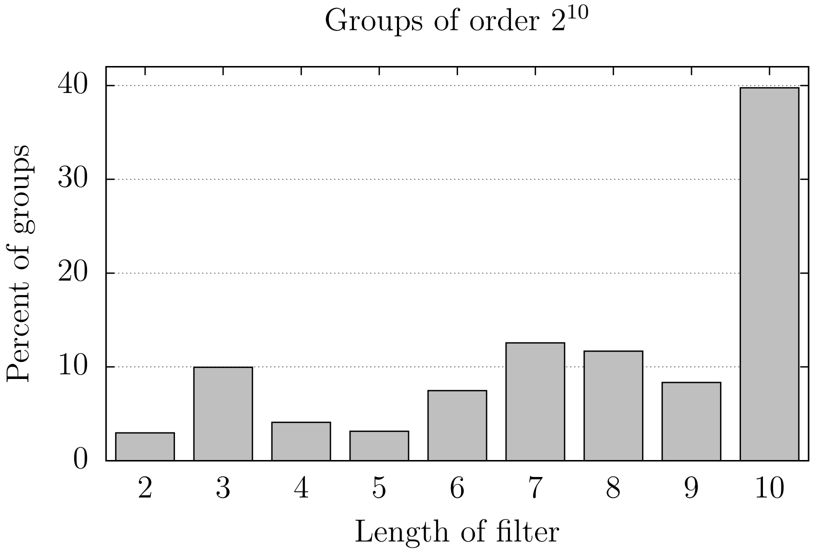


FIGURE 3.3. Together with J.B. Wilson, we surveyed 500,000,000 p-class 2 groups of order 2^{10}. We refined their filters until all the algebras in Section 3.2 were semisimple. In 97% of groups, we were able to find at least one subgroup to refine the filter, and in 40% of groups, we found a characteristic composition series.

Chapter 4

FILTERS AND LATTICES

We begin by stating definitions that enable the use of filters to get automorphisms of groups. In particular, these definitions are satisfied by standard characteristic series like the lower central series. And in the language of [21], full filters over totally-ordered monoids all satisfy the following definitions. Our main motivation is to develop a generating set that interacts nicely with filters, and the inspiration comes from permutation groups, specifically bases and strong generating sets, see [29, Chapter 4]. Unsurprisingly, the lack of a total order and the full generality of allowing for *any* commutative, pre-ordered monoid makes this task a bit challenging.

We begin with a natural condition on generating sets.

Definition 4.0.1. *A generating set $X \subseteq G$ is* weakly-filtered *by $\phi : M \to 2^G$ if for all $s \in M$, $\langle \phi_s \cap X \rangle = \phi_s$.*

The next example shows that if X generates G, it may not be weakly-filtered by $\phi : M \to 2^G$. The solution is then to include more elements until X becomes weakly-filtered.

Example 4.0.2. Consider $G = D_8 = \langle r, s \mid r^4, s^2, [r, s]r^{-2} \rangle$, and let $\gamma : \mathbb{N} \to 2^G$ be the lower central series, with $\gamma_0 = \gamma_1 = G$. The set $X = \{r, s\}$ is not weakly-filtered by γ. Although, $\langle \gamma_0 \cap X \rangle = \langle \gamma_1 \cap X \rangle = \langle r, s \rangle = G$, the problem is that $\langle \gamma_2 \cap X \rangle = \langle \emptyset \rangle = 1 \neq \gamma_2$. This is remedied by including r^2. Thus, $X = \{r, s, r^2\}$ is weakly-filtered by γ. □

The property of a generating set X being weakly-filtered can be rephrased in the context of partially-ordered sets. Suppose $X \subseteq G$ is weakly-filtered. Define functions on partially-ordered sets 2^G and 2^X; namely, $\cap X : 2^G \to 2^X$ where $H \mapsto H \cap X$ and $\langle \cdot \rangle : 2^X \to 2^G$

where $Y \mapsto \langle Y \rangle$. These functions are isotone because $H, K \in 2^G$ with $H \subseteq K$ implies $H \cap X \subseteq K \cap X$, and if $Y, Z \in 2^X$ with $Y \subseteq Z$, then $\langle Y \rangle \leq \langle Z \rangle$.

Lemma 4.0.3. *If $X \subseteq G$ is weakly-filtered by ϕ, then the restriction of $\cap X$ on $\mathrm{im}(\phi)$ is an (order) isomorphism with inverse $\langle \cdot \rangle : \mathrm{im}(\phi) \cap X \to 2^G$.*

Proof. This follows from the definition of weakly-filtered. □

We need a stronger property for our purposes. The set $\mathrm{im}(\phi)$ is, in general, not a lattice, so let $\mathrm{Lat}(\phi)$ denote the complete meet and join closure of $\mathrm{im}(\phi)$. That is, any family of meets and joins are contained in $\mathrm{Lat}(\phi)$, so $\mathrm{Lat}(\phi)$ is a complete lattice and $\mathrm{im}(\phi) \subseteq \mathrm{Lat}(\phi) \subseteq \mathrm{Norm}(G) = \{H \mid H \trianglelefteq G\}$. If every subgroup of G is finitely generated (e.g. G is polycyclic), then we do not need completeness as a family of meets and joins is equivalent to finite meets and joins. Let $\mathrm{Lat}(\phi) \cap X$ denote the image of $\mathrm{Lat}(\phi)$ in 2^X under $\cap X$. Note that since $\mathrm{Lat}(\phi)$ is closed under joins, $\mathrm{im}(\partial\phi) \subseteq \mathrm{Lat}(\phi)$.

The map $\cap X : \mathrm{Lat}(\phi) \to \mathrm{Lat}(\phi) \cap X$ is isotone and, by definition, surjective. However, if $H, K \in \mathrm{Lat}(\phi)$ and $H \cap X \subseteq K \cap X$, then H need not be a subgroup of K, as seen in Example 4.0.5. Therefore, even as partially-ordered sets $\mathrm{Lat}(\phi)$ need not be isomorphic to $\mathrm{Lat}(\phi) \cap X$. The strength of the following definition comes when $\cap X$ and $\langle \cdot \rangle$ are complete *lattice* homomorphisms. This gives us a combinatorial structure on $\mathrm{Lat}(\phi)$ that we exploit later.

Definition 4.0.4. *A generating set $X \subseteq G$ is* filtered *by ϕ if it is weakly-filtered and for all $S \subseteq M$,*

$$\bigcap_{s\in S} \phi_s = \left\langle \bigcap_{s\in S} (\phi_s \cap X) \right\rangle \qquad \text{and} \qquad \left(\prod_{s\in S} \phi_s \right) \cap X = \bigcup_{s\in S} (\phi_s \cap X).$$

If $H \in \mathrm{Lat}(\phi)$ implies that $\langle H \cap X\rangle = H$, then X may not be filtered by ϕ. In this case, it satisfies the first condition on meets, but it may not satisfy the second condition on joins. Therefore, X being filtered by ϕ is stronger than X being "weakly-filtered" by $\mathrm{Lat}(\phi)$. The following example demonstrates the subtles between generating sets X that are weakly-filtered and not filtered by ϕ. It is worth pointing out that the generating set that *is* filtered by ϕ in the next example is a basis for associated Lie ring.

Example 4.0.5. Let $G = \mathbb{Z}_{60}$, and $M = \mathbb{N}^2$ be ordered by the direct product ordering. Define a filter $\phi : M \to 2^G$ where

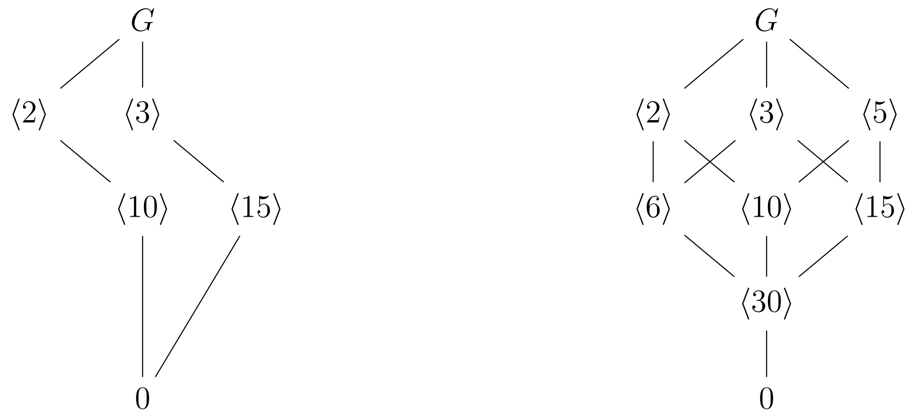
$$\phi_s = \begin{cases} G & \text{if } s = 0, \\ \langle 2\rangle & \text{if } s = e_1, \\ \langle 3\rangle & \text{if } s = e_2, \\ \langle 10\rangle & \text{if } s = 2e_1, \\ \langle 15\rangle & \text{if } s = 2e_2 \\ 0 & \text{otherwise.} \end{cases}$$

Set $X = \{2, 3, 10, 15\}$, and observe that X is weakly-filtered by ϕ. In Figure 4.1, we plot the Hasse diagram of ϕ and the lattice of $\mathrm{Lat}(\phi)$. Set $H = \langle 6\rangle$ and $K = \langle 30\rangle$. Then $H \cap X = \varnothing = K \cap X$, but $\langle 6\rangle = H \not\leq K = \langle 30\rangle$. If, instead, we set $X = \{2, 3, 5, 6, 10, 15, 30\}$, then for all $H \in \mathrm{Lat}(\phi)$, $\langle H \cap X\rangle = H$. However, X is not filtered by ϕ as

$$(\phi_{2e_1}\phi_{2e_2}) \cap X = \langle 5\rangle \cap X = \{5, 10, 15, 30\}$$

$$(\phi_{2e_1} \cap X) \cup (\phi_{2e_2} \cap X) = (\langle 10\rangle \cap X) \cup (\langle 15\rangle \cap X) = \{10, 15, 30\}.$$

If $X = \{6, 10, 15, 30\}$, then X is filtered by ϕ. □



(A) The Hasse diagram of ϕ.

(B) The lattice $\mathrm{Lat}(\phi)$.

FIGURE 4.1. Hasse diagrams related to ϕ from Example 4.0.5.

If X is filtered by ϕ, then $\cap X$ is not just a lattice homomorphism but an isomorphism, and therefore, the lattice $\mathrm{Lat}(\phi)$ inherits properties of the subset lattice $\mathrm{Lat}(\phi) \cap X$. Since subset lattices are distributive, it follows that $\mathrm{Lat}(\phi)$ is a distributive lattice, and this will be an important property used throughout.

PROPOSITION 4.0.6. *The set $X \subseteq G$ is filtered by ϕ if, and only if, $\cap X : \mathrm{Lat}(\phi) \to \mathrm{Lat}(\phi) \cap X$ and $\langle \cdot \rangle : \mathrm{Lat}(\phi) \cap X \to \mathrm{Lat}(\phi)$ are complete lattice isomorphisms. In such a case, $\mathrm{Lat}(\phi)$ is a distributive lattice.*

PROOF. Suppose X is filtered by ϕ and $S \subseteq M$. By the definition of meet and since X is filtered,

$$\left(\bigcap_{s\in S} \phi_s\right) \cap X = \bigcap_{s\in S}(\phi_s \cap X) \quad \text{and} \quad \left(\prod_{s\in S} \phi_s\right) \cap X = \bigcup_{s\in S}(\phi_s \cap X).$$

Hence $\cap X : \mathrm{Lat}(\phi) \to \mathrm{Lat}(\phi) \cap X$ is a lattice homomorphism. Since X is filtered by ϕ it is also weakly-filtered. Therefore,

$$\left\langle \bigcup_{s\in S}(\phi_s \cap X) \right\rangle = \prod_{s\in S}\langle \phi_s \cap X\rangle = \prod_{s\in S} \phi_s \quad \text{and} \quad \left\langle \bigcap_{s\in S}(\phi_s \cap X) \right\rangle = \bigcap_{s\in S} \phi_s.$$

Therefore, $\langle\cdot\rangle : \mathrm{Lat}(\phi) \cap X \to \mathrm{Lat}(\phi)$ is a lattice homomorphism. Both homomorphisms $\cap X$ and $\langle\cdot\rangle$ are isotone. Since X is weakly-filtered, $\langle\cdot\rangle$ is the inverse of $\cap X$, and hence, $\mathrm{Lat}(\phi) \cong \mathrm{Lat}(\phi) \cap X$.

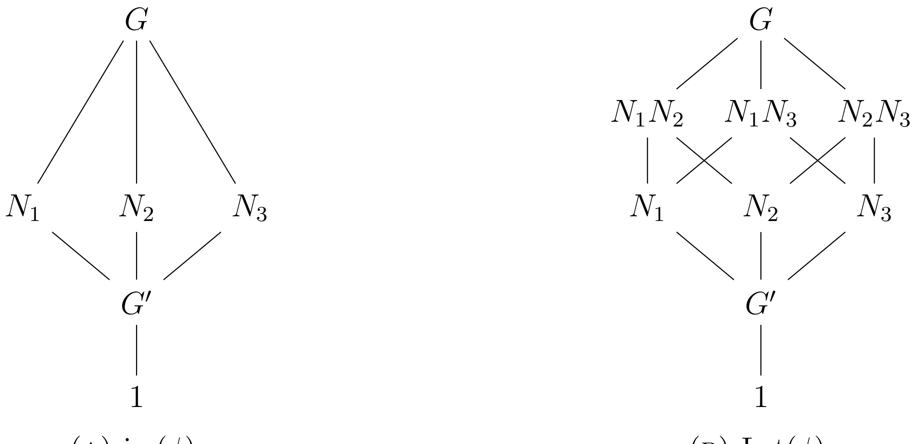
Conversely, suppose $\cap X$ and $\langle\cdot\rangle$ are complete lattice isomorphisms. By construction of $\cap X$ and $\langle\cdot\rangle$, X is weakly-filtered by ϕ. Let $S \subseteq M$, so $\bigcap_{s\in S} \phi_s \in \mathrm{Lat}(\phi)$. Since $\langle\cdot\rangle$ is a complete lattice homomorphism,

$$\left\langle \left(\bigcap_{s\in S} \phi_s \right) \cap X \right\rangle = \left\langle \bigcap_{s\in S} (\phi_s \cap X) \right\rangle = \bigcap_{s\in S} \phi_s.$$

Furthermore, since $\cap X$ is a complete lattice homomorphism,

$$\left(\prod_{s\in S} \phi_s \right) \cap X = \bigcup_{s\in S} (\phi_s \cap X). \qquad \square$$

Now we give an example of a filter where $\mathrm{im}(\phi)$ is not a lattice. In fact, if $\mathrm{Lat}(\phi) = \mathrm{im}(\phi)$, then this would contradict Proposition 4.0.6 as $\mathrm{im}(\phi)$ is not distributive. This follows from the fact that $\mathrm{Lat}(\phi)$ is modular and that the shape of the Hasse diagram of $\mathrm{im}(\phi)$ implies that it is not distributive, c.f. [6, Chapter 5].



(A) $\mathrm{im}(\phi)$.

(B) $\mathrm{Lat}(\phi)$.

FIGURE 4.2. Hasse diagrams related to ϕ.

Example 4.0.7. Let

$$G = \left\{ \left[\begin{array}{c|cc|cc} 1 & b & c & u & v \\ \hline & \multicolumn{2}{c|}{I_2} & a & \\ & & & & a \\ \hline & & & \multicolumn{2}{c}{I_2} \end{array} \right] \,\middle|\, a,b,c,u,v \in \mathbb{F}_p \right\},$$

and let A denote the element with $a = 1$ and $b = c = u = v = 0$. Define B, C, U, and V similarly. Let $N_1 = \langle A, G' \rangle$, $N_2 = \langle B, G' \rangle$, and $N_3 = \langle C, G' \rangle$. Each N_i is normal in G, so define a filter $\phi : \mathbb{N}^3 \to 2^G$ where $\phi_{(0,0,0)} = G$, $\phi_{(1,0,0)} = N_1$, $\phi_{(0,1,0)} = N_2$, $\phi_{(0,0,1)} = N_3$, and

$$\phi_{(i,j,k)} = \begin{cases} G' & \text{if } i + j + k = 2, \\ G' & \text{if } (i,j,k) = (1,1,1), \\ 1 & \text{otherwise.} \end{cases}$$

The Hasse diagrams for the subgroups in $\text{im}(\phi)$ and $\text{Lat}(\phi)$ are in Figure 4.2. If $X = \{A, B, C, U, V\}$, then X is filtered by ϕ. □

Now we look at filtered generating sets with respect to the boundary filters. We eventually prove that if $X \subseteq G$ is filtered by $\phi : M \to 2^G$, then X is filtered by $\partial\phi$. Important steps in this direction are Proposition 4.0.6 and Lemma 4.0.8.

Lemma 4.0.8. *If $X \subseteq G$ is weakly-filtered with respect to $\phi : M \to 2^G$, then*

(1) *for all $s, t \in M$, $\langle (\phi_s \phi_t) \cap X \rangle = \phi_s \phi_t$, and*

(2) *X is weakly-filtered by $\partial\phi$.*

Proof. $\langle (\phi_s \phi_t) \cap X \rangle \geq \langle (\phi_s \cap X) \cup (\phi_t \cap X) \rangle = \phi_s \phi_t$, and (2) follows from (1). □

The proof of the following theorem is technical and depends greatly on the fact that the lattice $\text{Lat}(\phi)$ is distributive, c.f. Proposition 4.0.6. The distributive condition forces the following equality, which may not be true in general,

$$\prod_{u,v\in M-0}(\phi_{s+u}\cap\phi_{t+v})=\partial\phi_s\cap\partial\phi_t, \tag{5}$$

and equation (5) is used throughout the proof of Theorem 4.0.9.

THEOREM 4.0.9. *If X is filtered by $\phi : M\to 2^G$, then X is also filtered by $\partial\phi$.*

PROOF. By Lemma 4.0.8, X is weakly-filtered by $\partial\phi$. We show that $\cap X : \mathrm{Lat}(\partial\phi)\to \mathrm{Lat}(\partial\phi)\cap X$ and $\langle\cdot\rangle : \mathrm{Lat}(\partial\phi)\cap X\to\mathrm{Lat}(\partial\phi)$ are lattice homomorphisms. All products and joins are over $M-0$. By definition

$$(\partial\phi_s\cap X)\cap(\partial\phi_t\cap X)=\left(\left(\prod_u\phi_{s+u}\right)\cap X\right)\cap\left(\left(\prod_v\phi_{t+v}\right)\cap X\right).$$

Since X is filtered, $\cap X$ is a lattice homomorphism and $\mathrm{Lat}(\phi)\cap X$ is distributive by Proposition 4.0.6. Therefore,

$$\begin{aligned}\left(\left(\prod_u\phi_{s+u}\right)\cap X\right)\cap\left(\left(\prod_v\phi_{t+v}\right)\cap X\right)&=\left(\bigcup_u(\phi_{s+u}\cap X)\right)\cap\left(\bigcup_v(\phi_{t+v}\cap X)\right)\\&=\bigcup_{u,v}((\phi_{s+u}\cap\phi_{t+v})\cap X).\end{aligned}$$

Because $\langle\cdot\rangle$ is a lattice homomorphism and since for all $H\in\mathrm{Lat}(\phi)$, $\langle H\cap X\rangle=H$,

$$\langle(\partial\phi_s\cap X)\cap(\partial\phi_t\cap X)\rangle=\prod_{u,v}\langle(\phi_{s+u}\cap\phi_{t+v})\cap X\rangle=\prod_{u,v}(\phi_{s+u}\cap\phi_{t+v}).$$

By Proposition 4.0.6, $\mathrm{Lat}(\phi)$ is a distributive lattice, so

$$\langle(\partial\phi_s\cap X)\cap(\partial\phi_t\cap X)\rangle=\prod_{u,v}(\phi_{s+u}\cap\phi_{t+v})=\partial\phi_s\cap\partial\phi_t.$$

For the second part, by definition $(\partial\phi_s\partial\phi_t) \cap X = \left(\prod_{u,v} \phi_{s+u}\phi_{t+v}\right) \cap X$. Since $\cap X$: $\mathrm{Lat}(\phi) \to \mathrm{Lat} \cap X$ is a lattice homomorphism,

$$\begin{aligned}
\left(\prod_{u,v} \phi_{s+u}\phi_{t+v}\right) \cap X &= \bigcup_{u,v}(\phi_{s+u}\phi_{t+v} \cap X) \\
&= \bigcup_{u}(\phi_{s+u} \cap X) \cup \bigcup_{v}(\phi_{t+v} \cap X) \\
&= \left(\left(\prod_{u} \phi_{s+u}\right) \cap X\right) \cup \left(\left(\prod_{v} \phi_{t+v}\right) \cap X\right) \\
&= (\partial\phi_s \cap X) \cup (\partial\phi_t \cap X). \qquad \square
\end{aligned}$$

4.1. Descending chain condition

Our goal is to construct automorphisms from filters by Noetherian induction from ϕ_0 down to the bottom of the lattice. Since we want our algorithms to terminate, we assume that every chain in $\mathrm{Lat}(\phi)$ has finite length.

