THE UNIVERSITY OF CHICAGO

LAZARD CORRESPONDENCE UP TO ISOCLINISM

A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

BY
VIPUL NAIK

CHICAGO, ILLINOIS
DECEMBER 2013

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

In this thesis we generalize the Lazard correspondence, introduced by Lazard in [30], to a correspondence *up to isoclinism*. The original Lazard correspondence is a correspondence between some groups and some Lie rings. The Lazard correspondence up to isoclinism is a correspondence between some equivalence classes of groups and some equivalence classes of Lie rings, where the equivalence relation on both sides is isoclinism. By relaxing the objects on both sides of the correspondence to equivalence classes up to isoclinism, we are able to generalize the domain of the correspondence somewhat. An overview of our proof strategy is in Section 1.2, and our final results are described in Section 7.7.

A typical application of the original Lazard correspondence is the situation where, for some prime p, the group is a finite p-group of nilpotency class at most $p-1$ and the Lie ring is a finite p-Lie ring[1] of nilpotency class at most $p-1$.

A typical application of the generalization we describe is the situation where the group is a finite p-group of nilpotency class at most p and the Lie ring is a finite p-Lie ring of nilpotency class at most p. Knowledge of either (the group or the Lie ring) determines the other only up to isoclinism and not up to isomorphism. Therefore, this correspondence is suited only for the study of attributes (of groups or Lie rings) that are invariant under isoclinism.

In cases where the original Lazard correspondence applies, it refines the Lazard correspondence up to isoclinism: if a group and Lie ring are in Lazard correspondence, then they are also in Lazard correspondence up to isoclinism. The interesting case covered by our correspondence is the case of finite p-groups of nilpotency class exactly p and finite p-Lie rings of nilpotency class exactly p. The original Lazard correspondence no longer applies in this situation,[2] so our generalization adds value.

1. This means that the additive group of the Lie ring is a finite p-group. In other words, the Lie ring is a Lie algebra over $\mathbb{Z}/p^k\mathbb{Z}$ for some positive integer k.

2. There is a subtle distinction between the global and the 3-local Lazard correspondence that we omit for the abstract, but describe in detail later

ACKNOWLEDGMENTS

I would like to thank George Glauberman, my research advisor, for help over many years with the research underlying this thesis and for detailed feedback on multiple drafts of the thesis. In addition I am thankful to Peter May, my second adviser, for helping me out with a number of the proofs and some of the underlying concepts. I would also like to thank Professor Jonathan Alperin, who provided help in person, via email, and by lending books and resources. In addition, I am grateful to Shmuel Weinberger, the Department Chair, and Laurie Wail, the Graduate Student Administrator, for being very accommodating in helping me finish my thesis and arranging for financial support.

I am grateful to many mathematicians, both within and outside the University of Chicago, for answering my many queries related to group theory and mathematics. A partial list includes Max Horn of Justus Liebig University Giessen, I. Martin Isaacs of the University of Wisconsin-Madison, Ronald Solomon of Ohio State University, and Justin Lynd, an assistant professor at Rutgers University. I am thankful to Anton Geraschenko and StackExchange for collaborating to create the mathematics question-and-answer website MathOverflow,[3] and to the numerous mathematicians who volunteered their time to answering questions of mine on MathOverflow, some of which have influenced proofs that appear in this thesis. In addition, I am grateful to the creators of GAP[4] for providing a software that around with and better understand groups, which are the central actors of my thesis.

I would also like to thank John Wiltshire-Gordon, who, while an undergraduate at the University of Chicago, worked with me on related problems. Some of the work we did together was the basis of Section 5.4.

I also greatly enjoyed and benefited from reading the work of the many mathematicians who are cited in this thesis, including Baer, Lazard, Hall and Senior, Isaacs, Glauberman, Ellis, Khukhro, and many others listed in the bibliography.

3. http://www.mathoverflow.net

4. Full list of authors at http://www.gap-system.org/Contacts/People/authors.html

CHAPTER 1

INTRODUCTION, OUTLINE, AND PRELIMINARIES

Background and notation

1.0.1 Background assumed

This document assumes that the reader is comfortable with group theory at an advanced undergraduate or beginning graduate student level. At minimum, the reader's knowledge should be approximately equivalent to the first six chapters of [10]. A knowledge of the material in [43] would make the document easy reading. There will be particular emphasis on knowledge of the structure of p-groups and nilpotent groups, including knowledge of the interplay between the upper central series and lower central series. A review of the most important definitions and basic results is available in the Appendix, Section A.3.1.

Rudimentary familiarity with the ideas of universal algebra and category theory will be helpful in understanding the motivating ideas. A review of the most important ideas is available in the Appendix, Sections A.2.1 and A.2.4.

It is assumed that the reader is familiar with the idea of Lie rings, which can be viewed as Lie algebras over $\mathbb{Z}$, the ring of integers. However, familiarity with Lie *algebras* over the real numbers or complex numbers will also be sufficient. A review of some basic definitions from the theory of Lie rings can be found in the Appendix, Section A.1.4.

1.0.2 Group and subgroup notation

Let G be a group. We will use the following notation throughout this document.

- We will use 1 to denote the trivial subgroup of G. Note that the same letter 1 will be used to denote both the trivial group as an abstract group and the trivial subgroup in all groups.

- We will also use 1 to denote the identity element of G.

- When working with groups that are known to be abelian groups, we will use additive notation: 0 to denote the trivial group and $+$ to denote the group operation. However, we will use multiplicative notation when dealing with abelian subgroups inside a (possibly) non-abelian group.

- $H \leq G$ will be understood to mean that H is a sub*group* of G.

- $Z(G)$ will refer to the center of G.

- G' and $[G, G]$ both refer to the derived subgroup of G.

- $\gamma_c(G)$ refers to the c^{th} member of the lower central series of G, given as follows: $\gamma_1(G) = G$, $\gamma_2(G) = G'$, and $\gamma_{i+1}(G) = [G, \gamma_i(G)]$.

- $Z^c(G)$ refers to the c^{th} member of the upper central series of G, given as follows: $Z^0(G)$ is the trivial subgroup, $Z^1(G) = Z(G)$, and $Z^{i+1}(G)/Z^i(G) = Z(G/Z^i(G))$ for $i \geq 1$.

- $G^{(i)}$ denotes the i^{th} member of the derived series of G, given by $G^{(0)} = G$, $G^{(1)} = G'$, and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$.

- $\mathrm{Inn}(G)$ is the inner automorphism group of G. It is canonically isomorphic to the quotient group $G/Z(G)$, and we will often abuse notation by treating $\mathrm{Inn}(G)$ as set-theoretically identical with $G/Z(G)$.

- $\mathrm{Aut}(G)$ is the automorphism group of G. We treat $\mathrm{Inn}(G)$ naturally as a subgroup of $\mathrm{Aut}(G)$. In fact, $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

- $\mathrm{End}(G)$ is the endomorphism *monoid* of G, i.e., the set of endomorphisms of G with the monoid structure given by composition.

1.0.3 Lie ring and subring notation

Let L be a Lie ring, i.e., a Lie algebra over $\mathbb{Z}$, the ring of integers. We will use the following notation throughout this document.

- We will use 0 to denote the zero subring of L. Note that 0 is used to describe both the abstract zero Lie ring and the zero subring in every Lie ring.
- We will also use 0 to denote the zero element of L.
- $M \leq L$ will be understood to mean that M is a Lie subring of L. This means that it is an additive subgroup of L and is closed under the Lie bracket.
- $Z(L)$ denotes the center of L, i.e., the subring of L comprising those elements whose Lie bracket with any element of L is zero.
- L' and $[L, L]$ both refer to the derived subring of L.
- $\gamma_c(L)$ refers to the c^{th} member of the lower central series of L, given as follows: $\gamma_1(L) = L$, $\gamma_2(L) = L'$, and $\gamma_{i+1}(L) = [L, \gamma_i(L)]$.
- $Z^c(L)$ refers to the c^{th} member of the upper central series of L, given as follows: $Z^0(L)$ is the trivial subring, $Z^1(L) = Z(L)$, and $Z^{i+1}(L)/Z^i(L) = Z(L/Z^i(L))$ for $i \geq 1$.
- $L^{(i)}$ denotes the i^{th} member of the derived series of L, given by $L^{(0)} = L$, $L^{(1)} = L'$, and $L^{(i+1)} = [L^{(i)}, L^{(i)}]$.
- $\text{Inn}(L)$ is the Lie ring of inner derivations of L. It is canonically isomorphic to the quotient Lie ring $L/Z(L)$, and we will often abuse notation by treating $\text{Inn}(L)$ as set-theoretically identical with $L/Z(L)$.
- $\text{Der}(L)$ is the Lie ring of all derivations of L. We treat $\text{Inn}(L)$ naturally as a Lie subring of $\text{Der}(L)$. In fact, $\text{Inn}(L)$ is an ideal in $\text{Der}(L)$.
- $\text{Aut}(L)$ is the automorphism group of L.

- $\mathrm{End}(L)$ is the endomorphism *monoid* of L considered as a Lie ring. Note that this is not necessarily closed under addition.

- $\mathrm{End}_{\mathbb{Z}}(L)$ is the endomorphism ring of the underlying additive group of L. To avoid confusion, we will explicitly specify that we are looking at all additive group endomorphisms whenever we use this notation.

1.0.4 Other conventions

We will adopt these conventions:

- As a *general* rule, when dealing with homomorphisms and other similar functions, we will apply functions on the left, in keeping with the convention used in most mathematics texts. Thus, $f \circ g$ is to be interpreted as saying that the function g is applied first and the function f is applied later.

- For the action of a group on itself, we denote by ${}^g x$ the action of g by conjugation on x as a left action, i.e., gxg^{-1}. We denote by x^g the action of g by conjugation on x as a right action, i.e., $g^{-1}xg$. When stating results whose formulation is sensitive to whether we use the left-action convention or the right-action convention, we will explicitly state the result using both conventions.

- If using the left-action convention, the group commutator $[x, y]$ is defined as $xyx^{-1}y^{-1}$. If using the right-action convention, the group commutator $[x, y]$ is defined as $x^{-1}y^{-1}xy$.

1.1 Introduction

1.1.1 The difference in tractability between groups and abelian groups

The *structure theorem for finitely generated abelian groups*, which in turn leads to a classification of all finite abelian groups, shows that the structure of *abelian* groups is fairly easy to understand and control. On the other hand, the structure of groups in general is wild. Even classifying finite groups is extremely difficult.

The difficulty is two-fold. On the one hand, the finite simple groups (which can be thought of as the building blocks of finite groups) have required a lot of effort to classify. While the original classification was believed to have been completed around 1980, some holes in parts of the proof were discovered later and it is believed that these holes were fixed only around 2004. The only finite simple abelian groups are the cyclic groups of order p. However, there are 17 infinite families and 26 sporadic groups among the finite simple non-abelian groups. For a quick background on the classification, see [2].

At the other extreme from finite simple groups are the finite p-groups. It is well known that any finite group of order p^n (for a prime p and natural number n) must be a nilpotent group and therefore it has n composition factors that are all cyclic groups of order p. In other words, there is no mystery about the building blocks of these groups. Despite this, the multiplicity of ways of putting the building blocks together makes it very difficult to obtain a concise description of all the groups of order p^n. The general consensus among people who have studied p-groups is that it is futile to even attempt to obtain a concise description of all the isomorphism types of groups of order p^n, and that it is likely that no such description exists. Rather, the goal of the study of p-groups is to identify methods that enable us to better understand the totality of p-groups, including aspects that are common to all of them and aspects that differentiate some p-groups from others. For a description of the state of knowledge regarding p-groups, see [32].[1]

This thesis is focused on one small part of the study of finite p-groups.

1.1.2 Nilpotent groups and their relation with abelian groups

A group is termed *nilpotent* if it has a central series of finite length. Nilpotent groups are considerably more diverse in nature than abelian groups, and as alluded to in the preceding

1. Although the article was published in 1999, progress has been modest since then.

section, even the finite nilpotent groups are difficult to classify.

A group is termed *solvable* if it has a normal series where all the quotient groups are abelian groups. Solvable groups are considerably more diverse than nilpotent groups.

Generally, statements that are true for abelian groups fall into one of these four classes:

1. The statement does not generalize much further from abelian groups

2. The statement generalizes all the way to nilpotent groups but not much further

3. The statement generalizes all the way to solvable groups but not much further

4. The statement generalizes to all groups, or to a fairly large class of groups

It might be worthwhile to attempt to understand why the properties of being nilpotent and being solvable differ qualitatively, and why the former is far closer to being abelian than the latter. In an abelian group, the commutativity relation holds precisely: $ab = ba$ for all a and b in the group. In general, ab and ba "differ" by a commutator, i.e., $ab = [a, b]ba$ if we use the left action convention for commutators.

When we consider expressions in a group and try to rearrange the terms of the expression, the process of rearrangement introduces commutators. These commutators themselves need to be moved past existing terms, which introduces commutators between the commutators and existing terms. In a nilpotent group, we eventually reach a stage where the iterated commutators that we obtain are central, and therefore can be freely moved past existing terms. In a solvable group, such a stage may never arise.

An alternative perspective is that of *iterative algorithms*, a common class of algorithms found in numerical analysis and other parts of mathematics. An iterative algorithm attempts to find a solution to a problem by guessing an initial solution and iteratively refining the guess by identifying and correcting the error in the initial solution. There are many iterative algorithms that are guaranteed to terminate only for nilpotent groups, and where the number of steps in which the algorithm is guaranteed to terminate is bounded by the nilpotency class of the group. These algorithms work in a single step for abelian groups, because commutativity allows for the necessary manipulations to happen immediately. For non-abelian nilpotent groups, the algorithms work by gradually refining guesses modulo members of a suitable central series (such as the upper central series or lower central series).

1.1.3 The Lie correspondence: general remarks

The *non-abelianness* of groups makes it comparatively difficult to keep track of group elements and to study the groups. It would be very helpful to come up with an alternate description of the structure of a group that replaces the (noncommutative) group multiplication with a commutative group multiplication, and stores the noncommutativity in the form of a separate operation. A *Lie ring* (defined in the Appendix, Section A.1.4) is an example of such a structure.

For readers familiar with the concept of *Lie algebras* over $\mathbb{R}$ or $\mathbb{C}$, note that the definition of Lie ring is similar, except that the underlying additive group is just an abelian group (rather than being a $\mathbb{R}$-vector space or $\mathbb{C}$-vector space) and the Lie bracket is just $\mathbb{Z}$-bilinear rather than being $\mathbb{R}$-bilinear or $\mathbb{C}$-bilinear. In particular, any Lie algebra over $\mathbb{R}$ or $\mathbb{C}$ is a Lie ring, but not every Lie ring is a Lie algebra over $\mathbb{R}$ or $\mathbb{C}$, and even if it is, there may be multiple ways of giving it such a Lie algebra structure.

The *Lie correspondence* is an important correspondence in the theory of real Lie groups. For an elementary exposition of this correspondence, see [46]. We recall here some of the key features of the correspondence.

To any finite-dimensional real Lie group, we can functorially associate a $\mathbb{R}$-Lie algebra called the *Lie algebra of the Lie group*. The underlying vector space of the Lie algebra is the tangent space at the identity to the Lie group, or equivalently, the space of left-invariant vector fields, and the Lie bracket is defined using the Lie bracket of vector fields. Note that the Lie algebra of a Lie group depends only on the connected component of the identity.

Additionally, there exists a map, called the *exponential map*, from the Lie algebra to the Lie group. This map need not be bijective globally, but it must be bijective in a small neighborhood of the identity. The inverse of the map, again defined in a small neighborhood of the identity, is the *logarithm* map. Note that the exponential map is globally defined, but the logarithm map is defined only locally.

The association is not quite a correspondence. The problem is that different Lie groups could give rise to isomorphic Lie algebras. However, if we restrict attention to *connected simply connected Lie groups*, then the association becomes a correspondence, and we can construct a functor in the reverse direction. Explicitly, the Lie correspondence is the following correspondence, functorial in both directions:

Connected simply connected finite-dimensional real Lie groups $\leftrightarrow$ Finite-dimensional real Lie algebras

1.1.4 The Lie algebra for the general linear group

Denote by $GL(n, \mathbb{R})$ the general linear group of degree n over the field of real numbers, i.e., the group of all invertible $n \times n$ matrices with real entries. Denote by $\mathfrak{gl}(n, \mathbb{R})$ the "general linear Lie algebra" of degree n over $\mathbb{R}$. Explicitly, $\mathfrak{gl}(n, \mathbb{R})$ is the vector space of all $n \times n$ matrices over $\mathbb{R}$, and the Lie bracket is defined as $[x, y] := xy - yx$.

$\mathfrak{gl}(n, \mathbb{R})$ is the Lie algebra of $GL(n, \mathbb{R})$. The exponential and logarithm maps in this case are the usual matrix exponential and matrix logarithm maps. The exponential map:

$$\exp : \mathfrak{gl}(n, \mathbb{R}) \to GL(n, \mathbb{R})$$

is defined as:

$$x \mapsto \sum_{i=0}^{\infty} \frac{x^i}{i!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

The matrix exponential is defined for all matrices. However, the exponential map is neither injective nor surjective:

- The exponential map is not surjective for any n. For $n = 1$, this is because the exponential of any real number is a *positive* real number. A similar observation holds for larger n, once we observe that the image of the exponential map is inside $GL^+(n, \mathbb{R})$, the subgroup of $GL(n, \mathbb{R})$ comprising the matrices of positive determinant. However, for $n > 1$, the exponential map is not surjective even to $GL^+(n, \mathbb{R})$. For instance, the following matrix is not the exponential of any matrix with real entries:

$$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$$

- The exponential map is not injective for $n > 1$. For instance, for any positive integer m, the following matrix has exponential equal to the identity matrix:

$$\begin{pmatrix} 0 & 1 \\ -4m^2\pi^2 & 0 \end{pmatrix}$$

Nonetheless, we can find an open neighborhood U of the zero matrix in $\mathfrak{gl}(n, \mathbb{R})$ and an open neighborhood V of the identity matrix in $GL(n, \mathbb{R})$ such that the exponential map is bijective (and in fact, is a homeomorphism) from U to V.

Note that $GL(n, \mathbb{R})$ is not a connected simply connected Lie group, so the above is not an instance of the Lie *correspondence*.

1.1.5 The nilpotent case of the Lie correspondence

The example of $\mathfrak{gl}(n, \mathbb{R})$ and $GL(n, \mathbb{R})$ illustrates that the exponential map does not always behave nicely. However, it turns out that the exponential map behaves much better when we apply the Lie correspondence in the *nilpotent* case. Explicitly, the nilpotent case of the Lie correspondence is a correspondence:

Connected simply connected finite-dimensional nilpotent real Lie groups $\leftrightarrow$

In the nilpotent case, it will turn out that the exponential map is *bijective*, and in fact, it defines a homeomorphism from the Lie algebra to the Lie group. Thus, we can define its inverse, the logarithm map, *globally*.

We now turn to an example.

1.1.6 The example of the unitriangular matrix group

A special case of interest for us is the correspondence between the Lie ring $NT(n, \mathbb{R})$ of $n \times n$ strictly upper triangular matrices over $\mathbb{R}$ and the group $UT(n, \mathbb{R})$ of $n \times n$ upper triangular matrices over $\mathbb{R}$ with all the diagonal entries equal to 1. This correspondence gives a bijection between the underlying sets of $NT(n, \mathbb{R})$ and $UT(n, \mathbb{R})$ via the exponential map. Explicitly, the matrix exponential defines a bijective set map:

$$\exp : NT(n, \mathbb{R}) \to UT(n, \mathbb{R})$$

given explicitly as:

$$\exp(x) = e^x = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^{n-1}}{(n-1)!}$$

Note that this coincides with the usual matrix exponential because $x^n = 0$ and all higher powers of x are therefore also zero. In other words, this exponential map is the restriction to $NT(n, \mathbb{R})$ of the exponential map described in the preceding section:

$$\exp : \mathfrak{gl}(n, \mathbb{R}) \to GL(n, \mathbb{R})$$

However, *unlike* the case of $GL(n, \mathbb{R})$, the exponential map from $NT(n, \mathbb{R})$ to $UT(n, \mathbb{R})$ is bijective, and in fact, is a homeomorphism. Topologically, both $NT(n, \mathbb{R})$ and $UT(n, \mathbb{R})$ are homemorphic (i.e., isomorphic in the category of topological spaces) to the vector space

$\mathbb{R}^{\binom{n}{2}}$.

The inverse set map is the matrix logarithm, now defined *globally*:

$$\log : UT(n, \mathbb{R}) \to NT(n, \mathbb{R})$$

given explicitly as:

$$\log x := (x-1) - \frac{(x-1)^2}{2} + \frac{(x-1)^3}{3} - \cdots + \frac{(-1)^n (x-1)^{n-1}}{n-1}$$

1.1.7 The Malcev correspondence and Lazard correspondence

The *Malcev correspondence* is a generalization of the nilpotent case of the Lie correspondence that applies to algebras over the field of rational numbers. Explicitly, the correspondence is:

Rationally powered nilpotent groups $\leftrightarrow$ Nilpotent $\mathbb{Q}$-Lie algebras

We will define "rationally powered" in Section 4.1, but a quick definition for our purpose is that every element has a unique n^{th} root for every positive integer n. The Malcev correspondence is a purely algebraic correspondence that does not deal with topological structure. Note that any $\mathbb{R}$-Lie algebra is a $\mathbb{Q}$-Lie algebra as well. It turns out that for any nilpotent $\mathbb{R}$-Lie algebra, the Lie correspondence coincides with the Malcev correspondence. Thus, for instance, under the Malcev correspondence, the group associated with $NT(n, \mathbb{R})$ is $UT(n, \mathbb{R})$.

The Malcev correspondence has a slight further generalization called the *Lazard correspondence*, introduced by Lazard in [30]. The Lazard correspondence relaxes the assumption of being "rationally powered" and replaces it with the assumption that unique division by specific primes (namely, primes that are less than or equal to the nilpotency class) is possible.

If we use the Lazard correspondence in the direction from groups to Lie rings, then it allows us to convert (a suitable type of) abstract nilpotent group to a nilpotent Lie ring. The addition operation of the Lie ring captures the abelian part of the group multiplication, whereas the Lie bracket captures the non-abelian part of the group multiplication.

Unfortunately, the Lazard correspondence applies only to *some* nilpotent groups and some nilpotent Lie rings. Specifically, for finite p-groups, it only works for finite p-groups where any subset of size three generates a subgroup of nilpotency class at most $p-1$. For the bulk of this document, we will restrict our attention to the case of small *global class*, i.e., the subcorrespondence that applies to finite p-groups of nilpotency class at most $p-1$.

This means that groups that have higher nilpotency class (a way of saying that the groups are relatively more non-abelian) cannot be studied directly using the Lazard correspondence.

We will describe the Malcev correspondence and the Lazard correspondence in detail in Sections 6.5, 6.6, and 6.7. For a textbook-style presentation of the correspondence, see Khukhro's book [29], Chapters 9 and 10.

1.1.8 Our generalization of the Lazard correspondence

The goal of this document is to describe a generalization of the Lazard correspondence that works for all p-groups of nilpotency class at most p. In other words, it allows us to generalize the Lazard correspondence to a slightly bigger collection of groups. The limitation of this generalization is that the correspondence only works between *equivalence classes of groups* and *equivalence classes of Lie rings*, with each equivalence class containing multiple isomorphism types. The equivalence relation of interest here is the equivalence relation of *isoclinism*. Informally, two groups are isoclinic if their commutator maps are equivalent, and two Lie rings are isoclinic if their Lie bracket maps are equivalent.

1.1.9 Similarities and differences between groups and Lie rings

The theories of groups and Lie rings are *structurally similar*. For many concepts related to groups, there are analogously defined concepts for Lie rings. In most cases, the analogous definition suggests itself naturally. Often, even the proofs are similar. In some cases, proofs are easier for Lie rings than for groups, primarily because the Lie bracket is bilinear.

There are *some* concepts that make sense only on the group side, and some concepts that make sense only on the Lie ring side. Similarly, there are some facts that are true only on the group side, and some facts that are true only on the Lie ring side.

The closer we are to abelianness, the more structurally similar the theory for groups is to the theory for Lie rings. In many cases, a fact is true for nilpotent Lie rings if and only if the "analogous" fact is true for nilpotent groups. There are many facts that are true in *general* for Lie rings and are not true in general for groups, but they are true for nilpotent groups.

In addition to *structural similarity*, we will also see some instances of *bijective correspondences* between certain types of groups and certain types of Lie rings (including the Lie correspondence and the Lazard correspondence). It will turn out that *analogous concepts* become *bijectively correspondent* under these correspondences. For instance, normal subgroups of groups are analogous to ideals in Lie rings. The Lazard correspondence between groups and Lie rings establishes a bijective correspondence between (certain kinds of) normal subgroups of the group and (certain kinds of) ideals of the Lie ring.

1.1.10 Our central tool: Schur multipliers

Our goal is to extend the domain of the Lazard correspondence by relaxing its strictness (from a correspondence up to isomorphism to a correspondence up to isoclinism). In particular, we are interested in extending the Lazard correspondence to *nilpotency class one higher* than where it applies. Thus, the groups (respectively, Lie rings) of interest to us arise as *central extensions* where the quotient group (respectively, quotient Lie ring) is in the domain of the Lazard correspondence.

Rather than directly trying to study the groups and Lie rings, we study the theory of central extensions for groups and Lie rings. We first develop the *general* theory of such central extensions. Then, we apply that general theory to the case where the quotient group (respectively quotient Lie ring) of the central extension lies in the domain of the Lazard correspondence. In the edge case of interest where the group is in the domain of the Lazard correspondence but its central extensions are "just outside" the domain, we can obtain new insights. For instance, if G is a p-group of nilpotency class exactly $p-1$, it is a Lazard Lie group. The central extensions with quotient group G are p-groups of nilpotency class either $p-1$ or p. The latter may lie outside the domain of the Lazard correspondence.

On both the group side and the Lie ring side, the theory of central extensions is governed by an abelian group called the *Schur multiplier*. There is a rich theory behind the Schur multiplier, and it connects with important ideas from algebraic topology and homological algebra. We will explore the necessary facets of this theory. Eventually, we will prove (in Theorem 7.7.3) that if a Lie ring and a group are in Lazard correspondence, then their Schur multipliers are isomorphic. A version of the statement for finite p-groups appeared as a conjecture in the paper [13] by Eick, Horn, and Zandi in September 2012, stated informally after Theorem 2 of the paper.[2] Once the Schur multipliers are established to be isomorphic, it is easy to establish the Lazard correspondence up to isoclinism.

1.1.11 Globally and locally nilpotent

The numbers 2 and 3 are particularly significant in the context of the axiomatization of groups and Lie rings, and they also play an important role in the Lazard correspondence. 2 is the maximum of the arities[3] of the operations used in the definition of groups. In particular, this means that if a function between groups restricts to a homomorphism on every subgroup generated by at most 2 elements, then the function is globally a homomorphism.

3 is the maximum of the number of variables that appear in the identities that define a group. In particular, this means that if an algebra has the same signature as a group (i.e., a 0-ary operation for the identity, a unary operation for the inverse map, and a binary

2. The authors write: "Based on various example computations, see also [7], we believe that Theorems 1 and 2 also hold for finite p-groups of class $p-1$. However, our proofs do not extend to this case." The reference [7] alluded to by the authors has not yet been published or made available online. For a more detailed discussion, see Section 7.7.4

3. The arity of an operation is the number of inputs it takes. For instance, group multiplication has arity 2. Arity is discussed in more detail in the Appendix, Section A.2.4.

operation for the group multiplication), and every subalgebra of the algebra generated by at most 3 elements is a *group*, then the algebra is globally a group.

The same is true for Lie rings: the maximum of the arities of the operations is 2, and the maximum of the number of terms that appear in the defining identities is 3. Thus, any function between Lie rings that restricts to a homomorphism on subrings generated by sets of size at most 2 is globally a homomorphism. Further, given an algebra with the same signature as a Lie ring, such that every subalgebra generated by at most 3 elements becomes a Lie ring with the induced operations, the algebra as a whole is a Lie ring.

The formulas used in the Lazard correspondence describe the group operations in terms of the Lie ring operations, and conversely describe the Lie ring operations in terms of the group operations. The *formulas* themselves refer to a maximum of two elements at a time. However, the *verification* that these formulas work (i.e., that starting from a Lie ring, we end up with a group, or that starting from a group, we end up with a Lie ring) relies on looking at three elements at a time. For instance, to verify that a formula describing group operations in terms of Lie ring operations does indeed define a group structure, we need to verify the associativity identity for three arbitrary elements. Similarly, to verify that a formula describing Lie ring operations in terms of group operations does indeed define a Lie ring structure, we need to verify the associativity of addition, bilinearity, and Jacobi identity for the Lie ring operations. Each of these identities requires considering three arbitrary elements at a time.

Thus, the conditions that we work out on groups (respectively, Lie rings) pertaining to the Lazard correspondence are 3-local conditions: they are conditions on what subgroups (respectively, Lie subrings) generated by subsets of size at most three look like.

1.1.12 The structure of this document

The document is quite long despite the fact that the eventual proofs are relatively short and simple. The reason is that the existing literature we draw upon is fragmented. We draw on literature with these five broad themes:

- Isoclinism and homoclinism.
- Schur multiplier and the relation with group extension theory.
- Exterior square and its generalizations.
- The Lazard correspondence.
- The behavior of groups and Lie rings where we can divide by specific primes.

Each of these themes has a well-developed body of literature. However, the connections between these ideas are not emphasized in the literature, and it often requires a careful reading to glean them. Thus, it would not be sufficient to simply cite the relevant literature. We use the next few sections to develop all the necessary background material in preparation for our results.

Our presentation will follow these features:

- For the foundational sections, we will systematically alternate sections between groups and Lie rings. A section about groups will develop a concept or construct in the context of groups. The next section about Lie rings will develop the analogous concept or construct in the context of Lie rings. To the extent possible, we will follow parallel modes of presentation in the two sections. Differences between the sections will be noted at the beginnings of the relevant sections.
- For the foundational sections, we will often begin by discussing a concept in the context of groups or Lie rings in the abstract, and then discuss an analogous concept in the context of extensions of groups or Lie rings. This will be done somewhat in reverse in the later sections, where we sometimes prove a result in the context of extensions (of groups or Lie rings) and *then* apply that to prove the result in the context of groups or Lie rings. This will be our *modus operandi* for the crucial proofs.

- Our key results involve generalizing certain correspondences (the Baer correspondence and Lazard correspondence) to a larger domain, but with a coarser equivalence relation (of isoclinism). For each correspondence that we generalize, we first explicitly describe the known correspondence and its key attributes (in one or more sections), and then describe our generalization.

1.1.13 For a quick reading

For readers who wish to understand the main results without delving into background concepts in unnecessary depth, the following reading sequence will work:

1. Chapter 1 (Introduction, outline, and preliminaries):
   - Section 1.2 contains the outline of our main proof techniques. It is worth reading in its entirety.
   - Section 1.3 (The abelian Lie correspondence): The contents of this section are straightforward, but it is worth reading because the methods used in this section form a template for later, more complicated, correspondences.
2. Chapter 2 (Isoclinism and homoclinism: basic theory):
   - Section 2.1 (Isoclinism and homoclinism of groups): It suffices to read Sections 2.1.1 – 2.1.4, and the statements of the theorems in Section 2.1.6. Readers already familiar with the definitions can skip this section and return if needed.
   - Section 2.2 (Isoclinism and homoclinism of Lie rings): It suffices to read Section 2.2.1. Readers already familiar with the definitions can skip this section and return if needed. Readers who thoroughly understand the general analogy between groups and Lie rings can extrapolate the definitions and results of this section from the preceding one, and hence may skip this section.
3. Chapter 3 (Extension theory):

- Section 3.1 (Short exact sequences of groups): Readers already familiar with the basics of short exact sequences and central extensions can read Sections 3.1.5 and 3.1.6.
- Section 3.2 (Short exact sequences and central extensions of Lie rings): Readers who understood the preceding section (Section 3.1), and understand how the analogy between groups and Lie rings works, can skip this section.
- Section 3.3 (Explicit description of second cohomology group): This section can be skipped without loss of continuity. The material in this section helps with understanding Section 5.4.9. However, the latter can also be skipped without loss of continuity.
- Section 3.4 (Exterior square, Schur multiplier, and homoclinism): This section is important to understand because it lays the foundation for later material, and the presentation is non-standard. Readers may skip proofs, many of which are tedious, and focus on the statements of the results.
- Section 3.5 (Exterior square, Schur multiplier, and homoclinism for Lie rings): Apart from Section 3.5.2, this section is mostly analogous to the preceding section. Hence, the rest of the section can be skipped.
- Section 3.6: This section is important to understand because it lays the foundation for later material, and the presentation is non-standard. Readers may skip proofs, many of which are tedious, and focus on the statements of the results.
- Section 3.7: This section may be skipped by readers who have a thorough understanding of the preceding section and understand how the analogy between groups and Lie rings works.
- Sections 3.8 and 3.9 (Exterior and tensor products for groups and Lie rings respectively): These sections can be skipped without loss of continuity, and interested readers can refer back to the explicit descriptions as needed later.

- Sections 3.10 and 3.11: These are worth skimming for their main results.

4. Chapter 4 (Powering over sets of primes):

    - Section 4.1 (Groups powered over sets of primes): Readers would benefit by reading the part of Section 4.1 up to and including Section 4.1.5 in order to familiarize themselves with the definitions. Some of the results presented in the rest of the section are useful, but they can be revisited as necessary.
    - Section 4.2 (Lie rings powered over sets of primes): It suffices to read Section 4.2.1.
    - Section 4.3 (Free powered groups and powering functors): The results in Sections 4.3.5 and 4.3.8 are the most important. The rest of the section may be skimmed.
    - Section 4.4 (Free powered Lie rings and powering functors): The results here are analogous to the preceding section, though the proofs are more straightforward. The section can be skipped and returned to as needed.

5. Chapter 5 (Baer correspondence):

    - Sections 5.1 and 5.2 (Baer correspondence): It suffices to read Sections 5.1.1-5.1.3 and Section 5.2.4. However, readers may benefit from skimming both sections in their entirety in order to get a better sense.
    - Section 5.3 may be skipped without loss of continuity.
    - Section 5.4 (Baer correspondence up to isoclinism): Reading the whole section is strongly recommended, but readers may skip Section 5.4.9 without loss of continuity.
    - Section 5.5 contains interesting examples worth reading but may be skipped without loss of continuity.

6. Chapter 6 (The Malcev and Lazard correspondences):

- Sections 6.1 and 6.2 (adjoint groups, exponential and logarithm maps, and free nilpotent groups): These sections may be skimmed without reading the proofs. They provide technical background for Section 6.3.
- Section 6.3 (Baker-Campbell-Hausdorff formula): This section should be read in its entirety. Readers may benefit from concentrating on the statements of the theorems and skimming the proofs.
- Section 6.4: This section is partly analogous to Section 6.3, so aside from the introduction, it may be skimmed.
- Sections 6.5, 6.6, and 6.7 (Malcev correspondence, global Lazard correspondence, and Lazard correspondence): These sections are worth reading, though people familiar with the correspondences may skim them.

7. Chapter 7 (Generalizing the Lazard correspondence to a correspondence up to isoclinism):

   - Section 7.1 (Group commutator and Lie bracket in terms of each other) is important.
   - Section 7.2 may be skimmed.
   - The theorems in Section 7.3 are important as stepping stones for the main results. However, the proofs are unilluminative and may be skipped.
   - The results in Sections 7.4 and 7.5 are important, but the proofs may again be skipped.
   - Sections 7.6 and 7.7 are extremely important and should be read carefully, though the proofs may be skimmed.

8. Chapter 8 (Applications and possible extensions): Sections 8.1 and 8.2 may be of interest to readers who want to understand potential applications.

9. Readers may refer to the sections in the Appendix based on their level of interest. Sections A.1, A.2, and A.3 cover technical background at the advanced undergraduate or beginning graduate level that is useful for understanding the main results of the thesis. Section A.5 covers a general theory that is helpful for understanding potential generalizations of the results presented here.

1.2 Outline of our main results

This section provides an overview of our main results and the strategy we will use to prove these results. Some of the technical details in this section may be accessible only to people with a strong background in group theory and some prior familiarity with the Lazard correspondence. However, all readers should be able to understand the ideas at a broad level.

1.2.1 The Lazard correspondence: a rapid review

The Lazard correspondence is a correspondence between certain kinds of groups and certain kinds of Lie rings. The groups, called *Lazard Lie groups*, satisfy a condition relating the set of primes over which they are powered and the nilpotency class of subgroups generated by subsets of size at most three. The Lie rings, called *Lazard Lie rings*, satisfy a similar condition relating the set of primes over which they are powered and the nilpotency class of Lie subrings generated by subsets of size at most three. The precise definition of the Lazard correspondence is in Section 6.7. A somewhat easier case of the correspondence, called the *global* Lazard correspondence, is described in Section 6.6. The global Lazard correspondence imposes a restriction on the nilpotency class of the whole group and of the whole Lie ring. It is more narrow than the Lazard correspondence but easier to deal with.

For a Lie ring L, the corresponding group, $\exp(L)$, has the *same underlying set* as L, and the group operations are defined in terms of the Lie ring operations based on fixed formulas.

Explicitly, the group multiplication is defined in terms of the Lie ring operations using the *Baker-Campbell-Hausdorff formula*. The Baker-Campbell-Hausdorff formula is described in detail in Section 6.3. Technically, the formula is different for different values of the (3-local) nilpotency class, but we can use a single infinite series whose truncations give all the formulas.

For a group G, the corresponding Lie ring, denoted $\log(G)$, has the *same underlying set* as G, and the Lie ring operations are defined in terms of the group operations based on fixed formulas called the *inverse Baker-Campbell-Hausdorff formulas* (one formula describing the Lie ring addition and another formula describing the Lie bracket in terms of the group operations). The inverse Baker-Campbell-Hausdorff formulas are described in Section 6.4.

exp and log define functors between appropriately defined subcategories of the category of groups and the category of Lie rings, and the functors are two-sided inverses of each other. Thus, they establish an isomorphism of categories over the category of sets[4] between the relevant subcategories of the category of groups and the category of Lie rings.

1.2.2 Isoclinism: a rapid review

An *isoclinism of groups* is a pair of group isomorphisms, one between their inner automorphism groups and the other between their derived subgroups, that are compatible with the commutator map. Intuitively, we can think of an isoclinism of groups as an equivalence between the commutator structures of the two groups. We will define and discuss isoclinisms in Section 2.1.

There is a similar notion of *isoclinism of Lie rings* (that uses the inner derivation Lie ring, the derived subring, and the Lie bracket) that we will define and discuss in Section 2.2. Intuitively, we can think of an isoclinism of Lie rings as an equivalence between the Lie bracket structures of the Lie rings.

We can use isoclinism of groups to define an *equivalence relation* on the collection of

4. This means an isomorphism of categories that preserves the underlying set

groups. Analogously, we can use isoclinism of Lie rings to define an equivalence relation on the collection of Lie rings.

1.2.3 The Lazard correspondence up to isoclinism

The Lazard correspondence up to isoclinism combines the idea of the Lazard correspondence and the idea of isoclinism. For a Lie ring L and a group G, a Lazard correspondence up to isoclinism includes two pieces of data satisfying a compatibility condition:

- A Lazard correspondence up to isomorphism between $\mathrm{Inn}(L)$ and $\mathrm{Inn}(G)$. This can be viewed as an isomorphism of groups between $\exp(\mathrm{Inn}(L))$ and $\mathrm{Inn}(G)$ or as an isomorphism of Lie rings between $\mathrm{Inn}(L)$ and $\log(\mathrm{Inn}(G))$.
- A Lazard correspondence up to isomorphism between L' and G'. This can be viewed as an isomorphism of groups between $\exp(L')$ and G' or as an isomorphism of Lie rings between L' and $\log(G')$.

The compatibility condition is tricky to specify. Naively, we might expect that the compatibility condition would say that the isomorphism converts the Lie bracket map $\mathrm{Inn}(L) \times \mathrm{Inn}(L) \to L'$ to the commutator map $\mathrm{Inn}(G) \times \mathrm{Inn}(G) \to G'$. The problem with this naive specification is that even with the ordinary Lazard correspondence, the Lie bracket of the Lie ring does not coincide with the commutator of the group. They *do* coincide when the class is at most two, and we discuss this special case, the *Baer correspondence up to isoclinism*, in Section 5.4.

To handle higher class, we need to first derive a formula valid for the usual Lazard correspondence that expresses the Lie bracket in terms of the commutator, and in the reverse direction, we need to derive a formula valid for the usual Lazard correspondence that expresses the commutator in terms of the Lie bracket. The compatibility condition we impose will make use of these formulas. The formulas themselves are described in Section 7.1. The compatibility condition based on these formulas is described in detail in Section 7.7.

1.2.4 The existence question

Defining the Lazard correspondence up to isoclinism is relatively easy. The harder part is establishing sufficient conditions for the existence of objects on the other side, i.e., establishing sufficient conditions for the existence of groups that are in Lazard correspondence up to isoclinism with a given Lie ring, and establishing sufficient conditions for the existence of Lie rings that are in Lazard correspondence up to isoclinism with a given group.

The results that we would like to aim for are:

- For a Lie ring L, if both $\mathrm{Inn}(L)$ and L' are Lazard Lie rings, then we can find a group G such that L is in Lazard correspondence up to isoclinism with G.
- For a group G, if both $\mathrm{Inn}(G)$ and G' are Lazard Lie groups, then we can find a Lie ring L such that L is in Lazard correspondence up to isoclinism with G.

Unfortunately, the proofs of these statements at a general level require more machinery than we can manage in this thesis. We therefore restrict our proofs here to the case of the global Lazard correspondence. The precise statements of the results we will prove are in Section 7.7. Essentially, we restrict attention to groups that satisfy global assumptions on the set of primes over which they powered, and for which the inner automorphism group and derived subgroup are both in the domain of the global Lazard correspondence.

The strategy that we use to demonstrate these facts is somewhat roundabout. Instead of trying to answer the question directly, we try to answer the question in the more general context of central extensions of groups and Lie rings. We will then apply the results that we obtain to the central extensions with short exact sequences:

$$0 \to Z(G) \to G \to G/Z(G) \to 1$$

and

$$0 \to Z(L) \to L \to L/Z(L) \to 0$$

We outline below the argument in the direction from Lie rings to groups.

We begin by viewing L as an extension with central subring $Z(L)$ and quotient ring $L/Z(L) \cong \mathrm{Inn}(L)$. We obtain the corresponding Lie bracket map $\mathrm{Inn}(L) \times \mathrm{Inn}(L) \to L'$. We then obtain a desired commutator map $\exp(\mathrm{Inn}(L)) \times \exp(\mathrm{Inn}(L)) \to \exp(L')$ by using the formula describing the commutator map in terms of the Lie bracket map. Finally, we demonstrate the existence of a group G that realizes this commutator map.

1.2.5 The realization of isoclinism types

We will show that equivalence classes of groups up to isoclinism can be described by storing the commutator structure in an abstract fashion, without reference to an actual group in that equivalence class.