Definition 4.1.1. *A filter $\phi : M \to 2^G$ satisfies the* descending chain condition (DCC) *if there does not exist a strictly decreasing infinite chain of subgroups in* $\mathrm{im}(\phi)$.

If a filter $\phi : M \to 2^G$ satisfies DCC, then its lattice $\mathrm{Lat}(\phi)$ may not satisfy DCC as the following example demonstrates.

Example 4.1.2. Let $G = \mathbb{Z}$ and $M = \mathbb{N} \cup \{\infty\}$ where for all $s, t \in M - 0$, $s + t = \infty$. Furthermore, for all assume 0 and ∞ are the minimal and maximal elements and for all $s, t \in \mathbb{Z}^+$, $s \parallel t$. Define a filter $\phi : M \to 2^G$ such that $\phi_0 = G$ and

$$\phi_s = \begin{cases} s\mathbb{Z} & \text{if } s \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

Then $\mathrm{im}(\phi) = \{\mathbb{Z}, 0\} \cup \{p\mathbb{Z} \mid p \text{ a prime }\}$ so all chains have at most three distinct subgroups. However, $\mathrm{Lat}(\phi) = \{n\mathbb{Z} \mid n \in \mathbb{N}\}$, which does not satisfy DCC. □

We prove that if a filter satisfies DCC, then it has a unique minimal subgroup as 0 is the unique minimal element of M.

LEMMA 4.1.3. *Let $\phi : M \to 2^G$ be a filter satisfying DCC. If $H \in \mathrm{im}(\phi)$ is the minimal subgroup of some maximal descending series in $\mathrm{im}(\phi)$, then $H = \bigcap_{s\in M} \phi_s$.*

PROOF. There exists $s \in M$ such that $\phi_s = H$. Let $t \in M$. Since $t \succeq 0$, it follows that $\phi_{s+t} \leq \phi_s \cap \phi_t$. By minimality of H, $\phi_{s+t} = H$; otherwise, H is not the minimal subgroup of a maximal descending chain. Hence, $H \leq \phi_t$, and the statement follows. □

If $H \in \mathrm{im}(\phi)$ is the minimal subgroup and $H \neq 1$, then we will instead consider the filter $\mu : M \to 2^{G/H}$, where $\mu_s = \phi_s/H$. Note that for all $s \in M$, $L_s(\mu) \cong L_s(\phi)$. Therefore, we assume $1 \in \mathrm{im}(\phi)$. This can be achieved superficially as well. If $\phi : M \to 2^G$, with $1 \notin \mathrm{im}(\phi)$, then define a new filter $\widetilde{\phi} : M \cup \{\infty\} \to 2^G$, where

$$\widetilde{\phi}_s = \begin{cases} \phi_s & \text{if } s \in M, \\ 1 & \text{if } s = \infty. \end{cases}$$

The addition in $M \cup \{\infty\}$ is standard: if $s \in M \cup \{\infty\}$, then $s + \infty = \infty$. Of course, if no minimal subgroup $H \in \mathrm{im}(\phi)$ exists, then this implies that there exists an infinite descending chain of subgroups in $\mathrm{im}(\phi)$.

This construction—including 1 in $\mathrm{im}(\phi)$ in this way—illustrates a potential problem with filters and their associated Lie rings. Observe that with the above monoid, $M \cup \{\infty\}$, if $s, t \in M$, then $s + t \in M$. In order for $s + t = \infty$, either $s = \infty$ or $t = \infty$, and if

$H = \bigcap_{s \in M} \phi_s \neq 1$, then H has the property that if $\phi_s = H$, then $\partial\phi_s = H = \phi_s$. Therefore, H makes no contribution to $L(\phi)$, which is the subject of the next section.

Chapter 5

INERT SUBGROUPS OF FILTERS

We start with an example of a property of filters we want to avoid. We show that $L(\phi) = 0$, even though there exists $X \subseteq G$ that is filtered by ϕ.

Example 5.0.1. Let G be the Heisenberg group over a field K, so

$$G = \left\{ \begin{bmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{bmatrix} \;\middle|\; a, b, c \in K \right\}.$$

Let $M = \mathbb{N}^2$ be totally-ordered by the lexicographical ordering, and set $Y = \{s \in M \mid s \preceq (1,0)\}$. Define a constant function $\pi : Y \to 2^G$ where $\mathrm{im}(\pi) = \{G\}$, and set $\phi = \overline{\pi}$. Thus,

$$\phi_s = \begin{cases} G & s \preceq (1,0), \\ Z(G) & (1,0) \prec s \preceq (2,0), \\ 1 & (2,0) \prec s. \end{cases}$$

We claim that ϕ and $\partial\phi$ have generating sets that are filtered, but $L(\partial\phi) = 0$. Observe that $\partial\phi : M \to 2^G$ is defined by

$$\partial\phi_s = \begin{cases} G & s \prec (1,0), \\ Z(G) & (1,0) \preceq s \prec (2,0), \\ 1 & (2,0) \preceq s. \end{cases}$$

Let

$$X = \left\{ \begin{bmatrix} 1 & a & 0 \\ & 1 & 0 \\ & & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ & 1 & b \\ & & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & c \\ & 1 & 0 \\ & & 1 \end{bmatrix} \;\middle|\; a, b, c \in K \right\}.$$

Thus, X is filtered by ϕ and, by Theorem 4.0.9, by $\partial\phi$ as well. However, for all $s \in M$, $\partial\phi_s = \partial^2\phi_s$. Therefore $L(\partial\phi) = 0$. □

Remark 5.0.2. Observe that $\mathbb{N}^2$ with the lex-order is isomorphic, as pre-ordered monoids, to the set of ordinals $\{\alpha \mid \alpha < \omega^2\}$, where $(a, b) \mapsto \omega \cdot a + b$. A problem with Example 5.0.1 is that for every group $H \in \mathrm{im}(\phi)$, the set $\{s \in \mathbb{N}^2 \mid \phi_s = H\}$ has a unique maximum that is also a *limit ordinal* (i.e. an ordinal of the form $\omega \cdot a$ under the isomorphism). Using the filters from Example 5.0.1, this implies the following: if $H \in \mathrm{im}(\partial\phi)$ the set $\{s \in \mathbb{N}^2 \mid \partial\phi_s = H\}$ has no maximal element. For filters over totally-ordered monoids, this is remedied in [21, Section 3.2].

In Example 5.0.1, the filter $\partial\phi : M \to 2^G$ has the property that $L(\partial\phi) = 0$. This is an extreme example, but this illustrates a property we want to avoid: essentially, a subgroup $H \in \mathrm{im}(\phi)$ is *inert* if it makes no contribution in $L(\phi)$. We give a more precise definition below in Definition 5.0.3.

Throughout this section we assume $\phi : M \to 2^G$ satisfies DCC and $1 \in \mathrm{im}(\phi)$. Define an ascending chain of subsets of $\mathrm{im}(\phi)$ as follows. Set $\mathtt{B}_0 = \{1\}$, and for $i \geq 0$, define

$$\mathtt{B}_{i+1} = \{\phi_s \mid \exists B \subseteq \mathtt{B}_i,\ \partial\phi_s = \langle B\rangle\}.$$

Therefore,

$$\{1\} = \mathtt{B}_0 \subseteq \mathtt{B}_1 \subseteq \mathtt{B}_2 \subseteq \cdots .$$

In some sense, the index of the series measures how far away a subgroup is from the trivial subgroup by taking boundaries. With this sequence, we are able to precisely define inert subgroups.

Definition 5.0.3. *A subgroup $H \in \mathrm{im}(\phi)$ is* inert *if for all $n \in \mathbb{N}$, $H \notin \mathtt{B}_n$.*

We now state our main theorems for this section.

Theorem 5.0.4 (Theorem B). *If $\phi : M \to 2^G$ is a filter of a nilpotent group G, then there exists a filter $\widehat{\phi} : \mathbb{N}^d \to 2^G$ such that $\mathrm{im}(\phi) \subseteq \mathrm{im}\left(\widehat{\phi}\right)$ where $\widehat{\phi}$ has no inert subgroups.*

Theorem 5.0.5. *If $\phi : M \to 2^G$ is a filter and every subgroup of G is finitely generated, then there exists a surjection $\pi : L(\phi) \to \partial\phi_0$.*

We characterize when filters have no inert subgroups using Noetherian induction. We find that if $\phi_s \in \mathtt{B}_n$, then there must be a subset $B \subseteq \mathtt{B}_{n-1}$ such that for every $\phi_t \in B$, $\partial\phi_t \neq \phi_t$. However, if this condition were not true, then we can use induction to replace the problem subgroups in B with a more appropriate selection. Therefore, ϕ_s is inert when there is no appropiate choice of replacement. The following proposition determines a method of (possibly transfinite) Noetherian induction on the subgroups in $\mathrm{im}(\phi)$, which will be used constantly throughout.

Proposition 5.0.6. *Suppose $\phi : M \to 2^G$ is a filter satisfying DCC, and set $\mathcal{I} = \{t \in M \mid \partial\phi_t \neq \phi_t\}$. The following are equivalent.*

1. *For all $s \in M$, there exists $I_s \subseteq \mathcal{I}$ such that $\partial\phi_s = \langle \phi_t \mid t \in I_s \rangle$.*
2. *For all $s \in M$, there exists $n \in \mathbb{N}$ such that $\phi_s \in \mathtt{B}_n$. In particular, if G is finite, then there exists $n \in \mathbb{N}$ such that $\mathtt{B}_n = \mathrm{im}(\phi)$.*

Proof. (1) $\Longrightarrow$ (2): By the assumption, for every $s \in M$, there exists $I_s \subseteq \mathcal{I}$ such that $\partial\phi_s = \langle \phi_t \mid t \in I_s \rangle$. If $t_1 \in I_s$, then

$$\phi_s \geq \partial\phi_s \geq \phi_{t_1} > \partial\phi_{t_1}.$$

Continue this indefinitely:

$$\phi_s \geq \partial\phi_s \geq \phi_{t_1} > \partial\phi_{t_1} \geq \phi_{t_2} > \partial\phi_{t_2} \geq \cdots .$$

Therefore, we have the following descending series in G

$$\phi_{t_1} > \phi_{t_2} > \phi_{t_3} > \cdots . \tag{6}$$

Since ϕ satisfies DCC, the series in (6) must stabilize, say, at ϕ_u. By (1), it follows that $\phi_u = 1$. Therefore, (1) implies (2).

(2) $\implies$ (1): Conversely, suppose for all $s \in M$ there exists $n \in \mathbb{N}$ such that $\phi_s \in \mathtt{B}_n$. Suppose there exists minimal $m \in \mathbb{N}$ and $\phi_s \in \mathtt{B}_m$ such that s does not satisfy (1); that is, for all $I \subseteq \mathcal{I}$, $\partial\phi_s \neq \langle \phi_t \mid t \in I\rangle$. Since $\phi_s \in \mathtt{B}_m$, there exists $B \subseteq \mathtt{B}_{m-1}$ such that $\partial\phi_s = \langle H \mid H \in B\rangle$. Therefore, there exists $\phi_u \in B$ such that $u \notin \mathcal{I}$. Let $J = \{t \in M \mid \phi_t = \phi_u\}$, so for all $t \in J$, $\partial\phi_t = \phi_t = \phi_u$. Since $\phi_u \in B \subseteq \mathtt{B}_{m-1}$ and since m is minimal, for each $t \in J$, there exists $I_t \subseteq \mathcal{I}$ such that

$$\phi_u = \phi_t = \partial\phi_t = \langle \phi_v \mid v \in I_t\rangle.$$

Replace u in I with I_t for some $t \in J$, so $I = (I - u) \cup I_t$. Since this holds for all $u \in I$, there exists $I_s \subseteq \mathcal{T}$ such that for each $t \in I_s$, $\phi_t \in \mathtt{B}_{m-1}$ and $\partial\phi_s = \langle \phi_t \mid t \in I_s\rangle$. □

If H is inert and $I = \{s \in M : \phi_s = H\}$, then by Proposition 5.0.6, for all $s \in I$, $\phi_s = \partial\phi_s$. This is only a necessary condition and is not sufficient, c.f. Examples 4.0.5 and 4.0.7: the group $G \in \mathrm{im}(\phi)$ is always equal to its boundary but is not inert. Note that all of the subgroups in the image of the filter $\partial\phi$ in Example 5.0.1 are inert, so $L(\partial\phi) = 0$. The following example will be revisited later, and seems like a more typical example of how inert subgroups can arise.

Example 5.0.7. Fix an odd prime p and let

$$G = \langle a, b, c, x, y \mid [a,b] = x, [a,c] = y, \text{class } 2\rangle,$$

where all missing power-commutator relations are assumed to be trivial. For each $i \in \{0, 1, \ldots, p-1\}$ define $H_i = \langle xy^i \rangle$. Each H_i is normal since it is central.

Define a filter $\phi : \mathbb{N}^{p+1} \to 2^G$ where

$$\phi_s = \begin{cases} \gamma_k & s = ke_1, \\ H_{i-2} & s = ke_i, i \geq 2, \\ 1 & \text{otherwise.} \end{cases}$$

The boundary filter is given by

$$\partial\phi_s = \begin{cases} \gamma_{k+1} & s = ke_1, \\ H_{i-2} & s = ke_i, i \geq 2, \\ 1 & \text{otherwise.} \end{cases}$$

Therefore, $L(\phi) \cong L(\gamma)$ as $\mathbb{Z}_p$-vector spaces. Moreover, they have the same Hilbert series. □

In the next section, we prove that we can always remove the inertia from filters, which enables Noetherian induction, via Proposition 5.0.6, that is used throughout. The chain of B_n enables induction going up, and the boundaries enables induction going down the filter.

5.1. Refreshing filters

In this section we show that for every filter ϕ, there exists a filter $\widehat{\phi}$ with no inert subgroups. To do this, we localize to the indices of a particular inert subgroup and redefine the filter on these indices. We do a two-step process to accomplish this: first, apply the generation formula from Theorem 2.5.6, then a closure operation to force the order-reversing property.

Suppose $\phi : M \to 2^G$ is a filter and $H \in \mathrm{im}(\phi)$ is inert. Throughout this section, we fix the following notation. Let $I = \{s \in M \mid \phi_s = H\}$, and let $J \subset I$ be defined such that

(1) J is finite,

(2) J contains all the minimal elements of I, and

(3) $(M - I) \cup J$ generates M.

Because we assume that M is finitely generated, such a subset J always exists.

Define a set of restricted partitions of M as follows: if $s \in M$, then

$$\mathcal{R}(s) = \{(r_1, \ldots, r_k) \mid k \in \mathbb{N},\ r_1 + \cdots + r_k = s,\ r_i \in (M - I) \cup J\}. \tag{7}$$

For each $s \in M$, define

$$\nu_s = \prod_{\mathbf{r} \in \mathcal{R}(s)} [\phi_{\mathbf{r}}], \tag{8}$$

where $[\phi_{\mathbf{r}}] = [\phi_{r_1}, \ldots, \phi_{r_k}]$. Observe that if $s \in (M - I) \cup J$, then $(s) \in \mathcal{R}(s)$. Since ϕ is a filter, $\nu_s = \phi_s$. Furthermore, if $s \in I$, then $\nu_s \leq \phi_s = H$.

In general, ν_* is not order-reversing, so define a function $\widehat{\phi} : M \to 2^G$ such that

$$\widehat{\phi}_s = \prod_{s \preceq t} \nu_t = \prod_{s \preceq t} \left(\prod_{\mathbf{r} \in \mathcal{R}(s)} [\phi_{\mathbf{r}}] \right). \tag{9}$$

We will prove that $\widehat{\phi}$ is a filter where $\mathrm{im}(\phi) \subseteq \mathrm{im}\left(\widehat{\phi}\right)$ and H is not inert.

It should come as no surprise that the next lemma follows the spirit of Wilson's Lemma 3.4 [32] by applying the Three Subgroups Lemma, seen in [28, **5.1.10**, p. 126]. However, the details are different enough to warrant a separate proof. The following proof considers the different cases that arise from the definition of ν_*.

Lemma 5.1.1. *If $s, t \in M$, then $[\nu_s, \nu_t] \leq \nu_{s+t}$.*

Proof. First, we consider the case when $s, t \in M - I$. If $s + t \notin I$, then the statement follows as ϕ is a filter, so if $s+t \in I$, then $(s, t) \in \mathcal{R}(s+t)$. Therefore, $[\nu_s, \nu_t] = [\phi_s, \phi_t] \leq \nu_{s+t}$.

Suppose now that $s, t \in I$. If $s + t \notin I$, then $[\nu_s, \nu_t] \leq [\phi_s, \phi_t] \leq \phi_{s+t} = \nu_{s+t}$ as ϕ is a filter and $\nu_u \leq \phi_u$ for all $u \in I$. Now consider the case when $s + t \in I$. If $\mathbf{s} \in \mathcal{R}(s)$ and $\mathbf{t} \in \mathcal{R}(t)$, then $(\mathbf{s}, \mathbf{t}) \in \mathcal{R}(s + t)$. From the definition of $\mathcal{R}(s)$, in (7), and since $s \in I$, if $(s) \in \mathcal{R}(s)$, then $s \in J$. Therefore, $\nu_s = \phi_s$ in this case. Furthermore, if $\mathbf{t} \in \mathcal{R}(t)$, then $(s, t_1, \ldots, t_\ell) \in \mathcal{R}(s + t)$, and

$$[\phi_s, [\phi_\mathbf{t}]] = [\phi_\mathbf{t}, \phi_s] \leq \nu_{s+t}.$$

Therefore, in the case where $(s) \in \mathcal{R}(s)$,

$$[\nu_s, \nu_t] = [\nu_t, \phi_s] \leq \nu_{s+t}.$$

Now we proceed by induction on the size of the partition $\mathbf{s} = (s_1, \ldots, s_k) \in \mathcal{R}(s)$. Let $\mathbf{s}' = (s_1, \ldots, s_{k-1})$, and let $A = [\phi_{\mathbf{s}'}]$, $B = \phi_{s_k}$, and $C = [\phi_\mathbf{t}]$. Then

$$[[\phi_\mathbf{s}], [\phi_\mathbf{t}]] = [A, B, C].$$

Since $(\mathbf{s}, \mathbf{t}) \in \mathcal{R}(s + t)$, all permutations of $(\mathbf{s}, \mathbf{t})$ are also contained in $\mathcal{R}(s + t)$. Hence, $(t_1, \ldots, t_\ell, s_k, s_1, \ldots, s_{k-1}) \in \mathcal{R}(s + t)$. If $\mathbf{t}' = (t_1, \ldots, t_\ell, s_k)$, then by induction

$$[B, C, A] = [C, B, A] = [\phi_{\mathbf{t}'}, \phi_{\mathbf{s}'}] \leq \nu_{s+t}.$$

Although $-s_k$ may not be contained M, we let $s - s_k$ denote $s_1 + \cdots + s_{k-1}$. Again, by induction

$$[C, A, B] \leq [\nu_{s-s_k+t}, \phi_{s_k}] \leq \nu_{s+t}.$$

By the Three Subgroups Lemma,

$$[[\phi_{\mathbf{s}}], [\phi_{\mathbf{t}}]] = [A, B, C] \leq [B, C, A][C, A, B] \leq \nu_{s+t}.$$

Therefore, in this case, $[\nu_s, \nu_t] \leq \nu_{s+t}$.

For the final case, suppose $s \in I$ and $t \in M - I$. This is similar to the base case above. If $\mathbf{s} \in \mathcal{R}(s)$, then $(\mathbf{s}, t) \in \mathcal{R}(s + t)$, so

$$[[\phi_{\mathbf{s}}], \phi_t] = [\phi_{\mathbf{s}}, \phi_t] \leq \nu_{s+t}.$$

Since $\nu_t = \phi_t$, it follows that $[\nu_s, \nu_t] \leq \nu_{s+t}$. Therefore, the lemma follows. □

Problems can arise due to the structure of the monoid: particularly, when a subset $S \subseteq M - 0$ forms a group under $+$. An element $s \in M$ is *cancellative* if for all $t, u \in M$, $s + t = s + u$ implies $t = u$. For the next theorem we need a weaker version of cancellative.

Definition 5.1.2. *An element $s \in M$ is* semi-cancellative *if $s + t = s$ implies $t = 0$; otherwise, s is a* sink.

Definition 5.1.3. *A filter is* progressive *if $\phi_s \neq 1$ implies that s is semi-cancellative.*

Observe that if $s \in M$ is cancellative, then s is semi-cancellative, and a filter is progressive if for all sinks $s \in M$, $\phi_s = 1$. Now we are ready to prove that we can refresh inert subgroups and construct filters with more vigor.

Theorem 5.1.4. *Suppose $\phi : M \to 2^G$ is an progressive filter satisfying DCC and that G is nilpotent. If $H \in \operatorname{im}(\phi)$ is a minimal inert subgroup, then there exists a filter satisfying DCC where $\operatorname{im}(\phi) \subseteq \operatorname{im}\left(\widehat{\phi}\right)$ and H is not inert.*

Proof. Let $s, t \in M$. By Lemma 5.1.1,

$$\left[\widehat{\phi}_s, \widehat{\phi}_t\right] = \prod_{s \preceq u} \prod_{t \preceq v} [\nu_u, \nu_v] \leq \prod_{s \preceq u} \prod_{t \preceq v} \nu_{u+v} \leq \widehat{\phi}_{s+t}.$$

If $s \preceq t$, then

$$\widehat{\phi}_s = \prod_{s \preceq u} \nu_u \geq \prod_{s \preceq t \preceq v} \nu_v = \widehat{\phi}_t.$$

Therefore, $\widehat{\phi}$ is a filter. For each $s \in (M - I) \cup J$, $\nu_s = \phi_s$ since ϕ is a filter and $(s) \in \mathcal{R}(s)$. Moreover, $\widehat{\phi}_s = \nu_s = \phi_s$. Therefore, $\operatorname{im}(\phi) \subseteq \operatorname{im}\left(\widehat{\phi}\right)$.

Now we show that H is not inert in $\widehat{\phi}$. Let $s \in J$ be a maximal element. By definition, $\widehat{\phi}_s = H$. Let $t \in M - 0$; we will show that $\widehat{\phi}_{s+t}$ is not inert and therefore, H is not inert. Since all semi-cancellative elements in M evaluate to $1 \in \operatorname{im}(\phi)$, it follows that $s \neq s + t$. If $s + t \notin I$, then $\widehat{\phi}_{s+t} = \phi_{s+t} \neq H$ by definition. Furthermore, $H = \phi_s > \phi_{s+t}$, so by minimality of H, $\widehat{\phi}_{s+t}$ is not inert. Suppose, on the other hand, $s+t \in I$. Because G is nilpotent and H is minimal, $\widehat{\phi}_{s+t}$ is not inert. Therefore, if $\widehat{\phi}_{s+t} = \partial\widehat{\phi}_{s+t}$, then by Proposition 5.0.6, there exists $I_{s+t} \subseteq \mathcal{I} = \left\{u \in M \;\middle|\; \partial\widehat{\phi}_u \neq \widehat{\phi}_u\right\}$ such that $\partial\widehat{\phi}_{s+t} = \left\langle \widehat{\phi}_u \mid u \in I_{s+t}\right\rangle$, and if $\widehat{\phi}_{s+t} \neq \partial\widehat{\phi}_{s+t}$, then $s + t \in \mathcal{I}$. Hence, there exists $I_s \in \mathcal{I}$ such that $\partial\widehat{\phi}_s = \langle \phi_u \mid u \in I_s\rangle$, so H is not inert. □

Corollary 5.1.5. *If $\phi : M \to 2^G$ is a progressive filter satisfying DCC and G is nilpotent, then there exists a filter $\widehat{\phi} : M \to 2^G$ with no inert subgroups such that $\operatorname{im}(\phi) \subseteq \operatorname{im}\left(\widehat{\phi}\right)$.*

5.2. Proof of Theorem B

By Corollary 5.1.5, if the monoid structure is nice enough, then we can fix the immobility of its inert subgroups. On the other hand if ϕ is not progressive, we can still fix the filter but over a different monoid: we move to the free commutative monoid $\mathbb{N}^d$, which eliminates sinks. Care is needed when constructing a partial order that meshes well the partial order on M. We let $\prec$ denote when $s \preceq t$ and $s \neq t$. Now we are in a position to prove Theorem B.

Proof of Theorem 5.0.4. Since M is finitely generated, there exists $d \in \mathbb{Z}$ and a congruence $\sim$ of $\mathbb{N}^d$ such that $\mathbb{N}^d/\sim \; \cong M$. Let $\mu : \mathbb{N}^d \to M$ be the induced surjection. Let $\preceq_+$ be the algebraic partial order on $\mathbb{N}^d$. That is, if $s \preceq_+ t$, then there exists $u \in \mathbb{N}^d$ such that $s + u = t$. Define a ordering $\preceq'$ on $\mathbb{N}^d$ as follows. For $s, t \in \mathbb{N}^d$, $s \preceq' t$ if either $\mu(s) \prec \mu(t)$ or if $\mu(s) = \mu(t)$, then $s \preceq_+ t$. Since μ is a monoid homomorphism, $\preceq$ a partial ordering of M, and $\preceq_+$ a partial order of $\mathbb{N}^d$, it follows that $\preceq'$ is a partial order for $\mathbb{N}^d$.

Define a function $\overrightarrow{\phi} : \mathbb{N}^d \to 2^G$ such that $\overrightarrow{\phi}_s = \phi_{\mu(s)}$. Since μ is a monoid homomorphism respecting the partial orders, it follows that $\overrightarrow{\phi}$ is a filter. Moreover, by construction, $\mathrm{im}(\phi) = \mathrm{im}\left(\overrightarrow{\phi}\right)$. Since every element of $\mathbb{N}^d$ is semi-cancellative, it follows that $\overrightarrow{\phi}$ is progressive. Now apply Corollary 5.1.5 to $\overrightarrow{\phi}$ for the desired result. □

5.3. Finitely generated groups

Throughout, we assume that G is finitely generated, and since we are bringing the associated Lie ring $L(\phi)$ into the picture. Throughout this section we make the following assumptions on filters $\phi : M \to 2^G$

(1) ϕ contains no inert subgroups,

(2) ϕ has DCC, and

(3) $1 \in \mathrm{im}(\phi)$.

Under these assumptions, then, we prove that $L(\phi)$ maps onto $\partial\phi_0$, a basic requirement if we are to construct automorphisms from derivations of $L(\phi)$. These assumptions force the composition factors of $\partial\phi_0$ to be contained in the composition factors of $L(\phi)$. Since $L(\phi)$ is an abelian group and $L_0 = 0$, it follows that $\partial\phi_0$ must be solvable.

Lemma 5.3.1. *If $\phi : M \to 2^G$ is a filter, then $\partial\phi_0$ is solvable.*

Proof. Assume via induction that every $\phi_s \in \mathtt{B}_{n-1}$ is solvable. If $\phi_s \in \mathtt{B}_n$, then by definition there exists $B \subseteq \mathtt{B}_{n-1}$ such that $\partial\phi_s = \langle H \mid H \in B\rangle$. By induction, $\partial\phi_s$ is a product of solvable normal subgroups, $\partial\phi_s$ is solvable. Since ϕ_s is an abelian-by-solvable group, ϕ_s is solvable. Since $\partial\phi_0$ is a product of solvable normal subgroups, the lemma follows. □

We refer to [28, Chapter 4] for definitions associated to abelian groups.

Definition 5.3.2. *A subset $\mathcal{B} \subseteq L$ is a* graded basis *if*

(1) *for all $b \in \mathcal{B}$, there exists $s \in M$ such that $b \in L_s$ and*

(2) *for all $s \in M$, the subset $\mathcal{B} \cap L_s = \{b \in \mathcal{B} \mid b \in L_s\}$ is a basis for L_s.*

Lemma 5.3.3. *Suppose $\phi : M \to 2^G$ is a filter. If $\mathcal{B}$ is a graded basis, then a preimage, X, is weakly-filtered by ϕ.*

Proof. Suppose $\phi_s \in \mathtt{B}_n - \mathtt{B}_{n-1}$. If $\partial\phi_s = \phi_s$, then by induction $\langle \phi_s \cap X\rangle = \phi_s$, so assume $\phi_s \neq \partial\phi_s$. Since $\mathcal{B}$ is a graded basis of $L(\phi)$, there exists a unique subset of $\mathcal{B}$ that is a basis for $L_s(\phi)$, where $s \neq 0$. Let X_s be a preimage of this unique subset generating $L_s(\phi)$. Therefore, $\langle \phi_s \cap X\rangle = \langle X_s \cup (\partial\phi_s \cap X)\rangle$. By induction,

$$\langle \partial\phi_s \cap X\rangle = \langle\langle \phi_u \mid \phi_u \in B\rangle \cap X\rangle \geq \langle \phi_u \cap X \mid \phi_u \in B\rangle = \langle \phi_u \mid u \in B\rangle = \partial\phi_s.$$

Hence, for all $s \in M$, $\langle \phi_s \cap X \rangle = \phi_s$. □

The above two lemmas basically prove that a pre-image of a graded basis, X, contains a polycyclic generating set, provided $\partial\phi_0$ is polycyclic. We will make this precise in the next proposition.

Proposition 5.3.4. *Suppose $\phi : M \to 2^G$ is a filter where every subgroup of $\partial\phi_0$ is finitely generated. If $\mathcal{B}$ is a graded basis, then a preimage X contains a pcgs for $\partial\phi_0$.*

Proof. By Lemma 5.3.1, $\partial\phi_0$ is solvable, and since every subgroup of $\partial\phi_0$ is finitely generated, by Proposition 2.4.3, $\partial\phi_0$ is polycyclic.

By Proposition 5.0.6, for all $s \in M$, there exists $I_s \subseteq \mathcal{I} = \{t \in M \mid \phi_t \neq \partial\phi_t\}$ such that $\partial\phi_s = \langle \phi_t \mid t \in I_s \rangle$. Let $B_s = \langle \partial\phi_t \mid t \in I_s \rangle$. From the filter properties it follows that $\partial\phi_s / B_s$ is abelian. By Lemma 5.3.3, X is weakly-filtered by ϕ, and by Lemma 4.0.8, X is weakly-filtered by $\partial\phi$. Therefore, $\langle \partial\phi_s \cap X \rangle = \partial\phi_s$, and

$$\langle B_s \cap X \rangle \geq \langle \partial\phi_t \cap X \mid t \in I_s \rangle = B_s.$$

Define $X_s = \{x \in X \mid x \in \partial\phi_s - B_s\}$, so $\langle X_s \rangle B_s = \partial\phi_s$. Since every $x \in X$ comes from a graded basis $\mathcal{B}$, there exists a subset of X that is a polycyclic generating sequence of $\partial\phi_s / B_s$. Since $B_s = \langle \partial\phi_t \mid t \in I_s \rangle$, for each $t \in I_s$, there exists $I_t \subseteq \mathcal{I}$ such that $\partial\phi_t = \langle \phi_u \mid u \in I_t \rangle$. Thus, by induction there exists a pcgs in X for B_s and, hence, for $\partial\phi_s$. □

By Proposition 5.3.4, there is little work left to do to prove Theorem 5.0.5. We define a map $\pi : L(\phi) \to \partial\phi_0$, since the image of a basis contains a pcgs of $\partial\phi_0$, the map is surjective.

Proof of Theorem 5.0.5. Let $\mathcal{B}$ be a graded basis of $L(\phi)$. Assign some total order to $\mathcal{B}$ so that $\mathcal{B}$ is an ordered basis for $L(\phi)$. For each $x \in L(\phi)$ and $b \in \mathcal{B}$, there exists unique

k_b such that

$$x = \sum_{b \in \mathcal{B}} k_b b,$$

where the sum runs through $\mathcal{B}$ in order. For each $b \in \mathcal{B}$, let $x_b \in X$ be the corresponding preimage of b. Define a function $\pi : L(\phi) \to G$ such that

$$x = \sum_{b \in \mathcal{B}} k_b b \mapsto \prod_{b \in \mathcal{B}} x_b^{k_b}, \tag{10}$$

where the product runs through $\mathcal{B}$ in ascending order. By Proposition 5.3.4, $\{x_b \mid b \in \mathcal{B}\}$ contains a pcgs of $\partial\phi_0$, so π is surjective. □

Chapter 6

FAITHFUL FILTERS

In this section, we define some properties we want out of filters to extract information about automorphisms of G from derivations and automorphisms of $L(\phi)$. Recall the surjecton $\pi : L(\phi) \to G$ from Theorem 5.0.5, c.f. equation (10). The main issue for $\pi : L(\phi) \to G$ not being injective comes down to the fact that $(\phi_s - \partial\phi_s) \cap (\phi_t - \partial\phi_t)$ might be nonempty. So there exists $x \in L_s(\phi)$ and $y \in L_t(\phi)$ that get mapped to the same image in G. This is problematic in the later sections because we will obtain automorphisms from derivations δ. If there is such a collision, where $g = \pi(x) = \pi(y)$ but $x \neq y$, then constructing an automorphism of G from δ requires a choice of where g gets mapped. We address this issue with the following definitions.

Definition 6.0.1. *A filter $\phi : M \to 2^G$ is* full *if a preimage of a graded basis of $L(\phi)$ is filtered by ϕ.*

Definition 6.0.2. *A generating set $X \subseteq G$ is* faithful *if for each $x \in X$, there exists a unique $s \in M$ such that $x \in \phi_s - \partial\phi_s$. If such a generating set X is also filtered, then X is* faithfully filtered *by ϕ.*

We prove the following theorems in this section.

Theorem 6.0.3. *Assume $\phi : M \to 2^G$ is faithful and has no inert subgroups and DCC. If $X \subseteq G$ is filtered by ϕ, then*

(1) *ϕ is full and*

(2) *every pre-image of every graded basis of $L(\phi)$ is filtered by ϕ.*

Theorem 6.0.4 (Theorem C). *If X is faithfully filtered by ϕ, then there exists a bijection from $L(\phi)$ to $\partial\phi_0$ that induces a bijection between the set of graded bases of $L(\phi)$ and the set of pcgs of $\partial\phi_0$ that are filtered by ϕ.*

The next lemma is fundamental to the proofs of the above theorems and for the next section. In essence, if X is faithfully filtered by ϕ, then the structure of ϕ is constrained. Namely, any element x contained in $\phi_s \cap \phi_t$ must also be contained in $\partial\phi_s \cap \partial\phi_t$. Otherwise, x is contained in, say, $\phi_s \cap \partial\phi_t$, but since ϕ has no inert subgroups, $\partial\phi_t$ is generated by subgroups ϕ_u strictly contained in ϕ_t. Since X is faithfully filtered, x must be contained in each $\partial\phi_u$, and eventually we reach the trivial subgroup as ϕ satisfies DCC.

Lemma 6.0.5. *Suppose $\phi : M \to 2^G$ is a filter, and suppose $X \subseteq G$ is faithfully filtered by ϕ. If $\phi_s \parallel \phi_t$, then $\phi_s \cap \phi_t = \partial\phi_s \cap \partial\phi_t$.*

Proof. Since X is filtered, there exists $x \in (\phi_s \cap \phi_t) \cap X$. Since X is faithful, $x \in \partial\phi_s$ or $x \in \partial\phi_t$. Without loss of generality, suppose $x \in \partial\phi_t$. Suppose, via contradiction, that $x \notin \partial\phi_s$. Since $\mathrm{im}(\phi)$ contains no inert subgroups, by Proposition 5.0.6, for all $u \in M$ there exists $I_u \subseteq \mathcal{I} = \{v \in M \mid \partial\phi_v \neq \phi_v\}$ such that $\partial\phi_u = \langle \phi_v \mid v \in I_u \rangle$. In particular, there exists $I_t \subseteq \mathcal{I}$ such that $\partial\phi_t = \langle \phi_v \mid v \in I_t \rangle$. By Proposition 4.0.6,

$$\partial\phi_t \cap X = \langle \phi_v \mid v \in I_t \rangle \cap X = \bigcup_{v \in I_t} (\phi_v \cap X).$$

Since $x \in \partial\phi_t \cap X$, there exists $u \in I_t$, such that $x \in \phi_u$. Since ϕ_u is not inert, there exists $I_u \subseteq \mathcal{I}$ such that $\partial\phi_u = \langle \phi_v \mid v \in I_u \rangle$ and for all $v \in I_u$, $\phi_u > \phi_v$. Since X is faithful and since $x \in \phi_s - \partial\phi_s$, it follows that $x \in \partial\phi_u$. Otherwise $x \in \phi_s - \partial\phi_s$ and $x \in \phi_u - \partial\phi_u$, which cannot happen. Therefore, by the same reasoning as before, there exists $v \in I_u$ such that $x \in \phi_v$. Continue this ad infinitum.

By Proposition 5.0.6, this stops at $\mathtt{B}_0 = \{1\}$. This implies that $x = 1$, so $x \in \partial\phi_s$, a contradiction. Therefore, if $x \in \phi_s \cap \phi_t$, then $x \in \partial\phi_s \cap \partial\phi_t$. Since X is filtered,

$$\phi_s \cap \phi_t = \langle X \cap (\phi_s \cap \phi_t)\rangle \leq \partial\phi_s \cap \partial\phi_t.$$

Since $\phi_s \geq \partial\phi_s$, the other containment follows. □

From Lemma 6.0.5, we are led to the following definition concerning filters—independent of generating sets.

Definition 6.0.6. *A filter is* faithful *if for all $s, t \in M$, $\phi_s \parallel \phi_t$ implies that $\phi_s \cap \phi_t = \partial\phi_s \cap \partial\phi_t$.*

Note then that if ϕ is a faithful filter and X is filtered by ϕ, then X is faithfully filtered by ϕ. From the above lemma, faithful filters are highly structured filters. We show that faithful implies full, provided there exists X that is filtered by ϕ. The basic argument is that the image of X in $L(\phi)$ will contain a graded basis $\mathcal{B}$ of $L(\phi)$, and because X is filtered, a pre-image of $\mathcal{B}$ will be filtered as well.

Lemma 6.0.7. *Suppose $\phi : M \to 2^G$ is a faithful filter with no inert subgroups and satisfies DCC. If $X \subseteq G$ is filtered by ϕ, then ϕ is full.*

Proof. We show that X induces a graded basis of $L(\phi)$. Since X is faithful, there exists a function $\omega : X \to M$ such that if $x \in X$, then $x \in \phi_{\omega(x)} - \partial\phi_{\omega(x)}$. Let $\mathcal{C} = \{\partial\phi_{\omega(x)}x \mid x \in X\}$.

Since X is filtered by ϕ, X is filtered by $\partial\phi$ by Theorem 4.0.9. Therefore there exists $X_s \subseteq X$ such that

$$\langle \phi_s \cap X\rangle = \langle X_s \cup (\partial\phi_s \cap X)\rangle = \phi_s.$$

Furthermore, the image of X_s in $L(\phi)$ spans $L_s(\phi)$. Since X is faithful, this holds for all $s \in M - 0$. Therefore, $\mathcal{C}$ spans $L(\phi)$.

Let $\mathcal{B} \subseteq \mathcal{C}$ be a basis for $L(\phi)$, and let $Y \subseteq X$ correspond to $\mathcal{B}$. Since Y is a preimage of a basis $\mathcal{B}$, by Lemma 5.3.3, Y is weakly-filtered by ϕ.