This will be useful to the final step of our proof of existence established above: instead of directly trying to construct the groups in the equivalence class up to isoclinism, we construct the commutator structure. In the notation above, we construct the desired commutator map $\exp(\mathrm{Inn}(L)) \times \exp(\mathrm{Inn}(L)) \to \exp(L')$.

Below, we provide a few more details about how we store the commutator structure abstractly. This discussion may be accessible only to people familiar either with group cohomology or with some other type of cohomology theory that is structurally similar. Note also that the group G that we use here is not the same as the group G used in Section 1.2.4. In fact, to apply what we discuss below to Section 1.2.4, we would need to set the group A below to $\exp(Z(L))$ and set the group G below to $\exp(L/Z(L))$.

Technical details: In Sections 3.4 and 3.6, we will show that we can classify central extensions up to isoclinism using a homomorphism from the Schur multiplier. Explicitly, when considering central extensions with central subgroup A and quotient group G, we can determine the type of the extension up to isoclinism by considering the induced map $M(G) \to A$ where $M(G)$ is the Schur multiplier of G. We will relate this to the universal coefficient theorem short exact sequence described in Section 3.6.4.

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, A) \to H^2(G; A) \to \mathrm{Hom}(M(G), A) \to 0$$

The key aspect of the above short exact sequence that is relevant for the existence question is the *surjectivity* of the map:

$$H^2(G; A) \to \mathrm{Hom}(M(G), A)$$

Thus, the homomorphism from $M(G)$ to A describes the equivalence class of extensions up to isoclinism, and every homomorphism from $M(G)$ to A describes some eqiuvalence class of extensions.

For results in the opposite direction, we develop a similar theory for Lie rings.

1.2.6 Powering assumptions

One complication that arises in the discussion of the Lazard correspondence and its generalizations is that the formulas involved require taking p^{th} roots for some primes p. Thus, in order to make sense of these expressions, we need to develop a basic theory of groups and Lie rings where these operations make sense. We develop that basic theory in Sections 4.1 and 4.3 (for groups) and in Sections 4.2 and 4.4 (for Lie rings).

1.2.7 Global Lazard correspondence preserves Schur multipliers

To complete the proof, we need to demonstrate that the global Lazard correspondence behaves well with respect to the structures that we use to classify extensions up to isoclinism. Explicitly, we need to show that if $L = \log(G)$ and $G = \exp(L)$, then the Schur multipliers $M(L)$ and $M(G)$ are canonically isomorphic, and also that the exterior squares $L \wedge L$ and $G \wedge G$ are in Lazard correspondence. We will demonstrate these facts in Sections 7.4 and 7.7 (specifically, in Theorem 7.7.3). A version of the statement for finite p-groups appeared as a conjecture in the paper [13] by Eick, Horn, and Zandi in September 2012, stated informally after Theorem 2 of the paper. Some technical details of our proof idea follow.

Technical details: The key idea behind our proof is to express our group as a quotient group of a free powered nilpotent group of class one more. Using a nilpotency class of one more allows us to use a variant of the Hopf formula to calculate the Schur multiplier, as described in 3.6.10 and 7.4.2. We can perform a similar construction on the Lie ring side. We now show that the groups used to compute the Schur multiplier of the group are in Lazard correspondence with the Lie rings used to compute the Schur multiplier of the Lie ring. The reason this is nontrivial is that the free nilpotent group and free nilpotent Lie ring of class one more need not themselves be in Lazard correspondence. We need to show that despite this, the groups that we eventually use in the formula for computing the Schur multiplier are in Lazard correspondence.

1.3 The abelian Lie correspondence

This section describes an obvious and straightforward correspondence: the correspondence between abelian groups and abelian Lie rings. An abelian Lie ring is a Lie ring that has trivial Lie bracket. Basic definitions related to Lie rings can be found in the Appendix, Section A.1.4.

All assertions made here are trivial to prove. The purpose of this section is to set up a basic prototype for the Lazard correspondence.

1.3.1 Abelian groups correspond to abelian Lie rings

We establish the abelian Lie correspondence:

$$\text{Abelian groups} \leftrightarrow \text{Abelian Lie rings}$$

The correspondence works as follows.

- From groups to Lie rings: Given an abelian group G, the corresponding abelian Lie ring $\log G$ is defined as the Lie ring whose underlying additive group coincides with G, and where the Lie bracket is trivial.

- From Lie rings to groups: Given an abelian Lie ring L, the corresponding abelian group $\exp L$ is defined as the underlying additive group of L.

Note that the symbols exp and log here are being used as abstract symbols. They do not describe exponential and logarithm maps in the conventional sense of the term. The relationship with the usual notions of exponential and logarithm will become clearer in subsequent sections leading up to the definition of the Lazard correspondence.

1.3.2 Preservation of homomorphisms: viewing exp *and* log *as functors*

The following observations follow immediately from the definitions:

- log defines a functor from abelian groups to abelian Lie rings: Suppose G_1 and G_2 are abelian groups and $\varphi : G_1 \to G_2$ is a group homomorphism. Then, there exists a unique Lie ring homomorphism $\log(\varphi) : \log(G_1) \to \log(G_2)$ that has the same underlying set map as φ.

- exp defines a functor from abelian Lie rings to abelian groups: Suppose L_1 and L_2 are abelian Lie rings and $\varphi : L_1 \to L_2$ is a Lie ring homomorphism. Then, there exists a unique group homomorphism $\exp(\varphi) : \exp(L_1) \to \exp(L_2)$ that has the same underlying set map as φ.

- The log and exp functors are two-sided inverses of each other: This assertion has four parts:
  - For every abelian group G, $G = \exp(\log(G))$.
  - For every abelian Lie ring L, $L = \log(\exp(L))$.
  - For every group homomorphism $\varphi : G_1 \to G_2$ of abelian groups, $\exp(\log(\varphi)) = \varphi$.

  - For every Lie ring homomorphism $\varphi : L_1 \to L_2$ of abelian Lie rings, $\log(\exp(\varphi)) = \varphi$.

The upshot of these is that the category of abelian groups and the category of abelian Lie rings are isomorphic categories, with the log and exp functors providing the isomorphisms.

1.3.3 Isomorphism over Set

Consider the following two categories:

- The category of abelian groups, with the forgetful functor to the category of sets that sends each abelian group to its underlying set.

- The category of abelian Lie rings, with the forgetful functor to the category of sets that sends each abelian Lie ring to its underlying set.

The correspondence we established above (in Sections 1.3.1 and 1.3.2) establishes an *isomorphism of categories over Set* between the two categories. There are two parts to this statement:

- The correspondence establishes an isomorphism between the category of abelian groups and the category of abelian Lie rings: The functor in the direction from groups to Lie rings is the log functor. The functor in the direction from Lie rings to groups is the exp functor. The details are in the preceding section (Section 1.3.2).

- This isomorphism has the property that applying it and then applying the forgetful functor to the category of sets gives the same result as directly applying the forgetful functor to the category of sets. This is a category-theoretic way of saying that the abelian group and abelian Lie ring have the same underlying set, and that the set maps that are group homomorphisms are precisely the same as the set maps that are Lie ring homomorphisms.

1.3.4 Equality of endomorphism monoids and of automorphism groups

Suppose L is an abelian Lie ring and $G = \exp(L)$, so that $L = \log(G)$. The functors exp and log are isomorphisms of categories, hence they induce isomorphisms between the endomorphism monoids. Further, since these isomorphisms of categories preserve the underlying set, the isomorphism between the endomorphism monoids sends each Lie ring endomorphism to a corresponding group endomorphism that is *the same as a set map*. Explicitly, the map $\exp : \mathrm{End}(L) \to \mathrm{End}(G)$ is an isomorphism. Further, for $\varphi \in \mathrm{End}(L)$, the corresponding map $\exp(\varphi) \in \mathrm{End}(G)$ coincides with φ as a set map. The isomorphism induced by exp between the endomorphism monoids $\mathrm{End}(L)$ and $\mathrm{End}(G)$ restricts to an isomorphism between the automorphism groups $\mathrm{Aut}(L)$ and $\mathrm{Aut}(G)$.

1.3.5 The correspondence up to isomorphism

We have so far considered the correspondence at the level of individual groups and Lie rings:

$$\text{Abelian groups} \leftrightarrow \text{Abelian Lie rings}$$

The correspondence defines an isomorphism of categories, and thus it descends to a correspondence between equivalence classes up to isomorphism on both sides, giving a correspondence:

$$\text{Isomorphism classes of abelian groups} \leftrightarrow \text{Isomorphism classes of abelian Lie rings}$$

Suppose L is an abelian Lie ring and G is an abelian group. Specifying an abelian Lie correspondence *up to isomorphism* between L and G amounts to specifying one of the following two equivalent pieces of data:

- An isomorphism of groups from $\exp L$ to G.
- An isomorphism of Lie rings from $\log G$ to L.

A common convention used to provide this data is to provide one of these:

- A *set* map $\exp : L \to G$ that, viewed as a set map from $\exp(L)$ to G, becomes a group isomorphism.
- A *set* map $\log : G \to L$ that, viewed as a set map from $\log(G)$ to L, becomes a Lie ring isomorphism.

In other words, we can specify the data in the form of one of these set maps:

$$\exp : L \to G, \log : G \to L$$

The set maps log and exp are two-sided inverses of each other.

It will turn out, later, that actual exponential and logarithm maps, with the usual power series expansions, occurring inside an associative ring, provide examples of an abelian Lie correspondence up to isomorphism.

In cases where we want to emphasize that we are talking of the abelian Lie correspondence and not the abelian Lie correspondence up to isomorphism, we will talk of the *strict* abelian Lie correspondence. In this section, our focus will be on the strict abelian Lie correspondence because that provides for an easier way to formulate our statements.

1.3.6 Isomorphism of categories versus equivalence of categories

When discussing what it means for two categories to be essentially the same, category theorists typically rely on a weaker notion than isomorphism of categories. An *equivalence of categories* $\mathcal{C}$ and $\mathcal{D}$ and a pair of functors $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ and $\mathcal{G} : \mathcal{D} \to \mathcal{C}$ along with natural isomorphism $\varepsilon : \mathcal{F} \circ \mathcal{G} \to \mathrm{Id}_{\mathcal{D}}$ and $\eta : \mathcal{G} \circ \mathcal{F} \to \mathrm{Id}_{\mathcal{C}}$. Two categories $\mathcal{C}$ and $\mathcal{D}$ are said to be equivalent if there exists an equivalence of categories between them. An alternative characterization is that two categories $\mathcal{C}$ and $\mathcal{D}$ are equivalent if there exists a functor $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ such that $\mathcal{F}$ is full, faithful, and essentially surjective. Here, *essentially surjective* means that for every object $B \in \mathcal{D}$, there exists $A \in \mathcal{C}$ such that $\mathcal{F}(A)$ is isomorphic to B.

The difference between the definitions of isomorphism of categories and equivalence of categories arises from the distinction between a functor being bijective (in the sense that *every* object is in the image of the functor and has a unique pre-image under the functor) and the functor being essentially surjective (in the sense that every object is *isomorphic* to an object in the image of the functor). Equivalence of categories is a more robust and useful notion because it is less sensitive to how strictly we define equality of objects. Thus, even though the correspondences we define are isomorphisms of categories over the category of sets, it will often be more helpful to think of them as equivalences of categories.

Note that any equivalence of categories establishes a bijective correspondence between isomorphism classes of objects in the two categories (in this case, the two categories are respectively the category of abelian groups and the category of abelian Lie rings). However, the equivalence of categories also includes additional data that allows us to identify homomorphism sets on both sides (in this case, identify abelian group homomorphisms with abelian Lie ring homomorphisms).

1.3.7 Subgroups, quotients, and direct products

The collection of abelian groups is a subvariety of the variety of groups (see the Appendix, Section A.2.4 for the definition of variety). There are three parts to this assertion:

- Every subgroup of an abelian group is abelian.
- Every quotient group of an abelian group is abelian.
- A direct product of (finitely or infinitely many) abelian groups is abelian.

Similarly, the collection of abelian Lie rings is a subvariety of the variety of Lie rings. There are three parts to this assertion:

- Every subring of an abelian Lie ring is abelian.
- Every quotient ring of an abelian Lie ring is abelian.

- A direct product of (finitely or infinitely many) abelian Lie rings is abelian.

A natural question is whether the abelian Lie correspondence behaves nicely with respect to taking subalgebras (subgroups and subrings respectively), quotient algebras (quotient groups and quotient rings respectively), and direct products. The answer is *yes*. Specifically, the following are true:

- *Subgroups correspond to subrings*: Suppose an abelian Lie ring L is in abelian Lie correspondence with an abelian group G, i.e., $L = \log(G)$ and $G = \exp(L)$. Then, for every subgroup H of G, $\log(H)$ is a subring of L, and the inclusion map of $\log(H)$ in L is obtained by applying the log functor to the inclusion map of H in G. In the opposite direction, for every subring M of L, $\exp(M)$ is a subgroup of G, and the inclusion map of $\exp(M)$ in G is obtained by applying the exp functor to the inclusion map of M in L. The abelian Lie correspondence thus gives rise to a correspondence:

  $$\text{Subgroups of } G \leftrightarrow \text{Subrings of } L$$

- *Quotient groups correspond to quotient rings*: Suppose an abelian Lie ring L is in abelian Lie correspondence with an abelian group G. Then, for every normal subgroup H of G,[5] $\log(G/H)$ is a quotient Lie ring of L, and the quotient map $L \to \log(G/H)$ is obtained by applying the log functor to the quotient map $G \to G/H$. In the opposite direction, for every ideal I of L, $\exp(L/I)$ is a quotient group of G, and the quotient map $G \to \exp(L/I)$ is obtained by applying the exp functor to the quotient map $L \to L/I$. The abelian Lie correspondence thus gives rise to correspondences:

  $$\text{Normal subgroups of } G \leftrightarrow \text{Ideals of } L$$

  $$\text{Quotient groups of } G \leftrightarrow \text{Quotient rings of } L$$

5. Note that since G is abelian, every subgroup is normal. However, we deliberately state the result in this fashion so that parallels with later generalizations are clearer.

- *Direct products correspond to direct products*: Suppose I is an indexing set, and $G_i, i \in I$ is a collection of abelian groups. For each $i \in I$, let $L_i = \log(G_i)$. Then, the external direct product $\prod_{i \in I} L_i$ is in abelian Lie correspondence with the external direct product $\prod_{i \in I} G_i$. Moreover, the projection maps from the direct product to the individual factors are in abelian Lie correspondence. Also, the inclusion maps of each direct factor in the direct product are in abelian Lie correspondence.

1.3.8 Characteristic and fully invariant

Suppose an abelian group G is in abelian Lie correspondence with an abelian Lie ring L. In Section 1.3.4, we saw that G and L have the same automorphism group as each other and the same endomorphism monoid as each other (where "same" here means that the actions agree on the underlying set). In Section 1.3.7, we saw that the abelian Lie correspondence induces a bijective correspondence between subgroups of G and subrings of L. Combining these ideas, we obtain two additional bijective correspondences:

$$\text{Characteristic subgroups of } G \leftrightarrow \text{Characteristic subrings of } L$$

$$\text{Fully invariant subgroups of } G \leftrightarrow \text{Fully invariant subrings of } L$$

Here, *characteristic* means invariant under all automorphisms and *fully invariant* means invariant under all endomorphisms.

1.3.9 How the template will be reused

The steps that we have outlined above will be used to construct and study a number of similar correspondences. The steps will be as follows:

- We will describe a way of writing group operations in terms of Lie ring operations and a way of describing Lie ring operations in terms of group operations, such that the formulas used satisfy the axioms for groups and Lie rings by definition, and such that the formulas are inverses of each other.

- We will then use this to construct a correspondence that defines an isomorphism over the category of sets between a full subcategory of the category of groups and a full subcategory of the category of Lie rings. We will use log to denote the functor from the group side to the Lie ring side, and exp to denote the functor from the Lie ring side to the group side.

- We will deduce that if a group and Lie ring are in correspondence, then their endomorphism monoids are naturally isomorphic, and their automorphism groups are naturally isomorphic.

- The correspondence can be weakened to a correspondence between isomorphism classes in the full subcategories.

- An instance of the correspondence up to isomorphism between a group G and a Lie ring L can be described by specifying the isomorphism from $\log(G)$ to L or by specifying the isomorphism from $\exp(L)$ to G. We will describe the correspondence in terms of the set map $\log : G \to L$ or, equivalently, the set map $\exp : L \to G$.

- Of the results in Section 1.3.7, the results for the direct product generalizes for each correspondence (note that this does not follow category-theoretically, but rather, it follows from the nature of the correspondence). The results for the correspondence between subgroups and subrings and the correspondence between quotient groups and quoitent rings generalize but only after we impose restrictions on the types of subgroups, subrings, quotient groups, and quotient rings under consideration.

For brevity, we will not repeat these steps in every instance. Rather, our focus will be on the first step: establishing that the formulas used make sense, satisfy the axioms, and are inverses of each other.

CHAPTER 2

ISOCLINISM AND HOMOCLINISM: BASIC THEORY

2.1 Isoclinism and homoclinism for groups

The goal of this section is to establish the basic theory of *isoclinism* and *homoclinism* for groups. Informally, a homoclinism of groups is a homomorphism between the *commutator structures* of the groups. Informally, two groups are isoclinic if their commutator maps are equivalent. Isoclinism defines an equivalence relation on the collection of groups. Under this equivalence relation, all abelian groups are equivalent to the trivial group.

The original results that we present later (Section 5.4 and 7.7) describe bijective correspondences between certain equivalence classes of groups and certain equivalence classes of Lie rings. The equivalence classes of groups are based on the equivalence relation of isoclinism.

Readers already familiar with the definitions of isoclinism and homoclinism may skip this section and return to it later if needed. Readers who want the bare minimum necessary for later sections can read Sections 2.1.1-2.1.4, and the statements of the theorems in Section 2.1.6. The proofs of the theorems in Section 2.1.6 can be skipped.

2.1.1 Isoclinism of groups: definition

The concept of isoclinism as introduced here was first defined in 1937 by Philip Hall in [23]. It was used by Philip Hall as an aid to the classification of finite groups of small prime power order. Hall's work was later extended by Marshall Hall and Senior, who published detailed information on the groups of order $2^n, n \leq 6$ in [22]. The basic definition and most of the elementary facts stated here about isoclinism can be found on Page 93 of Suzuki's group theory text [45].

For any group G, denote by $\mathrm{Inn}(G)$ the inner automorphism group of G, denote by G' the derived subgroup of G, and denote by $Z(G)$ the center of G (this and related notation used in this document are described in Section 1.0.2). Note that $\mathrm{Inn}(G) \cong G/Z(G)$.

For any group G, the commutator map in G descends to a map of sets:

$$\omega_G : \mathrm{Inn}(G) \times \mathrm{Inn}(G) \to G'$$

This map is well-defined because the commutator of two elements depends only on their cosets modulo the center. Note that this map is only a *set* map at this stage, not a homomorphism. Later, in Section 3.4.1, we will introduce the concept of the exterior square of a group, and we will be able to interpret ω_G as a homomorphism in that context.

Suppose now that G_1 and G_2 are groups. The commutator maps in the groups define the following respective maps:

$$\omega_{G_1} : \mathrm{Inn}(G_1) \times \mathrm{Inn}(G_1) \to G_1'$$

$$\omega_{G_2} : \mathrm{Inn}(G_2) \times \mathrm{Inn}(G_2) \to G_2'$$

An *isoclinism* from G_1 to G_2 is a pair of isomorphisms (ζ, φ) where ζ is an isomorphism from $\mathrm{Inn}(G_1)$ to $\mathrm{Inn}(G_2)$ and φ is an isomorphism from G_1' to G_2', satisfying the condition that:

$$\varphi \circ \omega_{G_1} = \omega_{G_2} \circ (\zeta \times \zeta) \tag{2.1}$$

More explicitly, for any $x, y \in \mathrm{Inn}(G_1)$, we require that:

$$\varphi(\omega_{G_1}(x, y)) = \omega_{G_2}(\zeta(x), \zeta(y)) \tag{2.2}$$

In other words, taking the commutator and then applying the isomorphism of derived subgroups is equivalent to applying the isomorphism between inner automorphism groups and then taking the commutator.

Pictorially, this can be represented as saying that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Inn}(G_1) \times \mathrm{Inn}(G_1) & \stackrel{\zeta\times\zeta}{\to} & \mathrm{Inn}(G_2) \times \mathrm{Inn}(G_2) \\ \downarrow^{\omega_{G_1}} & & \downarrow^{\omega_{G_2}} \\ G_1' & \stackrel{\varphi}{\to} & G_2' \end{array}$$

Note that both the inner automorphism group and the derived subgroup are quantitative measurements of the "non-abelianness" of the group. The notion of isoclinism can thus properly be thought of as saying "equivalent modulo the subvariety of abelian groups." In particular, a group is abelian if and only if it is isoclinic to the trivial group.

There is a precise way of formulating this using the more general notion of isologism, which we describe in the Appendix, Section A.5.

2.1.2 Homoclinism of groups

The notion of *homoclinism of groups* relates to isoclinism of groups in the same way as homomorphism of groups relates to isomorphism of groups. We have not been able to confirm the first use of the term, but a somewhat more general definition called n-homoclinism appears in [24]. We have chosen this presentation, despite its being non-standard, because it is a convenient framework for understanding later results. Although the presentation is non-standard, none of the results in this or the next few sections are substantively different from results available in the literature.

Suppose G_1 and G_2 are groups. A *homoclinism of groups* from G_1 to G_2 is a pair of homomorphisms (ζ, φ) where ζ is a homomorphism from $\mathrm{Inn}(G_1)$ to $\mathrm{Inn}(G_2)$ and φ is a homomorphism from G_1' to G_2', satisfying Equation 2.1 (that can alternatively be stated as 2.2).

Pictorially, this can be represented as saying that the following diagram commutes:

$$\begin{tikzcd}
\mathrm{Inn}(G_1) \times \mathrm{Inn}(G_1) \arrow[r, "\zeta \times \zeta"] \arrow[d, "\omega_{G_1}"] & \mathrm{Inn}(G_2) \times \mathrm{Inn}(G_2) \arrow[d, "\omega_{G_2}"] \\
G_1' \arrow[r, "\varphi"] & G_2'
\end{tikzcd}$$

Note that this is the same as the diagram for isoclinisms. The only difference is that the horizontal maps are no longer required to be bijective.

2.1.3 Composition of homoclinisms

Suppose G_1, G_2, and G_3 are groups. Suppose $(\zeta_{12}, \varphi_{12})$ is a homoclinism from G_1 to G_2 and $(\zeta_{23}, \varphi_{23})$ is a homoclinism from G_2 to G_3. We then define the *composite* of these homoclinisms to be the following homoclinism from G_1 to G_3:

$$(\zeta_{23}, \varphi_{23}) \circ (\zeta_{12}, \varphi_{12}) = (\zeta_{23} \circ \zeta_{12}, \varphi_{23} \circ \varphi_{12})$$

To see that this composite is indeed a homoclinism, we need to check that both the component maps are homomorphisms, and that the corresponding diagram commutes. The component maps are homomorphisms because a composite of homomorphisms is a homomorphism. The fact that the diagram commutes can be seen from the full diagram below. The left square commutes because $(\zeta_{12}, \varphi_{12})$ is a homoclinism. The right square commutes because $(\zeta_{23}, \varphi_{23})$ is a homoclinism. Thus, the overall diagram commutes.

$$\begin{tikzcd}
\mathrm{Inn}(G_1) \times \mathrm{Inn}(G_1) \arrow[r, "\zeta_{12} \times \zeta_{12}"] \arrow[d, "\omega_{G_1}"] & \mathrm{Inn}(G_2) \times \mathrm{Inn}(G_2) \arrow[r, "\zeta_{23} \times \zeta_{23}"] \arrow[d, "\omega_{G_2}"] & \mathrm{Inn}(G_3) \times \mathrm{Inn}(G_3) \arrow[d, "\omega_{G_3}"] \\
G_1' \arrow[r, "\varphi_{12}"] & G_2' \arrow[r, "\varphi_{23}"] & G_3'
\end{tikzcd}$$

2.1.4 Category of groups with homoclinisms

We define a category that will be useful to work with.

Definition (Category of groups with homoclinisms)**.** The *category of groups with homoclinisms* is defined as the following category:

- The *objects* of the category are groups.
- The *morphisms* of the category are homoclinisms.
- Composition of morphisms is composition of homoclinisms.
- The identity morphism is the identity homoclinism: it is the identity map on both the inner automorphism group and the derived subgroup.

In the category of groups with homoclinisms, the isomorphisms (i.e., the invertible morphisms) are precisely the isoclinisms.

2.1.5 Homomorphisms and homoclinisms

Suppose G_1 and G_2 are groups and $\theta : G_1 \to G_2$ is a homomorphism of groups. If θ satisfies the property that $\theta(Z(G_1)) \leq Z(G_2)$, then θ induces a homoclinism of groups. Explicitly the homoclinism induced by θ is defined as (ζ, φ) where ζ and φ are as defined below.

- Since $\theta(Z(G_1)) \leq Z(G_2)$, θ descends to a homomorphism from $G_1/Z(G_1) \cong \mathrm{Inn}(G_1)$ to $G_2/Z(G_2) \cong \mathrm{Inn}(G_2)$. Denote by ζ the induced homomorphism $\mathrm{Inn}(G_1) \to \mathrm{Inn}(G_2)$.
- The restriction of θ to G_1' maps inside G_2'. Denote by φ the induced map $G_1' \to G_2'$.

It is easy to verify that (ζ, φ) defines a homoclinism.

Note that the condition $\theta(Z(G_1)) \leq Z(G_2)$ is necessary in order to be able to construct ζ.

The following are true:

- Every *surjective* homomorphism $\theta : G_1 \to G_2$ satisfies the condition that $\theta(Z(G_1)) \leq Z(G_2)$. Thus, every surjective homomorphism induces a homoclinism.

- The inclusion of a subgroup H in a group G satisfies the condition if and only if $Z(H) \leq Z(G)$, or equivalently, $Z(H) = H \cap Z(G)$. Thus, these are the subgroups whose inclusions induce homoclinisms.

2.1.6 Miscellaneous results on homoclinisms and words

Lemma 2.1.1. Suppose (ζ, φ) is a homoclinism of groups G_1 and G_2, where $\zeta : \mathrm{Inn}(G_1) \to \mathrm{Inn}(G_2)$ and $\varphi : G_1' \to G_2'$ are the component homomorphisms. Denote by $\theta_1 : G_1' \to \mathrm{Inn}(G_1)$ the composite of the inclusion of G_1' in G_1 and the projection from G_1 to $G_1/Z(G_1) = \mathrm{Inn}(G_1)$. Similarly define $\theta_2 : G_2' \to \mathrm{Inn}(G_2)$. Then, we have:

$$\zeta \circ \theta_1 = \theta_2 \circ \varphi$$

or equivalently, for any $w \in G_1'$:

$$\zeta(\theta_1(w)) = \theta_2(\varphi(w))$$

Proof. To show the equality of the two expressions, it suffices to show equality on a generating set for G_1'. By definition, the set of commutators of elements in G_1 is a generating set for G_1'. Thus, it suffices to show that:

$$\zeta(\theta_1([u, v])) = \theta_2(\varphi([u, v])) \ \forall \ u, v \in G_1$$

This is equivalent to showing that:

$$\zeta(\theta_1(\omega_{G_1}(x, y))) = \theta_2(\varphi(\omega_{G_1}(x, y))) \ \forall \ x, y \in \mathrm{Inn}(G_1)$$

Let us examine the left and right sides separately.

The left side: The expression $\theta_1(\omega_{G_1}(x, y))$ first computes the commutator of lifts of x and y in G_1, then projects to $G_1/Z(G_1)$. This is equivalent to directly computing the commutator in $G_1/Z(G_1)$, so $\theta_1(\omega_{G_1}(x,y)) = [x,y]$. Thus, the left side becomes $\zeta([x,y])$.

The right side: By the definition of homoclinism, $\varphi(\omega_{G_1}(x,y)) = \omega_{G_2}(\zeta(x),\zeta(y))$. The right side now becomes $\theta_2(\omega_{G_2}(\zeta(x),\zeta(y)))$. In other words, we are taking the lifts of $\zeta(x)$ and $\zeta(y)$ in G_2, then computing the commutator, then projecting to $G_2/Z(G_2)$. This is equivalent to directly computing the commutator in $G_2/Z(G_2)$, so the right side simplifies to $[\zeta(x),\zeta(y)]$. Since ζ is a homomorphism, this is equal to $\zeta([x,y])$, and hence agrees with the left side. $\square$

We state two important theorems. Both theorems reference the concept of a *word map*. The concept is defined and some of the properties of word maps are described in the Appendix, Section A.5.1 and the subsequent sections. However, we do not use any nontrivial facts about word maps, so it is not necessary to read that section to understand the theorems that follow.

Theorem 2.1.2. Suppose $w(g_1,g_2,\ldots,g_n)$ is a word in n letters with the property that w evaluates to the identity element in *any* abelian group. This is equivalent to saying that w, viewed as an element of the free group on $g_1,g_2,\ldots,g_n$, is in the derived subgroup. Then, for any group G, the word map $w : G^n \to G$ obtained by evaluating w descends to a map:

$$\chi_{w,G} : (\mathrm{Inn}(G))^n \to G'$$

Any word w that is an iterated commutator (with any bracketing) satisfies this condition.

Proof. Denote by $\nu : G \to \mathrm{Inn}(G)$ the quotient map.

w can be written in the form (note that the product is in general noncommutative):

$$w(g_1,g_2,\ldots,g_n) = \prod_{i=1}^{m}[u_i(g_1,g_2,\ldots,g_n), v_i(g_1,g_2,\ldots,g_n)]$$

where $u_i, v_i, 1 \leq i \leq m$ are words. Suppose $y_i \in G$ are elements for which $\nu(y_i) = x_i$.

Then:

$$w(y_1, y_2, \ldots, y_n) := \prod_{i=1}^{m} [u_i(y_1, y_2, \ldots, y_n), v_i(y_1, y_2, \ldots, y_n)]$$

We have that:

$$\nu(u_i(y_1, y_2, \ldots, y_n)) = u_i(x_1, x_2, \ldots, x_n), \qquad \nu(v_i(y_1, y_2, \ldots, y_n)) = v_i(x_1, x_2, \ldots, x_n)$$

Thus, we obtain that:

$$[u_i(y_1, y_2, \ldots, y_n), v_i(y_1, y_2, \ldots, y_n)] = \omega_G(u_i(x_1, x_2, \ldots, x_n), v_i(x_1, x_2, \ldots, x_n))$$

In particular, the expression $[u_i(y_1, y_2, \ldots, y_n), v_i(y_1, y_2, \ldots, y_n)]$ depends only on x_1, x_2, $\ldots$, x_n and not on the choice of lifts y_i. Thus, the product $w(y_1, y_2, \ldots, y_n)$ also depends only on the values of x_i, and we obtain the function:

$$\chi_{w,G}(x_1, x_2, \ldots, x_n) = \prod_{i=1}^{m} \omega_G(u_i(x_1, x_2, \ldots, x_n), v_i(x_1, x_2, \ldots, x_n))$$

□

Theorem 2.1.3. Suppose (ζ, φ) is a homoclinism of groups G_1 and G_2, where $\zeta : \mathrm{Inn}(G_1) \to \mathrm{Inn}(G_2)$ and $\varphi : G_1' \to G_2'$ are the component homomorphisms. Then for any word $w(g_1, g_2, \ldots, g_n)$ that is trivial in every abelian group (as described above), we have:

$$\chi_{w,G_2}(\zeta(x_1), \zeta(x_2), \ldots, \zeta(x_n)) = \varphi(\chi_{w,G_1}(x_1, x_2, \ldots, x_n))$$

for all $x_1, x_2, \ldots, x_n \in \text{Inn}(G)$.

Any word w that is an iterated commutator (with any order of bracketing) satisfies this condition, and the theorem applies to such word maps.

Proof. Denote by $\nu_1 : G_1 \to \text{Inn}(G_1)$ and $\nu_2 : G_2 \to \text{Inn}(G_2)$ the canonical quotient maps.

We use the same notation and steps in the proof of the preceding theorem, replacing G by G_1. We obtain:

$$w(g_1, g_2, \ldots, g_n) = \prod_{i=1}^{m} [u_i(g_1, g_2, \ldots, g_n), v_i(g_1, g_2, \ldots, g_n)]$$

where $u_i, v_i, 1 \leq i \leq m$ are words. Suppose $y_i \in G_1$ are elements for which $\nu_1(y_i) = x_i$. As demonstrated in the proof of the preceding theorem:

$$\chi_{w,G_1}(x_1, x_2, \ldots, x_n) = \prod_{i=1}^{m} \omega_{G_1}(u_i(x_1, x_2, \ldots, x_n), v_i(x_1, x_2, \ldots, x_n)) \tag{†}$$

Suppose $z_i \in G_2$ are elements for which $\nu_2(z_i) = \zeta(x_i)$. Similar reasoning to the above yields that:

$$\chi_{w,G_2}(\zeta(x_1), \zeta(x_2), \ldots, \zeta(x_n)) = \prod_{i=1}^{m} \omega_{G_2}(u_i(\zeta(x_1), \zeta(x_2), \ldots, \zeta(x_n)), v_i(\zeta(x_1), \zeta(x_2), \ldots, \zeta(x_n))) \tag{††}$$

Apply φ to both sides of (†), use the defining property of homoclinisms, and compare with (††) to obtain the result. □

2.1.7 Isoclinic groups: how similar are they?

We say that groups G_1 and G_2 are *isoclinic groups* if there exists an isoclinism from G_1 to G_2. The relation of being isoclinic is an equivalence relation. Briefly:

- The relation of being isoclinic is *reflexive* because we can choose both the isomorphisms to be the respective identity maps. Explicitly, for any group G, $(\mathrm{id}_{\mathrm{Inn}(G)}, \mathrm{id}_{G'})$ defines an isoclinism from G to itself.

- The relation of being isoclinic is *symmetric* because we can take the inverse isomorphisms to both the isomorphisms. Explicitly, if (ζ, φ) describes the isoclinism from G_1 to G_2, then $(\zeta^{-1}, \varphi^{-1})$ describes the isoclinism from G_2 to G_1.

- The relation of being isoclinic is *transitive* because we can compose both kinds of isomorphisms separately. Explicitly, if $(\zeta_{12}, \varphi_{12})$ describes the isoclinism from G_1 to G_2 and $(\zeta_{23}, \varphi_{23})$ describes the isomorphism from G_2 to G_3, then $(\zeta_{23} \circ \zeta_{12}, \varphi_{23} \circ \varphi_{12})$ describes the isoclinism from G_1 to G_3.

Here is an alternative way of seeing that being isoclinic is an equivalence relation: isoclinisms are precisely the isomorphisms in the category of groups with homoclinisms, and being isomorphic in any category is an equivalence relation.

We first list some very obvious similarities between isoclinic groups.

- They have isomorphic derived subgroups: This is direct from the definition, which includes an isomorphism between the derived subgroups.

- They have isomorphic inner automorphism groups: This is direct from the definition, which includes an isomorphism between the inner automorphism groups.

- They have precisely the same non-abelian composition factors (if the composition factors do exist): Since the center is abelian, all the non-abelian composition factors occur inside the inner automorphism group for both, which we know to be isomorphic.

- If one is nilpotent, so is the other, and they have the same nilpotency class (with the exception of class zero getting conflated with class one): The nilpotency class is one more than the nilpotency class of the inner automorphism group.

- If one is solvable, so is the other, and they have the same derived length (with the exception of length zero getting conflated with length one): The derived length is one more than the derived length of the derived subgroup.

We move to the first straightforward but somewhat non-obvious fact: isoclinic finite groups have the same *proportions* of conjugacy class sizes. The statement of the theorem is below. The proof can be found in the Appendix, Section B.3.

Theorem 2.1.4. Suppose G_1 and G_2 are isoclinic finite groups. Suppose c is a positive integer. Let m_1 be the number of conjugacy classes in G_1 of size c (so that the *total* number of elements in such conjugacy classes is m_1c). Let m_2 be the number of conjugacy classes in G_2 of size c (so that the *total* number of elements in such conjugacy classes is m_2c). Then, m_1 is nonzero if and only if m_2 is nonzero, and if so, $m_1/m_2 = |G_1|/|G_2|$.

In particular, if G_1 and G_2 additionally have the same order, then they have precisely the same multiset of conjugacy class sizes.

The next theorem is a similar result for the degrees of irreducible representations. The proof of this is also in the Appendix, Section B.3.

Theorem 2.1.5. Suppose G_1 and G_2 are isoclinic finite groups. Suppose d is a positive integer. Let m_1 denote the number of equivalence classes of irreducible representations of G_1 over $\mathbb{C}$ that have degree d. Let m_2 denote the number of equivalence classes of irreducible representations of G_2 over $\mathbb{C}$ that have degree d. Then, m_1 is nonzero if and only if m_2 is nonzero, and if so, $m_1/m_2 = |G_1|/|G_2|$.

In particular, if G_1 and G_2 additionally have the same order, then they have precisely the same multiset of degrees of irreducible representations.

Theorem 2.1.6. 1. Suppose G_1 and G_2 are isoclinic finite groups. Then, the ratio of the number of conjugacy classes in G_1 to the number of conjugacy classes in G_2 is $|G_1|/|G_2|$. In particular, if G_1 and G_2 also have the same order, they have the same number of conjugacy classes.

2. Suppose G_1 and G_2 are isoclinic finite groups. Then, the centers of their respective group algebras over $\mathbb{C}$ are both algebras that are direct products of copies of $\mathbb{C}$. The ratio of the number of copies used for G_1 and for G_2 is $|G_1|/|G_2|$. In particular, if G_1 and G_2 also have the same order, then the centers of their group algebras are isomorphic.

Proof. These follow quite directly from either of the preceding theorems. More specifically, the proof for part (1) can be deduced from either Theorem 2.1.4 or Theorem 2.1.5. Note that we can use the latter because the number of conjugacy classes equals the number of irreducible representations.

For (2), note that the center of the group algebra is a direct product of as many copies of $\mathbb{C}$ as the number of conjugacy classes. We can use the conjugacy class element sums as a basis. Alternatively, we can use the centers of the irreducible constituents in a direct sum decomposition into two-sided ideals as a basis. Thus, (2) follows directly from (1). $\square$

2.1.8 Isoclinism defines a correspondence between some subgroups

Suppose G_1 and G_2 are isoclinic groups with an isoclinism $(\zeta, \varphi) : G_1 \to G_2$ where $\zeta : \mathrm{Inn}(G_1) \to \mathrm{Inn}(G_2)$ and $\varphi : G_1' \to G_2'$ are the component isomorphisms. Then, ζ gives a correspondence:

$$\text{Subgroups of } G_1 \text{ that contain } Z(G_1) \leftrightarrow \text{Subgroups of } G_2 \text{ that contain } Z(G_2)$$

This correspondence does not preserve the isomorphism type of the subgroup, but it preserves some related structure. Explicitly, the following hold whenever a subgroup H_1 of G_1 containing $Z(G_1)$ corresponds with a subgroup H_2 of G_2 containing $Z(G_2)$:

- $H_1/Z(G_1)$ is isomorphic to $H_2/Z(G_2)$.
- H_1 and H_2 are isoclinic.
- H_1 is normal in G_1 if and only if H_2 is normal in G_2, and if so, then G_1/H_1 is isomorphic to G_2/H_2.

We have a similar correspondence given by φ:

$$\text{Subgroups of } G_1 \text{ that are contained in } G_1' \leftrightarrow \text{Subgroups of } G_2 \text{ that are contained in } G_2'$$

This correspondence preserves a number of structural features. Explicitly, the following hold if a subgroup H_1 of G_1' is in correspondence with a subgroup H_2 of G_2':

- H_1 is isomorphic to H_2
- H_1 is normal in G_1' if and only if H_2 is normal in G_2', and if so, then G_1'/H_1 is isomorphic to G_2'/H_2.
- H_1 is normal in G_1 if and only if H_2 is normal in G_2, and if so, then G_1/H_1 is isoclinic to G_2/H_2.

The two correspondences discussed above may partially overlap, and they agree with each other wherever they overlap. Explicitly, if H_1 is a subgroup of G_1 that satisfies *both the conditions* (it contains $Z(G_1)$ and is contained in G_1'), then the subgroup H_2 obtained by both correspondences is identical.

2.1.9 Characteristic subgroups, quotient groups, and subquotients determined by the group up to isoclinism

The vast majority of characteristic subgroups that we see defined (particularly for p-groups) are either contained in the derived subgroup or contain the center. The exceptions are those such as the socle and Frattini subgroup, which are smaller than the center and larger than the derived subgroup respectively.

Based on the correspondences discussed in the preceding section, we can deduce the following regarding important subgroups, quotients, and subquotients of a group G that are determined up to isomorphism by knowing G up to isoclinism:

- All lower central series member subgroups $\gamma_c(G), c \geq 2$. Note that $\gamma_1(G) = G$ needs to be excluded. Further, the isomorphism types of successive quotients between lower central series members of the form $\gamma_i(G)/\gamma_j(G)$ with $j \geq i \geq 2$ are also determined by the knowledge of G up to isoclinism. Note that the quotient groups $G/\gamma_c(G)$ are in general determined only up to isoclinism and not up to isomorphism.

- All derived series member subgroups $G^{(i)}$, $i \geq 1$. Note that we need to exclude $G^{(0)} = G$. Further, the isomorphism types of quotients between derived series members of the form $G^{(i)}/G^{(j)}$ with $j \geq i \geq 1$ are also determined by the knowledge of G up to isoclinism. Note that the quotient groups $G/G^{(i)}$ are determined only up to isoclinism and not up to isomorphism.

- Quotients $G/Z^c(G)$ for all upper central series member subgroups $Z^c(G)$, $c \geq 1$. We need to exclude $c = 0$ which would give $G/Z^0(G) = G$. Further, the isomorphism types of subquotients of the form $Z^i(G)/Z^j(G)$ where $i \geq j \geq 1$ are also determined up to isomorphism by the knowledge of G up to isoclinism. Note that the subgroups $Z^i(G)$ themselves are determined only up to isoclinism and not up to isomorphism.

2.1.10 Correspondence between abelian subgroups

Suppose G_1 and G_2 are isoclinic groups. The following are true:

- The isoclinism establishes a correspondence between abelian subgroups of G_1 containing $Z(G_1)$ and abelian subgroups of G_2 containing $Z(G_2)$. Note that the abelian subgroups that are in correspondence are not necessarily isomorphic to each other. In fact, unless $Z(G_1)$ and $Z(G_2)$ have the same order, the abelian subgroups in correspondence need not even have the same order as each other.

- The isoclinism establishes a correspondence between the abelian subgroups of G_1 that are self-centralizing and the abelian subgroups of G_2 that are self-centralizing. A self-centralizing abelian subgroup is an abelian subgroup that equals its own centralizer, or equivalently, it is a subgroup that is maximal among abelian subgroups of the group.

- In the case that G_1 and G_2 are both finite, the isoclinism establishes a correspondence between abelian subgroups of maximum order in G_1 and abelian subgroups of maximum order in G_2.