By definition, $(\phi_s \phi_t) \cap Y \supseteq (\phi_s \cap Y) \cup (\phi_t \cap Y)$. Suppose $y \in (\phi_s \phi_t) \cap Y$. Then $y \in (\phi_s \phi_t) \cap X = (\phi_s \cap X) \cup (\phi_t \cap X)$, so y is contained in either ϕ_s or ϕ_t. Therefore, $y \in (\phi_s \cap Y) \cup (\phi_t \cap Y)$, so for all $s, t \in M$,

$$(\phi_s \phi_t) \cap Y = (\phi_s \cap Y) \cup (\phi_t \cap Y). \tag{11}$$

For the other equality, note that if $\phi_s \leq \phi_t$, then $\phi_s \cap \phi_t = \langle (\phi_s \cap \phi_t) \cap Y \rangle$. Therefore, we assume $\phi_s \parallel \phi_t$. By Lemma 6.0.5, $\phi_s \cap \phi_t = \partial \phi_s \cap \partial \phi_t$. Since $\mathtt{B}_0 = \{1\}$, assume that for all $\phi_s, \phi_t \in \mathtt{B}_n$,

$$\phi_s \cap \phi_t = \langle (\phi_s \cap \phi_t) \cap Y \rangle.$$

Let $\phi_s, \phi_t \in \mathtt{B}_{n+1}$, so there exists $S, T \subseteq \mathtt{B}_n$ such that $\partial \phi_s = \langle H \mid H \in S \rangle$ and $\partial \phi_t = \langle H \mid H \in T \rangle$. Since ϕ is filtered, the lattice $\mathrm{Lat}(\phi)$ is distributive by Proposition 4.0.6. By equation (11) and induction,

$$\begin{aligned}
\langle (\phi_s \cap \phi_t) \cap Y \rangle &= \langle \partial \phi_s \cap \partial \phi_t \cap Y \rangle \\
&= \big\langle (\langle H \mid H \in S \rangle \cap \langle K \mid K \in T \rangle) \cap Y \big\rangle \\
&= \big\langle \langle H \cap K \mid H \in S, K \in T \rangle \cap Y \big\rangle \\
&= \langle (H \cap K) \cap Y \mid H \in S, K \in T \rangle \\
&= \langle H \cap K \mid H \in S, K \in T \rangle
\end{aligned}$$

$$= \langle H \mid H \in S\rangle \cap \langle K \mid K \in T\rangle$$

$$= \partial\phi_s \cap \partial\phi_t$$

$$= \phi_s \cap \phi_t.$$

Therefore, Y is filtered by ϕ. □

6.1. Proof of Theorem 6.0.3

Now we are ready to prove that if X is faithfully filtered by $\phi : M \to 2^G$, then every graded basis of $L(\phi)$ induces a faithfully filtered generating set of G. This can be turned into an algorithm to decide if there exists a generating set X that is filtered by the faithful filter ϕ.

The following proof uses Noetherian induction, going up the sequence

$$\{1\} = \mathtt{B}_0 \subseteq \mathtt{B}_1 \subseteq \cdots .$$

This sequence is defined in Section 5. The basic idea is to assume that a pre-image Y of an arbitrary graded basis of $L(\phi)$ is filtered by ϕ up to some $\mathtt{B}_n$. This is certainly true for $\mathtt{B}_0$. Then for every group $\phi_s \in \mathtt{B}_{n+1}$, $\partial\phi_s \in \mathtt{B}_n$. Thus, $\partial\phi_s$ is handled by induction, and all that is left are quotients $\phi_s/\partial\phi_s = L_s(\phi)$.

Proof. For (1), apply Lemma 6.0.7. For (2), let $\mathcal{B}$ be the graded basis whose pre-image is filtered by ϕ (using condition (1)), and suppose $\mathcal{B}'$ is some other graded basis of $L(\phi)$. By Lemma 5.3.3, a pre-image, Y of $\mathcal{B}'$ is weakly-filtered by ϕ. Suppose that for all $B \subseteq \mathtt{B}_n$,

$$\bigcap_{H\in B} H = \left\langle \bigcap_{H\in B} (H \cap X) \right\rangle \qquad \text{and} \qquad \left(\prod_{H\in B} H\right) \cap X = \bigcup_{H\in B} (H \cap X).$$

Let $B \subseteq \mathtt{B}_{n+1}$, and set $\partial B = \{\partial\phi_u \mid \phi_u \in B\} \subseteq \mathtt{B}_n$.

Then

$$\left(\prod_{H\in B} H\right) \cap Y = \left(\prod_{H\in B} H - \prod_{K\in\partial B} K\right) \cap Y \cup \left(\prod_{K\in\partial B} K\right) \cap Y.$$

By induction, we only need to show that

$$\left(\prod_{H\in B} H - \prod_{K\in\partial B} K\right) \cap Y \subseteq \prod_{H\in B} (H \cap Y).$$

Suppose there exists $y \in HK \cap Y$ for some $H, K \in B$. Since $\mathcal{B}'$ is a graded basis, there exists a unique $s \in M$ such that $\overline{y} \in L_s(\phi)$. Therefore, $y \in \phi_s - \partial\phi_s$. By Lemma 6.0.5, either $y \in H$, $y \in K$, or $y \in \prod_{K\in\partial B} K$. Thus,

$$\left(\prod_{H\in B} H\right) \cap Y = \bigcup_{H\in B} (H \cap Y).$$

Finally, there exists a subset $C \subseteq B$ such that for all $H, K \in C$, $H \parallel K$ and

$$\bigcap_{H\in B} H = \bigcap_{H\in C} H.$$

By Lemma 6.0.5, if $\partial C = \{\partial\phi_u \mid \phi_u \in C\}$, then by induction

$$\bigcap_{H\in B} H = \bigcap_{H\in C} H = \bigcap_{H\in\partial C} H = \left\langle \bigcap_{H\in\partial C} H \cap Y \right\rangle = \left\langle \bigcap_{H\in B} H \cap Y \right\rangle.$$

Therefore, the theorem follows. □

The following example illustrates one instance where a filter cannot have an associated X that is faithful. In Section 7.1, we show that this issue can naturally arise and one way to address it. However, it is not known if a method exists in general, see Question 3 in Section 9.

Example 6.1.1. Let G be the Heisenberg group over the finite field $\mathbb{F}_p$. Let $\gamma : \mathbb{N} \to 2^G$ be the lower central series, so

$$G = \gamma_0 = \gamma_1 = \left\{ \begin{bmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{bmatrix} \right\}, \qquad \gamma_2 = Z(G) = \left\{ \begin{bmatrix} 1 & 0 & * \\ & 1 & 0 \\ & & 1 \end{bmatrix} \right\},$$

and $\gamma_i = 1$ for $i \geq 3$. If

$$X = \left\{ \begin{bmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ & 1 & 0 \\ & & 1 \end{bmatrix} \right\},$$

then X is faithfully filtered by γ. Moreover, γ is fully faithful.

Let $Y = \{0, (1,0), (0,1)\} \subset \mathbb{N}^2$, and define $\pi : Y \to 2^G$ to be the constant function where $\mathrm{im}(\pi) = \{G\}$. Then the closure, $\phi = \overline{\pi} : \mathbb{N}^2 \to 2^G$, is realized as

$$\phi_{(i,j)} = \gamma_{i+j}.$$

Since $\mathrm{im}(\phi) = \mathrm{im}(\gamma)$ and since X is filtered by γ, X is also filtered by ϕ. However, X is not faithful:

$$G = \phi_{(1,0)} = \phi_{(0,1)},$$

$$Z(G) = \phi_{(2,0)} = \phi_{(1,1)} = \phi_{(0,2)},$$

$$1 = \phi_{(3,0)} = \phi_{(2,1)} = \phi_{(1,2)} = \phi_{(0,3)} = \dots.$$

Since G is finite, $|L(\phi)| = |G/\gamma_2|^2|\gamma_2|^3$. This example applies in more generality to nilpotent groups of class c. □

If ϕ is faithful, $\partial\phi$ may not be faithful because there need not exist a faithful generating set X for $\partial\phi$ as illustrated in Example 5.0.1, where the boundary filter contains *only* inert subgroups. Essentially, we cannot guarantee that $\partial\phi$ has no inert subgroups regardless of the inertia of ϕ.

6.2. Proof of Theorem C

To prove Theorem C, we apply Theorem 5.0.5 since we assume ϕ has no inert subgroups. Furthermore, we use the fact that elements of a polycyclic group have a *unique* normal word with respect to a pcgs. This gives us injectivity.

Proof of Theorem 6.0.4. Let $\mathcal{B}$ be a graded basis for $L(\phi)$. By Theorem 6.0.3, if X is a pre-image of $\mathcal{B}$, then X is filtered by ϕ. From the proof of Theorem 5.0.5, the map the $\pi : L(\phi) \to \partial\phi_0$ given by

$$x = \sum_{b\in\mathcal{B}} k_b b \mapsto \prod_{b\in\mathcal{B}} x_b^{k_b}$$

is a surjection.

If X is a pcgs for $\partial\phi_0$, then π is injective. Indeed, if

$$\prod_{b\in\mathcal{B}} x_b^{k_b} = \pi\left(\sum_{b\in\mathcal{B}} k_b b\right) = \pi\left(\sum_{b\in\mathcal{B}} \ell_b b\right) = \prod_{b\in\mathcal{B}} x_b^{\ell_b},$$

then, since X is a pcgs of $\partial\phi_0$, for all $b \in \mathcal{B}$, $k_b = \ell_b$. Therefore, we prove that X is a pcgs of $\partial\phi_0$.

By Proposition 5.3.4, X contains a pcgs of $\partial\phi_0$. Suppose for some $x \in X$, the set $X - x$ still contains a pcgs for $\partial\phi_0$, say $\{x_1, \ldots, x_n\} \subseteq X - x$ is a pcgs. Then there exists some unique normal word for x:

$$x = x_1^{e_1} \cdots x_n^{e_n},$$

for integers e_i. This implies that there exists $S \subseteq M$ such that

$$x = x_1^{e_1} \cdots x_n^{e_n} \in \prod_{t \in S} \phi_t.$$

Since every subgroup of G is finitely generated, we can take S to be finite. Because $x \in \phi_s - \partial\phi_s$ and $x \in \prod_{t\in S} \phi_t$, we apply Lemma 6.0.5 to obtain a contradiction. Therefore, $X - x$ cannot contain a pcgs of $\partial\phi_0$. Hence, X is a pcgs for $\partial\phi_0$ and π is a bijection. □

The crux of Theorem C is not the bijection between $\partial\phi_0$ and $L(\phi)$, though that is necessary for our purposes. The main point is actually the induced bijection between graded bases of $L(\phi)$ and pcgs of $\partial\phi_0$ filtered by ϕ. This allows us to get a well-defined bijection on $\partial\phi_0$ from a linear transformation on $L(\phi)$ as graded bases $L(\phi)$ induce pcgs of G. Furthermore, derivations of $L(\phi)$ are determined by how they transform a (graded) basis, and from this, we can construct a function of G. A bijection between $L(\phi)$ and $\partial\phi_0$ can be accomplished without the assumptions of Theorem 6.0.4 as the next example shows.

Example 6.2.1. Let V be a $\mathbb{Z}_p$-vector space of dimension d and $\circ : V \times V \rightarrowtail V$ an alternating bilinear map. Set

$$G = \left\{ \begin{bmatrix} 1 & u & w \\ & 1 & v \\ & & 1 \end{bmatrix} \middle| \; u, v, w \in V \right\},$$

using $\circ$ to define the multiplication in G. Define normal subgroups

$$N_1 = \left\{ \begin{bmatrix} 1 & u & w \\ & 1 & 0 \\ & & 1 \end{bmatrix} \middle| \; u, w \in V \right\}, N_2 = \left\{ \begin{bmatrix} 1 & u & w \\ & 1 & u \\ & & 1 \end{bmatrix} \middle| \; u, w \in V \right\},$$

$$N_3 = \left\{ \begin{bmatrix} 1 & 0 & w \\ & 1 & v \\ & & 1 \end{bmatrix} \middle| \; v, w \in V \right\}.$$

Using the direct product ordering on $\mathbb{N}^3$, let $\phi : \mathbb{N}^3 \to 2^G$ such that $\phi_0 = G$ and

$$\phi_s = \begin{cases} N_i & \text{if } s = e_i, \\ Z(G) & \text{otherwise.} \end{cases}$$

Hence, $L(\phi) \cong V \oplus V \oplus V$, so there exists a bijection between G and $L(\phi)$. However, every pre-image of a basis for $L(\phi)$ is not filtered by ϕ. □

The filter in Example 6.2.2 is an example of a faithful filter with the properties we seek. There exists X that is filtered by ϕ. Therefore, ϕ is full and $|L(\phi)| = |\partial\phi_0|$. In Example 6.2.3, we show that with more subgroups in the filter we lose some of these properties. This also illustrates some of the algorithmic challenges of producing an X that is faithfully filtered.

Example 6.2.2. Let G be an extraspecial group of order p^{2n+1}. Therefore, $G/\Phi(G)$ is a $\mathbb{Z}_p$-vector space of dimension $2n$ and $Z(G) = G' = \Phi(G)$ is a $\mathbb{Z}_p$-vector space of dimension 1. Choose some basis $\{b_1, \dots, b_{2n}\}$ for $G/\Phi(G)$, and for each b_i, let $H_i/\Phi(G) = \langle b_i \rangle$. Therefore, each H_i is normal in G.

Let $M = \mathbb{N}^{2n}$ with the direct product ordering, and define $\phi : M \to 2^G$ such that $\phi_0 = G$ and for all $s \neq 0$,

$$\phi_s = \begin{cases} H_i & \text{if } s = e_i, \\ G' & \text{if } (\forall i)(s \neq e_i) \text{ and } s \preceq e_1 + \cdots + e_{2n}, \\ 1 & \text{otherwise.} \end{cases}$$

This filter has a generating set $X \subseteq G$ that is faithfully filtered by ϕ: let $X = \{x_1, \dots, x_{2n}, z\}$, where x_i is a pre-image of b_i and z a nontrivial element of $Z(G)$. Observe that $\dim_{\mathbb{Z}_p}(L(\phi)) = 2n + 1$. Therefore, there exists a bijection between G and $L(\phi)$, and furthermore all graded bases of $L(\phi)$ induce a pcgs that is filtered by ϕ. □

We contrast Example 6.2.2 with Example 6.2.3. We construct a faithful filter that is not full. Moreover, there is no $X \subseteq G$ that is filtered by ϕ. There are, however, no inert subgroups, so $|L(\phi)| \geq |\partial\phi_0|$.

Example 6.2.3. Let G be the same group from Example 6.2.2. There are $d = \binom{2n}{1}_p$ distinct 1-dimensional subspaces of $G/\Phi(G)$. Let $\{c_1, \dots, c_d\}$ be a collection of vectors whose 1-dimensional subspaces are pairwise disjoint. Set $H_i/\Phi(G) = \langle c_i \rangle$.

Let $M = \mathbb{N}^d$ with the direct product ordering. We will define a similar filter to Example 6.2.2: define $\phi : M \to 2^G$ such that $\phi_0 = G$ and for all $s \neq 0$, set

$$\phi_s = \begin{cases} H_i & \text{if } s = e_i, \\ G' & \text{if } (\forall i)(s \neq e_i) \text{ and } s \preceq e_1 + \cdots + e_d, \\ 1 & \text{otherwise.} \end{cases}$$

The filter ϕ is faithful, but it is not full. To see this, let $X = \{c_1, \dots, c_d, z\}$, where z is a nontrivial element of $Z(G)$. Although X is weakly-filtered, it is not filtered as a plane has more than two lines:

$$(\phi_{e_1}\phi_{e_2}) \cap X \neq (\phi_{e_1} \cap X) \cup (\phi_{e_2} \cap X).$$

Here, $L(\phi) \cong \mathbb{Z}_p^{d+1}$, which is drastically larger than G. □

6.3. Decompositions within filters

Given the structure theorems from the previous subsection, we see how these influence the filter on the operators on G, namely $\Delta\phi : M \to 2^A$. Recall, if $\phi : M \to 2^G$ is an A-invariant filter and A is a group, then we define a new filter on A, where

$$\Delta\phi_s = \{\alpha \in A \mid (\forall t)(\forall x)(x \in \phi_t \implies [x, \alpha] \in \phi_{s+t})\}.$$

Throughout we assume that G is an A-group, where A is also a group. Let $\phi : M \to 2^G$ be a filter with no inert subgroups and DCC. Furthermore, $X \subseteq G$ is faithfully filtered by ϕ.

Definition 6.3.1. *For a fixed $s \in M$, a set $U_s \subset M$* generates ϕ_s *if $\langle \phi_u \mid u \in U_s \rangle = \phi_s$, and U_s is a* decomposition ϕ_s *if no proper subset of U_s generates ϕ_s.*

Because of Lemma 6.0.5 we prove that if $U_s \subset M$ is a decomposition of ϕ_s, then ϕ_s splits into a direct decomposition of ϕ_u, for $u \in U_s$. More importantly, this direct decomposition influences the filter on the operators $A = \mathrm{Aut}(G)$. In this section, we prove the following.

Theorem 6.3.2 (Theorem D). *If $\phi : M \to 2^G$ is an A-invariant filter and $V_s \subset M$ generates ϕ_s, for $s \neq 0$, then there exists $U_s \subset M - 0$ such that*

$$\langle \Delta\phi_u \mid u \in U_s \rangle / \langle \partial\Delta\phi_u \mid u \in U_s \rangle \cong \bigoplus_{u \in U_s} L_u(\Delta\phi).$$

First we prove a lemma that will satisfy the existence part of Theorem 6.3.2.

Lemma 6.3.3. *If V_s generates ϕ_s, then there exists $U_s \subset M$ that is a decomposition of ϕ_s such that for all $u \in U_s$, $\partial\phi_u \neq \phi_u$.*

Proof. Suppose there exists $u \in V_s$ such that $\partial\phi_u = \phi_u$. Since ϕ has no inert subgroups and has DCC, by Proposition 5.0.6, there exists $I_u \subseteq \mathcal{I} = \{t \in M \mid \partial\phi_t \neq \phi_t\}$ such that $\partial\phi_u = \langle \phi_t \mid I_u \rangle$ and for all $t \in I_u$, $\phi_u > \phi_t$. Choose a minimal $I_u \subseteq \mathcal{I}$. Set $U_s = (V_s \backslash \{u\}) \cup I_u$. Therefore the lemma follows. □

The proof of the next lemma skates around a structural issue between ϕ and $\Delta\phi$. In this section, we prove similarities between these filters, but it only goes so far. For example, if $\phi_0 = \phi_s$, for some $s \neq 0$, then $U_s = \{0\}$ is a decomposition of ϕ_s (this happens in, for example, the lower central series $\gamma_0 = \gamma_1 = G$). However, in this case $\Delta\phi_0$ does not need to be contained in $\Delta\phi_s$ in general.

Lemma 6.3.4. *Suppose $\phi : M \to 2^G$ is a filter. If $U_s \subseteq M - 0$ is a decomposition of ϕ_s where for all $u \in U_s$, there exists $t \in M$ such that $s + t = u$, then $\langle \Delta\phi_u \mid u \in U\rangle \leq \Delta\phi_s$.*

Proof. Suppose $\alpha \in \Delta\phi_u$, for some $u \in U_s$. Therefore, there exists $t \in M$ such that $s + t = u$. For all $v \in M$ and for all $x \in \phi_v$, $[x, \alpha] \in \phi_{u+v} = \phi_{s+t+v} \leq \phi_{s+v}$. Therefore, $\alpha \in \Delta\phi_s$. □

The intermediate step to proving Theorem 6.3.2 is to show that decompositions, together with Lemma 6.0.5, are really direct decompositions. Therefore if a part of an A-invariant filter $\phi : M \to 2^G$ decomposes, then that same part of $\Delta\phi : M \to 2^A$ filter decomposes. The following proposition is important in its own right, and gives a general description of decompositions of groups (e.g. central decompositions).