- Each of the correspondences above preserves normality.

- If G_1 and G_2 are both finite, then each of the correspondences above preserves the index of the subgroups.

In particular, this means that isoclinic finite p-groups of the same order have the same value for the maximum order of abelian subgroup, the same value for the maximum order of abelian normal subgroup, and the same values for the orders of self-centralizing abelian normal subgroups.

2.1.11 Constructing isoclinic groups

Here are some ways of constructing groups isoclinic to a given group:

- Take a direct product with an abelian group.

- Find a subgroup whose product with the center is the whole group. In symbols, if H is a subgroup of G and $HZ(G) = G$ (where $Z(G)$ denotes the center of G), then H is isoclinic to G. Note that for finite groups, this is the only way to find isoclinic subgroups to the whole group: a subgroup is isoclinic to the whole group if and only if its product with the center of the whole group is the whole group.

2.1.12 Hall's purpose in introducing isoclinism

Although this is not directly relevant, it might be helpful for historical motivation to understand why Philip Hall introduced the concept of isoclinism. At the time that Hall wrote his paper [23], very few systematic lists of finite p-groups of small order were available. Existing classifications tended to be *ad hoc* and use a bunch of invariants. In hindsight, many of these invariants were invariants up to isoclinism. As we saw in the preceding section, this is true for information about conjugacy classes and irreducible representations, and many important attributes related to characteristic subgroups and their quotient groups. However, since they were purely numerical invariants rather than invariants capturing structural information, they were too weak to meaningfully distinguish groups once the orders got large. Below are some invariants that are "good enough" to uniquely determine groups up to isoclinism for small orders, but fail at larger orders. The second column gives the smallest n for which there exist groups of order 2^n that have the same value of the invariant but are not isoclinic to each other.

Table 2.1: The smallest n for which a given isoclinism-invariant fails to classify groups of order 2^n up to isoclinism

Isoclinism-invariant (fixed order)	Smallest n where it fails to classify
Derived length	4
Nilpotency class	5
Conjugacy class sizes	5
Degrees of irreducible representations	5
Inner automorphism group	6
Derived subgroup	5
Inner automorphism group, derived subgroup	6

As the orders get bigger, numerical invariants becomes progressively more inadequate in describing the structure. They are also not helpful to computing the algebraic structure of the group.

As indicated in the table above, even knowledge of the inner automorphism group and the derived subgroup up to isomorphism does not determine the group uniquely up to isoclinism, with the smallest counterexamples occurring for order 2^6. The commutator *map* is crucial to describing the group structure up to isoclinism.

Hall sought to introduce a systematic procedure that could be used to generate all the p-groups of a particular order based on smaller groups, and group them together in ways that made it easy to compute and remember important invariants (such as their nilpotency class, number of conjugacy classes, etc.)

The use of isoclinism allows for a recursive procedure to go from order p^{n-1} to p^n. In broad strokes, the idea is as follows:

- Assume we have classified all the groups of order up to p^{n-1}, and we need to classify groups of order p^n.

- First, we need to identify the equivalence classes up to isoclinism for groups of order p^n. This involves identifying candidate pairs of inner automorphism group and derived subgroup with a candidate for the commutator map. Note that the concept of "candidate for the commutator map" is somewhat problematic without reference to the ambient group, but we will see later that it can be made precise using the concept of exterior squares. Hall did not have this formalism at his disposal, but used a similar idea in a more *ad hoc* fashion in his classification efforts.

- For each such equivalence class up to isoclinism, identify all the groups of order p^n up to isomorphism in that equivalence class up to isoclinism.

Our purpose differs somewhat from Hall's, but is broadly in the same spirit. Instead of classifying groups, we are interested in identifying some regular aspects of their behavior.

For a detailed classification that builds on Hall's ideas, see [22], which classifies groups of order 2^n for $n \leq 6$. The classification of groups of order 2^n for $n \geq 7$ was done using somewhat different methods. Specifically, the focus shifted from using isoclinism (which is based on the central series) to using the exponent-p central series, and computing immediate descendants based on the exponent-p central series. This is more amenable to computation because we are working with central extensions where the base group is elementary abelian. Algorithms in this genre are termed *nilpotent quotient algorithms*. See [27] (classification for order $2^7 = 128$), [39] (classification for order $2^8 = 256$), and [14] (general description of the classification strategy) for more details.

2.1.13 Stem groups for a given equivalence class under isoclinism

Every equivalence class of groups under isoclinism contains one or more *stem groups*. A group G is a stem group if $Z(G) \leq G'$. All stem groups for a given equivalence class under isoclinism have the same order, and the order of any isoclinic group is a multiple of this order.

Hall stated this fact, with a sketch of a proof, in his 1937 paper introducing isoclinism. We will provide a proof of the statement in Section 3.6.7 using modern language.

Here are some examples of stem groups:

- For the class of abelian groups, the unique stem group is the trivial group.
- For groups of class two with inner automorphism group a Klein four-group and derived subgroup of order two, there are two possibilities for the stem group: the dihedral group of order eight and the quaternion group of order eight.

Unlike what one might naively expect, it is not true that all groups in the equivalence class under isoclinism contain a stem group as a subquotient. For instance, the group $M_{16} = M_4(2)$ given as $\langle a, x \mid a^8 = x^2 = 1, xax = a^5 \rangle$ is a non-abelian group of order 16.[1]

1. The group has ID (16,6) in the SmallGroups library available for GAP and Magma.

This group is isoclinic to the dihedral group of order eight and the quaternion group of order eight, which are the only stem groups in that equivalence class up to isoclinism. However, M_{16} does not have any subgroup, quotient, or subquotient isomorphic to either of these groups. In fact, every proper subquotient of M_{16} is abelian.

2.1.14 Some low order classification information

In this section, we provide a quick summary of the classification of groups of order 2^n and groups of order p^n (for odd p) for small n, based on isoclinism. A detailed exposition can be found in [22] and also in some online sources included in the appendix. is also possible to explore these groups using a computational algebra package such as GAP or Magma. More information about exploring group information in GAP is available in the appendix.

The most salient information is provided below.

For groups of order 2^n: Note that the last column is the number of equivalence classes up to isoclinism of the preceding column. It can be computed by subtracting from the value of the preceding column the value in the row above for the preceding column.

Table 2.2: Number of equivalence classes up to isoclinism for groups of order 2^n

n	2^n	Number of groups	Number up to isoclinism	"New" equivalence classes
0	1	1	1	1
1	2	1	1	0
2	4	2	1	0
3	8	5	2	1
4	16	14	3	1
5	32	51	8	5
6	64	267	27	19
7	128	2328	115	88

For groups of order p^n**,** $p \geq 3$: The details depend on p, but the classification up to p^4 is independent of p, so we construct the table for n up to 4:

Table 2.3: Number of equivalence classes up to isoclinism for groups of order p^n

n	p^n	Number of groups	Number up to isoclinism	"New" equivalence classes
0	1	1	1	1
1	2	1	1	0
2	4	2	1	0
3	8	5	2	1
4	16	15	3	1

2.2 Isoclinism and homoclinism for Lie rings

The goal of this section is to establish the basic theory of *isoclinism* and *homoclinism* for *Lie rings*. The theory is analogous to the theory for groups developed in the preceding section (Section 2.1.

Informally, a homoclinism of Lie rings is a homomorphism between the *Lie bracket structures* of the Lie rings. Informally, two Lie rings are isoclinic if their Lie bracket maps are equivalent. Isoclinism defines an equivalence relation on the collection of Lie rings. Under this equivalence relation, all abelian Lie rings are equivalent to the trivial group.

The original results that we present later (Section 5.4 and 7.7) describe bijective correspondences between certain equivalence classes of groups and certain equivalence classes of Lie rings. The equivalence classes of Lie rings are based on the equivalence relation of isoclinism of Lie rings.

2.2.1 Definitions of homoclinism and isoclinism

The notion of isoclinism of Lie algebras seems to have been introduced by Moneyhun in [38]. We introduce a corresponding notion of homoclinism to parallel the notion for groups. The historical origin of the notion of homoclinism for Lie rings is unclear, but it appears for instance in the paper [40] published in 2011.

For simplicity, we restrict attention to the case of Lie *rings*, which are Lie algebras over the ring of integers. All our definitions and theorems here have very natural analogues in Lie algebras over other commutative unital rings. Note that if two Lie algebras over a commutative unital ring are isoclinic as Lie algebras over that ring, they are also isoclinic as Lie rings. In the Appendix, Section A.1.4, we describe the theory of Lie algebras over arbitrary commutative unital rings, and how the general theory of Lie algebras relates to the theory of Lie rings.

For a Lie ring L, denote by $\mathrm{Inn}(L)$ the inner derivation Lie ring of L, denote by L' the derived subring of L, and denote by $Z(L)$ the center of L. $\mathrm{Inn}(L)$ is canonically isomorphic to the quotient ring $L/Z(L)$. (For other notation related to Lie rings that we use in this document, see Section 1.0.3).

The *Lie bracket* map in L descends to a map:

$$\omega_L : \mathrm{Inn}(L) \times \mathrm{Inn}(L) \to L'$$

Note that ω_L is $\mathbb{Z}$-bilinear, but the additional structure on it (that is forced from its arising as a Lie bracket) is hard to describe explicitly. In Section 3.5.1, we will describe a structure called the exterior square of a Lie ring and reframe the condition on ω_L as being a bilinear map that induces a homomorphism from the exterior square. This situation is similar to the situation for groups we discussed earlier, but somewhat easier to describe because of the underlying additive group structure.

Suppose L_1 and L_2 are Lie rings. The Lie brackets of L_1 and L_2 respectively induce $\mathbb{Z}$-bilinear maps:

$$\omega_{L_1} : \mathrm{Inn}(L_1) \times \mathrm{Inn}(L_1) \to L_1'$$

$$\omega_{L_2} : \mathrm{Inn}(L_2) \times \mathrm{Inn}(L_2) \to L_2'$$

A *homoclinism* from L_1 to L_2 is a pair of homomorphisms (ζ, φ) where ζ is a homomorphism from $\mathrm{Inn}(L_1)$ to $\mathrm{Inn}(L_2)$ and φ is an homomorphism from L_1' to L_2', satisfying the condition that:

$$\varphi \circ \omega_{L_1} = \omega_{L_2} \circ (\zeta \times \zeta)$$

More explicitly, for any $x, y \in \mathrm{Inn}(L_1)$, we require that:

$$\varphi(\omega_{L_1}(x, y)) = \omega_{L_2}(\zeta(x), \zeta(y))$$

Pictorially, the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Inn}(L_1) \times \mathrm{Inn}(L_1) & \stackrel{\zeta \times \zeta}{\rightarrow} & \mathrm{Inn}(L_2) \times \mathrm{Inn}(L_2) \\ \downarrow^{\omega_{L_1}} & & \downarrow^{\omega_{L_2}} \\ L_1' & \stackrel{\varphi}{\rightarrow} & L_2' \end{array}$$

The homoclinism (ζ, φ) from L_1 to L_2 is termed an *isoclinism* if both ζ and φ are isomorphisms of Lie rings.

We compose homoclinisms of Lie rings by separately composing the homomorphisms on the inner derivation Lie rings and on the derived subrings. Explicitly, suppose $(\zeta_{12}, \varphi_{12})$ is a homoclinism from L_1 to L_2 and suppose $(\zeta_{23}, \varphi_{23})$ is a homoclinism from L_2 to L_3. Then, the composite $(\zeta_{23}, \varphi_{23}) \circ (\zeta_{12}, \varphi_{12})$ is $(\zeta_{23} \circ \zeta_{12}, \varphi_{23} \circ \varphi_{12})$. The proof that this works follows from the commutativity of this diagram.

$$\begin{array}{ccccc} \mathrm{Inn}(L_1) \times \mathrm{Inn}(L_1) & \stackrel{\zeta_{12} \times \zeta_{12}}{\rightarrow} & \mathrm{Inn}(L_2) \times \mathrm{Inn}(L_2) & \stackrel{\zeta_{23} \times \zeta_{23}}{\rightarrow} & \mathrm{Inn}(L_3) \times \mathrm{Inn}(L_3) \\ \downarrow^{\omega_{G_1}} & & \downarrow^{\omega_{G_2}} & & \downarrow^{\omega_{G_3}} \\ L_1' & \stackrel{\varphi_{12}}{\rightarrow} & L_2' & \stackrel{\varphi_{23}}{\rightarrow} & L_3' \end{array}$$

As was the case with groups, we can define a category where the morphisms are homoclinisms.

Definition (Category of Lie rings with homoclinisms)**.** The *category of Lie rings with* *homoclinisms* is defined as the following category:

- The *objects* of the category are Lie rings.
- The *morphisms* of the category are homoclinisms of Lie rings.
- Composition of morphisms is composition of homoclinisms.
- The identity morphism is the identity homoclinism: it is the identity map both on the inner derivation Lie ring and on the derived subring.

In the category of Lie rings with homoclinisms, the isomorphisms (i.e., the invertible morphisms) are precisely the isoclinisms.

2.2.2 Homomorphisms and homoclinisms

Suppose L_1 and L_2 are Lie rings and $\theta : L_1 \to L_2$ is a homomorphism of Lie rings. If θ satisfies the property that $\theta(Z(L_1)) \leq Z(L_2)$, then θ induces a homoclinism of Lie rings. Explicitly the homoclinism induced by θ is defined as (ζ, φ) where ζ and φ are as defined below.

- Since $\theta(Z(L_1)) \leq Z(L_2)$, θ descends to a homomorphism from $L_1/Z(L_1) \cong \mathrm{Inn}(L_1)$ to $L_2/Z(L_2) \cong \mathrm{Inn}(L_2)$. Denote by ζ the induced homomorphism $\mathrm{Inn}(L_1) \to \mathrm{Inn}(L_2)$.
- The restriction of θ to L_1' maps inside L_2'. Denote by φ the induced map $L_1' \to L_2'$.

It is easy to verify that (ζ, φ) defines a homoclinism.

Note that the condition $\theta(Z(L_1)) \leq Z(L_2)$ is necessary in order to be able to construct ζ.

The following are true:

- Every *surjective* homomorphism $\theta : L_1 \to L_2$ satisfies the condition that $\theta(Z(L_1)) \leq Z(L_2)$. Thus, every surjective homomorphism induces a homoclinism.

- The inclusion of a Lie subring M in a Lie ring L satisfies the condition if and only if $Z(M) \leq Z(L)$, or equivalently, $Z(M) = M \cap Z(L)$. Thus, these are the subrings whose inclusions induce homoclinisms.

2.2.3 Miscellaneous results on homoclinisms and words

Lemma 2.2.1. Suppose (ζ, φ) is a homoclinism of Lie rings L_1 and L_2, where $\zeta : \mathrm{Inn}(L_1) \to \mathrm{Inn}(L_2)$ and $\varphi : L_1' \to L_2'$ are the component homomorphisms. Denote by $\theta_1 : L_1' \to \mathrm{Inn}(L_1)$ the composite of the inclusion of L_1' in L_1 and the projection from L_1 to $L_1/Z(L_1) = \mathrm{Inn}(L_1)$. Similarly define $\theta_2 : L_2' \to \mathrm{Inn}(L_2)$. Then, we have:

$$\zeta \circ \theta_1 = \theta_2 \circ \varphi$$

or equivalently, for any $w \in L_1'$:

$$\zeta(\theta_1(w)) = \theta_2(\varphi(w))$$

Proof. To show the equality of the two expressions, it suffices to show equality on a generating set for L_1'. By definition, the set of Lie brackets of elements in L_1 is a generating set for L_1'. Thus, it suffices to show that:

$$\zeta(\theta_1([u, v])) = \theta_2(\varphi([u, v])) \ \forall \ u, v \in L_1$$

This is equivalent to showing that:

$$\zeta(\theta_1(\omega_{L_1}(x, y))) = \theta_2(\varphi(\omega_{L_1}(x, y))) \ \forall \ x, y \in \mathrm{Inn}(L_1)$$

Let us examine the left and right sides separately.

The left side: The expression $\theta_1(\omega_{L_1}(x, y))$ first computes the Lie bracket of lifts of x and y in L_1, then projects to $L_1/Z(L_1)$. This is equivalent to directly computing the Lie bracket in $L_1/Z(L_1)$, so $\theta_1(\omega_{L_1}(x, y)) = [x, y]$. Thus, the left side becomes $\zeta([x, y])$.

The right side: By the definition of homoclinism, $\varphi(\omega_{L_1}(x, y)) = \omega_{L_2}(\zeta(x), \zeta(y))$. The right side now becomes $\theta_2(\omega_{L_2}(\zeta(x), \zeta(y)))$. In other words, we are taking the lifts of $\zeta(x)$ and $\zeta(y)$ in L_2, then computing the Lie bracket, then projecting to $L_2/Z(L_2)$. This is equivalent to directly computing the Lie bracket in $L_2/Z(L_2)$, so the right side simplifies to $[\zeta(x), \zeta(y)]$. Since ζ is a homomorphism, this is equal to $\zeta([x, y])$, and hence agrees with the left side. $\square$

We state two important theorems.

Theorem 2.2.2. Suppose $w(g_1, g_2, \ldots, g_n)$ is a word in n letters with the property that w evaluates to the zero element in *any* abelian Lie ring. This is equivalent to saying that w, viewed as an element of the free Lie ring on $g_1, g_2, \ldots, g_n$, is in the derived subring. Then, for any Lie ring L, the word map $w : L^n \to L$ obtained by evaluating w descends to a map:

$$\chi_{w,L} : (\mathrm{Inn}(L))^n \to L'$$

Any word w that is an iterated Lie bracket (with any bracketing) satisfies this condition.

Proof. Denote by $\nu : L \to \mathrm{Inn}(L)$ the quotient map.

w can be written in the form:

$$w(g_1, g_2, \ldots, g_n) = \sum_{i=1}^{m} [u_i(g_1, g_2, \ldots, g_n), v_i(g_1, g_2, \ldots, g_n)]$$

where $u_i, v_i, 1 \le i \le m$ are words. Suppose $y_i \in L$ are elements for which $\nu(y_i) = x_i$. Then:

$$w(y_1, y_2, \ldots, y_n) = \sum_{i=1}^{m} [u_i(y_1, y_2, \ldots, y_n), v_i(y_1, y_2, \ldots, y_n)]$$

We have that:

$$\nu(u_i(y_1, y_2, \ldots, y_n)) = u_i(x_1, x_2, \ldots, x_n), \qquad \nu(v_i(y_1, y_2, \ldots, y_n)) = v_i(x_1, x_2, \ldots, x_n)$$

Thus, we obtain that:

$$[u_i(y_1, y_2, \ldots, y_n), v_i(y_1, y_2, \ldots, y_n)] = \omega_L(u_i(x_1, x_2, \ldots, x_n), v_i(x_1, x_2, \ldots, x_n))$$

In particular, the expression $[u_i(y_1, y_2, \ldots, y_n), v_i(y_1, y_2, \ldots, y_n)]$ depends only on x_1, x_2, $\ldots$, x_n and not on the choice of lifts y_i. Thus, the sum $w(y_1, y_2, \ldots, y_n)$ also depends only on the values of x_i, and we obtain the function:

$$\chi_{w,L}(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{m} \omega_L(u_i(x_1, x_2, \ldots, x_n), v_i(x_1, x_2, \ldots, x_n))$$

□

Theorem 2.2.3. Suppose (ζ, φ) is a homoclinism of Lie rings L_1 and L_2, where $\zeta : \mathrm{Inn}(L_1) \to \mathrm{Inn}(L_2)$ and $\varphi : L_1' \to L_2'$ are the component homomorphisms. Then for any word $w(g_1, g_2, \ldots, g_n)$ that is trivial in every abelian Lie ring (as described above), we have:

$$\chi_{w,L_2}(\zeta(x_1), \zeta(x_2), \ldots, \zeta(x_n)) = \varphi(\chi_{w,L_1}(x_1, x_2, \ldots, x_n))$$

for all $x_1, x_2, \ldots, x_n \in \mathrm{Inn}(L)$.

Any word w that is an iterated Lie bracket (with any order of bracketing) satisfies this condition, and the theorem applies to such word maps.

Proof. Denote by $\nu_1 : L_1 \to \mathrm{Inn}(L_1)$ and $\nu_2 : L_2 \to \mathrm{Inn}(L_2)$ the canonical quotient maps.

We use the same notation and steps in the proof of the preceding theorem, replacing L by L_1. We obtain:

$$w(g_1, g_2, \dots, g_n) := \sum_{i=1}^{m} [u_i(g_1, g_2, \dots, g_n), v_i(g_1, g_2, \dots, g_n)]$$

where $u_i, v_i, 1 \leq i \leq m$ are words. Suppose $y_i \in L_1$ are elements for which $\nu_1(y_i) = x_i$. As demonstrated in the proof of the preceding theorem:

$$\chi_{w,L_1}(x_1, x_2, \dots, x_n) = \sum_{i=1}^{m} \omega_{L_1}(u_i(x_1, x_2, \dots, x_n), v_i(x_1, x_2, \dots, x_n)) \tag{†}$$

Suppose $z_i \in L_2$ are elements for which $\nu_2(z_i) = \zeta(x_i)$. Similar reasoning to the above yields that:

$$\chi_{w,L_2}(\zeta(x_1), \zeta(x_2), \dots, \zeta(x_n)) = \sum_{i=1}^{m} \omega_{L_2}(u_i(\zeta(x_1), \zeta(x_2), \dots, \zeta(x_n)), v_i(\zeta(x_1), \zeta(x_2), \dots, \zeta(x_n))) \tag{††}$$

Apply φ to both sides of (†), use the defining property of homoclinisms, and compare with (††) to obtain the result. $\square$

2.2.4 Isoclinic Lie rings: how similar are they?

We say that L_1 and L_2 are isoclinic Lie rings if there is an isoclinism of Lie rings from L_1 to L_2. The relation of being isoclinic is an equivalence relation. Briefly:

- The relation of being isoclinic is *reflexive* because we can choose both the isomorphisms to be the identity maps. Explicitly, for any Lie ring L, $(\mathrm{id}_{\mathrm{Inn}(L)}, \mathrm{id}_{L'})$ defines an isoclinism from L to itself.

- The relation of being isoclinic is *symmetric* because we can take the inverse isomorphisms to both the isomorphisms. Explicitly, if (ζ, φ) describes the isoclinism from L_1

to L_2, then $(\zeta^{-1}, \varphi^{-1})$ describes the isoclinism from L_2 to L_1.

- The relation of being isoclinic is *transitive* because we can compose both kinds of isomorphisms separately. Explicitly, if $(\zeta_{12}, \varphi_{12})$ describes the isoclinism from L_1 to L_2 and $(\zeta_{23}, \varphi_{23})$ describes the isomorphism from L_2 to L_3, then $(\zeta_{23} \circ \zeta_{12}, \varphi_{23} \circ \varphi_{12})$ describes the isoclinism from L_1 to L_3.

Here is an alternative way of seeing that being isoclinic is an equivalence relation: isoclinisms are precisely the isomorphisms in the category of Lie rings with homoclinisms, and being isomorphic in any category is an equivalence relation.

We first list some very obvious similarities between isoclinic Lie rings.

- They have isomorphic derived subrings: This is direct from the definition, which includes an isomorphism of the derived subrings.

- They have isomorphic inner derivation Lie rings: This is direct from the definition, which includes an isomorphism between the inner derivation Lie rings.

- They have precisely the same non-abelian composition factors (if the composition factors do exist): Since the center is abelian, all the non-abelian composition factors occur inside the inner derivation Lie ring for both, which we know to be isomorphic.

- If one is nilpotent, so is the other, and they have the same nilpotency class (with the exception of class zero getting conflated with class one): The nilpotency class is one more than the nilpotency class of the inner derivation Lie ring.

- If one is solvable, so is the other, and they have the same derived length (with the exception of length zero getting conflated with length one): The derived length is one more than the derived length of the derived subring.

Note that conjugacy class sizes and degrees of irreducible representations do not make direct sense for Lie rings. But there are important analogues of these statements that apply in a number of cases. In Section 8.2.6, we discuss the Kirillov orbit method, which relates the irreducible representations of a group with its Lazard Lie ring.

2.2.5 Isoclinism defines a correspondence between some subrings

Suppose L_1 and L_2 are isoclinic Lie rings with an isoclinism $(\zeta, \varphi) : L_1 \to L_2$ where $\zeta : \mathrm{Inn}(L_1) \to \mathrm{Inn}(L_2)$ and $\varphi : L_1' \to L_2'$ are the component isomorphisms. Then, ζ gives a correspondence:

Lie subrings of L_1 that contain $Z(L_1) \leftrightarrow$ Lie subrings of L_2 that contain $Z(L_2)$

This correspondence does not preserve the isomorphism type of the subring, but it preserves some related structure. Explicitly, the following hold whenever a subring M_1 of L_1 corresponds with a subring M_2 of L_2:

- $M_1/Z(L_1)$ is isomorphic to $M_2/Z(L_2)$.
- M_1 and M_2 are isoclinic.
- M_1 is an ideal in L_1 if and only if M_2 is an ideal in L_2, and if so, then L_1/M_1 is isomorphic to L_2/M_2.

We have a similar correspondence given by φ:

Lie subrings of L_1 that are contained in $L_1' \leftrightarrow$ Lie subrings of L_2 that are contained in L_2'

This correspondence preserves a number of structural features. Explicitly, the following hold whenever a subring M_1 of L_1 is in correspondence with a subring M_2 of L_2:

- M_1 is isomorphic to M_2
- M_1 is an ideal in L_1' if and only if M_2 is an ideal in L_2', and if so, then L_1'/M_1 is isomorphic to L_2'/M_2.
- M_1 is an ideal in L_1 if and only if M_2 is an ideal in L_2, and if so, then L_1/M_1 is isoclinic to L_2/M_2.

The two correspondences discussed above overlap somewhat, and they agree with each other wherever they overlap. Explicitly, if M_1 is a subring of L_1 that contains $Z(L_1)$ and is contained in L_1', then the M_2 obtained by both correspondences is identical.

2.2.6 Characteristic subrings, quotient rings, and subquotients determined by the Lie ring up to isoclinism

We can deduce the following regarding important characteristic subrings, quotients, and subquotients of a Lie ring L that are determined up to isomorphism by knowing L up to isoclinism:

- All lower central series member subrings $\gamma_c(L), c \geq 2$. Note that $\gamma_1(L) = L$ needs to be excluded. Further, the isomorphism types of successive quotients between lower central series members of the form $\gamma_i(L)/\gamma_j(L)$ with $j \geq i \geq 2$ are also determined by the knowledge of L up to isoclinism. Note that the quotient rings $L/\gamma_c(L)$ are in general determined only up to isoclinism and not up to isomorphism.

- All derived series member subrings $L^{(i)}$, $i \geq 1$. Note that we need to exclude $L^{(0)} = L$. Further, the isomorphism types of quotients between derived series members of the form $L^{(i)}/L^{(j)}$ with $j \geq i \geq 1$ are also determined by the knowledge of L up to isoclinism. Note that the quotient Lie rings $L/L^{(i)}$ are determined only up to isoclinism and not up to isomorphism.

- Quotients $L/Z^c(L)$ for all upper central series member subrings $Z^c(L)$, $c \geq 1$. We need to exclude $c = 0$ which would give $L/Z^0(L) = L$. Further, the isomorphism types of subquotients of the form $Z^i(L)/Z^j(L)$ where $i \geq j \geq 1$ are also determined up to isomorphism by the knowledge of L up to isoclinism. Note that the subrings $Z^i(L)$ themselves are determined only up to isoclinism and not up to isomorphism.

2.2.7 Correspondence between abelian subrings

Suppose L_1 and L_2 are isoclinic Lie rings. The following are true:

- The isoclinism establishes a correspondence between abelian subrings of L_1 containing $Z(L_1)$ and abelian subrings of L_2 containing $Z(L_2)$. Note that the abelian subrings that are in correspondence are not necessarily isomorphic to each other. In fact, unless $Z(L_1)$ and $Z(L_2)$ have the same order, the abelian subrings in correspondence need not even have the same order as each other.

- The isoclinism establishes a correspondence between the abelian subrings of L_1 that are self-centralizing and the abelian subrings of L_2 that are self-centralizing. A self-centralizing abelian subring is an abelian subring that equals its own centralizer, or equivalently, it is maximal among abelian subrings of the Lie ring.

- In the case that L_1 and L_2 are both finite, the isoclinism establishes a correspondence between abelian subrings of maximum order in L_1 and abelian subrings of maximum order in L_2.

If L_1 and L_2 are both finite, then each of the correspondences above preserves the index of the subrings. In particular, this means that isoclinic finite Lie rings of the same order have the same value for the maximum order of abelian subring, the same value for the maximum order of abelian ideal, and the same value for the orders of self-centralizing abelian subrings.

2.2.8 Constructing isoclinic Lie rings

Here are some ways of constructing Lie rings isoclinic to a given Lie ring:

- Take a direct product with an abelian Lie ring.

- Find a Lie subring whose sum with the center is the whole Lie ring. In symbols, if M is a subring of L and $M + Z(L) = L$ (where $Z(L)$ denotes the center of L), then M

is isoclinic to L. Note that for finite Lie rings, this is the only way to find isoclinic subrings to the whole Lie ring: a subring is isoclinic to the whole Lie ring if and only if its sum with the center of the whole ring is the whole ring.

CHAPTER 3

EXTENSION THEORY

3.1 Short exact sequences and central group extensions

Central extensions are fundamental to how we think about nilpotent groups: nilpotent groups can be thought of as groups that can be obtained by iteratively taking central extensions, starting with an abelian group. The notion of central extension is also closely related to the notion of isoclinism, although we will defer the explicit connection for later. Central extensions are instrumental to formulating and proving the generalizations that we develop in Sections 5.4 and 7.7.

In this section, we develop the rudimentary vocabulary of central extensions.

3.1.1 Definition of short exact sequence and group extension

A *short exact sequence of groups* is an exact sequence of groups with homomorphisms as follows:

$$1 \to A \to E \to G \to 1$$

In words, the homomorphism from A to E is injective, the homomorphism from E to G is surjective, and the image of A in E equals the kernel of the homomorphism from E to G. The standard abuse of notation identifies A with its image in E (so A is viewed as a normal subgroup of E) and G with the quotient group E/A.

We may also frame this as follows: E is a *group extension* with normal subgroup A and quotient group G.

A *morphism of short exact sequences* from a short exact sequence:

$$1 \to A_1 \to E_1 \to G_1 \to 1$$

to another short exact sequence:

$$1 \to A_2 \to E_2 \to G_2 \to 1$$

is defined as a triple of homomorphisms $A_1 \to A_2$, $E_1 \to E_2$, $G_1 \to G_2$, such that the following diagram commutes:

$$\begin{array}{ccccc} 1 & \to A_1 & \to E_1 & \to G_1 & \to 1 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & \to A_2 & \to E_2 & \to G_2 & \to 1 \end{array}$$

Note that the arrows at the extremes do not convey useful information, so the above is equivalent to asserting that the following diagram commutes:

$$\begin{array}{ccccc} 1 & \to A_1 & \to E_1 & \to G_1 & \to 1 \\ & \downarrow & \downarrow & \downarrow & \\ 1 & \to A_2 & \to E_2 & \to G_2 & \to 1 \end{array}$$

We can compose two morphisms of short exact sequences in the obvious way. In the diagram below, this corresponds to composing the vertical morphisms:

$$\begin{array}{ccccc} 1 & \to A_1 & \to E_1 & \to G_1 & \to 1 \\ & \downarrow & \downarrow & \downarrow & \\ 1 & \to A_2 & \to E_2 & \to G_2 & \to 1 \\ & \downarrow & \downarrow & \downarrow & \\ 1 & \to A_3 & \to E_3 & \to G_3 & \to 1 \end{array}$$

We can thus define a *category of short exact sequences*. An *isomorphism of short exact sequences* is defined as an isomorphism in this category. Explicitly, it is defined as a morphism of short exact sequences where all the component homomorphisms are isomorphisms.

3.1.2 Group extensions with fixed base and quotient; congruence and pseudo-congruence

We often study group extensions of the form:

$$1 \to A \to E \to G \to 1$$

where A and G are both fixed in advance and different possibilities for E are considered. Two group extensions:

$$1 \to A \to E_1 \to G \to 1$$

and

$$1 \to A \to E_2 \to G \to 1$$

are said to be *congruent* if there is an isomorphism $\varphi : E_1 \to E_2$ such that the triple comprising the identity map $A \to A$, the map $\varphi : E_1 \to E_2$, and the identity map $G \to G$ give an isomorphism of short exact sequences. In other words, we can get an isomorphism from E_1 to E_2 that induces the identity maps both on the subgroup A and the quotient group G.

Congruence defines an equivalence relation on the set of all group extensions with normal subgroup A and quotient group G. The equivalence classes for this equivalence relation are termed *congruence classes*.

Two group extensions:

$$1 \to A \to E_1 \to G \to 1$$

and

$$1 \to A \to E_2 \to G \to 1$$

are said to be *pseudo-congruent* if there is an isomorphism between the short exact sequences. The isomorphism need not induce the identity map on A and need not induce the identity map on G.

Pseudo-congruence defines an equivalence relation on the set of all group extensions with normal subgroup A and quotient group G. The equivalence classes for this equivalence relation are termed *pseudo-congruence classes*.

Pseudo-congruence is a coarser equivalence relation than congruence because it allows for "re-labeling" on both the subgroup side and the quotient group side.

3.1.3 Abelian normal subgroups

In the case that A is an abelian group, the short exact sequence:

$$1 \to A \to E \to G \to 1$$

may also be written as

$$0 \to A \to E \to G \to 1$$

This is because when working with abelian groups, we denote the trivial group by 0 instead of 1.

3.1.4 Central extensions and stem extensions

In this document, we use the term *central subgroup* for a subgroup that is contained inside the center.

A *central extension* refers to a group extension where the subgroup is central. Explicitly, consider a short exact sequence of the following form, where A is abelian:

$$0 \to A \to E \to G \to 1$$

We say that E is a *central extension* with central subgroup A and quotient group G if the image of A in E is a central subgroup of E. If we engage in the usual abuse of notation that conflates A with its image in E, we could shorten this to saying that A is a central subgroup of E.

We will often say "E is a central extension of G" as shorthand for "there exists an abelian group A such that E is a central extension with central subgroup A and quotient group G."

A *stem extension* is a central extension where the central subgroup is also contained in the derived subgroup of the extension group. Explicitly, consider a short exact sequence of the following form, where A is abelian:

$$0 \to A \to E \to G \to 1$$

We say that E is a *stem extension* with central subgroup A and quotient group G if the image of A in E is contained in $E' \cap Z(E)$.

3.1.5 *The use of cohomology groups to classify central extensions*

Suppose A is an abelian group and G is a group. The group $H^2(G; A)$ (also denoted $H^2(G, A)$), called the *second cohomology group for trivial group action* of G on A, is a group whose elements correspond to the congruence classes of central extensions with central subgroup A and quotient group G. Here, by "congruence class" we mean equivalence class under the equivalence relation of being congruent group extensions. The group structure on $H^2(G; A)$ is not *prima facie* obvious. We will describe it in detail in Section 3.3.

Further, there is a natural action of $\mathrm{Aut}(G) \times \mathrm{Aut}(A)$ on $H^2(G; A)$ and the orbits of $H^2(G; A)$ under this natural action correspond precisely to the pseudo-congruence classes of central extensions with central subgroup A and quotient group G.

Note that there is a more general definition of the second cohomology group that works for non-central extensions where the action of the quotient group G on the abelian normal subgroup A is specified. Throughout this document, however, when referring to the second cohomology group, we mean the second cohomology group for trivial group action.

Basic background about the second cohomology group can be found in [3], [28], [10], or in any standard reference on group cohomology.

3.1.6 Homomorphism of central extensions

In the discussion so far, we have fixed both the normal subgroup A and the quotient group G and considered possibilities for the group extension. We now consider the case where the quotient group G is fixed. We are interested in all central extensions with quotient group G. The theory undergirding these should be hidden within the group structure of G. Our goal is to make that theory more explicit. Unfortunately, this is a long task, and we therefore only include a first step here. We will pick up from where we leave here in Section 3.4.1.

We begin by defining the concept of *homomorphism of central extensions*. Consider two central extensions, both of which have G as the quotient group:

$$0 \to A_1 \to E_1 \to G \to 1$$

and

$$0 \to A_2 \to E_2 \to G \to 1$$

A homomorphism of central extensions from the first central extension to the second is a pair of homomorphisms $A_1 \to A_2$, $E_1 \to E_2$, that, together with the identity map $G \to G$, give a homomorphism of short exact sequences.

We can consider the *category of central extensions* of G:

- The *objects* of this category are the central extensions with quotient group G.
- The *morphisms* of this category are homomorphisms of central extensions of G, as defined above.
- Composition of morphisms is defined as the usual composition of homomorphisms of short exact sequences.

An object in the category of central extensions can be completely described up to isomorphism in this category simply by specifying its right map. Explicitly, consider two central extensions:

$$0 \to A_1 \to E \xrightarrow{\nu} G \to 1$$

and

$$0 \to A_2 \to E \xrightarrow{\nu} G \to 1$$

where the map ν is the same in both cases. In that case, the central extensions are isomorphic in the category. Explicitly, this is because if we consider the partial commutative diagram:

$$\begin{array}{ccccccc} 0 & \to A_1 & \to E & \xrightarrow{\nu} G & \to 1 \\ & & \downarrow^{\text{id}} & \downarrow^{\text{id}} & \\ 0 & \to A_2 & \to E & \xrightarrow{\nu} G & \to 1 \end{array}$$

there is a unique choice of isomorphism $A_1 \to A_2$ so that the diagram as a whole commutes:

$$\begin{array}{ccccccc} 0 & \to A_1 & \to E & \xrightarrow{\nu} G & \to 1 \\ & \downarrow & \downarrow^{\text{id}} & \downarrow^{\text{id}} & \\ 0 & \to A_2 & \to E & \xrightarrow{\nu} G & \to 1 \end{array}$$

Further, specifying a homomorphism from one object:

$$0 \to A_1 \to E_1 \stackrel{\nu_1}{\to} G \to 1$$

to another:

$$0 \to A_2 \to E_2 \stackrel{\nu_2}{\to} G \to 1$$

is equivalent to simply specifying the homomorphism $E_1 \to E_2$, because the homomorphism $A_1 \to A_2$ is uniquely determined by it. Explicitly, this is because in the commutative diagram:

$$\begin{array}{ccccccccc}
0 & \to A_1 & \to E_1 & \stackrel{\nu_1}{\to} G & \to 1 \\
 & & \downarrow^{\theta} & \downarrow^{\text{id}} & \\
0 & \to A_2 & \to E_2 & \stackrel{\nu_2}{\to} G & \to 1
\end{array}$$

there is a unique morphism $A_1 \to A_2$ that completes the commutative diagram.

Further, the set of permissible homomorphisms $E_1 \to E_2$ is precisely the set of homomorphisms $\theta : E_1 \to E_2$ such that $\nu_2 \circ \theta = \nu_1$.

The *category of central extensions* of G thus has the following alternative description. Note that strictly speaking, this is a different category, but the preceding remarks establish that there is a canonical *equivalence of categories* between the categories.

- The *objects* of the category are "central extensions" of G in the sense of being pairs (E, ν) where $\nu : E \to G$ is a surjective group homomorphism and the kernel of ν is central in G.

- Given two objects (E_1, ν_1) and (E_2, ν_2) in the category, a *morphism* between them is a homomorphism $\theta : E_1 \to E_2$ such that $\nu_2 \circ \theta = \nu_1$.

The equivalence of categories is given by the obvious forgetful functor from the short exact sequence category to this new category, that sends a short exact sequence $0 \to A \to$

$E \xrightarrow{\nu} G \to 1$ to the quotient map $E \xrightarrow{\nu} G$. The functor is clearly essentially surjective (in fact, it is surjective on objects). The preceding remarks establish that the functor is full and faithful, and therefore an equivalence of categories. From this point onward, we we talk of the "category of central extensions of G" we will refer to the latter category.

We might hope that this category has an initial object, which could then serve as the "source" classifying central extensions of G. However, such an initial object does not always exist. We will show in Section 3.4.7 that there *do* exist objects in this category that admit homomorphisms to every other object in the category. These are not in general initial objects because the homomorphisms admitted are not unique.

3.2 Short exact sequences and central extensions of Lie rings

In this section, we develop the theory of short exact sequences of Lie rings parallel to the development in the preceding section (Section 3.1) of the theory for groups. The sections are almost completely analogous and readers who have thoroughly understood the preceding section can safely skip this section. The reasons behind developing the theory are also analogous to those offered for groups.

The underlying theory for the cohomology group is different in substantive ways for groups and Lie rings. However, these differences do not show up at the level of abstraction at which we are dealing with groups and Lie rings in this and the preceding section.

3.2.1 Definition of short exact sequence and Lie ring extension

A *short exact sequence of Lie rings* is an exact sequence of Lie rings with homomorphisms as follows:

$$0 \to A \to N \to L \to 0$$

In words, the homomorphism from A to N is injective, the homomorphism from N to L

is surjective, and the image of A in N equals the kernel of the homomorphism from N to L. The standard abuse of notation identifies A with its image in N (so A is viewed as an ideal of N) and L with the quotient Lie ring N/A.

We may also frame this as follows: N is a *Lie ring extension* with (base) ideal A and quotient Lie ring L.

A *morphism of short exact sequences* from a short exact sequence:

$$0 \to A_1 \to N_1 \to L_1 \to 0$$

to another short exact sequence:

$$0 \to A_2 \to N_2 \to L_2 \to 0$$

is defined as a triple of homomorphisms $A_1 \to A_2$, $N_1 \to N_2$, $L_1 \to L_2$, such that the following diagram commutes:

$$\begin{array}{ccccc} 0 & \to A_1 & \to N_1 & \to L_1 & \to 0 \\ \downarrow & \downarrow & \downarrow & \downarrow & \\ 0 & \to A_2 & \to N_2 & \to L_2 & \to 0 \end{array}$$

Note that the arrows at the extremes do not convey useful information, so this is equivalent to saying that the following diagram commutes:

$$\begin{array}{ccccc} 0 & \to A_1 & \to N_1 & \to L_1 & \to 0 \\ & \downarrow & \downarrow & \downarrow & \\ 0 & \to A_2 & \to N_2 & \to L_2 & \to 0 \end{array}$$

We can compose two morphisms of short exact sequences in the obvious way. In the diagram below, this corresponds to composing the vertical morphisms:

$$
\begin{array}{ccccccccc}
0 & \to A_1 & \to N_1 & \to L_1 & \to 0 \\
 & \downarrow & \downarrow & \downarrow & \\
0 & \to A_2 & \to N_2 & \to L_2 & \to 0 \\
 & \downarrow & \downarrow & \downarrow & \\
0 & \to A_3 & \to N_3 & \to L_3 & \to 0
\end{array}
$$

We can thus define a *category of short exact sequences*. An *isomorphism of short exact sequences* is defined as an isomorphism in this category. Explicitly, it is defined as a morphism of short exact sequences where all the component homomorphisms are isomorphisms.