Proposition 6.3.5. *Suppose $X \subseteq G$ is faithfully filtered by $\phi : M \to 2^G$. If U_s is a decomposition of ϕ_s, then*

$$\phi_s/\langle \partial\phi_u \mid u \in U_s\rangle \cong \bigoplus_{u\in U_s} L_u(\phi).$$

Proof. Let $N = \langle \partial\phi_u \mid u \in U_s\rangle$. Since U_s is a decomposition of ϕ_s, it follows that for all distinct $u, v \in U_s$, $\phi_u \parallel \phi_v$. Fix $u \in U_s$. By Proposition 4.0.6, since X is filtered by ϕ, $\mathrm{Lat}(\phi)$ is a distributive lattice. Hence, applying Lemma 6.0.5,

$$\begin{aligned}
\phi_u \cap N &= \langle \phi_u \cap \partial\phi_v \mid v \in U_s\rangle \\
&= \partial\phi_u\langle \phi_u \cap \partial\phi_v \mid v \in U_s - u\rangle \\
&\leq \partial\phi_u\langle \phi_u \cap \phi_v \mid v \in U_s - u\rangle
\end{aligned}$$

$$= \partial\phi_u \langle \partial\phi_u \cap \partial\phi_v \mid v \in U_s - u\rangle$$

$$= \partial\phi_u.$$

Since $\phi_u \cap N \geq \partial\phi_u$ by definition, equality follows. Therefore,

$$\phi_u N/N \cong \phi_u/(\phi_u \cap N) \cong \phi_u/\partial\phi_u = L_u(\phi).$$

Because $\phi_u \cap \phi_v = \partial\phi_u \cap \partial\phi_v \leq N$,

$$\phi_s/N \cong \bigoplus_{u\in U_s} (\phi_u N)/N \cong \bigoplus_{u\in U_s} L_u(\phi). \qquad \square$$

6.4. Proof of Theorem D

The next proof follows almost entirely from Proposition 6.3.5, and a key component of this comes from Lemma 6.0.5. By construction, $\Delta\phi$ inherits much of the structure of ϕ. In particular, if ϕ is a faithful filter, then $\Delta\phi$ is also a faithful filter. From this fact, we are able to prove that there is a direct decomposition, and by Proposition 6.3.5, we obtain our desired result.

Proof of Theorem 6.3.2. Since V_s generates ϕ_s, apply Lemma 6.3.3, to obtain a decomposition U_s of ϕ_s where for all $u \in U_s$ $\partial\phi_u \neq \phi_u$. Therefore, for all $u, v \in U_S$, $\phi_u \parallel \phi_v$. In addition, suppose $\alpha \in \Delta\phi_u \cap \Delta\phi_v$. By Lemma 6.0.5, for all $t \in M$ and for all $x \in \phi_t$,

$$[x, \alpha] \in \phi_{t+u} \cap \phi_{t+v} = \partial\phi_{t+u} \cap \partial\phi_{t+v}.$$

Therefore, $\alpha \in \partial\Delta\phi_u \cap \partial\Delta\phi_v$, so $\Delta\phi_u \cap \Delta\phi_v = \partial\Delta\phi_u \cap \partial\Delta\phi_v$. Set $S = \langle \Delta\phi_u \mid u \in U_s\rangle$ and $N = \langle \partial\Delta\phi_u \mid u \in U_s\rangle$. If $\beta \in N$, then for all $x \in \phi_t$, there exists $y \in \langle \partial\phi_{u+t} \mid u \in U_s\rangle$ such that $x^\beta = xy$. If $\alpha \in S$ and $\beta \in N$, then for all $x \in \phi_t$,

$$[x, \beta\alpha] = x^{-1}x^{\beta\alpha} = x^{-1}(xy)^\alpha = [x, \alpha]y^\alpha \equiv [x, \alpha] \mod \langle \partial\phi_{u+t} \mid u \in U_s \rangle$$

as ϕ is an A-invariant filter. Therefore, if $\overline{\alpha} \in S/N$, then for all $x \in \phi_t$, $[x, \overline{\alpha}] \equiv \overline{[x, \alpha]}$ modulo $\langle \partial\phi_{u+t} \mid u \in U_s \rangle$. By Proposition 6.3.5,

$$\langle \phi_u \mid u \in U_s \rangle / \langle \partial\phi_u \mid u \in U_s \rangle \cong \bigoplus_{u \in U_s} L_u(\phi).$$

Therefore, the statement follows. □

Now we consider an example to illustrate Proposition 6.3.5 and Theorem 6.3.2. We borrow an example from [8]: we construct a central product of groups with small genus. By Proposition 6.3.5, there will be a decomposition in the filter corresponding to the central product of the groups. The automorphism group of these groups are therefore easily computed from work in [8]. In this next example, $\partial\Delta\phi_0$ is the subgroup of central automorphisms of $\mathrm{Aut}(G)$.

Example 6.4.1. We consider a central product of a genus 2 group with a genus 1 group (whose centroid is a quadratic field extension), c.f. [8]. Let p be an odd prime with ω a nonsquare, and set

$$H = UT\left(3, \mathbb{Z}_p[x]/(x^2 - \omega)\right),$$

$$F = \left\{ \left[\begin{array}{c|cc|cc} 1 & b & c & u & v \\ \hline & \multicolumn{2}{c|}{\multirow{2}{*}{I_2}} & a & \\ & & & & a \\ \hline & & & \multicolumn{2}{c}{I_2} \end{array} \right] \;\middle|\; a, b, c, u, v \in \mathbb{F}_p \right\}.$$

Define an isomorphism $\theta : Z(H) \to Z(F)$ such that

$$\begin{bmatrix} 1 & 0 & u+vx \\ & 1 & 0 \\ & & 1 \end{bmatrix} \mapsto \left[\begin{array}{c|cc|cc} 1 & 0 & 0 & u & v \\ \hline & \multicolumn{2}{c|}{} & 0 & \\ & \multicolumn{2}{c|}{I_2} & & \\ & \multicolumn{2}{c|}{} & & 0 \\ \hline & & & \multicolumn{2}{c}{I_2} \end{array}\right].$$

Finally, let $G = H \circ_\theta F \cong H \times F / \langle (x,1)(1,x\theta)^{-1} \mid x \in Z(H) \rangle$. We will abuse notation and say that $H, F \leq G$; both H and F are characteristic in G.

Let $M = \mathbb{N}^2$ be ordered by the direct product ordering. Define $\phi : M \to 2^G$ such that $\phi_0 = G$ and for all $s \neq 0$,

$$\phi_s = \begin{cases} H & \text{if } s = e_1, \\ F & \text{if } s = e_2, \\ Z(G) & \text{if } s = e_1 + e_2, \\ 1 & \text{otherwise.} \end{cases}$$

If $A = \mathrm{Aut}(G)$, then ϕ is an A-invariant filter.

Since $\phi_0 = G = \langle H, F \rangle = \langle \phi_{e_1}, \phi_{e_2} \rangle$, by Proposition 6.3.5,

$$\phi_0 / \langle \partial\phi_{e_1}, \partial\phi_{e_2} \rangle = G/Z(G) \cong H/Z(G) \oplus F/Z(G) = L_{e_1}(\phi) \oplus L_{e_2}(\phi).$$

Chapter 7

EXAMPLES

We first define some standard finite commutative monoids. Not surprisingly, it is easy to describe all cyclic monoids. Let $r \in \mathbb{N}$, $s \in \mathbb{Z}^+$ (this is the *index* and *period*, respectively). Define a congruence $\sim$ on $\mathbb{N}$ where $i, j \in \mathbb{N}$,

$$i \sim j \iff \begin{cases} i = j & \text{if } i, j < r \\ i \equiv j \pmod{s} & \text{if } i, j \geq r. \end{cases}$$

Define $C_{r,s} = \mathbb{N}/{\sim}$, and note that $|C_{r,s}| = r + s$.

Proposition 7.0.1 ([16, Proposition 5.8]). *If M is a cyclic monoid, then either $M \cong \mathbb{N}$ or there exists $r, s \in \mathbb{N}$ such that $M \cong C_{r,s}$.*

The only cyclic monoids where $\preceq_+$ is a pre-order are $\mathbb{N}$ and $C_{r,1}$. The reason is akin to why finite fields cannot be (totally) ordered. Of course every monoid has a partial order: let 0 be the minimal element and every pair of nonzero elements are incomparable.

Example 7.0.2. If G is a nilpotent group of class c, then $\gamma : \mathbb{N} \to 2^G$ can be defined over $C_{c+1,1}$ instead of $\mathbb{N}$ as $1 = \gamma_{c+1} = \gamma_{c+2} = \cdots$. □

This leads to an interesting question about the relationship between congruences of M and filters $\phi : M \to 2^G$. In particular, if $\sim$ is a congruence on M and $\sim$ is compatible with ϕ, i.e. if $s \sim t$, then $\phi_s = \phi_t$, then there exists a new filter $\gamma : M/{\sim} \to 2^G$ defined in a natural way. In [21], we construct filters over infinite, totally-ordered monoids. In that case, and more generally, if $\text{im}(\phi)$ is finite but M is infinite, does there exist a congruence $\sim$ of M that is compatible with ϕ such that $M/{\sim}$ is a finite commutative monoid?

7.1. Upper unitriangular matrices

Let $UT(d, K)$ denote the $d \times d$ upper unitriangular matrix group over the ring K. Let $G = UT(5, K)$, for some commutative ring K. The terms of the lower central series can be easily visualized

$$G = \begin{bmatrix} 1 & * & * & * & * \\ & 1 & * & * & * \\ & & 1 & * & * \\ & & & 1 & * \\ & & & & 1 \end{bmatrix}, \qquad \gamma_2 = \begin{bmatrix} 1 & 0 & * & * & * \\ & 1 & 0 & * & * \\ & & 1 & 0 & * \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix},$$

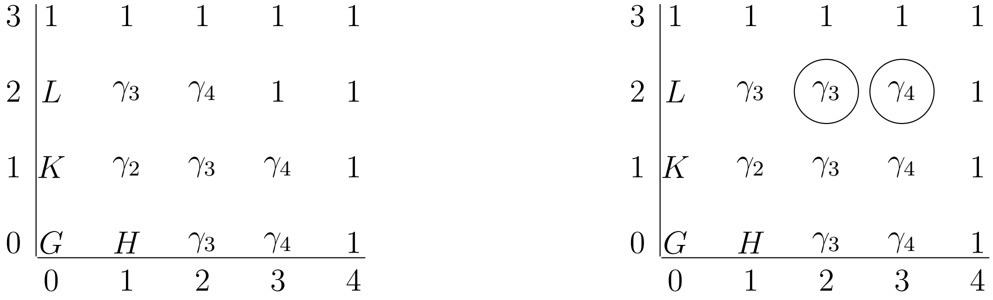
$$\gamma_3 = \begin{bmatrix} 1 & 0 & 0 & * & * \\ & 1 & 0 & 0 & * \\ & & 1 & 0 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix}, \qquad \gamma_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & * \\ & 1 & 0 & 0 & 0 \\ & & 1 & 0 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix}.$$

We define three more characteristic subgroups

$$H = \begin{bmatrix} 1 & * & * & * & * \\ & 1 & 0 & * & * \\ & & 1 & 0 & * \\ & & & 1 & * \\ & & & & 1 \end{bmatrix}, \quad K = \begin{bmatrix} 1 & 0 & * & * & * \\ & 1 & * & * & * \\ & & 1 & * & * \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix}, \quad L = \begin{bmatrix} 1 & 0 & 0 & * & * \\ & 1 & 0 & * & * \\ & & 1 & 0 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix}.$$

Note that H has class 3 and K has class 2.

Let $M = C_{4,1} \times C_{3,1}$, and set $e_1 = (1, 0)$ and $e_2 = (0, 1)$. We let M be ordered by the direct product ordering. Define a function $\pi : \{0, e_1, e_2\} \to 2^G$, where $\pi_0 = G$, $\pi_{e_1} = H$ and $\pi_{e_2} = K$. Set $\phi = \overline{\pi} : M \to 2^G$; the image of ϕ is plotted in Figure 7.1a. Notice that no generating set can be strongly-filtered with respect to ϕ because $\phi_{(2,2)} = \phi_{(3,1)} \neq \partial\phi_{(2,2)} = \partial\phi_{(3,1)}$. This can be fixed by altering ϕ slightly; see Figure 7.1b. That is, define $\lambda : M \to 2^G$ where for all $s \in M - \{(2, 2), (3, 2)\}$, $\lambda_s = \phi_s$, $\lambda_{(2,2)} = \gamma_3$, and $\lambda_{(3,2)} = \gamma_4$. Suppose E_{ij} is a 5×5 matrix over K with 1 in the (i, j) entry and 0 elsewhere. If $X = \{I_5 + E_{ij} \mid 1 \leq i < j \leq 5\}$, then X is strongly-filtered by λ.



	0	1	2	3	4
3	1	1	1	1	1
2	L	γ_3	γ_4	1	1
1	K	γ_2	γ_3	γ_4	1
0	G	H	γ_3	γ_4	1

(A) $\phi : M \to 2^G$.

	0	1	2	3	4
3	1	1	1	1	1
2	L	γ_3	$\enclose{circle}{\gamma_3}$	$\enclose{circle}{\gamma_4}$	1
1	K	γ_2	γ_3	γ_4	1
0	G	H	γ_3	γ_4	1

(B) $\lambda : M \to 2^G$.

Figure 7.1. Plots of filters ϕ and λ.

7.2. An example from the literature

We consider a group examined in [13, Section 12.1] and [21, Section 5]. For a fixed prime p, we define a p-group G by a power-commutator presentation, where all trivial commutators are omitted

$$G = \langle g_1, ..., g_{13} \mid [g_{10}, g_6] = g_{11}, [g_{10}, g_7] = g_{12},$$

$$[g_2, g_1] = [g_4, g_3] = [g_6, g_5] = [g_8, g_7] = [g_{10}, g_9] = g_{13}, \text{exponent } p\rangle.$$

In [21], we defined a filter on $\mathbb{N}^2$, with a total ordering; here, we define the same filter, except over $M = C_{3,1} \times C_{5,1}$, totally-ordered by the lexicographical ordering. Denote this filter by ϕ.

Observe from the presentation that G has class 2 and $\gamma_2 = \langle g_{11}, g_{12}, g_{13}\rangle$. The following subgroups are characteristic

$$J_1 = \langle g_1, \ldots, g_9, \gamma_2\rangle, \qquad J_4 = \langle g_9, \gamma_2\rangle,$$

$$J_2 = \langle g_1, \dots, g_5, g_8, g_9, \gamma_2 \rangle, \qquad\qquad H = \langle g_{13} \rangle.$$

$$J_3 = \langle g_5, g_8, g_9, \gamma_2 \rangle,$$

The image of ϕ produces the following characteristic series

$$G > J_1 > J_2 > J_3 > J_4 > \gamma_2 > H > 1.$$

Using techniques developed in [9], the tensor $\circ : G/\gamma_2 \times G/\gamma_2 \rightarrowtail \gamma_2$ yields more characteristic subgroups. In fact, as $*$-algebras,

$$\mathrm{Adj}(\circ) \cong J \rtimes (\mathbf{X}(2, p) \oplus \mathbf{S}(4, p)).$$

The simple $*$-algebras $\mathbf{X}(2, p)$ and $\mathbf{S}(4, p)$ determine new characteristic subgroups:

$$E = \langle g_5, \dots, g_{10}, \gamma_2 \rangle, \qquad S = \langle g_1, \dots, g_4, \gamma_2 \rangle.$$

Let $M' = M \times \mathbb{N} \times \mathbb{N}$, where M' is ordered by the direct product ordering. Set $T = \{(m, 0, 0) \mid m \in M\} \cup \{e_2, e_3\}$, and define a function $\pi : T \to 2^G$, where $\pi_{(m,0,0)} = \phi_m$, $\pi_{e_2} = E$, and $\pi_{e_3} = S$. Let $\lambda = \overline{\pi}$. If $X = \{g_1, \dots, g_{13}\}$, then X is filtered by λ, and X satisfies the distributive property on λ as well. Since X is filtered, we can compute intersections of subgroups in $\mathrm{im}(\lambda)$ efficiently, so further refine λ to include $J_1 \cap E$. We cannot easily plot the refinement of λ as we did in Figures 7.1a and 7.1b, so we display the lattice of characteristic subgroups in Figure 7.2.

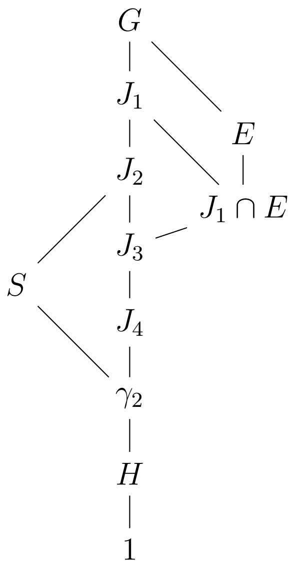


FIGURE 7.2. The lattice of subgroups in the refinement of $\lambda : M' \to 2^G$.

Chapter 8

LIFTING DERIVATIONS

Recall from Section 2 that if $\phi : M \to 2^G$ is an A-invariant filter and A is a group, then ϕ induces another filter, namely $\Delta\phi : M \to 2^A$. In addition, as Theorem 2.8.1 and Lemma 2.8.4 shows, there exists an injective map $\mathcal{D} : L(\Delta\phi) \to \mathrm{Der}(L(\phi))$. Our goal now is to reverse this map as best we can. One of the main hurdles is that we cannot explicitly compute a basis for $\mathrm{im}(\mathcal{D})$.

Throughout the rest of the paper, we assume that G is a finite p-group with exponent p, $\phi : M \to 2^G$ is a characteristic, faithful filter with no inert subgroups, and $\phi_0 = \partial\phi_0 = G$. In the next subsection, we show that the M-graded structure of $L(\phi)$ transfers to $\mathrm{Der}(L(\phi))$.

8.1. An approximation of $L(\Delta\phi)$

In Section 2, we showed how filters $\phi : M \to 2^G$ naturally induce filters on $\mathrm{Aut}(G)$, namely $\Delta\phi : M \to 2^{\mathrm{Aut}(G)}$. Here, we show that this extends to a grading of the derivation ring $D = \mathrm{Der}(L(\phi))$. Define

$$D_s = \left\{ d \in D \;\middle|\; (\forall t) \left(t \in M \implies L_t d \leq \bigoplus_{u \in M} L_{s+t+u} \right) \right\} \quad \& \quad \partial D_s = \sum_{t \in M - 0} D_{s+t}.$$

Proposition 8.1.1. *If $\phi : M \to 2^G$ is a filter, then $D = \mathrm{Der}(L(\phi))$ is M-graded and as M-graded rings,*

$$D \cong \bigoplus_{s \in M} D_s / \partial D_s.$$

Proof. Observe that $D_0 = D$. Fix $s, t \in M$, and let $\delta \in D_s$ and $\delta' \in D_t$. If $x \in L_u(\phi)$, then

$$x([\delta, \delta']) = x(\delta\delta' - \delta'\delta) = x\delta\delta' - x\delta'\delta \in \bigoplus_{v \in M} L_{s+t+u+v}(\phi),$$

so $[\delta, \delta'] \in D_{s+t}$. In particular, $[D_s, D_0] \leq D_s$, so each D_s is a Lie ideal. Therefore, ∂D_s is a Lie ideal as well. Suppose $s, t \in M$ are distinct, and $\delta \in D_s \cap D_t$. For all $x \in L_u(\phi)$,

$$x\delta \in \bigoplus_{v\in M} L_{s+u+v}(\phi) \cap \bigoplus_{v\in M} L_{t+u+v}(\phi).$$

Therefore, for all $v, w \in M$ where $s+v = t+w$, $\delta \in D_{s+v} = D_{t+w}$, and in particular, $\delta \in \partial D_s$ or $\delta \in \partial D_t$ since both v and w are not 0. Hence, the statement follows. □

Since $L = \bigoplus_{s\in M} L_s$, there exists a set of idempotents $\mathcal{E} \subset \mathrm{End}(L)$ associated to the direct decomposition of L, known as an *orthogonal frame*. That is, for $s \in M$, where $L_s \neq 0$, there exists $e \in \mathcal{E}$ such that $Le = L_s$, $e|_{L_s} = 1$, and $e^2 = e$. We may also index $\mathcal{E}$ by M, so that for $s \in M$, e_s is the idempotent associated to L_s. With this, we define a $\mathbb{Z}$-linear map $\mathcal{P} : \mathrm{Der}(L) \to \mathrm{End}_{\mathbb{Z}}(L)$ via

$$\mathcal{P} : \delta \mapsto \sum_{e\in\mathcal{E}} e\delta e. \tag{12}$$

In the next lemma, we prove that $\mathcal{P}$ is actually a Lie homomorphism with kernel ∂D_0. Because $\mathcal{P}$ can be computed without computing ∂D_0, this enables us to approximate $L(\Delta\phi)$.