3.2.2 Lie ring extensions with fixed base and quotient; congruence and pseudo-congruence

We often study Lie ring extensions of the form:

$$0 \to A \to N \to L \to 0$$

where A and L are both fixed in advance and different possibilities for N are considered. Two Lie ring extensions:

$$0 \to A \to N_1 \to L \to 0$$

and

$$0 \to A \to N_2 \to L \to 0$$

are said to be *congruent* if there is an isomorphism $\varphi : N_1 \to N_2$ such that the triple comprising the identity map $A \to A$, the map $\varphi : E_1 \to E_2$, and the identity map $L \to L$ give an isomorphism of short exact sequences. In other words, we can get an isomorphism from N_1 to N_2 that induces the identity maps both on the ideal A and the quotient Lie ring L.

Congruence defines an equivalence relation on the set of all Lie ring extensions with ideal A and quotient Lie ring L. The equivalence classes for this equivalence relation are termed *congruence classes.*

Two Lie ring extensions:

$$0 \to A \to N_1 \to L \to 0$$

and

$$0 \to A \to N_2 \to L \to 0$$

are said to be *pseudo-congruent* if there is an isomorphism between the short exact sequences. The isomorphism need not induce the identity map on A and need not induce the identity map on L.

Pseudo-congruence defines an equivalence relation on the set of all Lie ring extensions with ideal A and quotient Lie ring L. The equivalence classes for this equivalence relation are termed *pseudo-congruence classes.*

Pseudo-congruence is a coarser equivalence relation than congruence because it allows for "re-labeling" on both the ideal side and the quotient Lie ring side.

3.2.3 Central extensions and stem extensions

A *central extension* refers to a Lie ring extension where the ideal is central. Explicitly, consider a short exact sequence of the following form, where A is an abelian Lie ring:

$$0 \to A \to N \to L \to 0$$

We say that N is a *central extension* with central subring A and quotient Lie ring L if the image of A in N is a central subring of N. If we engage in the usual abuse of notation that conflates A with its image in N, we could shorten this to saying that A is a central subring (or equivalently, central ideal) of N.

We will often say "N is a central extension of L" as shorthand for "there exists an abelian Lie ring A such that N is a central extension with central subring A and quotient Lie ring L."

A *stem extension* is a central extension where the central subring is also contained in the derived subring of the extension Lie ring. Explicitly, consider a short exact sequence of the following form, where A is abelian:

$$0 \to A \to N \to L \to 0$$

We say that N is a *stem extension* with central subring A and quotient Lie ring L if the image of A in N is contained in $N' \cap Z(N)$.

3.2.4 The use of cohomology groups to classify central extensions

Suppose A is an abelian Lie ring and L is a Lie ring. The group $H^2_{\text{Lie}}(L; A)$, called the *second cohomology group for trivial Lie ring action* of L on A, is a group whose elements correspond to the congruence classes of central extensions with central subring A and quotient Lie ring L. Here, by "congruence class" we mean equivalence class under the equivalence relation of being congruent Lie ring extensions. The group structure on $H^2_{\text{Lie}}(L; A)$ is not *prima facie* obvious. For a detailed discussion of the group structure, please refer to Weibel's book [47]. $H^2_{\text{Lie}}(L; A)$ is simply denoted $H^2(L; A)$ in cases where there is no potential for ambiguity with the cohomology group describing group extensions.

Further, there is a natural action of $\text{Aut}(L) \times \text{Aut}(A)$ on $H^2(L; A)$ and the orbits of $H^2_{\text{Lie}}(L; A)$ under this natural action correspond precisely to the pseudo-congruence classes of central extensions with central subring A and quotient Lie ring L.

Note that there is some potential for abuse of notation here, namely, we often view A both as an abelian *group* and as an abelian *Lie ring*. From a pedantic perspective, it would be preferable to use the exp and log functors to transition between the abelian group and abelian Lie ring via the abelian Lie correspondence, as described in Section 1.3. However, doing so would complicate our notation considerably, so we avoid it in this section. Later, when applying the results here to the Baer correspondence up to isoclinism as described in Section 5.4, we will be more careful.

3.2.5 Homomorphism of central extensions

In the discussion so far, we have fixed both the central subring A and the quotient Lie ring L and considered possibilities for the extension Lie ring. We now consider the case where the quotient Lie ring L is fixed. We are interested in all central extensions with quotient Lie ring L. The theory undergirding these should be hidden within the internal structure of L as a Lie ring. Our goal is to make that theory more explicit.

We begin by defining the concept of *homomorphism of central extensions*. Consider two central extensions, both of which have L as the quotient Lie ring:

$$0 \to A_1 \to N_1 \to L \to 0$$

and

$$0 \to A_2 \to N_2 \to L \to 0$$

A homomorphism of central extensions from the first central extension to the second is a pair of homomorphisms $A_1 \to A_2$, $N_1 \to N_2$, that, together with the identity map $L \to L$, give a homomorphism of short exact sequences.

We can consider the *category of central extensions* of L:

- The *objects* of this category are the central extensions with quotient Lie ring L.

- The *morphisms* of this category are homomorphisms of central extensions of L, as defined above.

- Composition of morphisms is defined as the usual composition of homomorphisms of short exact sequences.

An object in the category of central extensions can be completely described up to isomorphism in this category simply by specifying its right map. Explicitly, consider two central extensions:

$$0 \to A_1 \to N \xrightarrow{\nu} L \to 0$$

and

$$0 \to A_2 \to N \xrightarrow{\nu} L \to 0$$

where the map ν is the same in both cases. In that case, the central extensions are isomorphic in the category. Explicitly, this is because if we consider the partial commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to A_1 & \to N & \xrightarrow{\nu} L & \to 0 \\ & & \downarrow^{\mathrm{id}} & \downarrow^{\mathrm{id}} & \\ 0 & \to A_2 & \to N & \xrightarrow{\nu} L & \to 0 \end{array}$$

there is a unique choice of isomorphism $A_1 \to A_2$ so that the diagram as a whole commutes:

$$\begin{array}{ccccccccc} 0 & \to A_1 & \to N & \xrightarrow{\nu} L & \to 0 \\ & \downarrow & \downarrow^{\mathrm{id}} & \downarrow^{\mathrm{id}} & \\ 0 & \to A_2 & \to N & \xrightarrow{\nu} L & \to 0 \end{array}$$

Further, specifying a homomorphism from one object:

$$0 \to A_1 \to N_1 \stackrel{\nu_1}{\to} L \to 0$$

to another:

$$0 \to A_2 \to N_2 \stackrel{\nu_2}{\to} L \to 0$$

is equivalent to simply specifying the homomorphism $N_1 \to N_2$, because the homomorphism $A_1 \to A_2$ is uniquely determined by it. Explicitly, this is because in the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to A_1 & \to N_1 & \stackrel{\nu_1}{\to} L & \to 0 \\ & & \downarrow^{\theta} & \downarrow^{\mathrm{id}} & \\ 0 & \to A_2 & \to N_2 & \stackrel{\nu_2}{\to} L & \to 0 \end{array}$$

there is a unique morphism $A_1 \to A_2$ that completes the commutative diagram.

Further, the set of permissible homomorphisms $N_1 \to N_2$ is precisely the set of homomorphisms $\theta : N_1 \to N_2$ such that $\nu_2 \circ \theta = \nu_1$.

The *category of central extensions* of L thus has the following alternative description. Note that strictly speaking, this is a different category, but the preceding remarks establish that there is a canonical *equivalence of categories* between the categories:

- The *objects* of the category are "central extensions" of L in the sense of being pairs (N, ν) where $\nu : N \to L$ is a surjective Lie ring homomorphism and the kernel of ν is central in L.

- Given two objects (N_1, ν_1) and (N_2, ν_2) in the category, a *morphism* between them is a homomorphism $\theta : N_1 \to N_2$ such that $\nu_2 \circ \theta = \nu_1$.

The equivalence of categories is given by the obvious forgetful functor from the short exact sequence category to this new category, that sends a short exact sequence $0 \to A \to$

$N \xrightarrow{\nu} L \to 0$ to the quotient map $N \xrightarrow{\nu} L$. The functor is clearly essentially surjective (in fact, it is surjective on objects). The preceding remarks establish that the functor is full and faithful, and therefore an equivalence of categories. From this point onward, we we talk of the "category of central extensions of L" we will refer to the latter category.

We might hope that this category has an initial object, which could then serve as the "source" classifying central extensions of L. However, such an initial object does not always exist. We will show in Section 3.5.9, there *do* exist objects in this category that admit homomorphisms to every other object in the category. These are not in general initial objects because the homomorphisms admitted are not unique.

3.3 Explicit description of second cohomology group using the bar resolution

In Section 3.1.5, we stated that the second cohomology group for trivial group action $H^2(G; A)$ is a group whose elements correspond with congruence classes of central extensions with central subgroup A and quotient group G. However, we did not specify the group structure at the time. In this section, we explicitly construct $H^2(G; A)$ as a group.

Interested readers can learn more from [3], [28], [10], or any standard reference on group cohomology.

3.3.1 Explicit description of second cohomology group using cocycles and coboundaries

Suppose G is a group and A is an abelian group. A *2-cochain for trivial group action* of G on A is defined as a set map $f : G \times G \to A$. With pointwise addition of functions, the set of 2-cochains acquires an abelian group structure. We denote this group as $C^2(G; A)$.

A 2-cochain $f : G \times G \to A$ is termed a *2-cocycle for trivial group action* if it satisfies the following condition:

$$f(g_1, g_2) + f(g_1 g_2, g_3) = f(g_1, g_2 g_3) + f(g_2 g_3) \ \forall \ g_1, g_2, g_3 \in G$$

The 2-cocycles form a subgroup of $C^2(G; A)$. This subgroup is denoted $Z^2(G; A)$.

A 2-cochain $f : G \times G \to A$ is termed a *2-coboundary for trivial group action* if there exists a set map $\varphi : G \to A$ such that:

$$f(g_1, g_2) = \varphi(g_1) + \varphi(g_2) - \varphi(g_1 g_2) \ \forall \ g_1, g_2 \in G$$

Every 2-coboundary is a 2-cocycle, and the 2-coboundaries form a subgroup of the group of 2-cocycles. We denote this subgroup as $B^2(G; A)$. The group $H^2(G; A)$, called the *second cohomology group for trivial group action* of G on A, is defined as the quotient group $Z^2(G; A)/B^2(G; A)$ (note that both are subgroups of the abelian group $C^2(G; A)$, hence $B^2(G; A)$ is normal in $Z^2(G; A)$). The elements of $H^2(G; A)$, i.e., the *cosets* of $B^2(G; A)$ in $Z^2(G; A)$, are termed *cohomology classes*. Given two elements of $Z^2(G; A)$ that are in the same cohomology class, we will say that they are *cohomologous* to each other.

We will reconcile this definition with the earlier definition from Section 3.1.5 in Section 3.3.3.

3.3.2 Functoriality and automorphism group action

Each of C^2, Z^2, B^2, and H^2, viewed in terms of G and A, is *contravariant* in the first argument G and *covariant* in the second argument A. Explicitly:

- If $\theta : G_1 \to G_2$ is a homomorphism, then θ induces a homomorphism $C^2(G_2; A) \to C^2(G_1; A)$ by composition: given a map $f : G_2 \times G_2 \to A$ that is an element of $C^2(G_2; A)$, its image in $C^2(G_1; A)$ is the map $(x, y) \mapsto f(\theta(x), \theta(y))$. This homomorphism restricts to homomorphisms $Z^2(G_2; A) \to Z^2(G_1; A)$ and $B^2(G_2; A) \to B^2(G_1; A)$. Thus, it also induces a homomorphism $H^2(G_2; A) \to H^2(G_1; A)$. All these induced homomorphisms define contravariant functors.

- If $\alpha : A_1 \to A_2$ is a homomorphism, then α induces a homomorphism $C^2(G; A_1) \to C^2(G; A_2)$ by composition: $f \mapsto \alpha \circ f$. This homomorphism restricts to homomorphisms $Z^2(G; A_1) \to Z^2(G; A_2)$ and $B^2(G; A_1) \to B^2(G; A_2)$. Thus, it also induces a homomorphism $H^2(G; A_1) \to H^2(G; A_2)$. All these induced homomorphisms define covariant functors.

Based on this functoriality, we obtain a natural action of $\mathrm{Aut}(G) \times \mathrm{Aut}(A)$ on each of the groups $C^2(G; A)$, $Z^2(G; A)$, $B^2(G; A)$, and $H^2(G; A)$. We compose on both sides. Note that, due to *contravariance* in the G-argument, we need to use the inverse of the element on the $\mathrm{Aut}(G)$ side to keep the action a left action. Explicitly, $(\varphi, \alpha) \circ f$ is defined as:

$$(x, y) \mapsto \alpha(f(\varphi^{-1}(x), \varphi^{-1}(y)))$$

3.3.3 Identifying cohomology classes with congruence classes of central extensions

We will now describe a bijection:

Elements of the second cohomology group $H^2(G; A) \leftrightarrow$ Congruence classes of central extensions with central subgroup A and quotient group G

We will describe the bijection in the reverse direction. Explicitly, given a central extension group E, we will describe how to use E to obtain a cohomology class.

We have the short exact sequence:

$$0 \to A \xrightarrow{\iota} E \xrightarrow{\nu} G \to 1$$

Pick any set map $s : G \to E$ that is a one-sided inverse to the surjective homomorphism $\nu : E \to G$ (such a set map is called a *section* of the extension). We can think of s as specifying the coset representatives in E for each element of G.

Now, define the following 2-cochain $f : G \times G \to A$: for $g_1, g_2 \in G$, consider the element of E given by $s(g_1g_2)(s(g_1)s(g_2))^{-1}$. This element of E maps to the identity element of G, hence is in the image of A. Define $f(g_1, g_2)$ to be its inverse image under ι in A.

Explicitly:

$$s(g_1g_2) = \iota(f(g_1, g_2))s(g_1)s(g_2) \ \forall \ g_1, g_2 \in G$$

We can think of f as measuring the extent to which s fails to be a homomorphism. Since $\nu \circ s$ is the identity map, s is a homomorphism *modulo* A. The "error term" for s therefore lies in A, and this is how we get a 2-cochain $f : G \times G \to A$.

We can now verify the following:

- The function f constructed for any section $s : G \to E$ is a 2-cocycle, i.e., an element of $Z^2(G; A)$. This follows from associativity of group multiplication. Explicitly, if we expand $s(g_1g_2g_3)$ using the two different ways of associating the expression, and compare, we get the result. Note that we need to use the centrality of $\iota(A)$ in E to commute elements.

- The set of all possible functions f that we can get by choosing different sections $s : G \to E$ for a *single* extension E correspond to a single cohomology class, i.e., a single coset of $B^2(G; A)$ in $Z^2(G; A)$, and therefore, a single element of $H^2(G; A)$.

- Two central extensions with central subgroup A and quotient group G are congruent if and only if they give the same element of $H^2(G; A)$.

We have now completely described one direction of the correspondence. The construction in the other direction is similar: we need to explicitly construct a group extension based on a cohomology class. We will omit the details, but they can be found in [10] or in any of the standard references on cohomology.

It also follows from the above that the orbits of $H^2(G; A)$ under the $\mathrm{Aut}(G) \times \mathrm{Aut}(A)$ action correspond with the pseudo-congruence classes of extensions.

3.3.4 Short exact sequence of coboundaries, cocycles, and cohomology classes

We have a natural short exact sequence:

$$0 \to B^2(G; A) \to Z^2(G; A) \to H^2(G; A) \to 0$$

This short exact sequence does not always split. For instance, consider the case where $G = \mathbb{Z}/2\mathbb{Z}$ and $A = \mathbb{Z}$. In this case, $C^2(G; A)$ is, as an abelian group, isomorphic to $A^{|G| \times |G|}$, which is $\mathbb{Z}^4$. In particular, it is a finitely generated free abelian group. Thus, both $B^2(G; A)$ and $Z^2(G; A)$, which are subgroups of $C^2(G; A)$, are also free abelian groups. However, $H^2(G; A) \cong \mathbb{Z}/2\mathbb{Z}$, which is not a free abelian group. If the short exact sequence *did* split, then $H^2(G; A)$ would have been free abelian. Therefore, the short exact sequence does not split.

In Section 5.4.9, we will see that in the special case that G and A are both 2-powered abelian groups, this short exact sequence splits *canonically*.

3.4 Exterior square, Schur multiplier, and homoclinism

In Sections 3.1 and 3.2, we introduced, for groups and for Lie rings, the notion of central extension. In this section, our goal is to understand, for a group G, the category of central extensions of G (introduced in Section 3.2.5) in terms of the isomorphism type of G.

We will attack this question by looking at one key attribute of the extension: how the commutator map behaves. Roughly speaking, the behavior of the commutator map classifies the central extension *up to isoclinism*, and if we want to study the collection of central extensions focusing *only* on this attribute, we consider the *category of central extensions with homoclinisms*, a variant of the category of central extensions with homomorphisms. We will establish key features of this category, including the fact that there is at most one morphism between any two objects, and the existence of initial objects. There are two structures in particular that store a lot of the information related to the central extensions of G. These are the exterior square $G \wedge G$ (which serves as a source object for the derived subgroups in all central extensions) and the Schur multiplier $M(G)$ (which is the kernel of the canonical map $G \wedge G \to [G, G]$).

We tangentially mention in this section the well-known fact that the Schur multiplier $M(G)$ has an alternative description as the second homology group $H_2(G; \mathbb{Z})$. We do not provide a proof here, since developing the underlying machinery of homology would take us too far afield. However, the techniques used to establish this are closely related to the explicit description of the second cohomology group in Section 3.3. For reference, see the exact sequence appearing as (2.8) in Loday and Brown's 1987 paper [8].

3.4.1 Exterior square

The exterior square of a group was originally considered (though not with that name) in the paper [36] by Clair Miller in 1952. It was later defined as a special case of a more general concept called the *exterior product of groups* in [8]. More information about the exterior square and related constructions can be found in [35] and [15].

The definition that we provide here for the exterior square is the "abstract" definition. We will provide a concrete definition (based on generators and relations) in Section 3.8.4. The equivalence of the two approaches is discussed in Miller's original paper, and we include some further discussion of the equivalence in Section 3.8.5. As we demonstrate in this section, however, the initial theory is best established using the abstract definition.

Suppose G is a group. The *exterior square* of G, denoted by $G \wedge G$, is defined as follows. Let $\mathcal{F}$ be the free group on the set $G \times G$.

For any central extension:

$$0 \to A \to E \to G \to 1$$

there is a set map:

$$\omega_{E,G} : G \times G \to [E, E]$$

given by:

$$\omega_{E,G}(x, y) = [\tilde{x}, \tilde{y}]$$

where $\tilde{x}$ denotes any element of E that maps to x and $\tilde{y}$ denotes any element of E that maps to y. Note that the map is well defined (i.e., it does not depend on the choice of the lifts $\tilde{x}$ and $\tilde{y}$) because the extension is a central extension.

Note that the set map $\omega_{E,G}$ described here differs from ω_E in the following important respect: $\omega_{E,G}$ is a map from $G \times G$, whereas ω_E is a map from $E/Z(E) \times E/Z(E)$. However, it is obvious that $\omega_{E,G}$ *factors through* ω_E.

$\mathcal{F}$ is the free group on $G \times G$, so $\omega_{E,G}$ gives rise to a group homomorphism:

$$\hat{\omega}_{E,G} : \mathcal{F} \to [E, E]$$

Note also that this homomorphism is *surjective*, because by definition, $[E, E]$ is the subgroup of E generated by the image of the set map $\omega_{E,G}$.

Define $\mathcal{R}$ as the intersection of the kernels of all such homomorphisms $\hat{\omega}_{E,G}$ where E varies over all central extension groups with quotient group G. Note that even though the collection of all such homomorphisms is too large to be a set, the collection of possible kernels is a set, so the intersection is well defined. In other words, $\mathcal{R}$ is the set of all products of formal pairs of elements and their inverses such that the corresponding commutator words become trivial in every central extension of G. We define the exterior square $G \wedge G$ as the quotient group $\mathcal{F}/\mathcal{R}$. The image of (x, y) in the group is denoted $x \wedge y$.

It is clear from the definition that, for any central extension E with short exact sequence:

$$0 \to A \to E \to G \to 1$$

there exists a unique natural homomorphism $\Omega_{E,G}$ from $G \wedge G$ to $[E, E]$ satisfying the condition that for any $x, y \in G$ we have:

$$\Omega_{E,G}(x \wedge y) = [\tilde{x}, \tilde{y}]$$

where $\tilde{x}$ and $\tilde{y}$ are elements of E that map to x and y respectively. Note also that $\Omega_{E,G}$ is *surjective*.

As a special case of the above, there is a natural homomorphism:

$$G \wedge G \to [G, G]$$

given on a generating set by:

$$x \wedge y \mapsto [x, y]$$

The kernel of this homomorphism is called the *Schur multiplier* of G and is denoted $M(G)$. We can easily deduce that $M(G)$ is a central subgroup of $G \wedge G$. We thus have a short exact sequence:

$$0 \to M(G) \to G \wedge G \to [G, G] \to 1$$

There are numerous other definitions of the Schur multiplier. The most common textbook definition is that $M(G) = H_2(G; \mathbb{Z})$, i.e., it is the second homology group for trivial group action with coefficients in the integers. [28] has a detailed description of techniques to compute the Schur multiplier for finite groups. [8] and [35] provide background on why the two definitions of Schur multiplier agree. In particular, see the exact sequence appearing as (2.8) in Loday and Brown's 1987 paper [8].

3.4.2 The existence of a single central extension that realizes the exterior square

Consider a group G. A natural question is whether there exists a central extension group E with quotient group G with the property that the natural homomorphism:

$$\Omega_{E,G} : G \wedge G \to [E, E]$$

is an isomorphism.

The answer to this question is *yes*. We provide one construction below. We will provide another construction in Section 3.4.7.

Recall the earlier description of $G \wedge G$ as a quotient $\mathcal{F}/\mathcal{R}$. The normal subgroup $\mathcal{R}$ was defined as the intersection of all possible normal subgroups arising as kernels of the natural homomorphisms $\mathcal{F} \to [E, E]$ for a central extension group E. For each possible normal subgroup $N_i, i \in I$ of $\mathcal{F}$ that arises this way, let E_i denote a corresponding central extension of G.

Define E_0 to be the pullback (also called the *fiber product* or the *subdirect product*) corresponding to all the quotient maps $E_i \to G$. We can verify that the natural mapping:

$$\mathcal{F} \to [E_0, E_0]$$

has kernel precisely $\mathcal{R}$, and hence, the mapping:

$$G \wedge G \to [E_0, E_0]$$

is an isomorphism.

3.4.3 Homoclinism of central extensions

Suppose G is a group. We define a certain category for which we are interested in computing the initial object. We will call this category the *category of central extensions of G with homoclinisms*. Explicitly, the objects of the category are short exact sequences of the form:

$$0 \to A \to E \to G \to 1$$

where the image of A is central in E.

The morphisms in the category, which we call *homoclinisms of central extensions*, are defined as follows. For two objects:

$$0 \to A_1 \to E_1 \to G \to 1$$

and

$$0 \to A_2 \to E_2 \to G \to 1$$

a morphism from the first to the second is a group homomorphism $\varphi : E_1' \to E_2'$ between the derived subgroups $E_1' = [E_1, E_1]$ and $E_2' = [E_2, E_2]$ such that the following holds. Let $\omega_1 : G \times G \to E_1'$ denote the map arising from the commutator map in E_1 and let $\omega_2 : G \times G \to E_2'$ denote the corresponding map in E_2. We require that $\varphi \circ \omega_1 = \omega_2$ as set maps.

The above condition can be reframed in terms of group homomorphisms if we use the exterior square: let $\Omega_1 : G \wedge G \to E_1'$, $\Omega_2 : G \wedge G \to E_2'$ denote the natural homomorphisms described in Section 3.4.1. The condition we need is that $\varphi \circ \Omega_1 = \Omega_2$.

3.4.4 Relation between the category of central extensions and the category of central extensions with homoclinisms

Any *homomorphism* of central extensions induces a *homoclinism* of central extensions. Explicitly, consider two central extensions:

$$0 \to A_1 \to E_1 \stackrel{\nu_1}{\to} G \to 1$$

and

$$0 \to A_2 \to E_2 \stackrel{\nu_2}{\to} G \to 1$$

As discussed in Section 3.1.6, the central extensions are completely described by the pairs (E_1, ν_1) and (E_2, ν_2) respectively. A homomorphism of central extensions can be specified as a homomorphism $\theta : E_1 \to E_2$ satisfying the condition that $\nu_2 \circ \theta = \nu_1$.

Any such homomorphism of central extensions induces a *homoclinism* of central extensions. Explicitly, for a homomorphism $\theta : E_1 \to E_2$ satisfying $\nu_2 \circ \theta = \nu_1$, define φ as the homomorphism $E_1' \to E_2'$ obtained by restricting θ to E_1'. We claim that φ defines a homoclinism of the central extensions. We now prove that this construction works.

Lemma 3.4.1. Suppose (E_1, ν_1) and (E_2, ν_2) are central extensions of a group G, and $\theta : E_1 \to E_2$ is a homomorphism of central extensions, i.e., $\nu_2 \circ \theta = \nu_1$. Denote by $\omega_1 : G \times G \to E_1'$ and $\omega_2 : G \times G \to E_2'$ the maps induced by the commutator maps in E_1 and E_2 respectively. Let $\varphi : E_1' \to E_2'$ be the homomorphism obtained by restricting θ to the derived subgroup E_1'. Then, φ is a homoclinism of central extensions, i.e., $\varphi \circ \omega_1 = \omega_2$.

Proof. Let u, v be arbitrary elements of G (possibly equal, possibly distinct). Our goal is to show that:

$$\varphi(\omega_1(u,v)) = \omega_2(u,v)$$

Let $x, y \in E_1$ be elements such that $\nu_1(x) = u$ and $\nu_1(y) = v$. Then, by definition, $\omega_1(u,v) = [x,y]$. Simplify the left side:

$$\varphi(\omega_1(u,v)) = \varphi([x,y]) = \theta([x,y]) = [\theta(x), \theta(y)] = \omega_2(\nu_2(\theta(x)), \nu_2(\theta(y)))$$

Now, use that $\nu_2 \circ \theta = \nu_1$ and simplify further to:

$$\omega_2(\nu_1(x), \nu_1(y)) = \omega_2(u,v)$$

which is the right side. $\square$

3.4.5 Uniqueness of homoclinism if it exists

We will show that if a homoclinism exists between two central extensions, it must be unique.

Lemma 3.4.2. Consider two short exact sequences that give central extensions of a group G:

$$0 \to A_1 \to E_1 \to G \to 1$$

$$0 \to A_2 \to E_2 \to G \to 1$$

Denote by $\omega_1 : G \times G \to E_1'$ and $\omega_2 : G \times G \to E_2'$ the commutator maps.

Suppose there exists homoclinisms φ, θ from the first central extension to the second. Explicitly, $\varphi : E_1' \to E_2'$ and $\theta : E_1' \to E_2'$ are homomorphisms such that $\varphi \circ \omega_1 = \omega_2$ and $\theta \circ \omega_1 = \omega_2$. Then, $\varphi = \theta$.

Proof. Denote by ν_1 the quotient map $E_1 \to G$ and by ν_2 the quotient map $E_2 \to G$.

It will suffice to show that φ and θ agree with each other on the set of all commutators, which is a generating set for E_1'. Consider a commutator $[x, y]$ with $x, y \in E_1$. Let $u = \nu_1(x)$ and $v = \nu_1(y)$.

By definition, $[x, y] = \omega_1(u, v)$. Thus, $\varphi([x, y]) = \varphi(\omega_1(u, v)) = \omega_2(u, v)$. Similarly, $\theta([x, y]) = \theta(\omega_1(u, v)) = \omega_2(u, v)$. We thus obtain that $\varphi([x, y]) = \theta([x, y])$, completing the proof. $\square$

Thus, if a homoclinism exists, it is unique. However, a homoclinism need not exist. The obstruction occurs if there are relations within the derived subgroup E_1' such that the corresponding relations are not valid in the derived subgroup E_2'.

3.4.6 Existence and description of initial objects in the category of central extensions up to homoclinisms

In category theory, an object X in a category $\mathcal{C}$ is termed an initial object if for every object $Y \in \mathcal{C}$, there is a unique morphism from X to Y, sometimes called the *initial morphism*. It can easily be seen using "abstract nonsense"[1] that if X_1 and X_2 are both initial objects in a category $\mathcal{C}$, then there exists a unique isomorphism between X_1 and X_2. In other words, the initial object in a category is uniquely determined up to (unique) isomorphism.

We are interested in identifying the initial objects in the category of extensions of G with homoclinisms discussed in Section 3.4.3.

Lemma 3.4.3 (Existence and description of initial objects)**.** For a group G, consider the category of central extensions of G with homoclinisms. The following are true for this category.

1. "Abstract nonsense" is a non-derogatory term used to refer to proof methods that rely on formalistic ideas, typically from category theory, rather than on the specifics of the structures being studied. Statements proved using abstrcat nonsense are often very general.

1. There exists a central extension E_0 of G for which the natural homomorphism $\Omega_0 : G \wedge G \to E_0'$ is an isomorphism.

2. Any central extension E_0 of G for which the natural homomorphism $\Omega_0 : G \wedge G \to E_0'$ is an isomorphism is an initial object of the category.

3. If a central extension E_1 of G is an initial object of the category, the corresponding homomorphism $\Omega_1 : G \wedge G \to E_1'$ is an isomorphism.

4. Combining all the above: the category of central extensions of G with homoclinisms admits initial objects, and a central extension $E \to G$ is an initial object for the category if and only if the commutator map homomorphism $\Omega_{E,G} : G \wedge G \to [E, E]$ is an isomorphism.

Proof.

- Proof of (1): In Section 3.4.2, we constructed a central extension group E_0 for which the natural map $\Omega_0 : G \wedge G \to E_0'$ is an isomorphism.

- Proof of (2): Suppose E_0 is a central extension for which the commutator map $\Omega_0 : G \wedge G \to E_0'$ is an isomorphism. For any central extension E_2, there is a natural homomorphism $\Omega_2 : G \wedge G \to E_2'$. Composing this with the inverse of Ω_0, we obtain a homomorphism $\varphi : E_0' \to E_2'$ that defines a homoclinism of the extensions. Moreover, by Lemma 3.4.2, this is the *unique* homoclinism of the extensions.

- Proof of (3): We already know of the existence of a central extension E_0 for which $\Omega_0 : G \wedge G \to E_0'$ is an isomorphism by (1). We also know that it is an initial object by (2). By the uniqueness of initial objects up to isomorphism, E_0 and E_1 are isomorphic in the category of central extensions of G with homoclinisms. Thus, there exists an isomorphism $\varphi_1 : E_0' \to E_1'$ such that $\varphi_1 \circ \Omega_0 = \Omega_1$. Since both φ_1 and Ω_0 are isomorphisms, Ω_1 is also an isomorphism.

- Proof of (4): This follows by combining (1), (2), and (3).

$\square$

3.4.7 An alternate construction of the initial object

Here is an alternative way of constructing a central extension E_1 for which the natural map:

$$\Omega_1 : G \wedge G \to E_1$$

is an isomorphism.

Write G as the quotient of a free group F by a normal subgroup R of F. Let $\nu : F \to G$ denote the quotient map. The kernel of ν is R.

The group E_1 that we are interested in is $F/[F, R]$. This group E_1 is a central extension of G in a natural fashion. Denote by $\overline{\nu}$ the corresponding quotient map $E_1 \to G$. Consider the commutator map $\omega_1 : G \times G \to E_1$ and denote by Ω_1 the corresponding group homomorphism:

$$\Omega_1 : G \wedge G \to [E_1, E_1]$$

Consider any extension:

$$0 \to A \to E_2 \stackrel{\mu}{\to} G \to 1$$

with the natural commutator map $\omega_2 : G \times G \to E_2$ and the corresponding commutator map homomorphism:

$$\Omega_2 : G \wedge G \to [E_2, E_2]$$

Our goal is to show that there there exists a unique homomorphism $\varphi : [E_1, E_1] \to [E_2, E_2]$ such that $\varphi \circ \omega_1 = \omega_2$, or equivalently, $\varphi \circ \Omega_1 = \Omega_2$.

The map $\nu : F \to G$ lifts to a map $\psi : F \to E_2$ because F is a free group (note that the lift is not necessarily unique). Explicitly, this means that $\mu \circ \psi = \nu$.

We know that $\nu(R)$ is trivial, so $\mu(\psi(R))$ is trivial. Thus, $\psi(R)$ lands inside the kernel of μ, which is the image of A in E_2. Thus, $\psi(R)$ is a central subgroup of E_2. Therefore, $\psi([F,R]) = [\psi(F), \psi(R)]$ is trivial.

Thus, ψ descends to a homomorphism $\theta : E_1 \to E_2$, where $E_1 = F/[F,R]$ as defined above, with the property that $\mu \circ \theta = \overline{\nu}$. The condition $\mu \circ \theta = \overline{\nu}$ can be interpreted as saying that θ is a homomorphism from the central extensions $(E_1, \overline{\nu})$ to the central extension (E_2, μ). Denote by $\varphi : E_1' \to E_2'$ the restriction of θ to E_1'. Thus, by Lemma 3.4.1, φ defines a homoclinism of the central extensions. Lemma 3.4.2 now establishes that the homoclinism is unique. Finally, Lemma 3.4.3 establishes from this that $(E_1, \overline{\nu})$ defines an initial object in the category of central extensions of G with homoclinisms.

Clarification regarding uniqueness: In the discussion above, the lift $\psi : F \to E_2$ of $\nu : F \to G$ is not unique, because it involves picking *arbitrary* coset representatives of G in E_2 for the freely generating set of F. The homomorphism $\theta : E_1 \to E_2$ also need not be unique. However, the map $\varphi : E_1' \to E_2'$, obtained by restricting θ to E_1', *is* unique.

Canonical choice of E_1

The description of E_1 above is unique once we fix the description of G of the form F/R where F is a free group. Specifying a description of this form is equivalent to specifying a generating set for G, and thus, the description relies on a choice of generating set for G.

It is possible to make a *canonical* choice of E_1 by making a canonical choice of generating set for G, namely, the entire underlying set of G. In this case, the free group F is the free group on the underlying set of G, and the normal subgroup R is generated by the multiplication table of G, viewed as relations within F (explicitly, for any product relation of the form $gh = k$ in G, we introduce the relation ghk^{-1} in F).

There is an alternative description of the group E_1 that demonstrates its canonical nature:

E_1 is the freest possible group admitting G as a quotient by a central subgroup.[2]

3.4.8 Functoriality of exterior square and Schur multiplier

The exterior square and Schur multiplier are both *functorial.* Explicitly, for any homomorphism $\varphi : G \to H$ of groups, there are homomorphisms $\varphi \wedge \varphi : G \wedge G \to H \wedge H$ and $M(\varphi) : M(G) \to M(H)$ and the associations are functorial. This means that for homomorphisms $\varphi : G \to H$ and $\theta : H \to K$, $(\theta \circ \varphi) \wedge (\theta \circ \varphi) = (\theta \wedge \theta) \circ (\varphi \wedge \varphi)$ and also $M(\theta \circ \varphi) = M(\theta) \circ M(\varphi)$.

The proofs of both assertions are straightforward, but we are not including them here because we do not use the functoriality of the Schur multiplier. See a more detailed discussion of functoriality in the Appendix, Section A.2.1.

3.4.9 Homoclinisms and words for central extensions

We state and prove some results that are similar in spirit to the results in Section 2.1.6.

Lemma 3.4.4. Suppose G is a group and $w(g_1, g_2, \dots, g_n)$ is a word in n letters with the property that w evaluates to the identity element in every abelian group. The following are true.

1. For every central extension E of G, w can be used to define a set map $\chi_{w,E} : G^n \to [E, E]$.

2. For any homoclinism between central extensions E_1 and E_2, with the central extension specified via a homomorphism $\varphi : [E_1, E_1] \to [E_2, E_2]$, we have that:

$$\varphi \circ \chi_{w,E_1} = \chi_{w,E_2}$$

2. This might tempt one to think that $(E_1, \overline{\nu})$ is an initial object in the category of central extensions of G with *homomorphisms*, but the non-uniqueness of homomorphisms involved, along with some other considerations, makes this false.

Proof. Proof of (1): This is similar to the proof of Theorem 2.1.2. Alternatively, we can deduce it from the *result* of Theorem 2.1.2 by noting that the map factors as follows:

$$G^n \to (E/Z(E))^n \to [E, E]$$

Proof of (2): This is similar to the proof of Theorem 2.1.3. Alternatively, we can deduce it from the *result* of Theorem 2.1.3 by factoring through $E/Z(E)$. $\square$

We can now prove the theorem.

Theorem 3.4.5. Suppose G is a group and $w(g_1, g_2, \ldots, g_n)$ is a word in n letters with the property that w evaluates to the identity element in every abelian group. Then, there exists a set map $X_w : G^n \to G \wedge G$ with the property that for any central extension E of G, $\Omega_{E,G} \circ X_w = \chi_{w,E}$.

Proof. Apply Part (1) of Lemma 3.4.4 to the case where the extension E_0 is an initial object in the category of central extensions of G, so that the map $\Omega_{E_0,G} : G \wedge G \to [E_0, E_0]$ is an isomorphism. Define $X_w = \Omega_{E_0,G}^{-1} \circ \chi_{w,E_0}$. For any central extension E of G, there is a homoclinism from the extension E_0 to the extension E defined via the homomorphism $\varphi : [E_0, E_0] \to [E, E]$. By Part (2) of Lemma 3.4.4, we have:

$$\varphi \circ \chi_{w,E_0} = \chi_{w,E}$$

We can rewrite χ_{w,E_0} as $\Omega_{E,G} \circ X_w$, and obtain:

$$\varphi \circ (\Omega_{E,G} \circ X_w) = \chi_{w,E}$$

Using associativity of composition, we obtain:

$$(\varphi \circ \Omega_{E,G}) \circ X_w = \chi_{w,E}$$

Ω itself commutes with homoclinisms, so we obtain:

$$\Omega_{E_0,G} \circ X_w = \chi_{w,E}$$

$\square$

3.5 Exterior square, Schur multiplier, and homoclinism for Lie rings

A large part of this section repeats for Lie rings what the previous section did for groups. The main exception is the content in Sections 3.5.2 and Section 3.5.3. The material presented in Section 3.5.2 has no natural group analogue, while the results Section 3.5.3 have group analogues that are harder to prove, and are deferred to Sections 3.6.11 and 5.4.3.

For background on the homology and cohomology theory of Lie rings, see Weibel's homological algebra textbook [47].

3.5.1 Exterior square

The concept of exterior square of a Lie ring appears to have first been explicitly discussed in the literature in the paper [16] by Graham Ellis.

The definition that we provide here for the exterior square is the "abstract" definition. We will provide a concrete definition (based on generators and relations) in Section 3.9.3. The equivalence of the two approaches follows from the work in [16]. Background theory on the homology of Lie rings is discussed in [13] and the references therein.

Suppose L is a Lie ring. The *exterior square* of L, denoted by $L \wedge L$, is defined as follows. Let $\mathcal{F}$ be the free Lie ring on the set $L \times L$.

For any central extension:

$$0 \to A \to N \to L \to 0$$

there is a set map (in fact, a $\mathbb{Z}$-bilinear map):

$$\omega_{N,L} : L \times L \to [N, N]$$

given by:

$$\omega_{N,L}(x, y) = [\tilde{x}, \tilde{y}]$$

where $\tilde{x}$ denotes any element of N that maps to x and $\tilde{y}$ denotes any element of N that maps to y. Note that the map is well defined (i.e., it does not depend on the choice of the lifts $\tilde{x}$ and $\tilde{y}$) because the extension is a central extension.

$\mathcal{F}$ is the free Lie ring on $L \times L$, so $\omega_{N,L}$ gives rise to a Lie ring homomorphism:

$$\hat{\omega}_{N,L} : \mathcal{F} \to [N, N]$$

Note also that this homomorphism is *surjective*, because by definition, $[N, N]$ is the subring of N generated by the image of the set map $\omega_{N,L}$.

Define $\mathcal{R}$ as the intersection of the kernels of all such homomorphisms $\hat{\omega}_{N,L}$ where N varies over all central extension Lie rings with quotient ring L. Note that even though the collection of all such homomorphisms is too large to be a set, the collection of possible kernels is a set, so the intersection is well defined. In other words, $\mathcal{R}$ is the set of all $\mathbb{Z}$-linear combinations of formal pairs such that the corresponding sums of Lie brackets would become trivial in every central extension of L. We define the exterior square $L \wedge L$ as the quotient Lie ring $\mathcal{F}/\mathcal{R}$. The image of (x, y) in the Lie ring is denoted $x \wedge y$.

It is clear from the definition that, for any central extension N with short exact sequence:

$$0 \to A \to N \to L \to 0$$

there exists a unique natural homomorphism Ω_N from $L \wedge L$ to $[N, N]$ satisfying the condition that for any $x, y \in L$ we have:

$$\Omega_N(x \wedge y) = [\tilde{x}, \tilde{y}]$$

where $\tilde{x}$ and $\tilde{y}$ are elements of N that map to x and y respectively. Note also that Ω_N is *surjective*.

As a special case of the above, there is a natural homomorphism:

$$L \wedge L \to [L, L]$$

given on a generating set by:

$$x \wedge y \mapsto [x, y]$$

The kernel of this homomorphism is called the *Schur multiplier* of L and is denoted $M(L)$. We can easily deduce that $M(L)$ is a central subring of $L \wedge L$. We thus have a short exact sequence:

$$0 \to M(L) \to L \wedge L \to [L, L] \to 0$$

3.5.2 Free Lie ring on an abelian group

Suppose G is an abelian group. The *free Lie ring* on G is defined as the initial object in the category of Lie rings L with group homomorphisms from G to them.

Lemma 3.5.1. The free Lie ring on G exists and is a $\mathbb{N}$-graded Lie ring where the degree

1 homogeneous component is isomorphic to G.

Proof. The free Lie ring on G is the quotient of the free ring on G by the ideal generated by all the Lie identities. The free ring on G is given as the infinite direct sum:

$$\bigoplus_{i=1}^{\infty} \bigotimes^{i} G$$

The ideal that we need to factor out by is a homogeneous ideal because all the Lie identities are homogeneous identities. Thus, the free Lie ring is naturally a $\mathbb{N}$-graded Lie ring. $\square$

Denote by $\mathcal{L}$ the free Lie ring on G. Then, for any positive integer c, we can define the free class c Lie ring on G as the quotient ring $\mathcal{L}/\gamma_{c+1}(\mathcal{L})$. Note that this is also a $\mathbb{N}$-graded Lie ring, but it is zero except in the first c homogeneous components. In particular, this is a quotient of:

$$\bigoplus_{i=1}^{c} \bigotimes^{i} G$$

Lemma 3.5.2. Suppose G is an abelian group. The degree 2 homogeneous component of the free Lie ring on G is isomorphic to the ring $G \wedge_{\mathbb{Z}} G$. Equivalently, the free class two Lie ring on G has additive group $G \oplus (G \wedge_{\mathbb{Z}} G)$ with Lie bracket:

$$[(x, u), (y, v)] = [0, x \wedge_{\mathbb{Z}} y]$$

Proof. Note that of the Lie ring identities, the Jacobi identity becomes redundant because of the class two condition. The only condition on the Lie bracket is that it is alternating. Taking the quotient of $G \oplus (G \otimes G)$ by this relation gives $G \oplus (G \wedge_{\mathbb{Z}} G)$. $\square$

3.5.3 Relation between exterior square of a Lie ring and exterior square in the abelian group sense

Recall that the additive group of L has an exterior square *as an abelian group.* Denote this as $L \wedge_{\mathbb{Z}} L$.