Lemma 8.1.2. *The $\mathbb{Z}$-linear map $\mathcal{P}$ is a Lie homomorphism, and the following is a split exact sequence of Lie rings, where ι is inclusion,*

$$0 \longrightarrow \partial D_0 \xrightarrow{\iota} \mathrm{Der}(L) \xrightarrow{\mathcal{P}} D_0/\partial D_0 \longrightarrow 0.$$

Proof. First we show that the kernel of $\mathcal{P}$ is ∂D_0. If $\delta \in D_s$, for $s \neq 0$, then for all $e \in \mathcal{E}$, $e\delta e = 0$:

$$Le\delta e = L_t\delta e \leq \bigoplus_{u\in M} L_{s+t+u} e = 0.$$

Therefore, $\delta \in \ker(\mathcal{P})$.

Suppose $\delta \in \ker(\mathcal{P})$. If for every $e \in \mathcal{E}$, $e\delta e = 0$, then there exists $s \neq 0$, such that $\delta \in D_s$. If, on the other hand, there exists $f \in \mathcal{E}$ such that $f\delta f \neq 0$, then write

$$\sum_{e\in\mathcal{E}-f} e\delta e = -f\delta f.$$

Since $ef = 0$ for all $e \in \mathcal{E} - f$ and $f^2 = f$, it follows that $f\delta f = 0$, a contradiction:

$$-f\delta f = -f^2\delta f^2 = \sum_{e\in\mathcal{E}-f} fe\delta ef = 0.$$

Hence, $\ker(\mathcal{P}) = \partial D_0$.

We prove that the image of $\mathcal{P}$ is $D_0/\partial D_0$. Let $\delta \in D_0\backslash\partial D_0$, $x \in L_s$, and $y \in L_t$. For some $x_s \in L_s$ and $x_\partial \in \bigoplus_{u\in M-0} L_{s+u}$, write $x\delta = x_s + x_\partial$, and similarly write $y\delta = y_t + y_\partial$. Let $e, f, g \in \mathcal{E}$ such that $Le = L_s$, $Lf = L_t$, and $Lg = L_{s+t}$. Then,

$$[x(\delta\mathcal{P}), y] + [x, y(\delta\mathcal{P})] = [x_s, y] + [x, y_t] = [x, y]\,(\delta\mathcal{P}).$$

Thus, $\delta\mathcal{P} \in D_0$. Furthermore, observe that for $\delta, \delta' \in \mathrm{Der}(L)$, $\delta\mathcal{P} = \delta'\mathcal{P}$ if, and only if, $\delta \equiv \delta' \mod \partial D_0$. By definition, $\mathcal{P}^2 = \mathcal{P}$, so $(\delta\mathcal{P} - \delta)\mathcal{P} = 0$. Therefore, $\delta\mathcal{P} \equiv \delta \mod \partial D_0$, so $\mathcal{P}$ is surjective. □

This implies the next proposition: essentially, $\mathcal{DP} = 0$.

Proposition 8.1.3. *Suppose $\phi : M \to 2^G$ is a characteristic filter of G. If $\mathcal{P}$: $\mathrm{Der}(L(\phi)) \to \mathrm{End}(L(\phi))$ is defined as in (12), then the following is a chain complex of Lie rings*

$$0 \longrightarrow L(\Delta\phi) \xrightarrow{\mathcal{D}} \mathrm{Der}(L(\phi)) \xrightarrow{\mathcal{P}} D_0/\partial D_0 \longrightarrow 0.$$

Proof. By Theorem 2.8.1, $L_s\mathcal{D} \leq D_s$ for $s \neq 0$. Therefore, $\mathrm{im}(\mathcal{D}) \leq \partial D_0 = \ker(\mathcal{P})$. The proposition follows by Lemmas 2.8.4 and 8.1.2. □

From Proposition 8.1.3 we can efficiently approximate $L(\Delta\phi)$ by $\ker(\mathcal{P})$.

Theorem 8.1.4. *Suppose $\phi : \mathbb{N}^d \to 2^G$ is a filter and $L(\phi)$ a K-algebra. There exists a polynomial-time algorithm that, given $L(\phi)$, returns a basis for ∂D_0.*

Before we prove Theorem 8.1.4, we prove some preliminary results. A key component of obtaining a basis for ∂D_0 are the following problems, which we prove are in polynomial time.

Problem. DerAlg

Input: *The structure constants for the K-algebra A;*

Return: *A basis for the derivation algebra* $\mathrm{Der}(A)$.

Problem. GrDerAlg

Input: *An $\mathbb{N}^d$-graded K-algebra A;*

Return: *A basis for the graded derivation algebra* $\mathrm{Der}(A)$.

It is known that DerAlg is in polynomial time, but we supply a proof for completeness.

Proposition 8.1.5. DerAlg *is in polynomial time requiring $O\left(\dim_K(A)^{2\omega}\log^2|K|\right)$ basic operations, where ω is the exponent of matrix multiplication.*

Proof. *Algorithm.* Suppose $\mathcal{B}$ is a basis for A, and suppose $M = \left(m_{ij}^{(k)}\right)$ is the matrix of structure constants for A, where each entry is a vector in A. For variables x_{ij}, set $X = (x_{ij})$. Solve the linear system $XM + MX^t = M^X$, where $M^X = (\mathbf{m}_{ij}X)$.

Correctness. Suppose D is a solution to the linear system. For all $a, b \in A$,

$$(aD)Mb^t + aM(bD)^t = a(DM + MD^t)b^t = a(M^D)b^t = (aMb^t)^D.$$

If $\delta \in \mathrm{Der}(A)$, then when written in the basis $\mathrm{End}_K(A)$, it also satisfies the linear system.

Timing. If $\dim_K(A) = n$, then this requires solving $O(n^2)$ linear equations in $O(n^2)$ variables. $\square$

The problem of efficiently constructing a basis for the graded derivation algebra is a variant of the DerAlg but for $\mathbb{N}^d$-graded K-algebras. Essentially, we require more information due to the grading on the algebra, and then we compute an intersection of vector spaces which is done efficiently. The input of an $\mathbb{N}^d$-graded K-algebra A is a basis $\mathcal{B}$ for A, a function $\tau : \mathcal{B} \to \mathbb{N}^d$ such that for all $b \in \mathcal{B}$, $b \in A_{\tau(b)}$, and structure constants $M = \left(m_{ij}^{(k)}\right)$ with respect to $\mathcal{B}$. Therefore, if $n = \dim_K(A)$ and $q = |K|$, then the input size of an $\mathbb{N}^d$-graded K-algebra is $O\left(n^3 \log q + dn\right)$. We choose $\mathbb{N}^d$ instead of an arbitrary monoid M so that we can efficiently decide if for each pair $b, c \in \mathcal{B}$, there exists $s \in \mathbb{N}^d$ such that $\tau(b) + s = \omega(c)$. Since we are concerned with computation, M is finitely generated; therefore, there exists a congruence such that $\mathbb{N}^d/{\sim} \cong M$.

Proposition 8.1.6. GrDerAlg *requires* $O(\dim_K(A)^{2\omega} \log^2 |K|)$ *basic operations, where* ω *is the exponent of matrix multiplcation.*

Proof. *Algorithm.* Let $\mathcal{B}$ be a graded basis for A and X a generating set for M. Define a basis for a subspace $S \leq \mathrm{End}_K(A)$ as follows: for each pair $b, c \in \mathcal{B}$ if $\tau(c) - \tau(b) \in \mathbb{N}^d$, then include the endomorphism that maps b to c and maps all other basis vectors to 0. Return $D = \mathrm{DerAlg}(A) \cap S$.

Correctness. This follows from the definition of a graded derivation.

Timing. This follows from the fact that DerAlg is in polynomial time, by Proposition 8.1.5, and computing intersections of subspaces in $\mathrm{End}_K(A)$ requires $O(\dim_K(A)^{2\omega}\log^2|K|)$ basic operations. □

Now we prove that ∂D_0 can be computed in polynomial time. To do this, we prove that we can construct the map $\mathcal{P}$, defined in (12), efficiently. Constructing $\mathcal{P}$ amounts to constructing the idempotents $e \in \mathcal{E}$. Since $\mathcal{P}$ is a linear map, we can efficiently compute its kernel and approximate $L(\Delta\phi)$.

Proof of Theorem 8.1.4. *Algorithm.* Let $D =$GrDerAlg$(L(\phi))$. For each $s \in \mathrm{im}(\tau)$, construct the idempotent $E_s \in \mathrm{End}_K(A)$. Let $\mathcal{C}$ be a basis for D, and construct the linear transformation $\mathcal{P} : D \to \mathrm{End}_K(A)$. That is, for each $\delta \in \mathcal{C}$, set $\delta\mathcal{P} = \sum_{s\in\mathrm{im}(\tau)} E_s\delta E_s$. Return a basis for $\ker(\mathcal{P})$.

Correctness. This follows from Lemma 8.1.2.

Timing. By Proposition 8.1.6, GrDerAlg uses $O(\dim_K(A)^{2\omega})$ field operations. Constructing the idempotents is done in $O(\dim_K(A))$ time, and constructing the map $\mathcal{P}$ is done in $O(\dim_K(A)^{2+\omega})$ time. A basis for the kernel of $\mathcal{P}$ is then returned after $O(\dim_K(A)^{2\omega})$ field operations. □

Now that we can compute ∂D_0 efficiently, we want to be able to use this information to aid in the construction of $\mathrm{Aut}(\partial\phi_0)$. In the next section, we build off of the work from Sections 4 through 6 and define bijections $\alpha : G \to G$ from derivations $\delta \in \partial D_0$. Our main algorithm to construct automorphisms from derivations *corrects* the bijections $\alpha : G \to G$ so that they are homomorphisms. It is possible that a derivation of $L(\phi)$ cannot be lifted to an automorphism G. In our algorithm in the next section, this will correspond to an inconsistent linear system.

8.2. Lifting ∂D_0

Let $X = \{a_1, \ldots, a_n\} \subset G$ be faithfully filtered by $\phi : M \to 2^G$. We will also assume that each $L_s(\phi)$ is elementary abelian. Otherwise, $\partial\phi_s\phi_s^p$ is a proper, nontrivial characteristic subgroup of $L_s(\phi)$, so refine the filter until $L(\phi)$ is a $\mathbb{Z}_p$-algebra. Since G is a finite p-group and $G = \partial\phi_0$, X is a pcgs for G by Theorem 6.0.4, up to relabeling.

Let $F = \langle x_1, \ldots, x_n\rangle$ be a free group, and define a surjection $\pi : F \to G$ where $x_i \mapsto a_i$. Thus, we have the following (polycyclic) presentation

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\pi} G \longrightarrow 1.$$

Since X is faithfully filtered by ϕ, there exists a unique $s_i \in M$ such that $a_i \in \phi_s \backslash \partial\phi_{s_i}$. Define a function $\omega : \{1, \ldots, n\} \to M$ such that $i \mapsto s_i$. Observe that since $\partial\phi_0 = G$, $\omega(i) \neq 0$ for all i.

As X is a pcgs of G, for every $g \in G$, there is a unique normal word

$$g = a_1^{e_1} \cdots a_n^{e_n},$$

where each $e_i \in \{0, \ldots, p-1\}$. For each $i, j \in \{1, \ldots, n\}$, define $W_{ij} \in F$ such that $[a_i, a_j] = W_{ij}\pi$ is the unique normal word. Similarly, for $k \in \{1, \ldots, n\}$ define $W_k \in F$ such that $a_k^p = W_k\pi$ is the unique normal word. Define relators:

$$R_{ij} = [x_i, x_j]W_{ij}^{-1} \qquad \text{and} \qquad R_k = x_k^p W_k^{-1}.$$

Because G is a p-group

$$R = \langle R_{ij},\ R_k \mid 1 \leq i, j, k \leq n\rangle^F.$$

With $D = \mathrm{Der}(L(\phi))$, let $\delta \in \partial D_s$, with $s \neq 0$. By Theorem 6.0.4, $\{\partial\phi_{\omega(i)}a_i \mid 1 \leq i \leq n\}$ is a basis for $L(\phi)$, so we can define an endomorphism of F from δ as follows.

Definition 8.2.1. *A* lift *of δ to F is an endomorphism $\lambda = \lambda(\delta) \in \mathrm{End}(F)$ such that*

$$[x_i, \lambda]\pi = (x_i^{-1}(x_i\lambda))\pi \equiv (\partial\phi_{\omega(i)}a_i)\delta \mod \partial\phi_{\omega(i)+s}.$$

That is, for $1 \leq i \leq n$, there exists $y_i \in F$ such that $y_i\pi \equiv (\partial\phi_{\omega(i)}a_i)\delta \mod \partial\phi_{\omega(i)+s}$ and $x_i\lambda \equiv x_iy_i \mod R$. Therefore, for each i, there exists $b_i \in \phi_{\omega(i)+s}$ such that $x_i\lambda\pi = a_ib_i$. There are many choices for a lift λ of δ: up to choices of $\partial\phi_{\omega(i)+s}$ for each $i \in \{1, \ldots, n\}$ and choices of $R = \ker(\pi)$.

Before we start attempting to construct automorphisms from derivations, the following proposition provides a necessary condition for lifts λ of a derivation δ should it induce an automorphism of G.

Proposition 8.2.2. *If $\alpha \in \Delta\phi_s \leq \partial\Delta\phi_0$ and λ is any lift of $\mathcal{D}_{\overline{\alpha}}$, then for all $i, j \in \{1, \ldots, n\}$, with $t = \omega(i) + \omega(j) + s$, $R_{ij}\lambda\pi \in \partial\phi_t$.*

First, we prove the following technical lemma. The statement is concerned with words in G, and the proof applies collection from the left. After proving Lemma 8.2.3, the proposition follows after a few computations.

Lemma 8.2.3. *With the established notation, $\left(W_{ij}^{-1}\pi\right)(W_{ij}\lambda\pi) \in \phi_t$.*

Proof. Suppose $W_{ij}\pi = a_1^{e_1} \cdots a_n^{e_n}$ and $W_{ij}\lambda\pi = (a_1b_1)^{e_1} \cdots (a_nb_n)^{e_n}$. As $a_\ell \in \phi_{\omega(\ell)}$ and $b_\ell \in \phi_{\omega(\ell)+s}$, it follows that

$$(a_\ell b_\ell)^{e_\ell} \equiv a_\ell^{e_\ell} b_\ell^{e_\ell} \mod \partial\phi_{\omega(\ell)+s}.$$

Therefore, for each $\ell \in \{1, \ldots, n\}$, there exists $c_\ell \in \partial\phi_{\omega(\ell)+s}$ such that

$$(a_\ell b_\ell)^{e_\ell} = a_\ell^{e_\ell} b_\ell^{e_\ell} c_\ell,$$

so $W_{ij}\varepsilon\pi = (a_1^{e_1} b_1^{e_1} c_1) \cdots (a_n^{e_n} b_n^{e_n} c_n)$.

For $1 \leq u, v \leq n$, set $w = \omega(u) + \omega(v) + s$, then

$$[b_u^{e_u} c_u, a_v^{e_v}] = [b_u^{e_u}, a_v^{e_v}]\, [b_u^{e_u}, a_v^{e_v}, c_u]\, [c_u, a_v^{e_v}] \in \phi_w$$

since ϕ is a filter. We employ a collection on the left, collecting all the $a_u^{e_u}$, and at each step, we apply the formula $xy = yx[x, y]$

$$\begin{aligned} W_{ij}\varepsilon\pi &= \left(a_1^{e_1} \underline{b_1^{e_1} c_1}\right) \left(\underline{a_2^{e_2}} b_2^{e_2} c_2\right) \cdots (a_n^{e_n} b_n^{e_n} c_n) \\ &= a_1^{e_1} a_2^{e_2} \;\; \underline{b_1^{e_1} c_1\, [b_1^{e_1} c_1, a_2^{e_2}]\, b_2^{e_2} c_2} \;\; \left(\underline{a_3^{e_3}} b_3^{e_3} c_3\right) \cdots (a_n^{e_n} b_n^{e_n} c_n) \\ &\;\;\vdots \\ &= (a_1^{e_1} a_2^{e_2} \cdots a_n^{e_n})\, W \\ &= (W_{ij}\pi)\, W. \end{aligned}$$

Note that if $e_\ell = 0$, then $c_\ell = 1$. If, on the other hand, $e_\ell \neq 0$, then $a_\ell \in \phi_{\omega(i)+\omega(j)}$ and $b_\ell \in \phi_t$ as ϕ is a filter and X a pcgs of G. Therefore, when $e_\ell \neq 0$, $c_\ell \in \partial\phi_t$. Thus, $W \in \phi_t$. □

Now we prove Proposition 8.2.2.

Proof of Proposition 8.2.2. For each $1 \leq \ell \leq n$, $x_\ell\lambda\pi = a_\ell b_\ell$, so

$$b_\ell \equiv (\partial\phi_{\omega(\ell)} a_\ell)\mathcal{D}_{\overline{\alpha}} \mod \partial\phi_{\omega(\ell)+s}.$$

By definition,

$$(\partial\phi_{\omega(\ell)}a_\ell)\mathcal{D}_{\overline{\alpha}} \equiv a_\ell^{-1}(a_\ell\alpha) \mod \partial\phi_{\omega(\ell)+s}.$$

Therefore, $a_\ell b_\ell(a_\ell\alpha)^{-1} \in \partial\phi_{\omega(\ell)+s}$, so for $1 \le \ell \le n$,

$$x_\ell\lambda\pi = a_\ell b_\ell \equiv a_\ell\alpha = x_\ell\pi\alpha \mod \partial\phi_{\omega(\ell)+s}. \tag{13}$$

By equation (13) and Lemma 8.2.3, for all $1 \le i, j \le n$,

$$W_{ij}\pi\alpha \equiv W_{ij}\lambda\pi \mod \partial\phi_t.$$

Since $x_\ell\pi\alpha \equiv a_\ell b_\ell \mod \partial\phi_{\omega(\ell)+s}$, it follows that for each $1 \le \ell \le n$, there exists $c_\ell \in \partial\phi_{\omega(\ell)+s}$ such that $x_\ell\pi\alpha = a_\ell b_\ell c_\ell$. Therefore, modulo $\partial\phi_t$,

$$\begin{aligned} R_{ij}\lambda\pi &= [a_ib_i, a_jb_j]\,(W_{ij}\lambda\pi)^{-1} \\ &\equiv [a_i,a_j][a_i,b_j][b_i,a_j]\,(W_{ij}\lambda\pi)^{-1} \\ &\equiv [a_i,a_j][a_i,b_j][b_i,a_j]\,(W_{ij}\pi\alpha)^{-1} \\ &\equiv [a_ib_ic_i, a_jb_jc_j]\left(W_{ij}^{-1}\pi\alpha\right) \\ &= \left([x_i,x_j]W_{ij}^{-1}\right)\pi\alpha \\ &= R_{ij}\pi\alpha. \end{aligned}$$

Since $R_{ij} \in \ker\pi$, it follows that $R_{ij}\lambda\pi \in \partial\phi_t$. □

It is not known if Proposition 8.2.2 is a sufficient condition for derivations that will induce automorphisms of G. We suspect that this is not the case, see Question 4 in Section 9 for a brief discussion about this issue.

Define an overgroup of $\mathrm{Aut}(G)$ as follows

$$\Psi(G) = \{\alpha : G \to G \mid \alpha \text{ a bijection, } \forall g, h \in G, [g\alpha, h\alpha] = [g, h]\alpha\}.$$

Since G is nilpotent, it follows that $\alpha \in \Psi(G)$ implies $1\alpha = 1$. If G is exponent p, then $\Psi(G) = \mathrm{Aut}(G)$. If G has class 2, then

$$\Psi(G) = C_{\mathrm{Aut}(G)}(G/G') \rtimes \Psi\mathrm{Isom}([,]).$$

We lift derivations to $\Psi(G)$.