We have a canonical abelian group homomorphism:

$$L \wedge_{\mathbb{Z}} L \to L \wedge L$$

The homomorphism is constructed as follows. For every central extension N of L, the map $\Omega_N : L \times L \to [N, N]$ is $\mathbb{Z}$-bilinear because the Lie bracket map itself is $\mathbb{Z}$-bilinear.

Thus, the natural map $L \times L \to L \wedge L$ given by $(x, y) \mapsto x \wedge y$ is $\mathbb{Z}$-bilinear. Hence, it induces an abelian group homomorphism $L \wedge_{\mathbb{Z}} L \to L \wedge L$. This is the homomorphism we seek.

The canonical homomorphism $L \wedge_{\mathbb{Z}} L \to L \wedge L$ is surjective: It is obvious that $L \wedge L$ is generated as a Lie ring by the image of $L \wedge_{\mathbb{Z}} L$. The main thing to verify is that, in fact, the image of $L \wedge_{\mathbb{Z}} L$ is closed under the Lie bracket. The following identity demonstrates this:

$$[(m_1 \wedge n_1), (m_2 \wedge n_2)] = -[n_1, m_1] \wedge [m_2, n_2]$$

We now turn to a proof of an important result. Note that this is subsumed by the explicit presentation of the exterior square in Section 3.9.3, but we give an explicit proof here for convenience.

Lemma 3.5.3. Suppose L is an abelian Lie ring. Then, the canonical surjective homomorphism $L \wedge_{\mathbb{Z}} L \to L \wedge L$ is an isomorphism. This

Proof. We have already established surjectivity, so to demonstrate injectivity, it suffices to construct a central extension N of L for which the composite map $L \wedge_{\mathbb{Z}} L \to [N, N]$ is an isomorphism. Taking N to be the free class two Lie ring on the additive group of L works, based on the discussion in Section 3.5.2. $\square$

3.5.4 *The existence of a single central extension that realizes the exterior square*

Consider a Lie ring L. A natural question is whether there exists a central extension Lie ring N with quotient Lie ring L with the property that the natural homomorphism:

$$\Omega_N : L \wedge L \to [N, N]$$

is an isomorphism.

The answer to this question is *yes*. We provide one construction below. We will provide another construction in Section 3.5.9.

Recall the earlier description of $L \wedge L$ as a quotient $\mathcal{F}/\mathcal{R}$. The ideal $\mathcal{R}$ was defined as the intersection of all possible ideals arising as kernels of the natural homomorphisms $\mathcal{F} \to [N, N]$ for a central extension Lie ring N. For each possible ideal $J_i, i \in I$ of $\mathcal{F}$ that arises this way, let N_i denote a corresponding central extension of L.

Define N_0 to be the pullback (also called the *fiber product* or the *subdirect product*) corresponding to all the quotient maps $N_i \to L$. We can verify that the natural mapping:

$$\mathcal{F} \to [N_0, N_0]$$

has kernel precisely $\mathcal{R}$, and hence, the mapping:

$$L \wedge L \to [N_0, N_0]$$

is an isomorphism.

3.5.5 Homoclinism of central extensions

Suppose L is a Lie ring. We define a certain category for which we are interested in computing the initial object. We will call this category the *category of central extensions of L with homoclinisms*. Explicitly, the objects of the category are short exact sequences of the form:

$$0 \to A \to N \to L \to 0$$

where the image of A is central in N.

The morphisms in the category, which we call *homoclinisms of central extensions*, are defined as follows. For two objects:

$$0 \to A_1 \to N_1 \to L \to 0$$

and

$$0 \to A_2 \to N_2 \to L \to 0$$

a morphism from the first to the second is a Lie ring homomorphism $\varphi : N_1' \to N_2'$ such that the following holds. Let $\omega_1 : L \times L \to N_1'$ denote the map arising from the Lie bracket map in N_1 and let $\omega_2 : L \times L \to N_2'$ denote the corresponding map in N_2. We require that $\varphi \circ \omega_1 = \omega_2$ as set maps.

The above condition can be reframed in terms of Lie ring homomorphisms if we use the exterior square: let $\Omega_1 : L \wedge L \to N_1'$, $\Omega_2 : L \wedge L \to N_2'$ denote the natural homomorphisms described in Section 3.5.1. The condition we need is that $\varphi \circ \Omega_1 = \Omega_2$.

3.5.6 Relation between the category of central extensions and the category of central extensions with homoclinisms

Any *homomorphism* of central extensions induces a *homoclinism* of central extensions. Explicitly, consider two central extensions:

$$0 \to A_1 \to N_1 \overset{\nu_1}{\to} L \to 0$$

and

$$0 \to A_2 \to N_2 \overset{\nu_2}{\to} L \to 0$$

As discussed in Section 3.2.5, the central extensions are completely described by the pairs (N_1, ν_1) and (N_2, ν_2) respectively. A homomorphism of central extensions can be specified as a homomorphism $\theta : N_1 \to N_2$ satisfying the condition that $\nu_2 \circ \theta = \nu_1$.

Any such homomorphism of central extensions induces a *homoclinism* of central extensions. Explicitly, for a homomorphism $\theta : N_1 \to N_2$ satisfying $\nu_2 \circ \theta = \nu_1$, define φ as the homomorphism $N_1' \to N_2'$ obtained by restricting θ to N_1'. We claim that φ defines a homoclinism of the central extensions. We now prove that this construction works.

Lemma 3.5.4. Suppose (N_1, ν_1) and (N_2, ν_2) are central extensions of a Lie ring L, and $\theta : N_1 \to N_2$ is a homomorphism of central extensions, i.e., $\nu_2 \circ \theta = \nu_1$. Denote by $\omega_1 : L \times L \to N_1'$ and $\omega_2 : L \times L \to N_2'$ the maps induced by the commutator maps in N_1 and N_2 respectively. Let $\varphi : N_1' \to N_2'$ be the homomorphism obtained by restricting θ to the derived subring N_1'. Then, φ is a homoclinism of central extensions, i.e., $\varphi \circ \omega_1 = \omega_2$.

Proof. Let u, v be arbitrary elements of L (possibly equal, possibly distinct). Our goal is to show that:

$$\varphi(\omega_1(u,v)) = \omega_2(u,v)$$

Let $x, y \in N_1$ be elements such that $\nu_1(x) = u$ and $\nu_2(y) = v$. Then, by definition, $\omega_1(u,v) = [x,y]$. Simplify the left side:

$$\varphi(\omega_1(u,v)) = \varphi([x,y]) = \theta([x,y]) = [\theta(x), \theta(y)] = \omega_2(\nu_2(\theta(x)), \nu_2(\theta(y)))$$

Now, use that $\nu_2 \circ \theta = \nu_1$ and simplify further to:

$$\omega_2(\nu_1(x), \nu_1(y)) = \omega_2(u,v)$$

which is the right side. $\square$

3.5.7 Uniqueness of homoclinism if it exists

We will show that if a homoclinism exists between two central extensions, it must be unique.

Lemma 3.5.5. Consider two short exact sequences that give central extensions of a Lie ring L:

$$0 \to A_1 \to N_1 \to L \to 0$$

$$0 \to A_2 \to N_2 \to L \to 0$$

Denote by $\omega_1 : L \times L \to N_1'$ and $\omega_2 : L \times L \to N_2'$ the Lie bracket maps.

Suppose there exists homoclinisms φ, θ from the first central extension to the second. Explicitly, $\varphi : N_1' \to N_2'$ and $\theta : N_1' \to N_2'$ are homomorphisms such that $\varphi \circ \omega_1 = \omega_2$ and $\theta \circ \omega_1 = \omega_2$. Then, $\varphi = \theta$.

Proof. Denote by ν_1 the quotient map $N_1 \to L$ and by ν_2 the quotient map $N_2 \to L$.

It will suffice to show that φ and θ agree with each other on the set of all Lie brackets, which is a generating set for N_1'. Consider a Lie bracket $[x, y]$ with $x, y \in N_1$. Let $u = \nu_1(x)$ and $v = \nu_1(y)$.

By definition, $[x, y] = \omega_1(u, v)$. Thus, $\varphi([x, y]) = \varphi(\omega_1(u, v)) = \omega_2(u, v)$. Similarly, $\theta([x, y]) = \theta(\omega_1(u, v)) = \omega_2(u, v)$. We thus obtain that $\varphi([x, y]) = \theta([x, y])$, completing the proof. □

Thus, if a homoclinism exists, it is unique. However, a homoclinism need not exist. The obstruction occurs if there are relations within the derived subring N_1' such that the corresponding relations are not valid in the derived subring N_2'.

3.5.8 *Existence and description of initial objects in the category of central extensions up to homoclinisms*

We are interested in identifying the initial objects in the category of extensions of L with homoclinisms discussed in Section 3.5.5.

Lemma 3.5.6 (Existence and description of initial objects)**.** For a Lie ring L, consider the category of central extensions of L with homoclinisms. The following are true for this category.

1. There exists a central extension N_0 of L for which the natural homomorphism $\Omega_0 : L \wedge L \to N_0'$ is an isomorphism.

2. Any central extension N_0 of L for which the natural homomorphism $\Omega_0 : L \wedge L \to N_0'$ is an isomorphism is an initial object of the category.

3. If a central extension N_1 of L is an initial object of the category, the corresponding homomorphism $\Omega_1 : L \wedge L \to N_1'$ is an isomorphism.

4. Combining all the above: the category of central extensions of L with homoclinisms admits initial objects, and a central extension $N \to L$ is an initial object for the category if and only if the Lie bracket map homomorphism $\Omega_N : L \wedge L \to [N, N]$ is an isomorphism.

Proof.
- Proof of (1): In Section 3.5.4, we constructed a central extension Lie ring N_0 for which the natural map $\Omega_0 : L \wedge L \to N_0'$ is an isomorphism.

- Proof of (2): Suppose N_0 is a central extension for which the Lie bracket map $\Omega_0 : L \wedge L \to N_0'$ is an isomorphism. For any central extension N_2, there is a natural homomorphism $\Omega_2 : L \wedge L \to N_2'$. Composing this with the inverse of Ω_0, we obtain a homomorphism $\varphi : N_0' \to N_2'$ that defines a homoclinism of the extensions. Moreover, by Lemma 3.5.5, this is the *unique* homoclinism of the extensions.

- Proof of (3): We already know of the existence of a central extension N_0 for which $\Omega_0 : L \wedge L \to N_0'$ is an isomorphism by (1). We also know that it is an initial object by (2). By the uniqueness of initial objects up to isomorphism, N_0 and N_1 are isomorphic in the category of central extensions of L with homoclinisms. Thus, there exists an isomorphism $\varphi_1 : N_0' \to N_1'$ such that $\varphi_1 \circ \Omega_0 = \Omega_1$. Since both φ_1 and Ω_0 are isomorphisms, Ω_1 is also an isomorphism.

- Proof of (4): This follows by combining (1), (2), and (3).

$\square$

3.5.9 An alternate construction of the initial object

Here is an alternative way of constructing a central extension N_1 for which the natural map:

$$\Omega_1 : L \wedge L \to N_1$$

is an isomorphism.

Write L as the quotient of a free Lie ring F by an ideal R of F. Let $\nu : F \to L$ denote the quotient map. The kernel of ν is R.

The Lie ring N_1 that we are interested in is $F/[F, R]$. This Lie ring N_1 is a central extension of L in a natural fashion. Denote by $\overline{\nu}$ the corresponding quotient map $N_1 \to L$. Consider the Lie bracket map $\omega_1 : L \times L \to N_1$ and denote by Ω_1 the corresponding Lie ring homomorphism:

$$\Omega_1 : L \wedge L \to [N_1, N_1]$$

Consider any extension:

$$0 \to A \to N_2 \xrightarrow{\mu} L \to 0$$

with the natural Lie bracket map $\omega_2 : L \times L \to N_2$ and the corresponding Lie bracket map homomorphism:

$$\Omega_2 : L \wedge L \to [N_2, N_2]$$

Our goal is to show that there there exists a unique homomorphism $\varphi : [N_1, N_1] \to [N_2, N_2]$ such that $\varphi \circ \omega_1 = \omega_2$, or equivalently, $\varphi \circ \Omega_1 = \Omega_2$.

The map $\nu : F \to L$ lifts to a map $\psi : F \to N_2$ because F is a free Lie ring (note that the lift is not necessarily unique). Explicitly, this means that $\mu \circ \psi = \nu$.

We know that $\nu(R)$ is trivial, so $\mu(\psi(R))$ is trivial. Thus, $\psi(R)$ lands inside the kernel of μ, which is the image of A in N_2. Thus, $\psi(R)$ is a central subring of N_2. Therefore, $\psi([F, R]) = [\psi(F), \psi(R)]$ is trivial.

Thus, ψ descends to a homomorphism $\theta : N_1 \to N_2$, where $N_1 = F/[F, R]$ as defined above, with the property that $\mu \circ \theta = \overline{\nu}$. The condition $\mu \circ \theta = \overline{\nu}$ can be interpreted as saying that θ is a homomorphism from the central extensions $(N_1, \overline{\nu})$ to the central extension

(N_2, μ). Denote by $\varphi : N_1' \to N_2'$ the restriction of θ to N_1'. Thus, by Lemma 3.5.4, φ defines a homoclinism of the central extensions. Lemma 3.5.5 now establishes that the homoclinism is unique. Finally, Lemma 3.5.6 establishes that (N_1, ν_1) defines an initial object in the category of central extensions of L with homoclinisms.

Clarification regarding uniqueness: In the discussion above, the lift $\psi : F \to N_2$ of $\nu : F \to L$ is not unique, because it involves picking *arbitrary* coset representatives of L in N_2 for the freely generating set of F. The homomorphism $\theta : N_1 \to N_2$ also need not be unique. However, the map $\varphi : N_1' \to N_2'$, obtained by restricting θ to N_1', *is* unique.

3.5.10 Functoriality of exterior square and Schur multiplier

The exterior square and Schur multiplier are both *functorial*. Explicitly, for any homomorphism $\varphi : L \to H$ of Lie rings, there are homomorphisms $\varphi \wedge \varphi : L \wedge L \to H \wedge H$ and $M(\varphi) : M(L) \to M(H)$ and the associations are functorial. This means that for homomorphisms $\varphi : L \to H$ and $\theta : H \to K$, $(\theta \circ \varphi) \wedge (\theta \circ \varphi) = (\theta \wedge \theta) \circ (\varphi \wedge \varphi)$ and also $M(\theta \circ \varphi) = M(\theta) \circ M(\varphi)$.

The proofs of both assertions are straightforward, but we are not including them here because we do not use the functoriality of the Schur multiplier. See a more detailed discussion of functoriality in the Appendix, Section A.2.1.

3.5.11 Homoclinisms and words for central extensions

We state and prove some results that are similar in spirit to the results in Section 2.2.3.

Lemma 3.5.7. Suppose L is a Lie ring and $w(g_1, g_2, \dots, g_n)$ is a Lie ring word in n letters with the property that w evaluates to the zero element in every abelian Lie ring. The following are true.

1. For every central extension N of L, w can be used to define a set map $\chi_{w,N} : L^n \to$

$[N, N]$.

2. For any homoclinism between central extensions N_1 and N_2, with the central extension specified via a homomorphism $\varphi : [N_1, N_1] \to [N_2, N_2]$, we have that:

$$\varphi \circ \chi_{w,N_1} = \chi_{w,N_2}$$

Proof. Proof of (1): This is similar to the proof of Theorem 2.2.2. Alternatively, we can deduce it from the *result* of Theorem 2.2.2 by noting that the map factors as follows:

$$L^n \to (N/Z(N))^n \to [N, N]$$

Proof of (2): This is similar to the proof of Theorem 2.2.3. Alternatively, we can deduce it from the *result* of Theorem 2.2.3 by factoring through $N/Z(N)$. □

We can now prove the theorem.

Theorem 3.5.8. Suppose L is a Lie ring and $w(g_1, g_2, \dots, g_n)$ is a word in n letters with the property that w evaluates to the identity element in every abelian Lie ring. Then, there exists a set map $X_w : L^n \to L \wedge L$ with the property that for any central extension N of L, $\Omega_{N,L} \circ X_w = \chi_{w,N}$.

Proof. Apply Part (1) of Lemma 3.5.7 to the case where the extension N_0 is an initial object in the category of central extensions of L, so that the map $\Omega_{N_0,L} : L \wedge L \to [N_0, N_0]$ is an isomorphism. Define $X_w = \Omega_{N_0,L}^{-1} \circ \chi_{w,E_0}$. For any central extension N of L, there is a homoclinism from the extension N_0 to the extension N defined via the homomorphism $\varphi : [N_0, N_0] \to [N, N]$. By Part (2) of Lemma 3.5.7, we have:

$$\varphi \circ \chi_{w,N_0} = \chi_{w,N}$$

We can rewrite χ_{w,N_0} as $\Omega_{N,L} \circ X_w$, and obtain:

$$\varphi \circ (\Omega_{N,L} \circ X_w) = \chi_{w,N}$$

Using associativity of composition, we obtain:

$$(\varphi \circ \Omega_{N,L}) \circ X_w = \chi_{w,N}$$

Ω itself commutes with homoclinisms, so we obtain:

$$\Omega_{N_0,L} \circ X_w = \chi_{w,N}$$

□

3.6 Exterior square, Schur multiplier, and the second cohomology group

In Section 3.4, we studied the category of central extensions of a group G using the groups $G \wedge G$ (the exterior square of G) and $M(G)$ (the Schur multiplier of G). Instead of studying the original category, we considered the category of central extensions with *homoclinisms* as the morphisms.

Our goal now is to consider, for any group G and abelian group A, the relation between the group $H^2(G; A)$ (described in Section 3.1.5) and the isomorphism types of G and A. More specifically, we will consider the equivalence relation of being isoclinic on $H^2(G; A)$. The equivalence classes turn out to be the fibers of a surjective map from $H^2(G; A)$ that is the right map of an important short exact sequence. We will construct the maps explicitly.

One crucial and nontrivial fact stated in this section will not be proved here, namely, that the sequence is right exact, and more specifically, that the short exact sequence under consideration is the same as the universal coefficient theorem short exact sequence. For a detailed description as well as proofs of these facts, see [6], Theorem 1.8, and in [12], Theorem 2.2.

3.6.1 Homomorphism from the Schur multiplier to the kernel of the extension

We will now describe a very important homomorphism. For any central extension of the form:

$$0 \to A \to E \to G \to 1$$

there is a natural homomorphism from the Schur multiplier of G to A, i.e., a homomorphism:

$$\beta : M(G) \to A$$

We now proceed to describe this homomorphism.

As discussed in Section 3.4.1, there is a natural homomorphism:

$$\Omega : G \wedge G \to [E, E]$$

Compose this with the inclusion of $[E, E]$ in E to get a map $G \wedge G \to E$. We obtain:

$$\begin{array}{ccccccccc} 0 & \to & M(G) & \to & G \wedge G & \to & [G,G] & \to & 1 \\ & & & & \downarrow & & \downarrow & & \\ 0 & \to & A & \to & E & \to & G & \to & 1 \end{array}$$

It is immediate that this diagram commutes.

By general diagram-chasing, we can construct a unique map $M(G) \to A$ such that the diagram continues to be commutative, and that is the homomorphism β that we want:

$$\begin{array}{ccccccccc} 0 & \to & M(G) & \to & G \wedge G & \to & [G,G] & \to & 1 \\ & & \downarrow^{\beta} & & \downarrow & & \downarrow & & \\ 0 & \to & A & \to & E & \to & G & \to & 1 \end{array}$$

3.6.2 Classification of extensions up to isoclinism

Given a group G and an abelian group A, we say that the central extensions E_1 and E_2 with short exact sequences:

$$0 \to A \to E_1 \to G \to 1$$

and

$$0 \to A \to E_2 \to G \to 1$$

are *isoclinic (fixing both G and A)* if there exists an isomorphism of groups $\varphi : E_1' \to E_2'$ satisfying *both* the following conditions:

- Isoclinic as extensions of G: If $\Omega_1 : G \wedge G \to E_1'$ and $\Omega_2 : G \wedge G \to E_2'$ are the commutator map homomorphisms, then $\varphi \circ \Omega_1 = \Omega_2$.
- Suppose B is the inverse image in A of $[E_1, E_1]$. Then, B is also the inverse image in A of $[E_2, E_2]$. Moreover, composing φ with the inclusion of B in $[E_1, E_1]$ gives the inclusion of B in $[E_2, E_2]$.

3.6.3 Relating the classification of extensions up to isoclinism with the homomorphism from the Schur multiplier

In Section 3.6.1, we noted that for any central extension:

$$0 \to A \to E \to G \to 1$$

we have a natural homomorphism $\beta : M(G) \to A$.

The homomorphism is uniquely determined by the choice of extension up to congruence, so we get a *set* map:

$$H^2(G; A) \to \operatorname{Hom}(M(G), A)$$

In Section 3.6.4, we will see that this set map is a *group homomorphism.* We alluded to the group structure on $H^2(G; A)$ in Section 3.1.5 and described it in detail in Section 3.3.

As we will see in Section 3.6.4, this group homomorphism is surjective and is the right map in an important short exact sequence. For now, however, we note that *this group homomorphism classifies extensions up to isoclinism.* Explicitly, two extensions E_1, E_2 are isoclinic in the sense of Section 3.6.2 if and only if they induce the same homomorphism $M(G) \to A$. We now proceed to explain why. Note that one direction, namely the direction that isoclinic extensions define the same homomorphism from $M(G)$ to A, is obvious from the definition. The other direction requires some work.

Consider the two short exact sequences below:

$$\begin{array}{ccccccccc} 0 & \to & M(G) & \to & G \wedge G & \to & [G, G] & \to & 1 \\ & & \downarrow^{\beta} & & \downarrow & & \downarrow^{\mathrm{id}} & & \\ 0 & \to & A & \to & E & \to & G & \to & 1 \end{array}$$

Suppose B is the subgroup of A that arises as the image of the homomorphism $\beta : M(G) \to A$ and $\beta' : M(G) \to B$ is the map obtained by restricting the co-domain. We then have the following two short exact sequences, where all the downward maps are surjective:

$$\begin{array}{ccccccccc} 0 & \to & M(G) & \to & G \wedge G & \to & [G, G] & \to & 1 \\ & & \downarrow^{\beta'} & & \downarrow^{\Omega_{E,G}} & & \downarrow^{\mathrm{id}} & & \\ 0 & \to & B & \to & [E, E] & \to & [G, G] & \to & 1 \end{array}$$

Note that the second row sequence is exact because all the downward maps are surjective.[3]

It is easy to see that if E_1 and E_2 are two central extensions of G that give the same map β, then we can obtain an isomorphism $[E_1, E_1] \to [E_2, E_2]$ such that in the diagram below, the composite of the downward maps in the middle column is $\Omega_{E_2,G}$, and the lower downward arrow in the middle column is an isomorphism.

$$\begin{array}{ccccccccc}
0 & \to & M(G) & \to & G \wedge G & \to & [G,G] & \to & 1 \\
 & & \downarrow^{\beta'} & & \downarrow^{\Omega_{E,G}} & & \downarrow^{\mathrm{id}} & & \\
0 & \to & B & \to & [E_1, E_1] & \to & [G,G] & \to & 1 \\
 & & \downarrow^{\mathrm{id}} & & \downarrow & & \downarrow^{\mathrm{id}} & & \\
0 & \to & B & \to & [E_2, E_2] & \to & [G,G] & \to & 1
\end{array}$$

3.6.4 The universal coefficient theorem short exact sequence

As before, let G be a group and let A be an abelian group. Our goal is to understand all central extension groups E, i.e., short exact sequences of the following form where the image of A in E is in the center of E:

$$0 \to A \to E \to G \to 1$$

As discussed earlier, the set of all congruence classes of extensions is classified by the group $H^2(G; A)$ (the second cohomology group for trivial group action). We now proceed to describe a related short exact sequence. The short exact sequence is discussed in [6], Theorem 1.8, and in [12], Theorem 2.2. The short exact sequence is as follows:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, A) \to H^2(G; A) \to \mathrm{Hom}(M(G), A) \to 0 \tag{3.1}$$

3. Some proof details involving diagram chasing are being omitted for brevity.

Interpretation of the left map of the sequence

The map:

$$\operatorname{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, A) \to H^2(G; A)$$

takes an abelian group extension with normal subgroup A and quotient group G^{ab}, and gives an extension with G on top of A that can loosely be described as follows: the restriction to the derived subgroup $[G, G]$ splits and the quotient sits as per the element of $\operatorname{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, A)$. Explicitly, it can be thought of as a composite of two maps:

$$\operatorname{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, A) \to H^2(G^{\mathrm{ab}}; A) \to H^2(G; A)$$

where the first map treats an abelian group extension simply as a group extension, and the second map uses the contravariance of H^2 in its first argument.

Interpretation of the right map of the sequence

The right map of the sequence:

$$H^2(G; A) \to \operatorname{Hom}(M(G), A)$$

sends an extension group to the corresponding map β described in Section 3.6.1. In Section 3.6.3, we showed that the map $H^2(G; A) \to \operatorname{Hom}(M(G), A)$ classifies extensions up to isoclinism.

What the existence of the short exact sequence tells us

Consider again the short exact sequence:

$$0 \to \operatorname{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, A) \to H^2(G; A) \to \operatorname{Hom}(M(G), A) \to 0$$

We now consider the three aspects of *exactness*:

- Left exactness, i.e., the injectivity of the map $\mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, A) \to H^2(G; A)$. This is the assertion that the only abelian group extension for G^{ab} on top of A that maps to $G \times A$ is the trivial extension. This is immediate from the definition.

- Middle exactness, i.e., the image of the map $\mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, A) \to H^2(G; A)$ is precisely the same as the kernel of the map $H^2(G; A) \to \mathrm{Hom}(M(G), A)$. This is easy to see from the definition.

- Right exactness, i.e., the surjectivity of the map $H^2(G; A) \to \mathrm{Hom}(M(G), A)$. This says that *every homomorphism* from $M(G)$ to A arises from an extension with central subgroup A and quotient group G. In other words, the set of extension types up to isoclinism can be identified with the group $\mathrm{Hom}(M(G), A)$. *This is the most important and least obvious of the three exactness statements.* Many of our later constructive results will rely crucially on right exactness.

How it is a special case of the dual universal coefficient theorem

The general version of the dual universal coefficient theorem for group cohomology is as follows:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(H_{k-1}(G; \mathbb{Z}), A) \to H^k(G; A) \to \mathrm{Hom}(H_k(G; \mathbb{Z}), A) \to 0$$

If we set $k = 2$ and use the fact that $M(G)$ is canonically isomorphic to $H_2(G; \mathbb{Z})$, and also that G^{ab} is canonically isomorphic to $H_1(G; \mathbb{Z})$, we get the short exact sequence we have been discussing.

The splitting of the short exact sequence

The dual universal coefficient theorem for group cohomology, in addition to providing the short exact sequence above, also states that the short exact sequence always splits, but the splitting is not in general canonical. Explicitly, the universal coefficient theorem states that:

$$H^k(G; A) \cong \mathrm{Ext}^1_{\mathbb{Z}}(H_{k-1}(G; \mathbb{Z}), A) \oplus \mathrm{Hom}(H_k(G; \mathbb{Z}), A)$$

In the special case of interest to us, we obtain:

$$H^2(G; A) \cong \mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, A) \oplus \mathrm{Hom}(M(G), A)$$

The direct sum decomposition is *not* in general canonical.

In Section 5.4.5, we will identify some special circumstances where the short exact sequence splits canonically.

3.6.5 An alternate characterization of initial objects, and the existence of Schur covering groups

Recall that, by Lemma 3.4.3, a central extension:

$$0 \to A \to E \to G \to 1$$

is an initial object in the category of central extensions of G with homoclinisms if the natural homomorphism:

$$\Omega_{E,G} : G \wedge G \to [E, E]$$

is an isomorphism. We now provide an alternative characterization.

Lemma 3.6.1. Consider a group G and a central extension:

$$0 \to A \to E \to G \to 1$$

The central extension is an initial object in the category of central extensions of G with homoclinisms if and only if the corresponding homomorphism $\beta : M(G) \to A$ (described in Section 3.6.1) is injective.

Proof. Let B be the image in A of β and let β' be the restriction of β to co-domain B, so β' is a surjective homomorphism from $M(G)$ to B. Note also that β is injective if and only if β' is an isomorphism.

As discussed in Section 3.6.3, we have the following morphism of short exact sequences, where all the downward maps are surjective:

$$\begin{array}{ccccccccc} 0 & \to & M(G) & \to & G \wedge G & \to & [G,G] & \to & 1 \\ & & \downarrow^{\beta'} & & \downarrow^{\Omega_{E,G}} & & \downarrow^{\mathrm{id}} & & \\ 0 & \to & B & \to & [E,E] & \to & [G,G] & \to & 1 \end{array}$$

Since the right-most downward map is the identity map, we see (from some elementary diagram chasing) that β' is an isomorphism if and only if $\Omega_{E,G}$ is an isomorphism. $\square$

Recall the definition of stem extension from Section 3.1.4. We provide an alternative characterization of such extensions:

Lemma 3.6.2. A central extension $0 \to A \to E \to G \to 1$ is a stem extension if and only if the corresponding map $\beta : M(G) \to A$ is surjective.

Proof. Let B be the image in A of β and let β' be the restriction of β to co-domain B, so β' is a surjective homomorphism from $M(G)$ to B. Note also that β is surjective if and only if $B = A$. Note also that $A \leq Z(E)$ by the assumption that the extension is central, so the challenge is to show that $A \leq [E, E]$ if and only if $B = A$.

As described in Section 3.6.3, we have the following morphism of two short exact sequences, with all the downward maps surjective:

$$\begin{array}{ccccccccc} 0 & \to & M(G) & \to & G \wedge G & \to & [G, G] & \to & 1 \\ & & \downarrow^{\beta'} & & \downarrow^{\Omega_{E,G}} & & \downarrow^{\mathrm{id}} & & \\ 0 & \to & B & \to & [E, E] & \to & [G, G] & \to & 1 \end{array}$$

Explicitly, B is the kernel of the homomorphism from $[E, E]$ to $[G, G]$. The homomorphism from $[E, E]$ to $[G, G]$ is obtained by restricting to $[E, E]$ the homomorphism from E to G.

Thus, $B = A \cap [E, E]$. It follows that $A \leq [E, E]$ if and only if $B = A$, completing the proof. $\square$

We are now prepared for a definition.

Definition (Schur covering group)**.** We define a *Schur covering group* of G as a group extension E of G with short exact sequence:

$$0 \to A \to E \to G \to 1$$

satisfying the condition that it is a central extension and the corresponding map $\beta : M(G) \to A$ (defined in Section 3.6.1) is an isomorphism. Equivalently, the extension must satisfy *both* these conditions:

- The extension is a stem extension, i.e., the image of A in E is contained in $Z(E) \cap [E, E]$.
- The natural homomorphism $\Omega_{E,G} : G \wedge G \to [E, E]$ is an isomorphism.

The equivalence of the two versions of the definition follows from the two preceding lemmas (Lemmas 3.6.1 and 3.6.2).

The existence of Schur covering groups is not *a priori* clear, but can be deduced from the short exact sequence of the preceding section.

Theorem 3.6.3. For any group G, Schur covering groups of G exist.

Proof. For any abelian group A, we have the short exact sequence described in Section 3.6.4:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, A) \to H^2(G; A) \to \mathrm{Hom}(M(G), A) \to 0$$

Now, set $A = M(G)$:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, M(G)) \to H^2(G; M(G)) \to \mathrm{Hom}(M(G), M(G)) \to 0$$

Consider the element $\mathrm{Id}_{M(G)} \in \mathrm{Hom}(M(G), M(G))$. By surjectivity (i.e., right exactness), there exists at least one element of $H^2(G; M(G))$ that maps to this. Note that the inverse image is in fact a coset in $H^2(G; M(G))$ of the image of $\mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, M(G))$. Each element in this inverse image corresponds to a Schur covering group. If $\mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, M(G))$ is nontrivial, the Schur covering group need not be unique. $\square$

3.6.6 Realizability of surjective homomorphisms from the exterior square

Suppose G and D are groups and $\alpha : G \wedge G \to D$ and $\delta : D \to [G, G]$ are surjective homomorphisms such that $\delta \circ \alpha : G \wedge G \to [G, G]$ is the canonical map sending $x \wedge y$ to $[x, y]$. We would like to know whether there is a central extension:

$$0 \to A \to E \to G \to 1$$

with the property that there is an isomorphism $\theta : E' \to D$ such that if we consider the homomorphism:

$$\Omega_{E,G} : G \wedge G \to E'$$

then $\theta \circ \Omega_{E,G} = \alpha$. The answer to this question is *yes*. In fact, we can even choose E to be a *stem* extension of G. We outline the construction below.

Recall that we have the following short exact sequence, describing $G \wedge G$ as a central extension of $[G, G]$:

$$0 \to M(G) \to G \wedge G \to [G, G] \to 1$$

Denote by A the image of $M(G)$ under the set map $\alpha : G \wedge G \to D$ and by $\beta : M(G) \to A$ the restricted map. We therefore have the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to & M(G) & \to & G \wedge G & \to & [G, G] & \to & 1 \\ & & \downarrow^{\beta} & & \downarrow^{\alpha} & & \downarrow^{\mathrm{id}} & & \\ 0 & \to & A & \to & D & \xrightarrow{\delta} & [G, G] & \to & 1 \end{array}$$

Now, consider the short exact sequence described in Section 3.6.4:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, A) \to H^2(G; A) \to \mathrm{Hom}(M(G), A) \to 0$$

The right map is surjective, so there exists an extension group E (corresponding to an element of $H^2(G, A)$) such that the map β corresponding to E (as described in Sections 3.6.1 and 3.6.3) is the map β that we specified. Also, for reasons discussed in Section 3.6.3, we can find an isomorphism $\theta : [E, E] \to D$ such that $\theta \circ \Omega_{E,G} = \alpha$.

3.6.7 The existence of stem groups

In Section 2.1.13, we defined a group G as a *stem group* if $Z(G) \leq G'$. Now that we have defined the concept of stem extension, we can provide an alternate definition of stem group: G is a stem group if the short exact sequence:

$$0 \to Z(G) \to G \to G/Z(G) \to 1$$

makes G a stem extension.

We now turn to the proof of a statement made in Section 2.1.13 without proof.

Theorem 3.6.4. Suppose G is a group. Then, the following are true:

1. There exists a stem group K that is isoclinic to G.
2. In case G is finite, all stem groups isoclinic to G are finite and have the same order as each other.

Proof. Proof of (1): Consider the short exact sequence:

$$0 \to Z(G) \to G \to G/Z(G) \to 1$$

This short exact sequence allows us to think of G as a central extension with central subgroup $Z(G)$ and quotient group $G/Z(G)$. We apply the construction in Section 3.6.1 (further discussed in Section 3.6.3) to obtain the natural map $\beta : M(G/Z(G)) \to Z(G)$. Let B be the image of β. By the explicit construction, note that the image of β is actually inside $Z(G) \cap G'$. Let $\beta' : M(G/Z(G)) \to B$ be the map obtained by restricting the co-domain of β to the image of β.

Consider now the short exact sequence of Section 3.6.4 for central subgroup B and quotient group $G/Z(G)$. The short exact sequence is:

$$0 \to \operatorname{Ext}^1_{\mathbb{Z}}((G/Z(G))^{\mathrm{ab}}, B) \to H^2(G/Z(G); B) \to \operatorname{Hom}(M(G/Z(G)), B) \to 0$$

In particular, the map:

$$H^2(G/Z(G); B) \to \mathrm{Hom}(M(G/Z(G)), B)$$

is surjective. This means that we can find a (possibly non-unique and non-canonical) central extension K with short exact sequence:

$$0 \to B \to K \to G/Z(G) \to 1$$

such that the map β_K corresponding to this extension (per Section 3.6.1) is the same as β'. The following are now easy to verify:

- The image of B in K is the center of K.
- The image of B in K is contained in the derived subgroup K'.
- G and K are isoclinic.

Proof of (2): It is easy to verify that any stem group isoclinic to G can be constructed in the above fashion, i.e., it is a central extension group K with quotient group $G/Z(G)$ and central subgroup B such that the map $\beta_K : M(G/Z(G)) \to B$ is equal to β'. In particular, if G is finite, then both $G/Z(G)$ and B are finite, so that K is finite. Further, the order of K is $|B||G/Z(G)|$, so all stem groups isoclinic to G have the same order.

Finally, we wish to show that the order of all stem groups is less than or equal to the order of G. For this, note that B is a subgroup of $Z(G) \cap G'$, so that $|B| \leq |Z(G)|$. Thus, $|K| = |B||G/Z(G)| \leq |Z(G)||G/Z(G)| = |G|$. □

Note that although stem groups exist, there may be no canonical choice of stem group. The problem is the absence of a canonical splitting of the short exact sequence, described in Section 3.6.4. If a canonical splitting did exist, we could use that splitting to obtain a canonical choice of extension.

3.6.8 The Stallings exact sequence

The *Stallings exact sequence* was defined by Stallings in [44] and explored further by Eckmann, Hilton, and Stammbach in [12] for arbitrary group extensions.

Start with a short exact sequence of groups (note that A is not necessarily abelian, but we use this notation to stay consistent with the other sections):

$$1 \to A \to E \to G \to 1$$

Then, the Stallings exact sequence is as follows:

$$M(E) \xrightarrow{\alpha} M(G) \xrightarrow{\beta} A/[E,A] \xrightarrow{\sigma} E^{\text{ab}} \xrightarrow{\tau} G^{\text{ab}}$$

The maps are described as follows:

- The homomorphism $\alpha : M(E) \to M(G)$ arises from the functoriality of the Schur multiplier, discussed in Section 3.4.8.
- The homomorphism $\beta : M(G) \to A/[E,A]$ arises from the corresponding map in the central extension case (discussed below) once we replace the original short exact sequence by the short exact sequence $1 \to A/[E,A] \to E/[E,A] \to G \to 1$.
- The homomorphism $\sigma : A/[E,A] \to E^{\text{ab}} = E/[E,E]$ arises directly from the natural inclusion $A \to E$ under which $[E,A]$ is mapped inside $[E,E]$.
- The homomorphism $\tau : E^{\text{ab}} \to G^{\text{ab}}$ arises from the quotient map $E \to G$ under which $[E,E]$ gets mapped inside $[G,G]$.

In the central extension case, the Stallings exact sequence simplifies to:

$$M(E) \xrightarrow{\alpha} M(G) \xrightarrow{\beta} A \xrightarrow{\sigma} E^{\text{ab}} \xrightarrow{\tau} G^{\text{ab}}$$

The maps are described as follows:

- The homomorphism $\alpha : M(E) \to M(G)$ arises from the functoriality of the Schur multiplier.

- The homomorphism $\beta : M(G) \to A$ is the same as that described in Section 3.6.1.

- The homomorphism $\sigma : A \to E^{\mathrm{ab}} = E/[E, E]$ arises directly from the natural inclusion $A \to E$ under which $[E, A]$ is mapped inside $[E, E]$.

- The homomorphism $\tau : E^{\mathrm{ab}} \to G^{\mathrm{ab}}$ arises from the quotient map $E \to G$ under which $[E, E]$ gets mapped inside $[G, G]$.

3.6.9 Hopf's formula: two proofs

Hopf's formula states that if a group G can be expressed in the form F/R where F is a free group and R is a normal subgroup of F, then:

$$M(G) \cong (R \cap [F, F])/([F, R]) \tag{3.2}$$

We provide two related proofs. The first proof relies on the observation in Section 3.4.7 that if we consider $E_1 = F/[F, R]$ as a central extension of G in a natural fashion, then this central extension is an initial object in the category of group extensions of G with homoclinisms. The exterior square $G \wedge G$ is therefore isomorphic to $E_1' = [F, F]/[F, R]$:

$$G \wedge G \cong [F, F]/[F, R] \tag{3.3}$$

The Schur multiplier $M(G)$ is isomorphic to the kernel of the natural homomorphism $E_1' \to G'$, which is the subgroup $(R \cap [F, F])/[F, R]$ inside $[F, F]/[F, R]$.

Alternately, Hopf's formula can be deduced from the Stallings exact sequence applied to the short exact sequence:

$$1 \to R \to F \to G \to 1$$

combined with the information that $M(F)$ is trivial. Explicitly, the Stallings exact sequence is:

$$M(F) \xrightarrow{\alpha} M(G) \xrightarrow{\beta} R/[F,R] \xrightarrow{\sigma} F/[F,F] \xrightarrow{\tau} G/[G,G]$$

Since $M(F)$ is trivial, we obtain from exactness that $M(G)$ is isomorphic to the kernel of the map σ. From this, we obtain Hopf's formula.

3.6.10 Hopf's formula: class one more version

The following is a slight variant of Hopf's formula for nilpotent groups. Its equivalence with the version of the preceding section (Section 3.6.9) is clear. It is computationally somewhat more useful.

Suppose G is a nilpotent group of nilpotency class c. Suppose G can be expressed in the form F/R where F is a free nilpotent group of class $c+1$ and R is a normal subgroup of F. Then:

$$M(G) \cong (R \cap [F,F])/([F,R]) \tag{3.4}$$

Also:

$$G \wedge G \cong [F,F]/[F,R] \tag{3.5}$$

Free nilpotent groups are described later in more detail in Section 3.10.

3.6.11 Exterior square of an abelian group

Suppose G is an abelian group. Denote by $G \wedge_{\mathbb{Z}} G$ the exterior square of G as an abelian group. We will show here that $G \wedge_{\mathbb{Z}} G$ is canonically isomorphic to $G \wedge G$.

For any central extension:

$$0 \to A \to E \to G \to 1$$

we know that E is a group of nilpotency class at most two. Further, the commutator map:

$$\omega_{E,G} : G \times G \to [E, E]$$

is $\mathbb{Z}$-bilinear. This observation is specific to G being abelian (see Lemma A.3.2 in the Appendix).

Based on this, we obtain that the map below is $\mathbb{Z}$-bilinear:

$$G \times G \to G \wedge G$$

Thus, it induces a map:

$$G \wedge_{\mathbb{Z}} G \to G \wedge G$$

Moreover, since $G \wedge G$ is generated by the elements $x \wedge y$, $x, y \in G$, the map above is surjective.

The part that is *not* immediately obvious is that the map above is injective. In other words, it is *prima facie* plausible that there are additional relations, beyond bilinearity, that are always satisfied in central extensions of G. The explicit description of the exterior square based on generators and relations in Section 3.8.4 will settle this point in a straightforward manner: for an abelian group G, it will turn out that the above map is an isomorphism (see Section 3.8.6 for a summary of the conclusions).