Now we describe a method for lifting derivations to bijections in $\Psi(G)$. Let λ be a lift of $\delta \in D_s \leq \partial D_0$. Therefore, λ induces the following map $\alpha : G \to G$ where $a_i \mapsto a_i b_i$, for some $b_i \in \phi_{\omega(i)+s}$. To make α a well-defined function, before evaluating α write $g \in G$ in its unique normal word in terms of the pcgs X. That is, for each $g \in G$, write $g = a_1^{e_1} \cdots a_n^{e_n}$ as the unique normal word, then

$$g\alpha = \left(a_1^{e_1} \cdots a_n^{e_n}\right)\alpha = (a_1 b_1)^{e_1} \cdots (a_n b_n)^{e_n}.$$

Since G is polycyclic, α is a bijection. Let $t = \omega(i) + \omega(j) + s$. By Proposition 8.2.2, for all i, j, we assume that

$$R_{ij}\lambda\pi = [a_i b_i, a_j b_j]([a_i, a_j]^{-1}\alpha) \in \partial\phi_t. \tag{14}$$

Since ϕ has no inert subgroups, there exists $I_t \subseteq \mathcal{I} = \{t \in M \mid \phi_t \neq \partial\phi_t\}$ such that $\partial\phi_t = \langle \phi_u \mid u \in I_t \rangle$. Let $N = \langle \partial\phi_u \mid u \in I_t \rangle$. By Proposition 6.3.5, the statement in (14) is equivalent to the following statement

$$N([a_ib_i, a_jb_j]([a_i, a_j]^{-1}\alpha)) \in \bigoplus_{u \in I_t} L_u(\phi).$$

Since ϕ has no inert subgroups, by Proposition 5.0.6, for each $i, j \in \{1, \ldots, n\}$ there exists $\mathtt{J}_{ij} \subseteq \mathcal{I}$ such that

$$\partial\phi_{\omega(i)+\omega(j)+s} = \langle \phi_t \mid t \in \mathtt{J}_{ij} \rangle.$$

Given $\alpha : G \to G$ such that

$$[a_i\alpha, a_j\alpha]\left([a_i, a_j]^{-1}\alpha\right) \in \partial\phi_{\omega(i)+\omega(j)+s} = \langle \phi_t \mid t \in \mathtt{J}_{ij} \rangle,$$

our goal is to find all $\beta : G \to G$ such that

$$[a_i\beta, a_j\beta]\left([a_i, a_j]^{-1}\beta\right) \in \mathcal{N}_{ij} := \langle \partial\phi_t \mid t \in \mathtt{J}_{ij} \rangle$$

or determine that no such β exists. The main thrust in this direction comes from the next technical lemma, but before stating that, we provide some notation that will be used throughout to simplify statements.

Notation 8.2.4. For each $i, j \in \{1, \ldots, n\}$ define the following.

(1) $\mathtt{J}_i \subseteq \mathcal{I}$ such that $\partial\phi_{\omega(i)+s} = \langle \phi_t \mid t \in \mathtt{J}_i \rangle$.

(2) $\mathtt{J}_{ij} \subseteq \mathcal{I}$ such that $\partial\phi_{\omega(i)+\omega(j)+s} = \langle \phi_t \mid t \in \mathtt{J}_{ij} \rangle$.

(3) $\mathcal{N}_i = \langle \partial\phi_t \mid t \in \mathtt{J}_i \rangle$.

(4) $\mathcal{N}_{ij} = \langle \partial\phi_t \mid t \in \mathtt{J}_{ij} \rangle$.

The essence of the following lemma is that given $\alpha : a_i \mapsto a_ib_i$, we can determine all possible β, that are corrections of α, by solving a linear system. If the system is consistent, then we can produce a β. However, we prove that *all* such β come from solving the linear system. Thus, the linear system is inconsistent if, and only if, no such β exists. The majority of the content of the proof is proving equivalences of expressions using commutator identities.

Lemma 8.2.5. *With the established notation, let $\beta : G \to G$ such that for each i there exists $c_i \in \langle \phi_t \mid t \in \mathtt{J}_i \rangle$ such that $a_i \mapsto a_i b_i c_i$. There exists $\overline{x}_k \in \bigoplus_{t \in \mathtt{J}_k} L_t(\phi)$ such that for all $i, j \in \{1, \dots, n\}$,*

$$[a_i b_i x_i, a_j b_j x_j] \left((a_1 b_1 x_1)^{e_1} \cdots (a_n b_n x_n)^{e_n}\right)^{-1} \equiv 0 \mod \mathcal{N}_{ij}$$

if, and only if, for all $i, j \in \{1, \dots, n\}$,

$$[a_i \beta, a_j \beta] \left(a_1^{e_1} \cdots a_n^{e_n}\right)^{-1} \beta \in \mathcal{N}_{ij},$$

where $[a_i, a_j] = a_1^{e_1} \cdots a_n^{e_n}$, for some $0 \leq e_\ell < p$.

Proof. The forward direction follows by definition. Suppose there exists a function β such that for all $i, j \in \{1, \dots, n\}$,

$$[a_i \beta, a_j \beta] \left(a_1^{e_1} \cdots a_n^{e_n}\right)^{-1} \beta \in \mathcal{N}_{ij}.$$

We will show that for all $k \in \{1, \dots, n\}$ and $d_k \in \mathcal{N}_k$, the function β' mapping a_i to $a_i b_i c_i d_i$ satisfies

$$[a_i \beta', a_j \beta'] \left(a_1^{e_1} \cdots a_n^{e_n}\right)^{-1} \beta' \in \mathcal{N}_{ij}.$$

In other words, we show that

$$[a_i b_i c_i d_i, a_j b_j c_j d_j] \left((a_1 b_1 c_1 d_1)^{e_1} \cdots (a_n b_n c_n d_n)^{e_n}\right)^{-1} \in \mathcal{N}_{ij}. \tag{15}$$

Applying commutator formulas, we have that the expression in (15) is equivalent, modulo $\mathcal{N}_{ij}$ to

$$[d_i, a_j\beta][a_i\beta, a_j\beta][a_i\beta, d_j]\left((a_1b_1c_1d_1)^{e_1}\cdots(a_nb_nc_nd_n)^{e_n}\right)^{-1}. \tag{16}$$

First we consider $[d_i, a_j\beta]$, the first commutator in (16). Since $d_i \in \mathcal{N}_i$ and $a_j\beta \in \phi_{\omega(j)}$, it follows by the filter properties that

$$[d_i, a_j\beta] \in \langle \partial\phi_{t+\omega(j)} \mid t \in \mathtt{J}_i\rangle \leq \langle \partial\phi_t \mid t \in \mathtt{J}_{ij}\rangle = \mathcal{N}_{ij}.$$

Similarly $[a_i\beta, d_j] \in \mathcal{N}_{ij}$. Thus, modulo $\mathcal{N}_{ij}$, the expression in (16) is equivalent to

$$[a_i\beta, a_j\beta]\left((a_1b_1c_1d_1)^{e_1}\cdots(a_nb_nc_nd_n)^{e_n}\right)^{-1}. \tag{17}$$

By the filter properties, if $e_k \neq 0$, then $a_k \in \phi_{\omega(i)+\omega(j)}$. Therefore, $b_k \in \phi_{\omega(i)+\omega(j)+s}$, $c_k \in \partial\phi_{\omega(i)+\omega(j)+s}$, and $d_k \in \mathcal{N}_{ij}$, provided $e_k \neq 0$. Hence, the expression in (17) is equivalent, modulo $\mathcal{N}_{ij}$, to

$$[a_i\beta, a_j\beta]\left((a_1b_1c_1)^{e_1}\cdots(a_nb_nc_n)^{e_n}\right)^{-1} \equiv [a_i\beta, a_j\beta]\left([a_i, a_j]^{-1}\beta\right) \equiv 0.$$

Therefore, the lemma follows. □

We summarize we what have done so far. If λ is a lift of $\delta \in D_s$, then we assume that $R_{ij}\lambda\pi \in \partial\phi_{\omega(i)+\omega(j)+s}$ by Proposition 8.2.2. Note that if λ does not satify this condition, then there is no automorphism contained in $\partial\Delta\phi_0$ that induces the derivation δ. The lift λ induces a bijection $\alpha : G \to G$ where $a_i\alpha = x_i\lambda\pi$ and extended to the unique normal word. From Lemma 8.2.5, there exists linear equations in $L(\phi)$ whose solutions yield functions

$\alpha' : G \to G$ such that for all $i, j \in \{1, \dots, n\}$,

$$[a_i\alpha', a_j\alpha'] \left([a_i, a_j]^{-1}\alpha'\right) \in \mathcal{N}_{ij}.$$

Of course, if the linear system is inconsistent, then λ does not induce a homomorphism of G, and we move onto other derivations. Lemma 8.2.5 is just the base case of the main algorithm. Next, we generalize Lemma 8.2.5 with Proposition 8.2.7, which allows for a recursive algorithm.

Now we work to generalize Lemma 8.2.5. All of this continues to greatly depend on Proposition 5.0.6: for all $u \in M$ there exists $I_u \subseteq \mathcal{I} = \{v \in M \mid \phi_v \neq \partial\phi_v\}$ such that $\partial\phi_u = \langle \phi_v \mid v \in I_u \rangle$. Since $\mathcal{N}_{ij} = \langle \partial\phi_t \mid t \in \mathtt{J}_{ij} \rangle$, for each $t \in \mathtt{J}_{ij}$, there exists $I_t \subseteq \mathcal{I}$ such that $\partial\phi_t = \langle \phi_u \mid u \in I_t \rangle$. Therefore,

$$\mathcal{N}_{ij} = \langle \phi_u \mid u \in I_t, t \in \mathtt{J}_{ij} \rangle .$$

Set $\mathtt{J}_{ij}^2 \subset M$ such that $\mathcal{N}_{ij} = \left\langle \phi_u \mid u \in \mathtt{J}_{ij}^2 \right\rangle$ and for all $u, v \in \mathtt{J}_{ij}^2$, $\phi_u \parallel \phi_v$. Similarly, do this for each $\mathcal{N}_i$, so there exists $\mathtt{J}_i^2$ such that $\mathcal{N}_i = \langle \phi_u \mid u \in \mathtt{J}_i^2 \rangle$. Thus, for each $i, j \in \{1, \dots, n\}$ define

$$\mathcal{N}_i^2 = \left\langle \partial\phi_u \mid u \in \mathtt{J}_i^2 \right\rangle \qquad\qquad \mathcal{N}_{ij}^2 = \left\langle \partial\phi_u \mid u \in \mathtt{J}_{ij}^2 \right\rangle .$$

If we continue this we get series for each $i \in \{1, \dots, n\}$

$$\mathcal{N}_i = \mathcal{N}_i^1 > \mathcal{N}_i^2 > \cdots > \mathcal{N}_i^k = 1,$$

and for each pair $i, j \in \{1, \ldots, n\}$

$$\mathcal{N}_{ij} = \mathcal{N}_{ij}^1 > \mathcal{N}_{ij}^2 > \cdots > \mathcal{N}_{ij}^\ell = 1.$$

To have consistent notation, for each $i, j \in \{1, \ldots, n\}$ set $\mathcal{N}_i^0 = \partial\phi_{\omega(i)+s}$ and $\mathcal{N}_{ij}^0 = \partial\phi_{\omega(i)+\omega(j)+s}$. This enables us to generalize Lemma 8.2.5 with the following proposition, but before we state it, we summarize the notation.

Notation 8.2.6. For each $i, j \in \{1, \ldots, n\}$ and for $k \geq 0$ define the following. Recall that $\mathcal{I} = \{s \in M \mid \phi_s \neq \partial\phi_s\}$. Let $\mathcal{N}_i^0 = \partial\phi_{\omega(i)+s}$ and $\mathcal{N}_{ij}^0 = \partial\phi_{\omega(i)+\omega(j)+s}$.

(1) $\mathsf{J}_i^k \subseteq \mathcal{I}$ such that $\mathcal{N}_i^{k-1} = \left\langle \phi_t \mid t \in \mathsf{J}_i^k \right\rangle$.

(2) $\mathsf{J}_{ij}^k \subseteq \mathcal{I}$ such that $\mathcal{N}_{ij}^{k-1} = \left\langle \phi_t \mid t \in \mathsf{J}_{ij}^k \right\rangle$.

(3) $\mathcal{N}_i^k = \left\langle \partial\phi_t \mid t \in \mathsf{J}_i^k \right\rangle$.

(4) $\mathcal{N}_{ij}^k = \left\langle \partial\phi_t \mid t \in \mathsf{J}_{ij}^k \right\rangle$.

Similar to Lemma 8.2.5, the proof of the next proposition is technical. The basic idea is, given $\alpha : a_i \mapsto a_i b_i$, we correct α recursively by solving linear systems. The following proposition is the induction step and Lemma 8.2.5 is the base case.

Proposition 8.2.7. *With the established notation, assume $k \geq 1$ and $\alpha : G \to G$ such that for all $i, j \in \{1, \ldots, n\}$,*

$$[a_i\alpha, a_j\alpha]\left([a_i, a_j]^{-1}\alpha\right) \in \mathcal{N}_{ij}^{k-1}.$$

Let $\beta : G \to G$ such that for each i there exists $c_i \in \langle \phi_t \mid t \in J_i^k \rangle$ such that $a_i \mapsto a_i b_i c_i$. For all i, j, there exists solutions $\overline{x}_\ell \in \bigoplus_{t \in \mathsf{J}_\ell^k} L_t(\phi)$ to the equations

$$[a_ib_ix_i, a_jb_jx_j]\left((a_1b_1x_1)^{e_1} \cdots (a_nb_nx_n)^{e_n}\right)^{-1} \equiv 0 \mod \mathcal{N}_{ij}^k$$

if, and only if, for all $i, j \in \{1, \dots, n\}$,

$$[a_i\beta, a_j\beta]\left(a_1^{e_1}\cdots a_n^{e_n}\right)^{-1}\beta \in \mathcal{N}_{ij}^k,$$

where $[a_i, a_j] = a_1^{e_1}\cdots a_n^{e_n}$, for some $0 \le e_\ell < p$.

Proof. We prove this by induction, where the base case $k = 1$ is handled by Lemma 8.2.5, and therefore, we assume it holds for $k-1$. Much of what is left to do comes straight from Lemma 8.2.5. Using the same reasoning we verify that, when $d_\ell \in \mathcal{N}_\ell^k$,

$$[d_i, a_j\beta][a_i\beta, a_j\beta][a_i\beta, d_j]\left((a_1b_1c_1d_1)^{e_1}\cdots(a_nb_nc_nd_n)^{e_n}\right)^{-1} \in \mathcal{N}_{ij}^k. \tag{18}$$

Our first task is to show that $[\mathcal{N}_i^k, \phi_{\omega(j)}] \le \mathcal{N}_{ij}^k$. By induction, $[\mathcal{N}_i^{k-1}, \phi_{\omega(j)}] \le \mathcal{N}_{ij}^{k-1}$. For $u \in J_i^{k-1}$, $\partial\phi_u \le \mathcal{N}_i^{k-1}$. There exists $I_u \subseteq \mathcal{I}$ such that $\partial\phi_u = \langle \phi_v \mid v \in I_u\rangle$. Therefore, $\langle \partial\phi_v \mid v \in I_u\rangle \le \mathcal{N}_i^k$. By induction, for all $v \in I_u$, $[\phi_v, \phi_{\omega(j)}] \le \mathcal{N}_{ij}^{k-1}$. Since $\phi_v \ne \partial\phi_v$, it follows then that $[\partial\phi_v, \phi_{\omega(j)}] \le \mathcal{N}_{ij}^k$. Hence, $[\mathcal{N}_i^k, \phi_{\omega(j)}] \le \mathcal{N}_{ij}^k$. Therefore,

$$[d_i, a_j\beta] \in [\mathcal{N}_i^k, \phi_{\omega(j)}] \le \mathcal{N}_{ij}^k \qquad\qquad [a_i\beta, d_j] \in [\phi_{\omega(i)}, \mathcal{N}_j^k] \le \mathcal{N}_{ij}^k,$$

and the expression in (18) is equivalent to

$$[a_i\beta, a_j\beta]\left((a_1b_1c_1d_1)^{e_1}\cdots(a_nb_nc_nd_n)^{e_n}\right)^{-1} \in \mathcal{N}_{ij}^k. \tag{19}$$

Now we show that if $e_\ell \ne 0$, then $\mathcal{N}_\ell^k \le \mathcal{N}_{ij}^k$. By induction suppose that $e_\ell \ne 0$ implies $\mathcal{N}_\ell^{k-1} \le \mathcal{N}_{ij}^{k-1}$. In other words, for all $u \in J_\ell^{k-1}$, $\partial\phi_u \le \mathcal{N}_{ij}^{k-1}$. By Proposition 5.0.6, there exists $I_u \subseteq \mathcal{I}$ such that $\partial\phi_u = \langle \phi_v \mid v \in I_u\rangle$. Thus, $\phi_v \le \partial\phi_u \le \mathcal{N}_{ij}^{k-1} = \langle \partial\phi_w \mid w \in \mathsf{J}_{ij}^{k-1}\rangle = \langle \phi_w \mid w \in \mathsf{J}_{ij}^k\rangle$, or more simply, for all $v \in I_u$, $\phi_v \le \langle \phi_w \mid w \in \mathsf{J}_{ij}^k\rangle$. Therefore,

$\partial\phi_v \leq \langle \partial\phi_w \mid w \in \mathtt{J}_{ij}^k \rangle = \mathcal{N}_{ij}^k$. It follows then that $e_\ell \neq 0$ implies $\mathcal{N}_\ell^k \leq \mathcal{N}_{ij}^k$, and thus the expression in (19) is equivalent to

$$[a_i\beta, a_j\beta]\left([a_i, a_j]^{-1}\beta\right) \equiv 0 \mod \mathcal{N}_{ij}^k. \qquad \square$$

Recall that we assume that $|G| = p^n$ and that G has exponent p. Assume $\phi : M \to 2^G$ is a filter and $X \subset G$ is faithfully filtered by ϕ. We use Proposition 8.2.7 to construct the following algorithm. Using Notation 8.2.6 we prove the following theorem.

THEOREM 8.2.8. *There exists a polynomial-time algorithm that, given $\alpha : G \to G$ such that for all $1 \leq i < j \leq n$,*

$$[a_i\alpha, a_j\alpha]\left([a_i, a_j]^{-1}\alpha\right) \in \mathcal{N}_{ij}^k,$$

returns a set of functions A such that for all $\beta \in A$ and for all $i, j, \ell \in \{1, \dots, n\}$

1. $a_\ell\alpha \equiv a_\ell\beta \mod \mathcal{N}_\ell^k$ *and*
2. $[a_i\beta, a_j\beta]\,([a_i, a_j]^{-1}\beta) \in \mathcal{N}_{ij}^{k+1}$.

If ω is the exponent of matrix multiplication, then the algorithm uses $O(\log^{3\omega}|G|)$ basic operations in $\mathbb{F}_p$.

PROOF. *Algorithm.* For each $1 \leq i < j \leq n$, solve the system of equations

$$[a_i\alpha, a_j\alpha]\left([a_i, a_j]^{-1}\alpha\right) \equiv 0 \mod \mathcal{N}_{ij}^{k+1}.$$

If no solution exists return false. Otherwise, for all solutions $\bar{c}_\ell$, for $1 \leq \ell \leq n$, choose a representative c_ℓ and define a function $\beta : G \to G$ such that $a_\ell \mapsto (a_\ell\alpha)c_\ell$. Return the (possibly empty) set of such functions.

Correctness. Apply Proposition 8.2.7.

Timing. Let $n = \log|G|$. There are $\binom{n}{2}$ linear equations of the form

$$[(a_i\alpha)x_i, (a_j\alpha)x_j]\left((a_1\alpha\ x_1)^{e_1}\cdots(a_n\alpha\ x_n)^{e_n}\right)^{-1} \equiv 0.$$

Applying commutator identities yields an equivalent equation

$$\overline{[x_i, a_j\alpha]} + \overline{[a_i\alpha, x_j]} + \overline{[a_i\alpha, a_j\alpha]\left((a_1\alpha\ x_1)^{e_1}\cdots(a_n\alpha\ x_n)^{e_n}\right)^{-1}} \equiv 0.$$

For each i, j there are $O(n)$ equations because of terms of the form $\overline{[x_i, a_j\alpha]}$. Therefore, there are $O\left(n\binom{n}{2}\right)$ equations and $O(n)$ variables. □

Remark 8.2.9. It is not yet known if there is a recursive version of Theorem 8.2.8 where only one β needs to be selected (or even if a subset of $O(\log|A|)$ functions need to be selected). If this is the case, then there would exist a polynomial-time algorithm that, given $\delta \in D_s/\partial D_s$, returns an automorphism induced by δ or returns `false` if none exist. Since there are $O(\log|G|)$ iterations, such an algorithm would use $O(\log^{3\omega+1}|G|)$ basic operations in $\mathbb{F}_p$, assuming there is an efficient way to choose β.