3.6.12 Relationship with K-theory

For any associative unital ring A, we can define a short exact sequence:

$$0 \to K_2(A) \to \mathrm{St}(A) \to E(A) \to 1$$

Here, $\mathrm{St}(A)$ denotes the Steinberg group of A and $E(A)$ denotes the group of elementary matrices over A (note that all these groups are the direct limits of the corresponding groups for $n \times n$ matrices under the obvious inclusion mappings). It is known that $K_2(A) = M(E(A))$ is the Schur multiplier of $E(A)$. It follows by unwinding the definitions that $\mathrm{St}(A)$ is the exterior square of $E(A)$. However, we have not been able to locate the statement (namely, that $\mathrm{St}(A)$ is the exterior square of $E(A)$) anywhere explicitly in the K-theory literature. This may well be because people who work in that area are unaware of the terminology related to the exterior square.

For more information about the Steinberg group and $K_2(A)$, see [37].

3.7 Exterior square, Schur multiplier, and the second cohomology group: Lie ring version

This section covers the Lie ring analogue of the material in Section 3.7. The motivation is largely the same. The analogous material to Section 3.6.11 was already covered in Section 3.5.3, and is therefore not repeated here.

3.7.1 Homomorphism from the Schur multiplier to the kernel of the extension

We will now describe a very important homomorphism. For any central extension of the form:

$$0 \to A \to N \to L \to 0$$

there is a natural homomorphism from the Schur multiplier of L to A, i.e., a homomorphism:

$$\beta : M(L) \to A$$

We now proceed to describe this homomorphism.

As discussed in Section 3.5.1, there is a natural homomorphism:

$$\Omega : L \wedge L \to [N, N]$$

Compose this with the inclusion of $[N, N]$ in N to get a map $L \wedge L \to N$. We obtain:

$$\begin{array}{ccccccccc} 0 & \to & M(L) & \to & L \wedge L & \to & [L, L] & \to & 0 \\ & & & & \downarrow & & \downarrow & & \\ 0 & \to & A & \to & N & \to & L & \to & 0 \end{array}$$

It is immediate that this diagram commutes.

By a special case of the snake lemma, we can construct a unique map $M(L) \to A$ such that the diagram continues to be commutative, and that is the homomorphism β that we want:

$$\begin{array}{ccccccccc} 0 & \to & M(L) & \to & L \wedge L & \to & [L, L] & \to & 0 \\ & & \downarrow^{\beta} & & \downarrow & & \downarrow & & \\ 0 & \to & A & \to & N & \to & L & \to & 0 \end{array}$$

3.7.2 Classification of extensions up to isoclinism

Given a Lie ring L and an abelian Lie ring A, we say that the central extensions N_1 and N_2 with short exact sequences:

$$0 \to A \to N_1 \to L \to 0$$

and

$$0 \to A \to N_2 \to L \to 0$$

are *isoclinic (fixing both L and A)* if there exists an isomorphism of Lie rings $\varphi : N_1' \to N_2'$ satisfying *both* the following conditions:

- Isoclinic as extensions of L: If $\Omega_1 : L \wedge L \to N_1'$ and $\Omega_2 : L \wedge L \to N_2'$ are the Lie bracket map homomorphisms, then $\varphi \circ \Omega_1 = \Omega_2$.
- Suppose B is the inverse image in A of $[N_1, N_1]$. Then, B is also the inverse image in A of $[N_2, N_2]$. Moreover, composing φ with the inclusion of B in $[N_1, N_1]$ gives the inclusion of B in $[N_2, N_2]$.

3.7.3 Relating the classification of extensions up to isoclinism with the homomorphism from the Schur multiplier

In Section 3.7.1, we noted that for any central extension:

$$0 \to A \to N \to L \to 0$$

we have a natural homomorphism $\beta : M(L) \to A$.

The homomorphism is uniquely determined by the choice of extension up to congruence, so we get a *set* map:

$$H^2(L; A) \to \operatorname{Hom}(M(L), A)$$

In Section 3.7.4, we will see that this set map is a *Lie ring homomorphism.* We alluded to the Lie ring structure on $H^2_{\text{Lie}}(L; A)$ in Section 3.2.4 and a detailed description is in the Appendix.

As we will see in Section 3.7.4, this Lie ring homomorphism is surjective and is the right map in an important short exact sequence. For now, however, we note that this Lie ring homomorphism classifies extensions up to isoclinism. Explicitly, two extensions N_1, N_2 are isoclinic in the sense of the preceding section if and only if they induce the same homomorphism $M(L) \to A$. We now proceed to explain why.

Consider the two short exact sequences below:

$$\begin{array}{ccccccccc} 0 & \to & M(L) & \to & L \wedge L & \to & [L,L] & \to & 0 \\ & & \downarrow^{\beta} & & \downarrow & & \downarrow & & \\ 0 & \to & A & \to & N & \to & L & \to & 0 \end{array}$$

Suppose B is the subring of A that arises as the image of the homomorphism $\beta : M(L) \to A$ and $\beta' : M(L) \to B$ is the map obtained by restricting the co-domain. We then have the following two short exact sequences, where all the downward maps are surjective:

$$\begin{array}{ccccccccc} 0 & \to & M(L) & \to & L \wedge L & \to & [L,L] & \to & 0 \\ & & \downarrow^{\beta'} & & \downarrow^{\Omega_{N,L}} & & \downarrow^{\mathrm{id}} & & \\ 0 & \to & B & \to & [N,N] & \to & [L,L] & \to & 0 \end{array}$$

Note that the second row sequence is exact because all the downward maps are surjective.[4]

It is easy to see that if N_1 and N_2 are two central Lie ring extensions of L that give the same map β, then we can obtain an isomorphism $[N_1, N_1] \to [N_2, N_2]$ such that in the diagram below, the composite of the downward maps in the middle column is $\Omega_{N_2,L}$, and the lower downward arrow in the middle column is an isomorphism.

4. Some proof details involving diagram chasing are being omitted for brevity.

$$
\begin{array}{ccccccccc}
0 & \to & M(L) & \to & L \wedge L & \to & [L,L] & \to & 0 \\
 & & \downarrow^{\beta'} & & \downarrow^{\Omega_{N,L}} & & \downarrow^{\mathrm{id}} & & \\
0 & \to & B & \to & [N_1,N_1] & \to & [L,L] & \to & 0 \\
 & & \downarrow^{\mathrm{id}} & & \downarrow & & \downarrow^{\mathrm{id}} & & \\
0 & \to & B & \to & [N_2,N_2] & \to & [L,L] & \to & 0
\end{array}
$$

3.7.4 The universal coefficient theorem short exact sequence

As before, let L be a Lie ring and let A be an abelian Lie ring. Our goal is to understand all central extension Lie rings N, i.e., short exact sequences of the following form where the image of A in N is in the center of N:

$$0 \to A \to N \to L \to 0$$

As discussed earlier, the set of all congruence classes of extensions is classified by the group $H^2_{\mathrm{Lie}}(L;A)$ (the second cohomology group for trivial Lie ring action). We now proceed to describe a related short exact sequence, analogous to the short exact sequence discussed in Section 3.6.4 for groups. The short exact sequence is as follows:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}, A) \to H^2(L;A) \to \mathrm{Hom}(M(L), A) \to 0 \tag{3.6}$$

Note that

Interpretation of the left map of the sequence

The map:

$$\mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}, A) \to H^2(L;A)$$

takes an abelian Lie ring extension with ideal A and quotient Lie ring L^{ab}, and gives an extension with L on top of A that can loosely be described as follows: the restriction to the derived subring $[L, L]$ splits and the quotient sits as per the element of $\mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}, A)$. Explicitly, it can be thought of as a composite of two maps:

$$\mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}, A) \to H^2(L^{\mathrm{ab}}; A) \to H^2(L; A)$$

where the first map treats an abelian Lie ring extension simply as a Lie ring extension, and the second map uses the contravariance of H^2 in its first argument.

Interpretation of the right map of the sequence

The right map of the sequence:

$$H^2(L; A) \to \mathrm{Hom}(M(L), A)$$

sends an extension Lie ring to the corresponding map β described in Section 3.7.1. In Section 3.7.3, we showed that the map $H^2(L; A) \to \mathrm{Hom}(M(L), A)$ classifies extensions up to isoclinism.

What the existence of the short exact sequence tells us

Consider again the short exact sequence:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}, A) \to H^2(L; A) \to \mathrm{Hom}(M(L), A) \to 0$$

We now consider the three aspects of *exactness*:

- Left exactness, i.e., the injectivity of the map $\mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}, A) \to H^2(L; A)$. This is the assertion that the only abelian Lie ring extension for L^{ab} on top of A that maps to $L \times A$ is the trivial extension. This is immediate from the definition.

- Middle exactness, i.e., the image of the map $\mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}, A) \to H^2(L; A)$ is precisely the same as the kernel of the map $H^2(L; A) \to \mathrm{Hom}(M(L), A)$. This is easy to see from the definition.

- Right exactness, i.e., the surjectivity of the map $H^2(L; A) \to \mathrm{Hom}(M(L), A)$. This says that *every homomorphism* from $M(L)$ to A arises from an extension with central subring A and quotient Lie ring L. In other words, the set of extension types up to isoclinism can be identified with the group $\mathrm{Hom}(M(L), A)$. *This is the most important and least obvious of the three exactness statements.* Many of our later constructive results will rely crucially on right exactness.

How it is a special case of the dual universal coefficient theorem

The general version of the dual universal coefficient theorem for Lie ring cohomology is as follows:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(H_{k-1}(L; \mathbb{Z}), A) \to H^k(L; A) \to \mathrm{Hom}(H_k(L; \mathbb{Z}), A) \to 0$$

If we set $p = 2$ and use the fact that $M(L)$ is canonically isomorphic to $H_2(L; \mathbb{Z})$, and also that L^{ab} is canonically isomorphic to $H_1(L; \mathbb{Z})$, we get the short exact sequence we have been discussing.

The splitting of the short exact sequence

The dual universal coefficient theorem for Lie ring cohomology, in addition to providing the short exact sequence above, also states that the short exact sequence always splits, but the splitting is not in general canonical. Explicitly, the universal coefficient theorem states that:

$$H^k(L; A) \cong \mathrm{Ext}^1_{\mathbb{Z}}(H_{k-1}(L; \mathbb{Z}), A) \oplus \mathrm{Hom}(H_k(L; \mathbb{Z}), A)$$

In the special case of interest to us, we obtain:

$$H^2(L; A) \cong \mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}, A) \oplus \mathrm{Hom}(M(L), A)$$

The direct sum decomposition is *not* in general canonical.

In Section 5.4.5, we will note that the short exact sequence splits canonically in the case that L itself is an abelian Lie ring.

3.7.5 An alternate characterization of initial objects, and the existence of Schur covering Lie rings

Recall that, by Lemma 3.5.6, a central extension:

$$0 \to A \to N \to L \to 0$$

is an initial object in the category of central extensions of L with homoclinisms if the natural homomorphism:

$$\Omega_{N,L} : L \wedge L \to [N, N]$$

is an isomorphism. We now provide an alternative characterization.

Lemma 3.7.1. Consider a Lie ring L and a central extension:

$$0 \to A \to N \to L \to 0$$

The central extension is an initial object in the category of central extensions of L with homoclinisms if and only if the corresponding homomorphism $\beta : M(L) \to A$ (described in Section 3.6.1) is injective.

Proof. Let B be the image in A of β and let β' be the restriction of β to co-domain B, so β' is a surjective homomorphism from $M(L)$ to B. Note also that β is injective if and only if β' is an isomorphism.

As discussed in Section 3.6.3, we have the following morphism of short exact sequences, where all the downward maps are surjective:

$$\begin{array}{ccccccccc} 0 & \to & M(L) & \to & L \wedge L & \to & [L,L] & \to & 0 \\ & & \downarrow^{\beta'} & & \downarrow^{\Omega_{N,L}} & & \downarrow^{\mathrm{id}} & & \\ 0 & \to & B & \to & [N,N] & \to & [L,L] & \to & 0 \end{array}$$

Since the right-most downward map is the identity map, we see (from some elementary diagram chasing) that β' is an isomorphism if and only if $\Omega_{N,L}$ is an isomorphism. □

Recall the definition of stem extension from Section 3.2.3. We provide an alternative characterization of such extensions:

Lemma 3.7.2. A central extension $0 \to A \to N \to L \to 0$ is a stem extension if and only if the corresponding map $\beta : M(L) \to A$ is surjective.

Proof. Let B be the image in A of β and let β' be the restriction of β to co-domain B, so β' is a surjective homomorphism from $M(L)$ to B. Note also that β is surjective if and only if $B = A$. Note also that $A \leq Z(N)$ by the assumption that the extension is central, so the challenge is to show that $A \leq [N,N]$ if and only if $B = A$.

As described in Section 3.7.3, we have the following morphism of two short exact sequences, with all the downward maps surjective:

$$\begin{array}{ccccccccc} 0 & \to & M(L) & \to & L \wedge L & \to & [L,L] & \to & 0 \\ & & \downarrow^{\beta'} & & \downarrow^{\Omega_{N,L}} & & \downarrow^{\mathrm{id}} & & \\ 0 & \to & B & \to & [N,N] & \to & [L,L] & \to & 0 \end{array}$$

Explicitly, B is the kernel of the homomorphism from $[N, N]$ to $[L, L]$. The homomorphism from $[N, N]$ to $[L, L]$ is obtained by restricting to $[N, N]$ the homomorphism from N to L.

Thus, $B = A \cap [N, N]$. It follows that $A \leq [N, N]$ if and only if $B = A$, completing the proof. $\square$

We are now prepared for a definition.

Definition (Schur covering Lie ring)**.** We define a *Schur covering Lie ring* of L as a Lie ring extension N of L with short exact sequence:

$$0 \rightarrow A \rightarrow N \rightarrow L \rightarrow 0$$

satisfying the condition that it is a central extension and the corresponding map $\beta : M(L) \rightarrow A$ (defined in Section 3.7.1) is an isomorphism. Equivalently, the extension must satisfy *both* these conditions:

- The extension is a stem extension, i.e., the image of A in N is contained in $Z(N) \cap [N, N]$.
- The natural homomorphism $\Omega_{N,L} : L \wedge L \rightarrow [N, N]$ is an isomorphism.

The equivalence of the two versions of the definition follows from the two preceding lemmas (Lemmas 3.7.1 and 3.7.2).

The existence of Schur covering Lie rings is not *a priori* clear, but can be deduced from the short exact sequence of the preceding section.

Theorem 3.7.3. For any Lie ring L, Schur covering Lie rings of L exist.

Proof. For any abelian Lie ring A, we have the short exact sequence described in Section 3.6.4:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}, A) \to H^2(L; A) \to \mathrm{Hom}(M(L), A) \to 0$$

Now, set $A = M(L)$:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}, M(L)) \to H^2(L; M(L)) \to \mathrm{Hom}(M(L), M(L)) \to 0$$

Consider the element $\mathrm{Id}_{M(L)} \in \mathrm{Hom}(M(L), M(L))$. By surjectivity (i.e., right exactness), there exists at least one element of $H^2(L; M(L))$ that maps to this. Note that the inverse image is in fact a coset in $H^2(L; M(L))$ of the image of $\mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}, M(L))$. Each element in this inverse image corresponds to a Schur covering Lie ring. If $\mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}, M(L))$ is nontrivial, the Schur covering Lie ring need not be unique. □

3.7.6 Realizability of surjective homomorphisms from the exterior square

Suppose L and D are Lie rings and $\alpha : L \wedge L \to D$ and $\delta : D \to [L, L]$ are surjective homomorphisms such that $\delta \circ \alpha : L \wedge L \to [L, L]$ is the canonical map sending $x \wedge y$ to $[x, y]$. We would like to know whether there is a central extension:

$$0 \to A \to N \to L \to 0$$

with the property that there is an isomorphism $\theta : N' \to D$ such that if we consider the homomorphism:

$$\Omega_{N,L} : L \wedge L \to N'$$

then $\theta \circ \Omega_{N,L} = \alpha$. The answer to this question is *yes.* In fact, we can even choose N to be a *stem* extension of L. We outline the construction below.

Recall that we have the following short exact sequence, describing $L \wedge L$ as a central extension of $[L, L]$:

$$0 \to M(L) \to L \wedge L \to [L, L] \to 0$$

Denote by A the image of $M(L)$ under the set map $\alpha : L \wedge L \to D$ and by $\beta : M(L) \to A$ the restricted map. We therefore have the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to & M(L) & \to & L \wedge L & \to & [L, L] & \to & 0 \\ & & \downarrow^{\beta} & & \downarrow^{\alpha} & & \downarrow^{\mathrm{id}} & & \\ 0 & \to & A & \to & D & \xrightarrow{\delta} & [L, L] & \to & 0 \end{array}$$

Now, consider the short exact sequence described in Section 3.7.4:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}, A) \to H^2(L; A) \to \mathrm{Hom}(M(L), A) \to 0$$

The right map is surjective, so there exists an extension Lie ring N (corresponding to an element of $H^2(L, A)$) such that the map β corresponding to N (as described in Sections 3.7.1 and 3.7.3) is the map β that we specified. Also, for reasons discussed in Section 3.7.3, we can find an isomorphism $\theta : [N, N] \to D$ such that $\theta \circ \Omega_{N,L} = \alpha$.

3.7.7 The existence of stem Lie rings

Define a Lie ring L as a *stem Lie ring* if $Z(L) \leq L'$. Now that we have defined the concept of stem extension, we can provide an alternate definition of stem Lie ring: L is a stem Lie ring if the short exact sequence:

$$0 \to Z(L) \to L \to L/Z(L) \to 0$$

makes L a stem extension.

Theorem 3.7.4. Suppose L is a Lie ring. There exists a stem Lie ring K that is isoclinic to L.

Proof. Consider the short exact sequence:

$$0 \to Z(L) \to L \to L/Z(L) \to 0$$

This short exact sequence allows us to think of L as a central extension with central subring $Z(L)$ and quotient Lie ring $L/Z(L)$. We apply the construction in Section 3.7.3 to obtain the natural map $\beta : M(L/Z(L)) \to Z(L)$. Let B be the image of β. By the explicit construction, note that the image of β is actually inside $Z(L) \cap L'$. Let $\beta' : M(L/Z(L)) \to B$ be the map obtained by restricting the co-domain of β to the image of β.

Consider now the short exact sequence of Section 3.7.4 for central subring B and quotient Lie ring $L/Z(L)$. The short exact sequence is:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}((L/Z(L))^{\mathrm{ab}}, B) \to H^2(L/Z(L); B) \to \mathrm{Hom}(M(L/Z(L)), B) \to 0$$

In particular, the map:

$$H^2(L/Z(L); B) \to \mathrm{Hom}(M(L/Z(L)), B)$$

is surjective. This means that we can find a (possibly non-unique and non-canonical) central extension K with short exact sequence:

$$0 \to B \to K \to L/Z(L) \to 0$$

such that the map β_K corresponding to this extension (per Section 3.6.3) is the same as β'. The following are now easy to verify:

- The image of B in K is the center of K.

- The image of B in K is contained in the derived subring K'.

- L and K are isoclinic.

$\square$

Note that although stem Lie rings exist, there may be no canonical choice of stem Lie ring. The problem is the absence of a canonical splitting of the short exact sequence. If a canonical splitting did exist, we could use that splitting to obtain a canonical choice of extension.

3.7.8 The Stallings exact sequence

The *Stallings exact sequence* was defined by Stallings in [44] and explored further by Eckmann, Hilton, and Stammbach in [12] for arbitrary Lie ring extensions.

Start with a short exact sequence of Lie rings (note that A is not necessarily abelian, but we use this notation to stay consistent with the other sections):

$$1 \to A \to N \to L \to 0$$

Then, the Stallings exact sequence is as follows:

$$M(N) \xrightarrow{\alpha} M(L) \xrightarrow{\beta} A/[N,A] \xrightarrow{\sigma} N^{\mathrm{ab}} \xrightarrow{\tau} L^{\mathrm{ab}}$$

The maps are described as follows:

- The homomorphism $\alpha : M(N) \to M(L)$ arises from the functoriality of the Schur multiplier, discussed in Section 3.4.8.

- The homomorphism $\beta : M(L) \to A/[N,A]$ arises from the corresponding map in the central extension case (discussed below) once we replace the original short exact sequence by the short exact sequence $1 \to A/[N,A] \to N/[N,A] \to L \to 0$.

- The homomorphism $\sigma : A/[N, A] \to N^{\text{ab}} = N/[N, N]$ arises directly from the natural inclusion $A \to N$ under which $[N, A]$ is mapped inside $[N, N]$.

- The homomorphism $\tau : N^{\text{ab}} \to L^{\text{ab}}$ arises from the quotient map $N \to L$ under which $[N, N]$ gets mapped inside $[L, L]$.

In the central extension case, the Stallings exact sequence simplifies to:

$$M(N) \xrightarrow{\alpha} M(L) \xrightarrow{\beta} A \xrightarrow{\sigma} N^{\text{ab}} \xrightarrow{\tau} L^{\text{ab}}$$

The maps are described as follows:

- The homomorphism $\alpha : M(N) \to M(L)$ arises from the functoriality of the Schur multiplier.

- The homomorphism $\beta : M(L) \to A$ is the same as that described in Section 3.6.1.

- The homomorphism $\sigma : A \to N^{\text{ab}} = N/[N, N]$ arises directly from the natural inclusion $A \to N$ under which $[N, A]$ is mapped inside $[N, N]$.

- The homomorphism $\tau : N^{\text{ab}} \to L^{\text{ab}}$ arises from the quotient map $N \to L$ under which $[N, N]$ gets mapped inside $[L, L]$.

3.7.9 Hopf's formula for Lie rings: two proofs

Hopf's formula for Lie rings states that if a Lie ring L can be expressed in the form F/R where F is a free Lie ring and R is an ideal of F, then:

$$M(L) \cong (R \cap [F, F])/([F, R]) \tag{3.7}$$

We provide two related proofs. The first proof relies on the observation in Section 3.5.9 that if we consider $N_1 = F/[F, R]$ as a central extension of L in a natural fashion, then this central extension is an initial object in the category of Lie ring extensions of L with homoclinisms. The exterior square $L \wedge L$ is therefore isomorphic to $N_1' = [F, F]/[F, R]$. The Schur multiplier $M(L)$ is isomorphic to the kernel of the natural homomorphism $N_1' \to L'$, which is the subring $(R \cap [F, F])/[F, R]$ inside $[F, F]/[F, R]$.

Alternately, Hopf's formula can be deduced from the Stallings exact sequence applied to the short exact sequence:

$$1 \to R \to F \to L \to 0$$

combined with the information that $M(F)$ is trivial. Explicitly, the Stallings exact sequence is:

$$M(F) \xrightarrow{\alpha} M(L) \xrightarrow{\beta} R/[F, R] \xrightarrow{\sigma} F/[F, F] \xrightarrow{\tau} L/[L, L]$$

Since $M(F)$ is trivial, we obtain from exactness that $M(L)$ is isomorphic to the kernel of the map σ. From this, we obtain Hopf's formula.

3.8 Exterior and tensor product for groups: explicit descriptions

The treatment of tensor products and exterior products found here is similar to that found in [8], [35], and [15].

In keeping with the literature on the topic, we use the convention of groups acting on the left. In particular, when talking of a conjugation action, we refer to the action $(g, x) \mapsto {}^g x = gxg^{-1}$.

The material included in this section can be skipped. Its relevance is primarily that it shows, as a special case, that the exterior square of an abelian group *as a group* is the same as its exterior square *as an abelian group*. We alluded to this, without proof, in Section 3.6.11. However, we also provide an alternative proof in Section 5.4.3.[5]

5. The proofs are not really different once we write down all the details.

3.8.1 Compatible pair of actions

Suppose G and H are groups and $\alpha : G \to \mathrm{Aut}(H)$ and $\beta : H \to \mathrm{Aut}(G)$ are group homomorphisms. We say that (α, β) form a *compatible pair of actions* if *both* the following conditions hold:

$$\begin{aligned} \beta(\alpha(g_1)(h))(g_2) &= {}^{g_1}(\beta(h)({}^{g_1^{-1}}(g_2)))) \ \forall\ g_1, g_2 \in G, h \in H \\ \alpha(\beta(h_1)(g))(h_2) &= {}^{h_1}(\alpha(g)({}^{h_1^{-1}}(h_2))) \ \forall\ h_1, h_2 \in H, g \in G \end{aligned}$$

If we use $\cdot$ to denote the action of each group on itself by conjugation *and* both the actions α and β, the above can be written as:

$$\begin{aligned} (g_1 \cdot h) \cdot g_2 &= g_1 \cdot (h \cdot (g_1^{-1} \cdot g_2)) \ \forall\ g_1, g_2 \in G, h \in H \\ (h_1 \cdot g) \cdot h_2 &= h_1 \cdot (g \cdot (h_1^{-1} \cdot h_2)) \ \forall\ h_1, h_2 \in H, g \in G \end{aligned}$$

The following is an alternate description of the axioms that is sometimes easier to work with:

$$\begin{aligned} {}^{g_1}(\beta(h)g_2) &= \beta(\alpha(g_1)h)({}^{g_1}(g_2)) \ \forall\ g_1, g_2 \in G, h \in H \\ {}^{h_1}(\alpha(g)h_2) &= \alpha(\beta(h_1)g)({}^{h_1}(h_2)) \ \forall\ g \in G, h_1, h_2 \in H \end{aligned}$$

With the $\cdot$ notation, this becomes:

$$
\begin{aligned}
g_1 \cdot (h \cdot g_2) &= (g_1 \cdot h) \cdot (g_1 \cdot g_2) \; \forall \; g_1, g_2 \in G, h \in H \\
h_1 \cdot (g \cdot h_2) &= (h_1 \cdot g) \cdot (h_1 \cdot h_2) \; \forall g \in G, h_1, h_2 \in H
\end{aligned}
$$

The g_2 of the first identity here equals the element $g_1^{-1} \cdot g_2$ of the preceding formulation. The h_2 of the second identity equals the element $h_1^{-1} \cdot h_2$ of the preceding formulation.

The following are examples of compatible pairs of actions:

- The trivial pair of actions is compatible. By "trivial pair of actions" we mean that both the homomorphisms $\alpha : G \to \mathrm{Aut}(H)$ and $\beta : H \to \mathrm{Aut}(G)$ are trivial homomorphisms.
- For a group G, setting $G = H$ and taking both actions to be the action of a group on itself by conjugation gives a compatible pair of actions.
- This generalizes both the preceding examples: if G and H can be embedded as subgroups inside a group Q such that G and H normalize each other in Q, then the actions of G and H on each other by conjugation are compatible. Note that this generalizes the trivial pair of actions because we can set $Q = G \times H$. It generalizes the action of a group on itself by conjugation because, if $G = H$, we can set $Q = G = H$.

3.8.2 Tensor product for a compatible pair of actions

Suppose G and H are groups and $\alpha : G \to \mathrm{Aut}(H)$, $\beta : H \to \mathrm{Aut}(G)$ form a compatible pair of actions. For simplicity of notation, we will use $\cdot$ to denote the action of each group on itself by conjugation *and* both the actions α and β.

The *tensor product* of G and H for this compatible pair of actions, denoted $G \otimes H$, is the quotient of the free group on the set $\{g \otimes h \mid g \in G, h \in H\}$ by the following relations:

$$(g_1g_2) \otimes h = ((g_1 \cdot g_2) \otimes (g_1 \cdot h))(g_1 \otimes h) \ \forall \ g_1, g_2 \in G, h \in H$$

$$g \otimes (h_1h_2) = (g \otimes h_1)((h_1 \cdot g) \otimes (h_1 \cdot h_2)) \ \forall \ g \in G, h_1, h_2 \in H$$

3.8.3 Exterior product of normal subgroups of a group

Suppose G and H are subgroups of a group Q such that G and H both normalize each other. Then, the actions of G and H on each other by conjugation form a compatible pair of actions. Note that we can assume without loss of generality that G and H are both normal in Q, because if not, then Q can be replaced by the subgroup GH of Q and the rest of the construction is unaffected.

We define the *exterior product* $G \wedge H$ as the quotient of the tensor product $G \otimes H$ by the normal subgroup generated by the set $\{x \otimes x \mid x \in G \cap H\}$. The image of $g \otimes h$ is denoted $g \wedge h$.

3.8.4 Tensor square and exterior square of a group

Let G be a group. The *tensor square* of G, denoted $G \otimes G$ or $\bigotimes^2 G$, is defined as the tensor product of G with itself for the compatible pair of actions where both actions equal the action of G on itself by conjugation.

The *exterior square* of G, denoted $G \wedge G$ or $\bigwedge^2 G$, is defined as the exterior product of G and G where both copies of G are viewed as normal subgroups inside G. Explicitly, $G = H = Q$ in the notation used in the preceding subsection.

Alternately the exterior square of G can be defined as the quotient of the tensor square of G by the normal subgroup generated by the subset $\{g \otimes g \mid g \in G\}$.

3.8.5 Reconciling the definitions of exterior square

Clair Miller, in her 1952 paper [36] introducing the concept of the exterior square, proved the equivalence of the two descriptions of exterior square.[6] A later paper [17] by Graham J. Ellis, published in 1993, discussed the matter and related questions in considerably greater detail.

3.8.6 The special case of abelian groups

There are pre-existing concepts of tensor product, tensor square, and exterior square for abelian groups. These coincide with our general definitions above when both definitions make sense. Explicitly, the following are true and can be readily verified from the definitions above. We will $\otimes_{\mathbb{Z}}$ and $\wedge_{\mathbb{Z}}$ to denote tensor and exterior product operations *as abelian groups*.

- The tensor product $G \otimes H$ for the trivial pair of actions of G and H on each other is an abelian group that is canonically isomorphic to the tensor product of abelian groups $G^{\mathrm{ab}} \otimes_{\mathbb{Z}} H^{\mathrm{ab}}$.
- In particular, the tensor square $G \otimes G$ for an abelian group G agrees with its tensor square *as an abelian group*, i.e., $G \otimes_{\mathbb{Z}} G \cong G \otimes G$.
- The exterior square $G \wedge G$ for an abelian group agrees with its exterior square *as an abelian group*, i.e., $G \wedge_{\mathbb{Z}} G \cong G \wedge G$.

3.9 Exterior and tensor product for Lie rings: explicit descriptions

This section does for Lie rings what the preceding section (Section 3.8) did for groups.

6. This is a somewhat hard-to-verify statement, since Miller's paper uses different terminology and language from what we use.

Our treatment here closely follows the 1989 paper [16] by Graham Ellis. Proofs of unproved assertions here can be found in the paper.

The section can be skipped without any loss of continuity.

3.9.1 Compatible pair of actions of Lie rings

Suppose M and N are Lie rings. Suppose $\alpha : M \to \mathrm{Der}(N)$ and $\beta : N \to \mathrm{Der}(M)$ are homomorphism of Lie rings, where $\mathrm{Der}(M)$ and $\mathrm{Der}(N)$ denote the Lie ring of derivations of M and of N respectively. We say that α, β form a *compatible pair of actions* if the following two conditions hold:

$$\begin{aligned}
\alpha(\beta(n_1)m)(n_2) &= [n_2, \alpha(m)n_1] \ \forall\ m \in M, n_1, n_2 \in N \\
\beta(\alpha(m_1)n)(m_2) &= [m_2, \beta(n)m_1] \ \forall\ m_1, m_2 \in M, n \in N
\end{aligned}$$

The above expressions are easier to write down if we use $\cdot$ to denote the actions. In this case, the above become:

$$\begin{aligned}
(n_1 \cdot m) \cdot n_2 &= [n_2, m \cdot n_1] \ \forall\ m \in M, n_1, n_2 \in N \\
(m_1 \cdot n) \cdot m_2 &= [m_2, n \cdot m_1] \ \forall\ m_1, m_2 \in M, n \in N
\end{aligned}$$

The following are true:

- For any Lie ring L, the adjoint action of L on itself forms a compatible pair of actions with itself.

- For any Lie rings M and N, the trivial Lie ring actions of M and N on each other form a compatible pair of actions.

- The following generalizes the preceding two examples: if M and N can be embedded as ideals inside a Lie ring Q, then the adjoint actions of M and N on each other form a compatible pair of actions. Note that it suffices to assume that M and N are Lie subrings that idealize each other, but there is no loss of generality since we can replace Q by the subring $M + N$.

3.9.2 Tensor product of Lie rings

Suppose M and N are Lie rings and $\alpha : M \to \mathrm{Der}(N)$ and $\beta : N \to \mathrm{Der}(M)$ is a compatible pair of actions of Lie rings. We define the *tensor product* $M \otimes N$ for this pair of actions as follows. It is the quotient of the free Lie ring on formal symbols of the form $m \otimes n$ $(m \in M, n \in N)$ by the following relations:

1. Additive in M: $(m_1 + m_2) \otimes n = (m_1 \otimes n) + (m_2 \otimes n)$ $\forall$ $m_1, m_2 \in M, n \in N$. Note that if we are dealing with Lie algebras instead of Lie rings, we will replace additivity by "linearity" in M with respect to the ground ring.

2. Additive in N: $m \otimes (n_1 + n_2) = (m \otimes n_1) + (m \otimes n_2)$ $\forall$ $m \in M, n_1, n_2 \in N$. Note that if we are dealing with Lie algebras instead of Lie rings, we will replace additivity by "linearity" in N with respect to the ground ring.

3. Expanding a tensor product involving one Lie bracket:

   - $[m_1, m_2] \otimes n = m_1 \otimes \alpha(m_2)(n) - m_2 \otimes \alpha(m_1)(n)$ $\forall$ $m_1, m_2 \in M, n \in N$
   - $m \otimes [n_1, n_2] = \beta(n_2)m \otimes n_1 - \beta(n_1)(m) \otimes n_2$ $\forall m \in M, n_1, n_2 \in N$

   If both the actions are rewritten using $\cdot$, this simplifies to:

   - $[m_1, m_2] \otimes n = m_1 \otimes (m_2 \cdot n) - m_2 \otimes (m_1 \cdot n)$ $\forall$ $m_1, m_2 \in M, n \in N$

- $m \otimes [n_1, n_2] = (n_2 \cdot m) \otimes n_1 - (n_1 \cdot m) \otimes n_2 \ \forall m \in M, n_1, n_2 \in N$

4. Expanding a Lie bracket of two pure tensors:

$$[(m_1 \otimes n_1), (m_2 \otimes n_2)] = -(\beta(n_1)(m_1)) \otimes (\alpha(m_2)(n_2))$$

5. If both the actions are rewritten using $\cdot$, this becomes:

$$[(m_1 \otimes n_1), (m_2 \otimes n_2)] = -(n_1 \cdot m_1) \otimes (m_2 \cdot n_2)$$

3.9.3 Exterior product of Lie rings

Suppose M, N are (possibly equal, possibly distinct) ideals in a Lie ring Q. Note that in fact it suffices to assume that they idealize each other, but there is no loss of generality in assuming that they are both ideals because we could replace Q by $M + N$.

Define a compatible pair of actions of Lie rings of M and N on each other via the adjoint action on each other, i.e., the action that each induces on the other by restricting the inner derivation given by the adjoint action in the whole Lie ring. The exterior product of M and N is then defined as the quotient of the tensor product of Lie rings $M \otimes N$ for this compatible pair of actions by the ideal generated by elements of the form $x \otimes x, x \in M \cap N$.

3.9.4 Tensor square and exterior square of a Lie ring

Let L be a Lie ring. The *tensor square* of L, denoted $L \otimes L$ or $\bigotimes^2 L$, is defined as the tensor product of L with itself for the compatible pair of actions where both actions equal the adjoint action of L on itself.

The *exterior square* of L, denoted $L \wedge L$ or $\bigwedge^2 L$, is defined as the exterior product of L and L where both copies of L are viewed as ideals inside L. Explicitly, $M = N = Q = L$ in the notation used in the preceding subsection.

Alternately the exterior square of L can be defined as the quotient of the tensor square of L by the ideal generated by the subset $\{x \otimes x \mid x \in L\}$.

3.10 Free nilpotent groups: basic facts about their homology groups

3.10.1 Free nilpotent group: definition

The free nilpotent group of class c on a set S can be defined as the free algebra on S in the variety of groups of nilpotency class at most c. Below is an explicit definition in terms of the free group.

Definition (Free nilpotent group)**.** Suppose S is a set and c is a positive integer. The *free nilpotent group* of class c on the set S is defined as the quotient group $F(S)/\gamma_{c+1}(F(S))$ where $F(S)$ is the free group on S. Equivalently, this group, along with the set map to it from S, is the initial object in the category of groups of nilpotency class at most c with set maps to them from S.

The functor sending a set to the free nilpotent group of class c is left adjoint to the forgetful functor from nilpotent groups of class c to sets.[7]

3.10.2 Homology of free nilpotent groups

Suppose G is the free nilpotent group of class c on a generating set S. G can be naturally identified with $F/\gamma_{c+1}(F)$ where F is the *free group* of class c (i.e., F is a free algebra in the variety of groups). We wish to compute the homology of G.

Setting $R = \gamma_{c+1}(F)$ and working out the details as discussed in Section 3.6.9, we obtain:

7. This means that given a set S and a group G of nilpotency class at most c, there is a canonical bijection between the set of *set maps* from S to G and the set of *group homomorphisms* from $F(S)$ to G. For more on adjoint functors, see the Appendix, Section A.2.3.

- The group $[F, R]$ equals $[F, \gamma_{c+1}(F)] = \gamma_{c+2}(F)$.
- The group $E = F/[F, R]$, with the natural quotient map $E \to G$, is an initial object in the category of central extensions of G with homoclinisms. Note that E is a free nilpotent group of class $c+1$ on the same generating set S.
- The exterior square $G \wedge G$ is canonically isomorphic to $[E, E]$, or equivalently, to $[F, F]/[F, R] = \gamma_2(F)/\gamma_{c+2}(F)$.
- The Schur multiplier $M(G)$ is canonically isomorphic to the quotient group $(R \cap [F, F])/[F, R] = \gamma_{c+1}(F)/\gamma_{c+2}(F)$.
- The canonical short exact sequence:

$$0 \to M(G) \to G \wedge G \to [G, G] \to 1$$

is isomorphic to the short exact sequence:

$$0 \to \gamma_{c+1}(F)/\gamma_{c+2}(F) \to \gamma_2(F)/\gamma_{c+2}(F) \to \gamma_2(F)/\gamma_{c+1}(F) \to 1$$

3.11 Free nilpotent Lie rings: basic facts about their homology groups

3.11.1 Free nilpotent Lie ring: definition

The free nilpotent Lie ring of class c on a set S can be defined as the free algebra on S in the variety of Lie rings of nilpotency Lie rings at most c. Below is an explicit definition in terms of the free group.

Definition (Free nilpotent Lie ring)**.** Suppose S is a set and c is a positive integer. The *free nilpotent* of class c on the set S is defined as the quotient Lie ring $F(S)/\gamma_{c+1}(F(S))$

where $F(S)$ is the free Lie ring on S. Equivalently, this Lie ring, along with the set map to it from S, is the initial object in the category of Lie rings of nilpotency class at most c with set maps to them from S.

The functor sending a set to the free nilpotent Lie ring of class c is left adjoint to the forgetful functor from nilpotent Lie rings of class c to sets.[8]

3.11.2 Homology of free nilpotent Lie rings

Suppose L is the free nilpotent Lie ring of class c on a generating set S. L can be naturally identified with $F/\gamma_{c+1}(F)$ where F is the *free Lie ring* of class c (i.e., F is a free algebra in the variety of Lie rings). We wish to compute the homology of L.

Setting $R = \gamma_{c+1}(F)$ and working out the details as discussed in Section 3.7.9, we obtain:

- The Lie ring $[F, R]$ equals $[F, \gamma_{c+1}(F)] = \gamma_{c+2}(F)$.
- The Lie ring $N = F/[F, R]$, with the natural quotient map $N \to L$, is an initial object in the category of central extensions of L with homoclinisms. Note that N is a free nilpotent Lie ring of class $c + 1$ on the same generating set S.
- The exterior square $L \wedge L$ is canonically isomorphic to $[N, N]$, or equivalently, to $[F, F]/[F, R] = \gamma_2(F)/\gamma_{c+2}(F)$.
- The Schur multiplier $M(L)$ is canonically isomorphic to the quotient Lie ring $(R \cap [F, F])/[F, R] = \gamma_{c+1}(F)/\gamma_{c+2}(F)$.
- The canonical short exact sequence:

$$0 \to M(L) \to L \wedge L \to [L, L] \to 0$$

8. This means that given a set S and a Lie ring L of nilpotency class at most c, there is a canonical bijection between the set of *set maps* from S to L and the set of *Lie ring homomorphisms* from $F(S)$ to L.

is isomorphic to the short exact sequence:

$$0 \to \gamma_{c+1}(F)/\gamma_{c+2}(F) \to \gamma_2(F)/\gamma_{c+2}(F) \to \gamma_2(F)/\gamma_{c+1}(F) \to 0$$

CHAPTER 4

POWERING OVER SETS OF PRIMES

4.1 Groups powered over sets of primes: key results

Abelian groups can be defined as modules over $\mathbb{Z}$, the ring of integers. We can therefore think of groups as the non-abelian analogues of modules over $\mathbb{Z}$. In other words, we can think of group theory as essentially happening "over $\mathbb{Z}$": we can raise group elements only to integer powers.

Working over $\mathbb{Z}$ is insufficient for the Lie correspondence and its generalizations. We saw in Section 1.1.6 that the Lie correspondence between $NT(n, \mathbb{R})$ and $UT(n, \mathbb{R})$ relies on the matrix exponential and logarithm maps, which involve division. This division happens inside the associative algebra of $n \times n$ matrices over $\mathbb{R}$, but it is also related to the question of existence of rational powers of elements in the group $UT(n, \mathbb{R})$.

The purpose of this section is to develop the general theory of π-powered groups: groups where it is possible to define p^{th} roots of elements uniquely for p in a specified set π of primes. The main purpose is to understand how "closed" this collection is under various operations including taking subgroups and quotient groups of important types. The theory will be useful in establishing key aspects of the behavior of the Malcev and Lazard correspondences, and their generalizations. When necessary, we will restrict attention to nilpotent groups, where we can derive stronger conclusions than for arbitrary groups.

4.1.1 Some important intermediate rings between the integers and the rationals

We denote the ring of integers as $\mathbb{Z}$ and the field of rational numbers as $\mathbb{Q}$. Clearly, $\mathbb{Z} \subseteq \mathbb{Q}$. The intermediate subrings between $\mathbb{Z}$ and $\mathbb{Q}$ can be described as follows. For any prime set π, denote by $\mathbb{Z}[\pi^{-1}]$ the subring of $\mathbb{Q}$ comprising those rational numbers such that, when the rational number is written as a reduced fraction, all prime divisors of the denominator are in π. Equivalently, it is the subring of $\mathbb{Q}$ generated by the elements $1/p, p \in \pi$. The following are some special cases of interest:

- The case that π is the empty set: In this case, $\mathbb{Z}[\pi^{-1}] = \mathbb{Z}$.
- The case that π is the set of all primes: In this case, $\mathbb{Z}[\pi^{-1}] = \mathbb{Q}$.
- The case that π is a singleton set $\{p\}$ for some prime number p: In this case, $\mathbb{Z}[\pi^{-1}] = \mathbb{Z}[1/p]$ is the subring generated by $1/p$.

In the language of commutative algebra, we would say that $\mathbb{Z}[\pi^{-1}]$ is the localization of $\mathbb{Z}$ at the multiplicative subset comprising all π-numbers. Here, a π-number is a number all of whose prime divisors are in π.

4.1.2 Background and motivation

While building the Lazard correspondence and its generalizations, one of the important operations we need to do is take n^{th} roots of elements (on the group side) or divide elements by n (on the Lie ring side). We need to be able to make sense of these operations.

There are two approaches to this:

1. The first approach is to impose conditions on the group and Lie ring of unique divisibility by specific primes. It suffices to restrict attention to primes because unique divisibility by specific primes gives unique divisibility by all products of powers of these, and conversely, unique divisibility by a number n implies unique divisibility by all the prime divisors of n. In this approach, the operation of taking p^{th} roots is not a separate operation but one uniquely determined by the group operations.
2. The second approach is to redefine the concept of group and/or Lie ring by including operations that correspond to taking p^{th} roots for specific primes p. On the Lie ring

side, this means that instead of a Lie ring, we are talking now of a Lie *algebra* over the ring $\mathbb{Z}[1/p]$. If there is more than one prime, we adjoin all their reciprocals, so that we are considering a Lie algebra over the ring $\mathbb{Z}[\pi^{-1}]$ where π is the set of primes for which we want to adjoint roots. If all primes are included, we simply get a Lie algebra over $\mathbb{Q}$. On the group side, we need to define an appropriate corresponding notion of group powered over a ring, then consider groups powered over $\mathbb{Z}[1/p]$ and similar rings. Note that in this approach, there is *additional structure* being imposed on the group and/or Lie ring. We would therefore revise the concept of "subgroup" and "quotient group" as being systems that are closed under the additional newly defined operations.

Both approaches have their advantages and disadvantages. The advantage of approach (1) is that since we are working with groups and Lie rings as we usually understand them (over $\mathbb{Z}$) we do not need to recheck any of the standard results, and conversely, any results we discover here apply to abstract groups without additional structures. The disadvantage is that we *do* need to verify that the subgroups and quotient groups of interest inherit the unique divisibility (powering) structure. This section focuses on a number of simple lemmas designed for that goal.

Approach (2) is also reasonably straightforward in this case, but it gets somewhat trickier when we want to deal with groups powered over arbitrary rings. The axioms are easy to pin down for arbitrary rings only in the case of nilpotent groups. For an exposition based on approach (2), Thomas Weigel's monograph [48] and the references therein are a good start. We will use some aspects of approach (2) for some of the trickier results.

4.1.3 Group powered over a prime

We begin with some definitions. Our definitions match those in Khukhro's text [29] and our treatment is quite similar to that in Khukhro's text.

Definition (Powered for a set of primes)**.** Suppose G is a group and π is a set of prime numbers. We say that G is *powered over* π, or π*-powered*, if it satisfies the following equivalent conditions:

- For any $g \in G$ and any $p \in \pi$, there is a unique element $h \in G$ such that $h^p = g$.
- For any $g \in G$ and any natural number n all of whose prime factors are in π, there is a unique element $h \in G$ such that $h^n = g$.

For a single prime p, we shorten $\{p\}$-powered to p-powered, following the time-honored abuse of notation conflating elements with singleton subsets. Note that [29] uses the notation $\mathbb{Q}_\pi$-powered for what we call π-powered.[1]

Definition (Local for a set of primes)**.** Suppose G is a group and π is a set of prime numbers. We say that G is π-local if G is powered over all the primes *not* in π.

For a single prime p, we shorten $\{p\}$-local to p-local.

The term "local" here is used in analogy with localizations of rings at prime ideals: when we localize at a prime ideal, we introduce inverses *for all other primes.* Note that this is not directly related to the sense of the word "local" in the context of *local analysis* used in the classification of finite simple groups.

For this section, we will frame all our results in terms of π-powered groups rather than π-local groups. Obviously, each result formulated in the language of π-powered groups can be formulated instead in the language of π-local groups.

An extreme case is the case of a *rationally powered group*:

Definition (Rationally powered group)**.** A group G is termed a *rationally powered group*

1. One reason we avoid this notation is that $\mathbb{Q}_p$ is often used for the p-adics, which are quite different from what we wish to consider here.

or a $\mathbb{Q}$-powered group if it is powered over the set of all primes.

Our interest throughout this document will be on nilpotent and locally nilpotent groups, but it is worth pointing out that there do exist non-nilpotent rationally powered groups. The easiest example is the group $GA^+(1, \mathbb{R})$, which is defined as $\mathbb{R} \rtimes (\mathbb{R}^*)^+$, i.e., the group of affine maps from $\mathbb{R}$ to $\mathbb{R}$ of the form $x \mapsto ax + b$ with $a > 0$, under composition. For any natural number n, every element of the group has a unique n^{th} root. Explicitly, the unique n^{th} root of $x \mapsto ax + b$ is the map:

$$x \mapsto a^{1/n}x + \frac{b}{1 + a^{1/n} + \cdots + a^{(n-1)/n}}$$

This is an example of a rationally powered solvable group that is not nilpotent.

It is also possible to construct *free* π-powered groups for any set of prime numbers and any size of generating set. When the generating set has size more than one, these are not solvable. The free π-powered groups are extremely difficult to work with because of the absence of an easily definable reduced form for words. We will discuss free constructions in Section 4.3.

The majority of the results in this section can either be found in the literature or are fairly easy to deduce, or both. The historical origins of many individual results are hard to trace. For this reason, we provide full proofs and avoid citations to papers for individual results in this section. A number of the results have appeared in [5], [34], [29], and other references.

4.1.4 The variety of powered groups and its forgetful functor to groups

Suppose π is a set of primes. The collection of π-powered groups forms a variety of algebras. The operations in the variety include the usual group operations (group multiplication, identity element, inverse map) as well as operations of the form $x \mapsto x^{1/p}$ for each prime

$p \in \pi$, with the following two identities for each $p \in \pi$:

- $(x^p)^{1/p} = x$: This condition shows that the p^{th} power map is *injective*, and that $u^{1/p}$ is the unique p^{th} root of u *if* u is a p^{th} power.
- $(x^{1/p})^p = x$: This condition shows that the p^{th} power map is *surjective*, i.e., that every element is a p^{th} power.

Suppose $\pi_1 \subseteq \pi_2$ are sets of primes. As discussed in Section A.2.5, there is a forgetful functor from the variety of π_2-powered groups to the variety of π_1-powered groups. Each of these forgetful functors turns out to be *full*. Essentially, this means that a set map $\varphi : G_1 \to G_2$ between π_2-powered groups G_1 and G_2 is a homomorphism of π_2-powered groups if and only if it is a homomorphism of π_1-powered groups. The reason is that for all primes $p \in \pi_2$, the $1/p$-powering map is preserved by the homomorphism simply on account of the homomorphism being a group homomorphism and p^{th} roots being unique in the target group G_2.

4.1.5 The concepts of divisible and torsion-free

We introduce some other useful definitions, again similar to those found in [29].

Definition (Divisibility for a set of primes)**.** Suppose G is a group and π is a set of primes. We say that G is π-*divisible* if it satisfies the following equivalent conditions:

- For any $g \in G$ and any $p \in \pi$, there exists $h \in G$ (not necessarily unique) such that $h^p = g$.
- For any $g \in G$ and any natural number n all of whose prime factors are in π, there exists $h \in G$ (not necessarily unique) such that $h^n = g$.

For a single prime p, we use the term p-divisible for $\{p\}$-divisible, with the usual abuse of notation conflating elements with singleton subsets.

When we say that G is *divisible* (without any set of primes specified) this will be understood to mean that G is divisible for the set of all primes.

We now define *torsion-free*.

Definition (Torsion-free for a set of primes)**.** Suppose G is a group and π is a set of primes. We say that G is π-*torsion-free* if it has no element of order p for any $p \in \pi$.

When we say that G is *torsion-free* (without any set of primes specified) this will be understood to mean that G is torsion-free for the set of all primes.

In a short while, we will prove that for nilpotent groups, being powered over a set of primes is equivalent to being both divisible and torsion-free for that set of primes. However, this is not completely obvious at the moment, and the corresponding result is false for non-nilpotent groups.

Most of the results that follow rely on the following two crucial observations, where $\gamma_i(G)$ denote the members of the lower central series of G:

- Each successive quotient $\gamma_i(G)/\gamma_{i+1}(G)$ is a homomorphic image of a tensor power of G/G', the abelianization of G, via the i-fold iterated commutator map:

$$G/G' \times G/G' \times \cdots \times G/G' \to \gamma_i(G)/\gamma_{i+1}(G)$$

  See Lemma A.3.2 for more details.

- In the quotient $G/\gamma_{i+1}(G)$, the subgroup $\gamma_i(G)/\gamma_{i+1}(G)$ is central.

For simplicity, we will state and prove the results in subsequent sections with respect to individual primes. However, the results easily extend to sets of primes. More explicitly, for each of our results, the corresponding result will hold if we uniformly replace "p-powered" by "π-powered," "p-divisible" by "π-divisible," and "p-torsion-free" by π-torsion-free" for an arbitrary set π of primes.

4.1.6 The case of finite groups

If our interest is solely in finite groups, then the machinery developed in this section is unnecessary. In particular, the finite version of all results of interest follows from these two lemmas.

Lemma 4.1.1. For a finite group G and a prime number p, the following are equivalent:

1. p does not divide the order of G.
2. p does not divide the exponent of G.
3. G is p-powered.
4. G is p-divisible.
5. G is p-torsion-free.

The proof is straightforward.

The next lemma builds on this.

Lemma 4.1.2. 1. Every subgroup, quotient group, and subquotient of a p-powered (respectively, p-divisible, p-torsion-free) finite group is p-powered (respectively, p-divisible, p-torsion-free).

2. If a finite group G has a normal subgroup H such that H and the quotient group G/H are both p-powered (respectively, p-divisible, p-torsion-free), then G is also p-powered (respectively p-divisible, p-torsion-free).

Proof. (1) follows directly by using the characterization in terms of p not dividing the order, and using Lagrange's theorem to note that the order of any subgroup and quotient group divides the order of the group.

(2) follows by combining the characterization in terms of p not dividing the order, and using Lagrange's theorem to note that the order of a group is the product of the orders of any normal subgroup and the corresponding quotient group. □

In particular, a finite p-group is powered over *all* primes *other than* p. Thus, it is in particular powered over all primes less than p (a very important observation) and also over all primes greater than p (a less important, but still useful, observation). An equivalent formulation is that any finite p-group is a p-local group.

Note that the result has some analogues for infinite groups in which every element has finite order, but we do not need to develop these for our purpose.

4.1.7 Some general results on powering and divisibility

We begin with some preliminary lemmas.

Lemma 4.1.3 (Divisibility is inherited by quotient groups)**.** Suppose G is a group and H is a normal subgroup. Suppose that G is p-divisible for some prime number p. Then, the quotient group G/H is also p-divisible. Explicitly, if $a \in G/H$, there exists $b \in G/H$ such that $b^p = a$.

Proof. Let $\varphi : G \to G/H$ be the quotient map. Pick $g \in G$ such that $\varphi(g) = a$. There exists $h \in G$ such that $h^p = g$ due to the p-divisibility of G. The element $b = \varphi(h)$ satisfies $b^p = a$. □

We next show that powering on the quotient group implies powering on the subgroup.

Lemma 4.1.4 (Quotient-to-subgroup powering implication)**.** Suppose G is a group and H is a normal subgroup of G. Suppose p is a prime number such that both G and G/H are p-powered groups. Then, H is also a p-powered group. In other words, for any $g \in H$, there exists a unique element $x \in H$ such that $x^p = g$.

Proof. Let $\varphi : G \to G/H$ be the quotient map.

Since G as a whole is p-powered, there exists $x \in G$ such that $x^p = g$, and this x is unique in G. It suffices to show that this unique x is an element of H. For this, note that $(\varphi(x))^p = \varphi(x^p) = \varphi(g)$ is the identity element of G/H. Thus, $\varphi(x)$ is an element of order 1 or p in G/H. Since G/H is p-powered, this forces $\varphi(x)$ to be the identity element of G/H, so $x \in H$, as desired. □

Theorem 4.1.18 gives a converse implication specific to the nilpotent context.

4.1.8 Results for the center

We begin with a lemma about the center.

Lemma 4.1.5. Suppose G is a group with center $Z(G)$. Suppose n is a natural number. If $z \in Z(G)$ is such that there is a unique $x \in G$ satisfying $x^n = z$, then $x \in Z(G)$.

In particular, if G is powered over a prime p, so is the center $Z(G)$.

The key feature of the center that we use in the proof here is that it is the fixed-point subgroup of a subgroup of $\mathrm{Aut}(G)$ (namely, $\mathrm{Inn}(G)$). The proof also works for fixed-point subgroups of other subgroups of $\mathrm{Aut}(G)$. In particular, the proof works for all subgroups arising as centralizers of subgroups of G.

Proof. It suffices to show that for any $y \in G$, $yxy^{-1} = y$.

Note that:

$$(yxy^{-1})^n = yx^ny^{-1} = yzy^{-1} = z$$

Thus, $(yxy^{-1})^n = z = x^n$. Now, the uniqueness of x (as a n^{th} root of z) forces that in fact $yxy^{-1} = x$, completing the proof. $\square$

Next:

Lemma 4.1.6. Suppose p is a prime number, G is a p-powered group, and H is a central subgroup of G that is also p-powered. Then, the quotient group G/H is also p-powered. Explicitly, for any $a \in G/H$, there is a unique $b \in G/H$ satisfying $b^p = a$.

The proof below seems notationally complicated, but the idea is simple. We first use the existence of p^{th} roots in the whole group to find a candidate p^{th} root in G/H. We now want to show uniqueness. Since the subgroup H is in the center, we can take p^{th} roots of the subgroup elements used to translate within a coset in order to figure out the appropriate translates on the p^{th} roots. Then, we use the uniqueness aspect to argue that all p^{th} roots of elements in a particular coset must lie in a single coset.

Proof. Let $\varphi : G \to G/H$ be the quotient map.

Let $g \in G$ be such that $\varphi(g) = a$. There exists $x \in G$ such that $x^p = g$.

For any $u \in H$, there exists $v \in H$ such that $v^p = u$ (due to our assumption that H is p-powered). Thus, for any element of G of the form gu with g as above and $u \in H$, we get $(xv)^p = x^pv^p = gu$ with v as the element satisfying $v^p = u$. Note that rewriting $(xv)^p = x^pv^p$ uses the assumption that H is in the center of G.

Now, we claim that the element $b = \varphi(x)$ is the unique element satisfying $b^p = a$. First, note that $b^p = a$ follows by applying φ to both sides of $x^p = g$. Suppose there is an element $c \in G/H$ satisfying $c^p = a$. Let $y \in G$ be such that $\varphi(y) = c$. Then, $y^p \in gH$, hence is of the form $gu, u \in H$, so by the preceding paragraph, it can also be written as $(xv)^p$, $v \in H$.

Thus, we get $y^p = (xv)^p$ as elements of G. Since G is p-powered, this forces $y = xv$, so $c = \varphi(y) = \varphi(xv) = \varphi(x)\varphi(v) = \varphi(x) = b$, thus proving the uniqueness of b as the p^{th} root of a. $\square$

The preceding two lemmas easily give us the following.

Lemma 4.1.7. Suppose G is a group and $Z(G)$ is the center of G. Then, if G is p-powered for a prime p, both the center $Z(G)$ and the quotient group $G/Z(G)$ are p-powered. Hence, the inner automorphism group $\mathrm{Inn}(G)$, which is isomorphic to $G/Z(G)$, is also p-powered.

We are now in a position to state the main result.

Theorem 4.1.8. Suppose G is a group (not necessarily nilpotent) and $Z^n(G)$ is the n^{th} member of the upper central series of G. Suppose p is a prime such that G is p-powered. Then, $Z^n(G)$ and $G/Z^n(G)$ are also p-powered.

Proof. The fact that $G/Z^n(G)$ is p-powered follows by using mathematical induction on the preceding lemma, and noting that $G/Z^n(G)$ is obtained by iteration of the operation of factoring out by the center (starting from G). We can then use Lemma 4.1.4 to conclude that $Z^n(G)$ is also p-powered. $\square$

Note that this result also extends to members of the transfinite upper central series. For simplicity, however, we avoid dealing with transfinite central series.

We can now state the bigger theorem. Note that this establishes a partial converse to Lemma 4.1.4.

Theorem 4.1.9. Suppose G is a group and H is a normal subgroup of G that is contained in a member of the upper central series of G. Suppose p is a prime number such that both G and H are p-powered. Then, G/H is also p-powered.

Note that if G is nilpotent, then the condition that H is contained in a member of the upper central series of G is always satisfied. We will return to this implication in Theorem 4.1.18, which is deferred to a later section.

Proof. Let $Z^0(G), Z^1(G), Z^2(G), \dots$ be the upper central series of G (the trivial subgroup is $Z^0(G)$, the center is $Z^1(G)$, the second center is $Z^2(G)$, and so on). Suppose H is contained in the member $Z^n(G)$ for some n. Intersecting with H, we get a series:

$$1 = H \cap Z^0(G) \leq H \cap Z^1(G) \leq H \cap Z^2(G) \leq \dots \leq H \cap Z^n(G) = H$$

All the subgroups in this series are normal (since each is an intersection of normal subgroups) and further, for $0 \leq i \leq n-1$, $(H \cap Z^{i+1}(G))/(H \cap Z^i(G))$ is a central subgroup of $G/(H \cap Z^i(G))$.

By Theorem 4.1.8, each $Z^i(G)$ is p-powered. Hence, each $H \cap Z^i(G)$ is also p-powered.

We will now prove by induction on i that each $G/(H \cap Z^i(G))$ is p-powered. The base case is clear. The inductive step is to show that if $G/(H \cap Z^i(G))$ is p-powered, so is $G/(H \cap Z^{i+1}(G))$. For this, note that by the third isomorphism theorem:

$$G/(H \cap Z^{i+1}(G)) \cong \frac{G/(H \cap Z^i(G))}{(H \cap Z^{i+1}(G))/(H \cap Z^i(G))} \qquad (*)$$

As noted above, $(H \cap Z^{i+1}(G))/(H \cap Z^i(G))$ is a central subgroup of $G/(H \cap Z^i(G))$. As also noted above, $H \cap Z^{i+1}(G)$ is p-powered, hence p-divisible. Combining this with Lemma 4.1.3, we see that $(H \cap Z^{i+1}(G))/(H \cap Z^i(G))$ is also p-divisible. Since $(H \cap Z^{i+1}(G))/(H \cap Z^i(G))$ is a subgroup of the p-powered group $G/(H \cap Z^i(G))$, $(H \cap Z^{i+1}(G))/(H \cap Z^i(G))$ must be p-powered. Thus, we have a p-powered group $G/(H \cap Z^i(G))$ and a p-powered central subgroup $(H \cap Z^{i+1}(G))/(H \cap Z^i(G))$. By Lemma 4.1.6, the quotient group is also p-powered, so by (*), $G/(H \cap Z^{i+1}(G))$ is p-powered.

This completes the proof of the inductive step. Thus, $G/(H \cap Z^i(G))$ is p-powered for all i. In particular, setting $i = n$, we get that $G/(H \cap Z^n(G)) = G/H$ is p-powered, completing the proof. $\square$

A quick note on the "duality" between divisible and torsion-free

There is a heuristic duality between some of the results that we will be exploring in the coming two sections. Unfortunately, it is difficult to make this duality rigorous. The following quick glossary will give an idea of how the duality generally works.

- divisible $\leftrightarrow$ torsion-free
- subgroup $\leftrightarrow$ quotient group
- injective $\leftrightarrow$ surjective
- lower central series $\leftrightarrow$ upper central series
- derived subgroup $\leftrightarrow$ inner automorphism group
- abelianization $\leftrightarrow$ center

The way the duality works is that for any statement involving these concepts, we can typically consider a "dual" statement that replaces each concept by its dual, and that dual statement is usually true. Unfortunately, this duality does *not* always work. We shall see examples where the "dual" statements to true statements are false. Nonetheless, it is a useful guide for interpreting some of our easier results.

4.1.9 Basic results on divisible and torsion-free

We first begin with a basic divisibility result.

Lemma 4.1.10. Suppose G is a group and H is a central subgroup of G such that both H and G/H are p-divisible groups. Then, G is a p-divisible group as well. In other words, for any $g \in G$, there exists $x \in G$ such that $x^p = g$.

Proof. Suppose $\varphi : G \to G/H$ is the quotient map. Let $a = \varphi(g)$, so $a \in G/H$. There exists $b \in G/H$ such that $b^p = a$. Suppose $y \in G$ is such that $\varphi(y) = b$. Then, $y^{-p}g \in H$. Say, it is an element $u \in H$. Let v be an element of H such that $v^p = u$. Then, $y^{-p}g = v^p$, so $g = y^p v^p = (yv)^p$ (because H is central). So, G is p-divisible. $\square$

We now turn to a result that is related to the idea of being torsion-free.

Lemma 4.1.11. Suppose G is a group and H is a central subgroup of G. Suppose p is a prime number such that both H and the quotient group G/H have the property that the map $x \mapsto x^p$ is injective in the group. Then, G also has the property that the map $x \mapsto x^p$ is injective in G. Explicitly, if $a, b \in G$ are elements such that $a^p = b^p$, then $a = b$.

The idea is to first show that the elements are in the same coset of H (i.e., they have the same image in G/H) then take their quotient and argue that that must be the identity element. The first part will use the injectivity of the power map in G/H. The second part will use the injectivity of the power map in H.

Proof. Let $\varphi : G \to G/H$ be the quotient map.

Since $a^p = b^p$, we have $\varphi(a)^p = \varphi(b)^p$. By the injectivity of the p-power map in G/H, we conclude that $\varphi(a) = \varphi(b)$. In other words, a and b are in the same coset of H, so the element $u = ab^{-1}$ is an element of H.

Since $u = ab^{-1}$, $a = ub$. Further, $u \in H$ so u is central, so $(ub)^p = u^p b^p$. Thus, $a^p = (ub)^p = u^p b^p$. Since $a^p = b^p$, we get that $u^p b^p = b^p$. Cancel b^p from both sides to get that u^p is the identity element of G, and hence also the identity element of the subgroup H.

We now use the injectivity of the p-power map in H to conclude that u itself is the identity element of H, and hence, $a = b$. $\square$

It easily follows that:

Lemma 4.1.12. Suppose G is a group and H is a central subgroup of G. Suppose p is a prime number such that both H and the quotient group G/H are p-powered. Then, G is p-powered.

Proof. This follows from the preceding lemma and Lemma 4.1.10. $\square$

Lemma 4.1.13. Suppose G is a group (not necessarily nilpotent) and p is a prime number. Suppose i is a positive integer such that the quotient group $Z^i(G)/Z^{i-1}(G)$ is p-torsion-free. Then, the quotient group $Z^{i+1}(G)/Z^i(G)$ in G is also p-torsion-free.

Proof. Suppose x is an element of $Z^{i+1}(G)$ whose image in $Z^{i+1}(G)/Z^i(G)$ has order 1 or p. Our goal will be to show that $x \in Z^i(G)$, i.e., the order of x modulo $Z^i(G)$ must be 1 and cannot be p.

For any $y \in G$, we have $[x, y] \in Z^i(G)$, and moreover, we have:

$$[x, y]^p = [x^p, y] \pmod{Z^{i-1}(G)}$$

Since $x^p \in Z^i(G)$, the right side is the identity element mod $Z^{i-1}(G)$, hence $[x, y]$ is an element of $Z^i(G)$ whose image in $Z^i(G)/Z^{i-1}(G)$ has p^{th} power the identity. Thus, $[x, y]$ taken modulo $Z^{i-1}(G)$ has order either 1 or p. The order cannot be p because by the inductive hypothesis, $Z^i(G)/Z^{i-1}(G)$ is p-torsion-free. Hence, $[x, y] \in Z^{i-1}(G)$.

Since the above is true for *all* $y \in G$, we obtain that $[x, y] \in Z^{i-1}(G)$ for all $y \in G$. This forces $x \in Z^i(G)$, so that the order of the image of x in $Z^{i+1}(G)/Z^i(G)$ is in fact 1. Thus, the order can never be p, showing that $Z^{i+1}(G)/Z^i(G)$ is p-torsion-free. $\square$

Note that the analogous result breaks down for the lower central series. Specifically, the problem with the lower central series is that the subgroups there are too small and the quotients too big, and something being central modulo a quotient does not guarantee its containment in the adjacent member.

[29] gives a somewhat different proof (Lemma 3.16) that uses the lower central series but "augments" it with the element of interest, thus overcoming the problem of the lower central series being too small.

4.1.10 Definition equivalence for torsion-free nilpotent groups with important corollaries

Theorem 4.1.14. The following are equivalent for a nilpotent group G and a prime number p.

1. The powering map $x \mapsto x^p$ is injective in G.
2. G is p-torsion-free.
3. The center $Z(G)$ is p-torsion-free.
4. Each of the successive quotients $Z^{i+1}(G)/Z^i(G)$ of the upper central series of G is a p-torsion-free group.
5. In any quotient of the form $Z^i(G)/Z^j(G)$, the powering map $x \mapsto x^p$ is injective.

Moreover, the implication (1) to (2) to (3) to (4) to (5) holds in all groups. The only implication that relies on G being nilpotent is the implication from (5) to (1).

Proof. (1) implies (2): This is direct from the definition.

(2) implies (3): This is immediate, since $Z(G)$ is a subgroup of G.

(3) implies (4): This follows from Lemma 4.1.13 and the principle of mathematical induction.

(4) implies (5): This relies on Lemma 4.1.11, the principle of mathematical induction, and the observation that in the base case (for abelian groups) being p-torsion-free is obviously equivalent to the p-power map being injective.

(5) implies (1): If G has class c, set $i = c$, $j = 0$. Note that this is the only step where we use that G is nilpotent. $\square$

An easy corollary is as follows:

Lemma 4.1.15. If G is a nilpotent group and p is a prime number, then the following are equivalent:

1. G is p-divisible and p-torsion-free.

2. G is p-powered.

Proof. This is immediate, once we use the preceding theorem (Theorem 4.1.14) to replace p-torsion-free by "the p-power map is injective." $\square$

Lemma 4.1.16. If G is a group and H is a normal subgroup such that both G and H are p-powered, then G/H is p-torsion-free.

Proof. Let $\varphi : G \to G/H$ be the quotient map and let $a \in G/H$ be such that a^p is the identity element of G/H. Suppose $g \in G$ is such that $\varphi(g) = a$. Then, $(\varphi(g))^p = \varphi(g^p)$ is the identity element of G/H, so $g^p \in H$. Let $h = g^p$. Since H is p-powered, there exists an element $x \in H$ such that $x^p = h$. Thus, $x^p = g^p$. since G is also p-powered, this forces $x = g$. Thus, $g \in H$, so $\varphi(g) = a$ is the identity element of G/H. Thus, there is no element of order p in G/H, as desired. $\square$

Theorem 4.1.17. Suppose G is a group and H is a normal subgroup of G such that the quotient group G/H is nilpotent. Then, if p is a prime such that both G and H are p-powered, the quotient group G/H is also p-powered.

Proof. Clearly, G/H is p-divisible by Lemma 4.1.3. It is also p-torsion-free because G and H are both p-powered and by the preceding lemma (Lemma 4.1.16).

Thus, by the lemma before last (Lemma 4.1.15), G/H is p-powered. □

We can now state a fundamental result about normal subgroups of nilpotent groups with *two* different proofs.

Theorem 4.1.18. Suppose G is a nilpotent group and H is a normal subgroup of G. Then, if p is a prime number such that both G and H are p-powered, then the quotient group G/H is also p-powered.

Proof. First proof alternative: Use Theorem 4.1.9, noting that since G is nilpotent, H must lie in an upper central series member of G, namely G itself.

Second proof alternative: Use Theorem 4.1.17, noting that since G is nilpotent, so is G/H. □

4.1.11 Definition equivalence for divisible nilpotent groups with important corollaries

This result is dual to Theorem 4.1.14, the chief result of the preceding section.

Theorem 4.1.19. The following are equivalent for a nilpotent group G and a prime number p.

1. G is p-divisible.
2. The abelianization of G is p-divisible.
3. For every positive integer i, the quotient group $\gamma_i(G)/\gamma_{i+1}(G)$ is p-divisible.
4. For all pairs of positive integers $i < j$, the quotient group $\gamma_i(G)/\gamma_j(G)$ is p-divisible.

Moreover, the implications (1) to (2) to (3) to (4) hold for *all* groups. It is only the implication from (4) to (1) that uses that the group is nilpotent.

Proof. (1) implies (2): This follows from Lemma 4.1.3. Note that this step does not use G being nilpotent.

(2) implies (3): Note that each $\gamma_i(G)/\gamma_{i+1}(G)$ is p-divisible on account of being a homomorphic image of a tensor power of the abelianization of G. This again does not use G nilpotent.

(3) implies (4): We do mathematical induction using Lemma 4.1.10. This step again does not use that G is nilpotent.

(4) implies (1): plug in $i = 1$, $j = c + 1$ where c is the nilpotency class of G. Note that this is the only step where we use that G is nilpotent. □

Theorem 4.1.20. Suppose G is a nilpotent group that is powered over a prime p. Then:

1. All members of the lower central series of G are p-powered, i.e., $\gamma_i(G)$ is p-powered for all p.

2. All quotients between members of the lower central series of G are p-powered, i.e., $\gamma_i(G)/\gamma_j(G)$ is p-powered for all $i < j$. In particular, the abelianization of G is p-powered.

Proof. Proof of (1): Since G is p-powered, it is p-divisible. Hence, by the preceding theorem (Theorem 4.1.19), all quotients $\gamma_i(G)/\gamma_j(G)$ are p-divisible. Let c be the nilpotency class of G. Setting $j = c + 1$, we get that all the lower central series members $\gamma_i(G)$ are p-divisible. But since G is *p-powered* (i.e., uniqueness of roots), this forces all of these subgroups to also be p-powered.

Proof of (2): Note that since G is nilpotent, so are $\gamma_i(G)$ and $\gamma_j(G)$ for any $i < j$. Further, $\gamma_j(G)$ is characteristic in G, hence normal in G, hence normal in $\gamma_i(G)$. Thus, the hypotheses of Theorem 4.1.18 apply, and we get the conclusion that the quotient group $\gamma_i(G)/\gamma_j(G)$ is p-powered. $\square$

4.1.12 Divisibility and the upper central series

We now mention and prove a result about the upper central series whose "dual" (in the heuristic sense) fails to hold.

Theorem 4.1.21. Suppose G is a nilpotent group and p is a prime number such that G is p-divisible. Then, all members of the upper central series of G are p-divisible.

The proof is somewhat unusual in the following sense: it proceeds using mathematical induction starting from the *largest* member of the upper central series and going down. Usually, when we use the upper central series for induction, we move upward. This is one reason why the proof is difficult to discover, even though it is not hard to explain.

Proof. Suppose G has nilpotency class $c \geq 2$ (note that if $c = 1$ there is nothing to prove).

Consider the c-fold left-normed Lie bracket map of the form:

$$T : (x_1, x_2, \dots, x_c) \mapsto [\dots[[x_1, x_2], x_3], \dots, x_c]$$

By Lemma A.3.2 in the Appendix, this map is a homomorphism in each coordinate holding the other coordinates fixed. Note that this fact is very specific to the class being c. It fails for higher class. Moreover, the set of values for x_1 for which the output is always the identity is precisely the subgroup $Z^{c-1}(G)$.

Now, suppose $g \in Z^{c-1}(G)$. Since G is p-divisible, there exists $x \in G$ such that $x^p = g$. The goal is to show that there exists such a value of x in $Z^{c-1}(G)$ satisfying $x^p = g$. In fact, we will do better. We will show that any $x \in G$ satisfying $x^p = g$ actually lies inside $Z^{c-1}(G)$. In other words, we want to show that $T(x, x_2, \dots, x_c)$ is the identity element of

G for all $x_2, x_3, \ldots, x_c \in G$.

Fix the values of $x_2, x_3, \ldots, x_c$ temporarily. Let u be an element of G such that $u^p = x_c$. Then, we know that:

$$T(g, x_2, \ldots, x_{c-1}, u) = T(x^p, x_2, \ldots, x_{c-1}, u) = T(x, x_2, \ldots, x_{c-1}, u)^p$$

Similarly:

$$T(x, x_2, \ldots, x_{c-1}, x_c) = T(x, x_2, \ldots, x_{c-1}, u^p) = T(x, x_2, \ldots, x_{c-1}, u)^p$$

The right sides of both equations are the same, so we get:

$$T(g, x_2, \ldots, x_{c-1}, u) = T(x, x_2, \ldots, x_{c-1}, x_c)$$

Since $g \in Z^{c-1}(G)$, the left side is the identity element, hence so is the right side. Since $x_2, \ldots, x_{c-1}, x_c$ are arbitrary, this shows that $x \in Z^{c-1}(G)$.

The result can now be extended further down the upper central series. The key trick in executing the extension is to replace the original c-fold commutator with smaller fold commutators, but now restrict the first input to being within the member one higher. In general when inducting down from $Z^i(G)$ to $Z^{i-1}(G)$, we consider a left-normed commutator of length i, restricting the first input to be within $Z^i(G)$ and allowing all other inputs to vary freely within G. We then use the same logic. Note that this logic works in each stage as long as $i \geq 2$, and hence we can do our induction all the way down to the center. We cannot use the induction to get down to the trivial subgroup, but we know that the trivial subgroup is p-divisible for all primes p, so this is unnecessary. $\square$

As we shall see in Example (4) in the next subsection, the naive dual statement for torsion-free and quotient groups with the lower central series fails to hold.

4.1.13 Collection of interesting counterexamples

For the examples below, we denote by $UT(3,R)$ the group whose underlying set is the set of unitriangular matrices of degree three over R under matrix multiplication where R is any unital ring. In other words, $UT(3,R)$ is the set:

$$\left\{ \begin{pmatrix} 1 & a_{12} & a_{13} \\ 0 & 1 & a_{23} \\ 0 & 0 & 1 \end{pmatrix} \mid a_{12}, a_{13}, a_{23} \in R \right\}$$

with the usual matrix multiplication.

1. *A group may be p-powered and have a subgroup that is not p-powered; in fact, we can choose an abelian example*: The subgroup $\mathbb{Z}$ inside $\mathbb{Q}$ is an example of a situation where the whole group is powered over every prime but the subgroup is not powered over any prime. Note that it is the "divisible" aspect, not the "torsion-free" aspect, that fails. The corresponding quotient group ($\mathbb{Q}/\mathbb{Z}$) is also not p-powered for any prime p. For the quotient, it is the "torsion-free" aspect that fails.

   We can tweak this example a bit to construct, for any pair of prime sets $\pi_2 \subseteq \pi_1$, an abelian group that is powered over π_1 and a subgroup that is powered *only* over the primes inside π_2.

2. *A characteristic subgroup of a p-powered group need not be p-powered*: It is possible to have a characteristic subgroup of a group that is not powered over some primes that the whole group is powered over. Recall that $GA^+(1,\mathbb{R}) = \mathbb{R} \rtimes (\mathbb{R}^*)^+$ is rationally powered. The subgroup $\mathbb{R} \rtimes (\mathbb{Q}^*)^+$ is characteristic, but is not powered over any prime.

   We can tweak this example a bit to construct, for any pair of prime sets $\pi_2 \subseteq \pi_1$, a group that is powered *precisely* over the primes in π_1 and a characteristic subgroup that is powered *precisely* over the primes inside π_2.

3. It is possible to have a nilpotent group G (in fact, we can choose G to have class two)

such that the abelianization of G is rationally powered (hence torsion-free), but G itself is not torsion-free: We can take G to be the quotient of $UT(3,\mathbb{Q})$ by a subgroup $\mathbb{Z}$ inside its central $\mathbb{Q}$. The abelianization of G is $\mathbb{Q} \times \mathbb{Q}$, while the center is $\mathbb{Q}/\mathbb{Z}$. Thus, the abelianization of G is rationally powered, whereas G has p-torsion for all primes p.

Explicitly, G is given as the set of matrices:

$$\left\{ \begin{pmatrix} 1 & a_{12} & \overline{a_{13}} \\ 0 & 1 & a_{23} \\ 0 & 0 & 1 \end{pmatrix} \mid a_{12}, a_{23} \in \mathbb{Q}, \overline{a_{13}} \in \mathbb{Q}/\mathbb{Z} \right\}$$

with the matrix multiplication defined as:

$$\begin{pmatrix} 1 & a_{12} & \overline{a_{13}} \\ 0 & 1 & a_{23} \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b_{12} & \overline{b_{13}} \\ 0 & 1 & b_{23} \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_{12}+b_{12} & \overline{a_{12}b_{23}} + \overline{a_{13}} + \overline{b_{13}} \\ 0 & 1 & a_{23}+b_{23} \\ 0 & 0 & 1 \end{pmatrix}$$

4. It is possible to have a nilpotent group G (in fact, we can choose G to have class two) such that G is torsion-free but the abelianization of G is not torsion-free: Let G be a central product of $UT(3,\mathbb{Z})$ by $\mathbb{Q}$ identifying a copy of $\mathbb{Z}$ inside $\mathbb{Q}$ with the center of $UT(3,\mathbb{Z})$. In this case, the abelianization is isomorphic to $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$, which has torsion for all primes.

   Explicitly, G is the following set with matrix multiplication:

$$\left\{ \begin{pmatrix} 1 & a_{12} & a_{13} \\ 0 & 1 & a_{23} \\ 0 & 0 & 1 \end{pmatrix} \mid a_{12}, a_{23} \in \mathbb{Z}, a_{13} \in \mathbb{Q} \right\}$$

   This result is the expected dual to Theorem 4.1.21 that fails to hold. The expected dual to that result should say that all quotients of a p-torsion-free nilpotent group by its lower central series members are also p-torsion-free. This fails to be true in this situation.

5. *It is possible to have a non-nilpotent p-divisible group whose center is not p-divisible*: The simplest example is $S^3 \cong SU(2, \mathbb{C})$, which can also be described as the group of unit quaternions. The center is $\{-1, 1\}$. The group S^3 as a whole is p-divisible for all primes p, and in particular, every element in the group has a square root in the group. However, the center of the group is not 2-divisible, because the element -1 has no square root in the center.

   Note that this example is an opposite of sorts to potential generalizations of Lemma 4.1.5 (which rules out similar examples for the p-powered case) and Theorem 4.1.21 (which rules out similar examples where the whole group is nilpotent).

6. *It is possible to have a non-nilpotent p-divisible group whose derived subgroup is not p-divisible*: Consider the group $GL(p, \mathbb{C})$. This is p-divisible (and in fact, also divisible by all other primes). The derived subgroup $SL(p, \mathbb{C})$ is not p-divisible (however, it is divisible by other primes). Specifically, the element in $SL(p, \mathbb{C})$ that is a single Jordan block with eigenvalue a primitive p^{th} root of unity has no p^{th} root within $SL(p, \mathbb{C})$, even though it does have p^{th} roots in $GL(p, \mathbb{C})$.

   More generally, for a finite set π of primes, we can take n as the product of all primes in π. Then $G = GL(n, \mathbb{C})$ is divisible by all primes, but $G' = SL(n, \mathbb{C})$ is divisible only by those primes that are not in π, and is not divisible by any of the primes in π.

4.1.14 Extra: a two-out-of-three theorem

We are now ready to prove or "two-out-of-three" result for powering. We begin with a lemma, which is structurally quite similar to, and in some ways a generalization of, Theorem 4.1.19.

Lemma 4.1.22. Suppose G is a nilpotent group, p is a prime number, and H is a p-divisible normal subgroup of G. Then, consider the descending chain:

$$H \geq [H, G] \geq [[H, G], G] \geq [[[H, G], G], G] \geq \cdots \geq 1$$

Note that this chain reaches the trivial subgroup because G is nilpotent.

Then, the following are true:

1. Each of the quotient groups between successive members of this descending series is p-divisible.
2. Each of the quotient groups between members of this descending series (not necessarily successive) is p-divisible.
3. Each of the members of this descending series is p-divisible.

Proof. Proof of (1): Once we note that divisibility inherits to quotient groups (Lemma 4.1.3), the situation for each quotient is similar to the situation for the last (final) quotient, so for notational simplicity, we prove the result only for the last quotient.

Suppose the penultimate member of the series involves $c - 1$ occurrences of G and one occurrence of H. Thus, there is a c-fold iterated commutator map:

$$T : H \times G \times G \times \cdots \times G \to G$$

whose image generates this subgroup. This map is multilinear, i.e., it is a homomorphism in each coordinate. We can therefore use the p-divisibility of H to obtain that the image set is p-divisible, and hence, so is the abelian subgroup generated by it.

Proof of (2): This follows from (1), Lemma 4.1.10, and mathematical induction.

Proof of (3): This is a special case of (2) where the lower end of the quotient is taken to be the trivial subgroup. $\square$

This is sufficient for the following theorem:

Theorem 4.1.23. Suppose G is a nilpotent group, H is a normal subgroup, and p is a prime number such that both H and G/H are p-divisible. Then, G is also p-divisible.

Proof. Consider the series:

$$H \geq [H, G] \geq [[H, G], G] \geq \cdots \geq 1$$

For simplicity, define $H_1 = H$ and $H_{i+1} = [H_i, G]$. Then the series is:

$$H_1 \geq H_2 \geq H_3 \geq \cdots \geq 1$$

By Lemma 4.1.22 and the fact that H is p-divisible, all the successive quotients H_i/H_{i+1} are also p-divisible. Further, by the nature of the series, each H_i is normal in G and each quotient H_i/H_{i+1} is central in the quotient G/H_{i+1}.

We can now prove, by upward induction on i, that each quotient G/H_i is p-divisible. The base case $i = 1$ follows from the stipulation that G/H is p-divisible. For the inductive step, suppose G/H_i is p-divisible and we need to show that G/H_{i+1} is p-divisible. We already have that H_i/H_{i+1} is p-divisible and central in G/H_{i+1}, and $G/H_i \cong (G/H_{i+1})/(H_1/H_{i+1})$ by the third isomorphism theorem, so $(G/H_{i+1})/(H_1/H_{i+1})$ is also p-divisible. Thus, by Lemma 4.1.10, G/H_{i+1} is also p-divisible. This completes the inductive step.

For large enough i, H_i is the trivial subgroup of G, so this indeed gives us that G is p-divisible. $\square$

The next lemma tries to do something similar for the torsion-free setting. It mimics and generalizes Theorem 4.1.14.