8.3. Proof of Theorem A

We provide an algorithm to construct $\partial\Delta\phi_0$ from ∂D_0. First, we detail an algorithm to construct $\Delta\phi_s$ given $s \neq 0$ and $D_s/\partial D_s$ called DerToAut. We define a function InducedMap(δ, s) which constructs a lift $\lambda \in \mathrm{End}(F)$ for a derivation $\delta \in D_s$ and then returns an induced map $\alpha : G \to G$. Furthermore, we denote the algorithm of Theorem 8.2.8 with LinearCorrect(α, s, k), where α, s, and k have the same roles as Theorem 8.2.8. We provide pseudo-code for this algorithm because it is fairly complex, but the spirit of the algorithm is just recursion.

Algorithm 1 Derivations to automorphisms

```
function DerToAut($s, D_s/\partial D_s$)
    $A = \emptyset$; $k = 0$;
    for $\delta \in D_s/\partial D_s$ do
        $\beta =$ InducedMap($\delta, s$); $A_k = \{\beta\}$;
        while ($|A_k| > 0$) and ($\forall \alpha \in A_k$, not IsEndomorphism($G, \alpha$)) do
            $A_{k+1} = \emptyset$;
            for $\alpha \in A_k$ do
                $A_{k+1} = A_{k+1} \cup$ LinearCorrect($\alpha, s, k$);
            end for
            $k = k + 1$;
        end while
        if ($|A_{k-1}| > 0$) and ($\exists \alpha \in A_k$, IsEndomorphism($G, \alpha$)) then
            $A = A \cup \{\alpha\}$;
        end if
    end for
    return $A$;
end function
```

Using the current algorithms, constructing automorphisms from derivations, requires a purely sequencial approach. Let $N_0 = \partial\phi_0$ and $I_0 \subseteq \mathcal{I} = \{s \in M \mid \phi_s \neq \partial\phi_s\}$ where $N_0 = \langle \phi_s \mid s \in I \rangle$ and for all $s \in I_0$, $N_0 \neq \langle \phi_t \mid t \in I_0 - s \rangle$. Now recursively define $N_{k+1} = \langle \partial\phi_s \mid s \in I_k \rangle$ and $I_{k+1} \subseteq \mathcal{I}$ such that $N_{k+1} = \langle \phi_s \mid s \in I_{k+1} \rangle$ where for all $s \in I_{k+1}$, $N_{k+1} \neq \langle \phi_t \mid t \in I_{k+1} - s \rangle$. For $s \in M$, let $\mathrm{T}(s, D_s/\partial D_s)$ denote the timing of $\textsc{DerToAut}(s, D_s/\partial D_s)$. Tradionally, constructing generators for $\partial\Delta\phi_0$ is done in time

$$O\left(\prod_{j=0}^{k} \prod_{s \in I_j} \mathrm{T}(s, D_s/\partial D_s)\right),$$

assuming $N_k \neq 1$ and $N_{k+1} = 1$. Without Theorem D, the complexity of Theorem 8.3.1 would be

$$O\left(\sum_{j=0}^{k} \prod_{s \in I_j} \mathrm{T}(s, D_s/\partial D_s)\right).$$

In the following theorem, we prove that the cost of lifting each $D_s/\partial D_s$, for each $s \in I_j$, is only additive in cost—not multiplicative.

THEOREM 8.3.1. *Using the established notation, there exists an algorithm that, given a characteristic filter $\phi : M \to 2^G$ and $X \subseteq G$ faithfully filtered by ϕ, returns generators for $\partial\Delta\phi_0$ using $O(\log|G|)$ processors. This is done in time*

$$O\left(\sum_{j=0}^{k}\sum_{s\in I_j} \mathrm{T}(s, D_s/\partial D_s)\right) = O\left(\sum_{s\in I_0} \mathrm{T}(s, D_s/\partial D_s)\right).$$

PROOF. *Algorithm.* Construct $\partial\phi : M \to 2^G$ and $L = L(\phi)$. Construct a basis for ∂D_0. For each $j \in \{0, \dots, k\}$, determine $I_j \subseteq \mathcal{I}$ such that $N_j = \langle \phi_s \mid s \in I_j\rangle$ where for all $s \in I_j$, $N_j \neq \langle \phi_t \mid t \in I_j - s\rangle$. For each $j \in \{0, \dots, k\}$ and for each $s \in I_j$, run DERTOAUT$(s, D_s/\partial D_s)$ in parallel.

Correctness. We have the following series

$$\partial\phi_0 = N_0 = \langle \phi_s \mid s \in I_0\rangle > \langle \partial\phi_s \mid s \in I_0\rangle = \langle \phi_s \mid s \in I_1\rangle = N_1.$$

This continues until $N_k = \langle \phi_s \mid s \in I_k\rangle = 1$. By Proposition 6.3.5,

$$N_j/N_{j+1} \cong \bigoplus_{s\in I_j} L_s(\phi),$$

and by Theorem 6.3.2,

$$\langle \Delta\phi_s \mid s \in I_j\rangle / \langle \partial\Delta\phi_s \mid s \in I_j\rangle \cong \bigoplus_{s\in I_j} L_s(\Delta\phi). \tag{20}$$

Applying $\mathcal{D}$ to (20) yields $\bigoplus_{s\in I_j} D_s/\partial D_s$. Therefore, running DERTOAUT for each $s \in I_j$ in parallel will return generators for the quotient in (20).

Because DerToAut is based on *correcting* bijections $\alpha : G \to G$, applying DerToAut to factors like

$$\bigoplus_{s\in I_j} D_s/\partial D_s \tag{21}$$

will not influence the outcome of other factors (for different j-values). Hence, for each $j \in \{0, \ldots, k\}$, we can parallelize the factors in (21).

It follows from a corollary of Theorem 6.0.4, that $|\operatorname{im}(\phi)| \leq \log |G|$. Since

$$\partial D_0 = \bigoplus_{j=0}^{k} \bigoplus_{s\in I_j} D_s/\partial D_s,$$

it follows that there $O(\log |G|)$ nontrivial factors of the form $D_s/\partial D_s$, where $s \neq 0$.

Timing. The computational complexity of lifting derivations $\delta \in D_s$, where $s \in I_0$, is more expensive than for derivations in D_t, where $t \in I_j$ and $j > 0$. Therefore, the computational complexity of the algorithm is

$$O\left(\sum_{j=0}^{k}\sum_{s\in I_j} \mathrm{T}(D_s/\partial D_s)\right) = O\left(\sum_{s\in I_0} \mathrm{T}(D_s/\partial D_s)\right). \qquad \square$$

Theorem 8.3.1 can be adapted to construct generators for $\Delta\phi_0$ as well. First we set up some notation. Let $\mathcal{E}$ be the orthogonal frame with respect to the direct decomposition decomposition of L, see Section 8.1. Set

$$\mathrm{Aut}_0(L) = \left\{ \sum_{e\in\mathcal{E}} e\alpha e \;\middle|\; \alpha \in \mathrm{Aut}(L) \right\}.$$

In the next lemma, we show that $\mathrm{Aut}_0(L)$ is a subgroup of $\mathrm{Aut}(L)$.

Lemma 8.3.2. $\mathrm{Aut}_0(L) \leq \mathrm{Aut}(L)$.

Proof. We only need to prove that for $\alpha_0 \in \mathrm{Aut}_0(L)$ for all $x \in L_s$ and $y \in L_t$, $[x\alpha_0, y\alpha_0] = [x, y]\alpha_0$. Let $\alpha \in \mathrm{Aut}(L)$. Let $x_s \in L_s$ and $x_\partial \in \bigoplus_{u \neq 0} L_{s+u}$ such that $x\alpha = x_s + x_\partial$. Define y_t and y_∂ similarly: $y\alpha = y_t + y_\partial$. Set $\alpha_0 = \sum_{e \in \mathcal{E}} e\alpha e$, so

$$\begin{aligned}
[x, y]\alpha_0 &= [x, y](e_{s+t}\alpha e_{s+t}) \\
&= [x_s + x_\partial, y_t + y_\partial]e_{s+t} \\
&= [x(e_s\alpha e_s), y(e_t\alpha e_t)] \\
&= [x\alpha_0, y\alpha_0].
\end{aligned}$$

□

Let $\mathrm{Aut}_\partial(L) = \{\alpha \in \mathrm{Aut}(L) \mid \forall s \in M, \alpha|_{L_s} = 1\}$. By Lemma 8.3.2, the following is a split exact sequence

$$1 \longrightarrow \mathrm{Aut}_\partial(L) \longrightarrow \mathrm{Aut}(L) \longrightarrow \mathrm{Aut}_0(L) \longrightarrow 1,$$

where the homomorphism $\mathrm{Aut}(L) \to \mathrm{Aut}_0(L)$ maps α to $\sum_{e \in \mathcal{E}} e\alpha e$. Therefore, $\mathrm{Aut}(L) = \mathrm{Aut}_\partial(L) \rtimes \mathrm{Aut}_0(L)$. Note that $\alpha \in \mathrm{Aut}_\partial(L)$ induces a derivation of L via $x \mapsto x\alpha - x$.

Remark 8.3.3. None of the proofs of Lemma 8.2.5, Proposition 8.2.7, or Theorems 8.2.8 and 8.3.1 required s to be nonzero, other than the fact that the subgroup of automorphisms of G that induce a derivation on $L(\phi)$ is exactly $\partial\Delta\phi_0$. Therefore, the proofs can easily be adapted for $s = 0$. Thus, Theorem 8.2.8 applies to bijections $\alpha : G \to G$ coming from $\mathrm{Aut}_0(L)$, and hence Theorem 8.3.1 can be adapted, given $\mathrm{Aut}_0(L)$. Of course, the real issue at hand here is *computing* $\mathrm{Aut}_0(L)$.

With this, we can construct $\mathrm{Aut}(G)$ using Theorem 8.3.1 and Lemma 8.3.2. If we do not have $\mathrm{Aut}_0(L)$, then we instead default to $\bigoplus_{s \in M} \mathrm{GL}(d_s, p)$, where $d_s = \dim_{\mathbb{Z}_p}(L_s)$. Therefore, given $\phi : M \to 2^G$ and X faithfully filtered by ϕ, we construct $\bigoplus_{s\in M} \mathrm{GL}(d_s, p)$ and ∂D_0 and apply Theorem 8.3.1 to both in parallel, which proves Theorem A.

Chapter 9

FUTURE WORK AND QUESTIONS

There are many directions to go from the work here. One major direction is to develop efficient algorithms for constructing filters with the various properties from Sections 4–6. It seems unlikely that there exists an efficient algorithm to produce a faithful filter from a given arbitrary filter. If there was, then computing the intersection of normal subgroups would be Turing reducible to such an algorithm. We explicitly state a few questions in computational directions.

Question 1. *Is there an polynomial-time algorithm that returns a filter with no inert subgroups, given a filter $\phi : M \to 2^G$ for a nilpotent group G?*

In order to address Question 1, it seems as though a polynomial-time algorithm for closures of prefilters is required. On the other hand, a polynomial-time algorithm for closures is certainly essential for efficiently refining filters, so it is of interest on its own.

Question 2. *Is there an algorithm that, given a prefilter π, returns $\overline{\pi}$ in polynomial time?*

An answer to Question 2 has applications to computing automorphism groups, but as we have seen the definition of a filter is not very restrictive. In [21], we give an affirmative answer in the case when the monoid is totally-ordered. Currently it seems that all prefilters come from refining a filter. Of course, we should not limit ourselves only to this case, but presumably Question 2 becomes easier when there exists $X \subseteq G$ for the filter we are refining. Does there exist such an algorithm for prefilters in this case?

It seems like there is an efficient algorithm that *decides* if, for a given filter $\phi : M \to 2^G$, there exists $X \subseteq G$ that is faithfully filtered by ϕ. By Theorem 6.0.3, it seems sufficient to test if a pre-image of a graded basis is faithfully filtered. However, it is not known if there is an efficient algorithm that returns a filter ϕ' and a set X faithfully filtered by ϕ', given a filter ϕ, even in favorable conditions.

Definition 9.0.1. *A filter $\rho : M' \to 2^G$* refines *a filter $\phi : M \to 2^G$ if for all $s \in M'$, there exists $t \in M$ such that $\partial\phi_t \leq \rho_s \leq \phi_t$.*

For the next question, suppose $\phi : M \to 2^G$ is a filter where L_s is elementary abelian for all $s \neq 0$, and in addition, there exists $X_\phi \subseteq G$ that is faithfully filter by ϕ. If G is a p-group, the lower exponent-p series is one example $\eta : \mathbb{N} \to 2^G$.

Question 3. *If $\rho : M' \to 2^G$ refines ϕ, then does there exist a polynomial-time algorithm that returns X_ρ that is faithfully filtered by ρ?*

Asserting that ρ refines ϕ means that intersections between ρ_s and ρ_t can be computed in polynomial time. Thus, when ρ is faithful, it seems that such an X_ρ can be efficiently computed. It may be the case that ρ is not faithful to begin with, and in this case can an optimal compromise be obtained? Presently, such a compromise is not well-defined and may never be. Regardless, if ρ is not faithful there seems to be two methods to fix this issue: (1) refine ρ by including appropriate intersections and (2) remove problematic subgroups. Are there general ways to address these two procedures?

Now we change directions to the graded derivation ring $D = \mathrm{Der}(L(\phi))$. In Theorem 8.1.4, we prove that we can efficiently construct

$$0 \longrightarrow \partial D_0 \longrightarrow D \xrightarrow{\mathcal{P}} D/\partial D_0 \longrightarrow 0.$$

Therefore,

$$0 \longrightarrow L(\Delta\phi) \xrightarrow{\mathcal{D}} D \xrightarrow{\mathcal{P}} D/\partial D_0 \longrightarrow 0 \tag{22}$$

is a chain complex of Lie rings, c.f. Proposition 8.1.3. Our main question concerns the homology of the chain complex in (22).

QUESTION 4. *Can* $\mathrm{im}(\mathcal{D})$ *be computed efficiently?*

A necessary condition for efficiently constructing automorphisms from derivations of $L(\phi)$ is to compute $\mathrm{im}(\mathcal{D})$ efficiently. If such an algorithm exists, then Theorem 8.3.1 can be altered slightly for an exponential speed-up. Indeed, instead of searching through all of $D_s/\partial D_s$, we need to only consider a basis of an appropriate space inside $\mathrm{im}(\mathcal{D})$. This is not enough to make Theorem 8.3.1 into an efficient algorithm, at least not in its current state.

Related to Theorem 8.3.1 is Remark 8.2.9. The algorithm of Theorem 8.2.8 returns a set of bijections A that have been corrected one step, given some bijection $\alpha : G \to G$.

QUESTION 5. *Does there exists a computable subset* $B \subset A$ *such that*

(1) *B can be computed efficiently,*

(2) $|B| \in O(1)$ *(or even* $|B| \in O(\log |A|)$*), and*

(3) *B has the property that α can be corrected to an automorphism of G if, and only if, there exists $\beta \in B$ that can be corrected to an automorphism of G?*

As mentioned in Remark 8.2.9, this would imply that there is an efficient algorithm to construct an automorphism of G from a derivation of $L(\phi)$. Maybe a more realistic question is if B is a random subset of A with $|B| \in O(\log |A|)$, does B satisfy the properties of Question 5 with high probability? Affirmative answers to Questions 4 and 5 would imply that there exists an efficient algorithm to construct $\partial\Delta\phi_0$ given a filter $\phi : M \to 2^G$ and a set X faithfully filtered by ϕ.

We end with a more open-ended question about filters with respect to computing automorphism groups: what other kinds of parallel algorithms exist to construct (or aid in the construction of) automorphisms?

Bibliography

[1] László Babai. Graph isomorphism in quasipolynomial time. `arXiv:1512.03547`.

[2] László Babai, Paolo Codenotti, Joshua A Grochow, and Youming Qiao. Code equivalence and group isomorphism. In *Proceedings of the twenty-second annual ACM-SIAM symposium on Discrete Algorithms*, pages 1395–1408. Society for Industrial and Applied Mathematics, 2011.

[3] László Babai, Paolo Codenotti, and Youming Qiao. Polynomial-time isomorphism test for groups with no abelian normal subgroups. *Automata, Languages, and Programming*, pages 51–62, 2012.

[4] Hans Ulrich Besche, Bettina Eick, and E. A. O'Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.*, 12(5):623–644, 2002.

[5] Simon R. Blackburn. Groups of prime power order with derived subgroup of prime order. *J. Algebra*, 219(2):625–657, 1999.

[6] T. S. Blyth. *Lattices and ordered algebraic structures.* Universitext. Springer-Verlag London, Ltd., London, 2005.

[7] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[8] Peter A. Brooksbank, Joshua Maglione, and James B. Wilson. A fast isomorphism test for groups whose Lie algebra has genus 2. *J. Algebra*, 473:545–590, 2017.

[9] Peter A. Brooksbank and James B. Wilson. Computing isometry groups of Hermitian maps. *Trans. Amer. Math. Soc.*, 364(4):1975–1996, 2012.

[10] John J. Cannon, Bettina Eick, and Charles R. Leedham-Green. Special polycyclic generating sequences for finite soluble groups. *J. Symbolic Comput.*, 38(5):1445–1460, 2004.

[11] John J. Cannon and Derek F. Holt. Automorphism group computation and isomorphism testing in finite groups. *J. Symbolic Comput.*, 35(3):241–267, 2003.

[12] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[13] Bettina Eick, C. R. Leedham-Green, and E. A. O'Brien. Constructing automorphism groups of p-groups. *Comm. Algebra*, 30(5):2271–2295, 2002.

[14] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.8.7*, 2017.

[15] Daniel Gorenstein, Richard Lyons, and Ronald Solomon. *The classification of the finite simple groups*, volume 40 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1994.

[16] P. A. Grillet. *Commutative semigroups*, volume 2 of *Advances in Mathematics (Dordrecht)*. Kluwer Academic Publishers, Dordrecht, 2001.

[17] George Havas and M. F. Newman. Application of computers to questions like those of Burnside. In *Burnside groups (Proc. Workshop, Univ. Bielefeld, Bielefeld, 1977)*, volume 806 of *Lecture Notes in Math.*, pages 211–230. Springer, Berlin, 1980.

[18] Michel Lazard. Sur les groupes nilpotents et les anneaux de Lie. *Ann. Sci. Ecole Norm. Sup. (3)*, 71:101–190, 1954.

[19] Mark L. Lewis and James B. Wilson. Isomorphism in expanding families of indistinguishable groups. *Groups Complex. Cryptol.*, 4(1):73–110, 2012.

[20] Joshua Maglione. Longer nilpotent series for classical unipotent subgroups. *J. Group Theory*, 18(4):569–585, 2015.

[21] Joshua Maglione. Efficient characteristic refinements for finite groups. *J. Symbolic Comput.*, 80(part 2):511–520, 2017.

[22] Gary L. Miller. Graph isomorphism, general remarks. *J. Comput. System Sci.*, 18(2):128–142, 1979.

[23] M. F. Newman and E. A. O'Brien. Application of computers to questions like those of Burnside. II. *Internat. J. Algebra Comput.*, 6(5):593–605, 1996.

[24] M. F. Newman, E. A. O'Brien, and M. R. Vaughan-Lee. Groups and nilpotent Lie rings whose order is the sixth power of a prime. *J. Algebra*, 278(1):383–401, 2004.

[25] E. A. O'Brien. The p-group generation algorithm. *J. Symbolic Comput.*, 9(5-6):677–698, 1990. Computational group theory, Part 1.

[26] E. A. O'Brien. Isomorphism testing for p-groups. *J. Symbolic Comput.*, 16(3):305–320, 1993.

[27] E. A. O'Brien and M. R. Vaughan-Lee. The groups with order p^7 for odd prime p. *J. Algebra*, 292(1):243–258, 2005.

[28] Derek J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.

[29] Ákos Seress. *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2003.

[30] Charles C. Sims. *Computation with finitely presented groups*, volume 48 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1994.

[31] James B. Wilson. New lie products for groups and their automorphisms. `arXiv:1501.04670`.

[32] James B. Wilson. More characteristic subgroups, Lie rings, and isomorphism tests for p-groups. *J. Group Theory*, 16(6):875–897, 2013.