Lemma 4.1.24. Suppose G is a nilpotent group, p is a prime number, and H is a p-

torsion-free normal subgroup of G. There exists some natural number n such that $H \leq Z^n(G)$. Consider the ascending chain of subgroups in H:

$$1 \leq H \cap Z(G) \leq H \cap Z^2(G) \leq \cdots \leq H \cap Z^n(G) = H$$

We have the following:

1. Each of the quotient groups between successive members of this ascending series is p-torsion-free.

2. Each of the quotient groups between members of this ascending series (not necessarily successive) is p-torsion-free.

3. Each of the members of this ascending series is p-torsion-free.

Proof. Proof of (1): We prove this for each quotient $(H \cap Z^i(G))/(H \cap Z^{i-1}(G))$ by induction on i. The base case for induction, namely, the statement that $H \cap Z(G)$ is p-torsion-free, follows from the fact that H is p-torsion-free. The proof method for the inductive step is similar to the proof method used for Lemma 4.1.13.

Explicitly, we want to show that if $(H \cap Z^i(G))/(H \cap Z^{i-1}(G))$ is p-torsion-free, then $(H \cap Z^{i+1}(G))/(H \cap Z^i(G))$ is p-torsion-free. We do this as follows.

Suppose x is an element of $H \cap Z^{i+1}(G)$ whose image in $(H \cap Z^{i+1}(G))/(H \cap Z^i(G))$ has order 1 or p. Our goal will be to show that $x \in H \cap Z^i(G)$, i.e., the order of the image of x must be 1 and cannot be p.

For any $y \in G$, we have $[x, y] \in H \cap Z^i(G)$, and moreover, we have:

$$[x, y]^p = [x^p, y] \pmod{H \cap Z^{i-1}(G)}$$

Since $x^p \in H \cap Z^i(G)$, the right side is the identity element mod $H \cap Z^{i-1}(G)$, hence $[x, y]$ is an element of $H \cap Z^i(G)$ whose image in $(H \cap Z^i(G))/(H \cap Z^{i-1}(G))$ has p^{th} power the identity. Thus, $[x, y]$ taken modulo $H \cap Z^{i-1}(G)$ has order either 1 or p. The order cannot be p because by the inductive hypothesis, $(H \cap Z^i(G))/(H \cap Z^{i-1}(G))$ is p-torsion-free. Hence, $[x, y] \in H \cap Z^{i-1}(G)$.

Since the above is true for *all* $y \in G$, we obtain that $[x, y] \in H \cap Z^{i-1}(G)$ and hence $[x, y] \in Z^{i-1}(G)$ for all $y \in G$. This forces $x \in Z^i(G)$ and hence $x \in H \cap Z^i(G)$, so that the order of the image of x in $(H \cap Z^{i+1}(G))/(H \cap Z^i(G))$ is in fact 1. Thus, the order can never be p, showing that $(H \cap Z^{i+1}(G))/(H \cap Z^i(G))$ is p-torsion-free.

Proof of (2): This follows from (1) and Lemma 4.1.11 (note that we have already established, in Theorem 4.1.14, that being p-torsion-free is equivalent to the p power map being injective).

Proof of (3): This is already obvious. □

We can now state the theorem:

Theorem 4.1.25. Suppose G is a nilpotent group, H is a normal subgroup, and p is a prime number such that both H and G/H are p-torsion-free. Then, G is also p-torsion-free.

Proof. By the preceding lemma, we have the ascending chain of subgroups in H:

$$1 \le H \cap Z(G) \le H \cap Z^2(G) \le \cdots \le H \cap Z^n(G) = H$$

and further, we have that each successive quotient between members of this ascending chain is p-torsion-free. We can now induct downward on i (going down from n to 0) to show that $G/(H \cap Z^i(G))$ is p-torsion-free. The base case, $i = n$, is given to us. To induct down from $G/(H \cap Z^i(G))$ to $G/(H \cap Z^{i-1}(G))$, we use Lemma 4.1.11, along with the observation that the abelian group $(H \cap Z^i(G))/(H \cap Z^{i-1}(G))$ is p-torsion-free if and only if the p-powering map in the group is injective. □

Combining the theorems for divisibility and torsion-free, we have that:

Theorem 4.1.26. Suppose G is a nilpotent group, H is a normal subgroup, and p is a prime number such that both H and G/H are p-powered. Then, G is also p-powered.

Proof. This is a direct combination of Theorems 4.1.23 and 4.1.25. $\square$

We can now state the two-out-of-three theorem.

Theorem 4.1.27. Suppose G is a nilpotent group, H is a normal subgroup, and p is a prime number. The following are true:

1. If any two of the three groups G, H, and G/H is p-powered, so is the third.
2. For p-divisibility, if G is p-divisible, so is G/H, and if H and G/H are p-divisible, so is G.
3. For p-torsion-free, if G is p-torsion-free, so is H, and if H and G/H are p-torsion-free, so is G.

Proof. Proof of (1):

- G and H to G/H: This follows from Theorem 4.1.18.
- G and G/H to H: This follows from Lemma 4.1.4.
- H and G/H to G: This follows from Theorem 4.1.26.

Proof of (2):

- G to G/H: This follows from Lemma 4.1.3.
- H and G/H to G: This follows from Theorem 4.1.23.

Proof of (3):

- G to H: This is obvious.

- H and G/H to G: This follows from Theorem 4.1.25.

$\square$

4.1.15 Is every characteristic subgroup invariant under powering?

The following is a conjecture.

Conjecture 4.1.28. Suppose G is a nilpotent group and H is a characteristic subgroup of G. Suppose π is a set of primes such that G is π-powered. Then, H is also π-powered.

The conjecture appears to be open.[2]

The corresponding result is false for solvable groups: for instance, the group $G = GA^{+}(1,\mathbb{R}) = \mathbb{R} \rtimes (\mathbb{R}^*)^+$ is powered over all primes, and the subgroup $H = \mathbb{R} \rtimes (\mathbb{Q}^*)^+$ is characteristic, but H is not powered over any prime.

The corresponding result is true for *abelian* groups, because the map $x \mapsto x^{1/p}$ (which in additive notation becomes $x \mapsto (1/p)x$) is an automorphism of G for every $p \in \pi$.

Apart from abelian groups, there are some important types of nilpotent groups for which the conjecture can be demonstrated to be true. For instance:

- The conjecture is trivially true for all finite nilpotent groups, because *every* subgroup of a π-powered finite group is π-powered by Lemma 4.1.2. Similarly, it is also true for periodic groups, i.e., groups in which every element has finite order.

- The conjecture is true for groups for which we can find an automorphism that behaves like a power map on the successive quotient groups for some central series of the group. For instance, suppose $\pi = \{p\}$ and G is a p-powered nilpotent group of nilpotency

2. See http://mathoverflow.net/questions/124295/characteristic-subgroup-of-nilpotent-group-that-is-not-invariant-under-powering

class two. The conjecture holds for G if we can find a central subgroup H of G and an automorphism σ of G such that σ induces the automorphism $x \mapsto x^{p^k}$ on G/H and σ behaves like $x \mapsto x^{p^{2k}}$ on H.

In Section 5.2.3, we will discuss some implications of this conjecture being true when restricted to the groups that participate in the Baer correspondence.

4.2 Lie rings powered over sets of primes: key results

This section covers Lie ring analogues of the material covered for groups in the preceding section (Section 4.1). The majority of results carry over, but many of the proofs are notably similar. We use results of the preceding section.

4.2.1 Definitions

We can define notions of powered, divisible, and torsion-free for Lie rings similar to the definitions for groups. In fact, we do not need to redefine these terms: we simply define them by invoking the corresponding definition for the additive group of the Lie ring. Thus, for instance, a Lie ring is called p-powered for a prime p if and only if the additive group of the Lie ring is p-powered. Similarly, for a prime set π, a Lie ring is called π-powered if and only if the additive group of the Lie ring is π-powered.

π-powered Lie rings are the same as $\mathbb{Z}[\pi^{-1}]$-Lie algebras. For a more detailed discussion of Lie algebras over rings other than $\mathbb{Z}$, see the Appendix, Section A.1.4.

We will now go over results analogous to the results we established about groups in the preceding section. The proofs in most cases are either the same or much simpler. For instance, we note the following two-out-of-three result in the Lie ring context which is not true in general for groups and took a lot of effort to establish for nilpotent groups:

Lemma 4.2.1. Suppose L is a Lie ring and I is an ideal in L. Suppose p is a prime number. Then, if any two of L, I, and L/I are p-powered, so is the third.

Proof. This is straightforward just from looking at the additive group structure and invoking the corresponding result for abelian groups, where it is obvious:

- L and I to L/I: This follows from Lemma 4.1.6, applied to the additive group of L and the additive subgroup I. Note that since L is abelian, the subgroup I is central in the additive group sense, regardless of whether I is central as an ideal in L.
- L and L/I to I: This follows from Lemma 4.1.4 applied the additive group of L and the additive subgroup I.
- I and L/I to L: This can be deduced from Lemma 4.1.12 applied to the additive group of L and the additive subgroup I. Note that since L is abelian, the subgroup I is central in the additive group sense, regardless of whether I is central as an ideal in L.

□

Another basic fact is this.

Lemma 4.2.2. The following are equivalent for a Lie ring L and a prime number p:

1. The multiplication by p map is injective from L to itself.
2. The additive group of L is p-torsion-free.

Proof. This follows from the additive group of L being an abelian group. □

4.2.2 Results for the center

Lemma 4.2.3. Suppose L is a Lie ring that is powered over a prime p and $Z(L)$ is the center of L. Then, $Z(L)$ is also powered over p. In other words, for any $g \in Z(L)$, there exists a unique $x \in Z(L)$ such that $px = g$.

Proof. Since L is p-powered, we know there exists unique $x \in L$ such that $px = g$. It therefore suffices to show that this unique x is in $Z(L)$. In other words, we need to show that for any $y \in L$, $[x, y] = 0$.

Note that $[g, y] = 0$ on account of g being in the center of L, so:

$$0 = [g, y] = [px, y] = p[x, y]$$

Since L is powered over p, it is in particular p-torsion-free. Thus, we must have $[x, y] = 0$, completing the proof. $\square$

Note that the analogous results to Lemma 4.1.6 and Theorem 4.1.9 are trivially obvious due to the two-out-of-three lemma noted above. Thus, we can jump straight to:

Theorem 4.2.4. Suppose L is a Lie ring (not necessarily nilpotent) and $Z^n(L)$ is the n^{th} member of the upper central series of L. Suppose p is a prime such that L is p-powered. Then, $Z^n(L)$ and $L/Z^n(L)$ are also p-powered.

Proof. Lemma 4.2.3 and the two-out-of-three lemma give that $L/Z(L)$ is p-powered. Iterating inductively, we get that $L/Z^n(L)$ is p-powered. Again using the two-out-of-three lemma, we get that $Z^n(L)$ is p-powered. $\square$

We now prove the Lie ring analogue to Lemma 4.1.13.

Lemma 4.2.5. Suppose L is a Lie ring (not necessarily nilpotent) and p is a prime number. Suppose i is a natural number. Then, if the quotient ring $Z^i(L)/Z^{i-1}(L)$ is p-torsion-free, so is the quotient ring $Z^{i+1}(L)/Z^i(L)$.

Proof. Suppose x is an element of $Z^{i+1}(L)$ whose image in $Z^{i+1}(L)/Z^i(L)$ has order 1 or p. Our goal will be to show that x must be in $Z^i(L)$, i.e., its image must be the zero element of $Z^{i+1}(L)/Z^i(L)$.

For any $y \in L$, we have $[x, y] \in Z^i(L)$, and moreover, we have:

$$p[x, y] = [px, y] \pmod{Z^{i-1}(L)}$$

Since $px \in Z^i(L)$, the right side is the zero element mod $Z^{i-1}(L)$, hence $[x, y]$ is an element of $Z^i(L)$ whose image in $Z^i(L)/Z^{i-1}(L)$, when multiplied by p, gives 0. Thus, $[x, y]$ taken modulo $Z^{i-1}(L)$ has order either 1 or p. The order cannot be p because by the inductive hypothesis, $Z^i(L)/Z^{i-1}(L)$ is p-torsion-free. Hence, $[x, y] \in Z^{i-1}(L)$.

Since the above is true for *all* $y \in L$, we obtain that $[x, y] \in Z^{i-1}(L)$ for all $y \in L$. This forces $x \in Z^i(L)$, so that the order of the image of x in $Z^{i+1}(L)/Z^i(L)$ is in fact 1. Thus, the order can never be p, showing that $Z^{i+1}(L)/Z^i(L)$ is p-torsion-free. □

4.2.3 Definition equivalence for torsion-free nilpotent Lie rings

Theorem 4.2.6. The following are equivalent for a nilpotent Lie ring L and a prime number p.

1. L is p-torsion-free.
2. The center $Z(L)$ is p-torsion-free.
3. Each of the successive quotients $Z^{i+1}(L)/Z^i(L)$ of the upper central series of L is a p-torsion-free Lie ring.

4. Each of the quotients $Z^i(L)/Z^j(L)$ is a p-torsion-free Lie ring.

Moreover, the implication (1) to (2) to (3) to (4) holds in all Lie rings. The only implication that relies on L being nilpotent is the implication from (4) to (1).

Proof. (1) implies (2): This is immediate, since $Z(L)$ is a subring, and hence additive subgroup, of L.

(2) implies (3): This follows from Lemma 4.2.5 and the principle of mathematical induction.

(3) implies (4): This relies on Lemma 4.1.11 and mathematical induction.

(4) implies (1): This is follows by setting $i = c, j = 0$. □

4.2.4 Definition equivalences for divisible nilpotent Lie rings

Theorem 4.2.7. The following are equivalent for a nilpotent Lie ring L and a prime number p.

1. L is p-divisible.
2. The abelianization of L is p-divisible.
3. For every positive integer i, the quotient group $\gamma_i(L)/\gamma_{i+1}(L)$ is p-divisible.
4. For all pairs of positive integers $i < j$, the quotient group $\gamma_i(L)/\gamma_j(L)$ is p-divisible.

Note that the implications (1) to (2) to (3) to (4) hold for *all* Lie rings. It is only the implication from (4) to (1) that uses that the Lie ring is nilpotent.

Proof. (1) implies (2): This follows from Lemma 4.1.3 applied to the additive group of L. Note that this step does not use L being nilpotent.

(2) implies (3): Note that each $\gamma_i(L)/\gamma_{i+1}(L)$ is p-divisible on account of being a homomorphic image of a tensor power of the abelianization of L (as an additive group). This again does not use L being nilpotent.

(3) implies (4): We do mathematical induction using Lemma 4.1.10. This step again does not use that L is nilpotent.

(4) implies (1): Plug in $i = 1$, $j = c + 1$ where c is the nilpotency class of L. Note that this is the only step where we use that L is nilpotent. $\square$

Note that the following is true for *any* Lie ring (not necessarily nilpotent). The corresponding statement for groups does not hold in the general case (see Section 4.1.13, Example 6).

Lemma 4.2.8. Suppose L is a Lie ring (not necessarily nilpotent) that is p-divisible for some prime number p. Then, the derived subring of L and all the members of the lower central series of L are also p-divisible. Moreover, if L is p-powered, then the derived subring of L and all the members of the lower central series of L are also p-powered.

Proof. Every Lie element of the form $[x, y]$ can be divided by p to give a Lie element. Explicitly, if $pu = x$, then $p[u, y] = [x, y]$. Since the derived subring is generated additively by Lie elements, every element of the derived subring can be divided by p within the derived subring.

A similar logic applies to other members of the lower central series.

The statement for the p-powered case also follows. $\square$

4.2.5 Divisibility and the upper central series

The result for the upper central series for a Lie ring has a similar formulation and a similar proof to the corresponding result for a group.

Theorem 4.2.9. Suppose L is a nilpotent Lie ring and p is a prime number such that L is p-divisible. Then, all members of the upper central series of L are p-divisible.

The proof is analogous to that for groups.

Proof. Suppose L has nilpotency class $c \geq 2$ (note that if $c = 1$ there is nothing to prove).

Consider the c-fold left-normed commutator map of the form:

$$T : (x_1, x_2, \ldots, x_c) \mapsto [\ldots[[x_1, x_2], x_3], \ldots, x_c]$$

Viewed as a map of the additive groups, this map is a homomorphism in each coordinate when one fixes the values of the other coordinates. Moreover, the set of values for x_1 for which the output is always the zero element is precisely the subring $Z^{c-1}(L)$.

Now, suppose $g \in Z^{c-1}(L)$. Since L is p-divisible, there exists $x \in L$ such that $px = g$. The goal is to show that there exists a value of x in $Z^{c-1}(L)$ satisfying $px = g$. In fact, we will do better. We will show that any $x \in L$ satisfying $px = g$ actually lies inside $Z^{c-1}(L)$. In other words, we want to show that $T(x, x_2, \ldots, x_c)$ is the zero element of L for all $x_2, x_3, \ldots, x_c \in L$.

Fix the values of $x_2, x_3, \ldots, x_c$ temporarily. Let u be an element of L such that $pu = x_c$. Then, we know that:

$$(g, x_2, \ldots, x_{c-1}, u) = T(px, x_2, \ldots, x_{c-1}, u) = pT(x, x_2, \ldots, x_{c-1}, u)$$

Similarly:

$$T(x, x_2, \ldots, x_{c-1}, x_c) = T(x, x_2, \ldots, x_{c-1}, pu) = pT(x, x_2, \ldots, x_{c-1}, u)$$

The right sides of both equations are the same, so we get:

$$T(g, x_2, \dots, x_{c-1}, u) = T(x, x_2, \dots, x_{c-1}, x_c)$$

Since $g \in Z^{c-1}(L)$, the left side is the zero element, hence so is the right side. Since $x_2, \dots, x_{c-1}, x_c$ are arbitrary, this shows that $x \in Z^{c-1}(L)$.

The result can now be extended further down the upper central series. The key trick in executing the extension is to replace the original c-fold commutator with smaller fold commutators, but now restrict the first input to being within the member one higher. In general when inducting down from $Z^i(L)$ to $Z^{i-1}(L)$, we consider a left-normed commutator of length i, restricting the first input to be within $Z^i(L)$ and allowing all other inputs to vary freely within L. We then use the same logic. Note that this logic works in each stage as long as $i \geq 2$, and hence we can do our induction all the way down to the center. We cannot use the induction to get down to the zero subring, but we know that the zero subring is p-divisible for all primes p, so this is unnecessary. $\square$

4.2.6 Counterexamples for Lie rings

For the examples below, we denote by $NT(3, R)$ the set of niltriangular matrices of degree three over R under matrix multiplication where R is any unital ring. In other words, $NT(3, R)$ is the set:

$$\left\{ \begin{pmatrix} 0 & a_{12} & a_{13} \\ 0 & 0 & a_{23} \\ 0 & 0 & 0 \end{pmatrix} \mid a_{12}, a_{13}, a_{23} \in R \right\}$$

with the usual matrix multiplication. To make it into a Lie ring, we define the Lie bracket as the additive commutator corresponding to the matrix multiplication. Explicitly, we define the Lie bracket of matrices x and y as $[x, y] = xy - yx$ where xy and yx are the products with respect to the usual matrix multiplication.

1. *A Lie ring may be p-powered and have a subring that is not p-powered; in fact, we can choose an abelian example*: The subgroup $\mathbb{Z}$ inside $\mathbb{Q}$ is an example of a situation where the whole group is powered over every prime but the subgroup is not powered over any prime. Viewing all the group as abelian Lie rings (with the trivial bracket) we obtain the desired examples for Lie rings. Note that it is the "divisible" aspect, not the "torsion-free" aspect, that fails. The corresponding quotient group ($\mathbb{Q}/\mathbb{Z}$) is also not p-powered for any prime p. For the quotient, it is the "torsion-free" aspect that fails.

   We can tweak this example a bit to construct, for any pair of prime sets $\pi_2 \subseteq \pi_1$, an abelian group (hence an abelian Lie ring) that is powered over π_1 and a subgroup (hence, subring) that is powered *only* over the primes inside π_2.

2. *A characteristic subring of a p-powered Lie ring need not be p-powered*: Consider the Lie ring $L = \mathbb{Q} \rtimes \mathbb{Q}$ where the action of the acting $\mathbb{Q}$ on the other $\mathbb{Q}$ is by rational number multiplication. The ring is rationally powered, i.e., it is a $\mathbb{Q}$-Lie algebra. However, the characteristic subring $\mathbb{Q} \rtimes \mathbb{Z}$ is not powered over any prime.

3. It is possible to have a nilpotent Lie ring L (in fact, we can choose L to have class two) such that the abelianization of L is rationally powered (hence torsion-free), but L itself is not torsion-free: We can take L to be the quotient of $NT(3, \mathbb{Q})$ by a subgroup $\mathbb{Z}$ inside its central $\mathbb{Q}$. The abelianization of L is $\mathbb{Q} \times \mathbb{Q}$, while the center is $\mathbb{Q}/\mathbb{Z}$. Thus, the abelianization of L is rationally powered, whereas L has p-torsion for all primes p.

   Explicitly, L is given as the set of matrices:

$$\left\{ \begin{pmatrix} 0 & a_{12} & \overline{a_{13}} \\ 0 & 0 & a_{23} \\ 0 & 0 & 0 \end{pmatrix} \mid a_{12}, a_{23} \in \mathbb{Q}, \overline{a_{13}} \in \mathbb{Q}/\mathbb{Z} \right\}$$

   with the Lie bracket defined as the bracket arising from matrix multiplication.

4. It is possible to have a nilpotent Lie ring L (in fact, we can choose L to have class two) such that L is torsion-free but the abelianization of L is not torsion-free: Let L be a central product of $NT(3,\mathbb{Z})$ by $\mathbb{Q}$ identifying a copy of $\mathbb{Z}$ inside $\mathbb{Q}$ with the center of $UT(3,\mathbb{Z})$. In this case, the abelianization is isomorphic to $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$, which has torsion for all primes.

   Explicitly, L is:

$$\left\{ \begin{pmatrix} 0 & a_{12} & a_{13} \\ 0 & 0 & a_{23} \\ 0 & 0 & 0 \end{pmatrix} \mid a_{12}, a_{23} \in \mathbb{Z}, a_{13} \in \mathbb{Q} \right\}$$

   This result is the expected dual to Theorem 4.1.21 that fails to hold. The expected dual to that result should say that all quotients of a p-torsion-free nilpotent group by its lower central series members are also p-torsion-free. This fails to be true in this situation.

4.2.7 Is every characteristic subring invariant under powering?

The following is a Lie ring analogue of Conjecture 4.1.28.

Conjecture 4.2.10. Suppose L is a nilpotent Lie ring and M is a characteristic subring of L. Suppose π is a set of primes such that L is π-powered. Then, M is also π-powered.

The corresponding result is false for solvable Lie rings. See (2) in the list of counterexamples in Section 4.2.6.

The corresponding result is true for *abelian* Lie rings, because the map $x \mapsto (1/p)x$ is an automorphism of L for every $p \in \pi$.

Apart from abelian Lie rings, there are some important types of nilpotent groups for which the conjecture can be demonstrated to be true. Remars about special cases similar to those found in Section 4.1.15 apply here.

In Section 5.2.3, we will discuss some implications of this conjecture being true when restricted to the Lie rings that participate in the Baer correspondence.

4.3 Free powered groups and powering functors

4.3.1 Construction of the free powered group

This section uses basic terminology from universal algebra. For background on the terminology, see Section A.2.4. The section also builds on Section 4.1.4, where we described how the collection of π-powered groups for a prime set π is a variety of algebras with a natural forgetful functor to the variety of groups.

For any variety of algebras, we can talk of the free algebra in that variety on any set. In particular, we can talk of the free π-powered group $F(S, \pi)$ on a set S. Working with this free group is difficult because, unlike the usual free group, it is difficult to work out a reduced form for elements of the free π-powered group. It is also obvious that the canonical map from S to $F(S, \pi)$ is injective. To see this, note that the free π-powered *abelian* group on S is the free $\mathbb{Z}[\pi^{-1}]$-module with basis indexed by S, and this is a quotient group of $F(S, \pi)$. Since the free π-powered abelian group on S has the property that the natural map from S to it is injective, the natural map from S to $F(S, \pi)$ is also injective.

An explicit construction of the free π-powered group on a set S is as follows. Start with the abstract free group $F(S)$. In each iteration, do the following:

- Adjoin p^{th} roots (for all $p \in \pi$) of all the elements so far.
- Take the free group generated by all these.
- For every pair of elements that have the same p^{th} power (for one or more $p \in \pi$), set them to be equal (i.e., factor out by the relation of their being equal).

The group constructed at each stage has a natural homomorphism to it from the previous group. The direct limit of this sequence is the desired group $F(S, \pi)$.

4.3.2 Free powered nilpotent groups

In Section 3.10, we defined the free nilpotent group of class c on a set S. We now define the π-powered analogue of that construction.

Definition (Free π-powered nilpotent group)**.** Suppose S is a set, π is a set of primes, and c is a positive integer. The *free π-powered nilpotent group* of class c on S is defined as the quotient group $F(S, \pi)/\gamma_{c+1}(F(S, \pi))$ where $F(S, \pi)$ is the free π-powered group on S. Equivalently, this group, along with the set map to it from S, is the initial object in the category of groups of nilpotency class at most c with set maps to them from S.

The functor sending a set to its free π-powered nilpotent group of class c is left adjoint to the forgetful functor from π-powered nilpotent groups of class (at most) c to sets.

4.3.3 π-powered words and word maps

Word maps (described in the Appendix, Section A.5.1) are an important tool in the study of the variety of groups and other varieties of algebras. In particular, we can define words and word maps relative to the variety of π-powered groups. We will use the jargon *π-powered word* to describe a word relative to the variety of π-powered groups. A π-powered word in n letters $g_1, g_2, \dots, g_n$ can be described using an expression that involves composing the operations of multiplication, inverses, and taking p^{th} roots for primes $p \in \pi$. Two such expressions define the same word if they give the same element in the free π-powered group $F(S, \pi)$ where $S = \{g_1, g_2, \dots, g_n\}$.

For any π-powered group G and any π-powered word w in n letters, we can define the π-powered word map on G corresponding to w. This is a map $G^n \to G$. By abuse of notation, we will denote this map by the letter w as well, i.e., for $x_1, x_2, \ldots, x_n \in G$, we denote the image of $(x_1, x_2, \ldots, x_n)$ under w by $w(x_1, x_2, \ldots, x_n)$.

For a prime set π and a positive integer c, we can also consider *π-powered class c words*. These are words with respect to the variety of π-powered groups of nilpotency class at most c. We can correspondingly considered *π-powered class c word maps*. For a π-powered class c word w in n letters and a π-powered class c group G, the word map induced by w is a set map $G^n \to G$.

4.3.4 Localization and powering functors

For a set π of primes, the π-powering functor is a functor from the category of groups to the category of π-powered groups that is left adjoint to the forgetful functor from the category of π-powered groups to the category of groups. More explicitly, for a group G, the π-powering of G is a group K along with a homomorphism $\varphi : G \to K$ such that for any homomorphism $\theta : G \to L$ from G to a π-powered group L, there is a unique homomorphism $\alpha : K \to L$ such that $\theta = \alpha \circ \varphi$.

For a prime set π, the π-*localization* functor refers to the powering functor for the set of primes *outside of* π.

We begin with a lemma.

Lemma 4.3.1. Suppose G is a group, π is a set of primes, and K is the π-powering of G with the π-powering homomorphism $\varphi : G \to K$. The following are true:

1. Let N be the kernel of φ. Then, N contains all the elements of G whose order is a π-number.

2. K is generated as a π-powered group by the image $\varphi(G)$. Equivalently, K does not have any proper π-powered subgroup containing $\varphi(G)$.

Proof. Proof of (1): If $g \in G$ has order a π-number, then $\varphi(g)$ also has order a π-number, since the order of $\varphi(g)$ divides the order of g. However, K is π-powered, hence π-torsion-free, so $\varphi(g)$ is the identity element of K. Thus, g is in N, the kernel of φ.

Proof of (2): Viewing the π-powering functor as a "free" functor, we see that K is generated as a π-powered group by the image of G. □

In general, we cannot say much more: the kernel of the homomorphism may be a lot bigger than the subgroup generated by π-torsion elements. However, in the case of nilpotent groups, the kernel is precisely the set of π-torsion elements (which in fact form a subgroup), and the π-powering is itself a nilpotent group with the same nilpotency class. We now develop the framework that will allow us to get to proofs. We will prove this at the end of Section 4.3.6.

4.3.5 Root set of a subgroup

Suppose G is a group and H is a subgroup of G. We denote by $\sqrt[\pi]{H}$ (relative to the ambient group G) the set of all elements $x \in G$ such that $x^n \in H$ for some π-number n. We begin with some lemmas. Note that if G is non-nilpotent, $\sqrt[\pi]{H}$ need not be a subgroup of G.[3] Thus, the results below do depend on the assumption of G being nilpotent.

Theorem 4.3.2.

1. Suppose G is a nilpotent group, H is a subgroup of G, and π is a set of primes. Then, $\sqrt[\pi]{H}$ is also a subgroup of G.
2. Suppose G is a nilpotent group, π is a set of primes, and A, B are subgroups of G with A normal in B. Then, $\sqrt[\pi]{A}$ is normal in $\sqrt[\pi]{B}$.

This appears as Theorem 10.19 in Khukhro's book [29]. The book does not prove this

3. For instance, let G be the symmetric group S_3 and H be the trivial subgroup. Let π be the set $\{2\}$. Then, $\sqrt[\pi]{H}$ is a subset of size four comprising the identity element and the three elements of order two, and it is not a subgroup.

result, but provides a similar, more specialized proof for a related result, Theorem 9.18.

Proof. Proof of (1): We can assume without loss of generality $G = \langle \sqrt[\pi]{H} \rangle$. If not, simply replace G by the subgroup $\langle \sqrt[\pi]{H} \rangle$ and proceed.

With this assumption, the goal is to show that $G = \sqrt[\pi]{H}$.

We note that for any quotient map $\varphi : G \to M$, $\varphi(G) = \langle \sqrt[\pi]{\varphi(H)} \rangle$. In particular, this is true for quotient maps by lower central series members.

We now prove that $G = \sqrt[\pi]{H}$ by induction on the nilpotency class of G. The base case for induction, namely the case of abelian groups, is obviously true. For the inductive step, assume we have established the result for class $c-1$, and need to prove it for G of class c.

Any element of $\gamma_c(G)$ is a product of iterated c-fold commutators involving elements of G. Since the c-fold iterated commutator is multilinear, the element can be expressed as a product of iterated c-fold commutators involving elements of $\sqrt[\pi]{H}$, which is a generating set for G. Each such iterated commutator is of the form:

$$u = [[\dots[[x_1, x_2], x_3], \dots, x_{c-1}], x_c]$$

with $x_i \in \sqrt[\pi]{H}$. For each x_i, there exists a π-number n_i such that $x_i^{n_i} \in H$, and then, using multilinearity, we get that:

$$u^{n_1 n_2 \dots n_c} = [[\dots[[x_1^{n_1}, x_2^{n_2}], x_3^{n_3}], \dots, x_{c-1}^{n_{c-1}}], x_c^{n_c}]$$

The number $n_1 n_2 \dots n_c$ is a π-number since each n_i is a π-number. Hence, a suitable power of u in in $H \cap \gamma_c(G)$, so $u \in \sqrt[\pi]{H \cap \gamma_c(G)}$. Thus, $\gamma_c(G)$ is abelian and is generated by elements in $\sqrt[\pi]{H \cap \gamma_c(G)}$. Since a product of commuting elements of $\sqrt[\pi]{H \cap \gamma_c(G)}$ must also be in $\sqrt[\pi]{H \cap \gamma_c(G)}$, we get that:

$$\gamma_c(G) \leq \sqrt[\pi]{H \cap \gamma_c(G)}$$

In particular, we get that:

$$\gamma_c(G) \leq \sqrt[\pi]{H}$$

By the observation regarding quotients, we also have that:

$$G/\gamma_c(G) = \langle \sqrt[\pi]{H\gamma_c(G)/\gamma_c(G)} \rangle$$

By the inductive hypothesis, this gives us that:

$$G/\gamma_c(G) = \sqrt[\pi]{H\gamma_c(G)/\gamma_c(G)}$$

We now complete the proof. Suppose $g \in G$. From the fact about $G/\gamma_c(G)$, there exists a π-number m such that $g^m \in H\gamma_c(G)$. Thus, $g^m = hu$ where $h \in H$ and $u \in \gamma_c(G)$ (which is in particular central). Since $\gamma_c(G) \leq \sqrt[\pi]{H}$, there exists a π-number n such that $u^n \in H$. Thus, $g^{mn} = (g^m)^n = (hu)^n = h^n u^n$ (since $u \in \gamma_c(G)$ is central) and this is an element of H. Thus, mn is a π-number such that $g^{mn} \in H$, so $g \in \sqrt[\pi]{H}$.

Proof of (2): Please see the reference ([29], Theorem 9.18 and 10.19). $\square$

Note in particular that this shows that in a nilpotent group G, $\sqrt[\pi]{1}$, i.e., the set of elements whose order is a π-number, is a subgroup of G.

4.3.6 Minimal powered group containing a torsion-free group

The following is a theorem from [29] (Theorem 10.20, Page 122).

Theorem 4.3.3. Suppose π is a set of primes and G is a π-torsion-free nilpotent group of class c.

1. There exists a π-powered group $\hat{G}^\pi$ of nilpotency class c containing G such that $\hat{G}^\pi = \sqrt[\pi]{G}$ is precisely the set of elements that arise as n^{th} roots of elements of G for n varying

over π-numbers.

2. The group $\hat{G}^{\pi}$ is uniquely determined up to isomorphism. In particular, any automorphism of G extends to an automorphism of $\hat{G}^{\pi}$.

3. If F is free nilpotent of class c, then $\hat{F}^{\pi}$ is the free nilpotent π-powered group of class c.

A few comments are in order here before we proceed. Note that π-powered groups are very nicely behaved – all their important characteristic subgroups, quotients, and subquotients are π-powered. For the most part, therefore, if we start with a π-powered group and use deterministic processes, we will stay with π-powered groups.

The π-torsion-free groups are not so nice. In the counterexamples section (section 4.1.13), we saw situations where a torsion-free group has an abelianization that is not torsion-free. This means that we need to proceed with a little more care.

We now prove a statement we made at the end of Section 4.3.4.

Theorem 4.3.4. The following are true for a set of primes π:

1. Suppose G is a π-torsion-free nilpotent group. Then, $\hat{G}^{\pi}$ is the π-powering of G and the inclusion map $G \to \hat{G}^{\pi}$ is the natural homomorphism.

2. Suppose G is a nilpotent group and T is the set of elements of G whose order is a π-number. The quotient group G/T is a π-torsion-free nilpotent group, $\widehat{G/T}^{\pi}$ is the π-powering of G, and the composite of the quotient map $G \to G/T$ and the inclusion $G/T \to (\widehat{G/T})^{\pi}$ is the natural homomorphism to the π-powering of G.

Proof. Proof of (1): Suppose $\varphi : G \to K$ is the natural homomorphism to the π-powering of G. Denote by $\theta : G \to \hat{G}^{\pi}$ the canonical inclusion map of Theorem 4.3.3. By the universality of K, there exists $\alpha : K \to \hat{G}^{\pi}$ such that $\theta = \alpha \circ \varphi$.

Since θ is injective, φ is also injective, so we can view G as a subgroup of K. Part (2) of Theorem 4.3.3 tells us that inside K, $\hat{G}^\pi = \sqrt[\pi]{G}$. Thus, $\hat{G}^\pi$ is a π-powered subgroup of K containing G. By Lemma 4.3.1, $\hat{G}^\pi = K$.

Proof of (2): By Theorem 4.3.2, $T = \sqrt[\pi]{1}$ is a subgroup of G. If any element in G/T has π-torsion, then any representative g for it in G has the property that $g^n \in T$ for n a π-number, and therefore, that $(g^n)^m = 1$ for n and m both π-numbers, forcing g to have order a π-number, so $g \in T$. Thus, G/T is π-torsion-free. The rest of the proof is similar to (1). □

4.3.7 Every π-powered class c word is expressible as a root of an ordinary class c word

This theorem follows from Theorem 4.3.3.

Theorem 4.3.5. Suppose w is a π-powered class c word in n letters. Then, w can be expressed as $v^{1/m}$ where v is an ordinary word (i.e., a word using the group operations only, without any powering operations), and m is a π-number, i.e., all the prime divisors of m are in π.

Proof. Denote by F the free group on n letters of nilpotency class c, and denote by $\hat{F}^\pi$ its π-powered envelope, which is clearly the free π-powered group on n letters. w can be described as an element of $\hat{F}^\pi$. By Theorem 4.3.3, $\hat{F}^\pi = \sqrt[\pi]{F}$. Thus, there exists a π-number m such that $w^m \in F$. Let $v = w^m$. The result follows. □

4.3.8 Results about isoclinisms for π-powered nilpotent groups

We now state and prove a π-powered analogue of Theorem 2.1.2. We will prove the results in the context of nilpotent groups, since this will be the area of primary application. Similar statements can be made for non-nilpotent groups, but the notation and proof become messier, so we restrict attention to the nilpotent case.

Theorem 4.3.6. Suppose $c \geq 1$ and π is any set of primes. Suppose $w(g_1, g_2, \ldots, g_n)$ is a π-powered class c word in n letters with the property that w evaluates to the identity element in *any* π-powered abelian group. Then, for any group G, the word map $w : G^n \to G$ obtained by evaluating w descends to a map:

$$\chi_{w,G} : (\mathrm{Inn}(G))^n \to G'$$

Any word w that is an iterated commutator (with any bracketing) satisfies this condition.

Proof. By Theorem 4.3.5, we can write w as $v^{1/m}$ where v is an ordinary word and m is a π-number. Moreover, since w is guaranteed to be satisfied in any π-powered abelian group, so is v. Thus, v is satisfied in the vector space over the rationals generated by the n letters. So, v is satisfied in the free abelian group generated by the n letters, and therefore v is satisfied in any abelian group. Thus, Theorem 2.1.2 applies to the word v, and we obtain that the map descends to a map:

$$\chi_{v,G} : \mathrm{Inn}(G))^n \to G'$$

Since $w = v^{1/m}$ and G' is π-powered by Theorem 4.1.20, we can obtain the map:

$$\chi_{w,G} : \mathrm{Inn}(G))^n \to G'$$

$\square$

The next theorem is related to Theorem 2.1.3.

Theorem 4.3.7. Suppose $c \geq 1$, π is a set of primes, and (ζ, φ) is a homoclinism of π-powered class c groups G_1 and G_2, where $\zeta : \mathrm{Inn}(G_1) \to \mathrm{Inn}(G_2)$ and $\varphi : G_1' \to G_2'$ are the component homomorphisms. Then for any π-powered class c word $w(g_1, g_2, \dots, g_n)$ that is trivial in every π-powered abelian group (as described above), we have:

$$\chi_{w,G_2}(\zeta(x_1), \zeta(x_2), \dots, \zeta(x_n)) = \varphi(\chi_{w,G_1}(x_1, x_2, \dots, x_n))$$

for all $x_1, x_2, \dots, x_n \in \mathrm{Inn}(G)$.

Any word w that is an iterated commutator (with any order of bracketing) satisfies this condition, and the theorem applies to such word maps.

Proof. By Theorem 4.3.5, we can write w as $v^{1/m}$ where v is an ordinary word and m is a π-number. Moreover, since w is guaranteed to be satisfied in any π-powered abelian group, so is v. Thus, v is satisfied in the vector space over the rationals generated by the n letters. So, v is satisfied in the free abelian group generated by the n letters, and therefore v is satisfied in any abelian group. Thus, Theorem 2.1.2 applies to the word v, and we obtain:

$$\chi_{v,G_2}(\zeta(x_1), \zeta(x_2), \dots, \zeta(x_n)) = \varphi(\chi_{v,G_1}(x_1, x_2, \dots, x_n))$$

Taking m^{th} roots on both sides, we obtain:

$$\chi_{w,G_2}(\zeta(x_1), \zeta(x_2), \dots, \zeta(x_n)) = \varphi(\chi_{w,G_1}(x_1, x_2, \dots, x_n))$$

as desired. $\square$

4.3.9 Results for the upper central series

We begin with a simple-looking result whose proof relies on *downward* induction with the upper central series. The technique used in the proof is similar to the technique used in the proof of Theorem 4.1.21.

Lemma 4.3.8. Suppose π is a set of primes and G is a π-torsion-free nilpotent group. Suppose H is a subgroup of G. Then, for any natural number n, $Z^n(\sqrt[\pi]{H}) = \sqrt[\pi]{Z^n(H)}$.

Proof. The direction $Z^n(\sqrt[\pi]{H}) \le \sqrt[\pi]{Z^n(H)}$ is obvious: note that any element in the group on the left has some π-multiple that is in H, and that therefore must also be in $Z^n(H)$ by definition. We thus concentrate on proving the opposite inclusion.

Suppose G has nilpotency class $c \ge 2$ (note that if $c = 1$ there is nothing to prove).

Consider the c-fold left-normed commutator map of the form:

$$T : (x_1, x_2, \dots, x_c) \mapsto [\dots[[x_1, x_2], x_3], \dots, x_c]$$

This map is a homomorphism in each coordinate holding the other coordinates fixed. Note that this fact is very specific to the class being c. It fails for higher class. Moreover, the set of values for $x_1 \in H$ for which the output is always the identity for the other inputs restricted to H is precisely the subgroup $Z^{c-1}(H)$.

Now, suppose $x \in \sqrt[\pi]{Z^{c-1}(H)}$. If we now consider:

$$T(x, x_2, \dots, x_c)$$

where each x_i in in $\sqrt[\pi]{H}$, we see that if we replace each input by a suitable power of it, the first input lands inside $Z^{c-1}(H)$ and the remaining inputs land inside H. Thus, a suitable π-multiple of $T(x, x_2, \dots, x_c)$ is the identity. Since G is π-torsion-free, this forces $T(x, x_2, \dots, x_c)$ to be the identity, so we obtain that $\sqrt[\pi]{Z^{c-1}(H)} \le Z^{c-1}(\sqrt[\pi]{H})$.

The result can now be extended further down the upper central series. The key trick in executing the extension is to replace the original c-fold commutator with smaller-fold commutators, but now restrict the first input to being within the member one higher. In general when inducting down from $Z^i(H)$ to $Z^{i-1}(H)$, we consider a left-normed commutator of length i, restricting the first input to be within $Z^i(H)$ and allowing all other inputs to vary freely within H or $\sqrt[\pi]{H}$. $\square$

We can apply this to the minimal π-powered group:

Lemma 4.3.9. Suppose G is a π-torsion-free nilpotent group and $\hat{G}^{\pi}$ is a minimal π-powered group containing G. Let $K = Z^n(G)$ Then, $\hat{K}^{\pi}$ is canonically isomorphic to $Z^n(\hat{G}^{\pi})$.

Proof. This follows from the preceding lemma (Lemma 4.3.8) and Theorem 4.3.3. $\square$

4.3.10 Results for the lower central series

Of the two results stated for the upper central series, only one has an analogue for the lower central series. The analogue of the first lemma breaks down, while the second still has a valid analogue.

To see why the analogue of the first lemma breaks down, let G be the central product of $UT(3, \mathbb{Z})$ and $\mathbb{Q}$ where we identify the central $\mathbb{Z}$ in $UT(3, \mathbb{Z})$ with a $\mathbb{Z}$ subgroup in $\mathbb{Q}$. Let H be the subgroup $UT(3, \mathbb{Z})$. Then, if we take π as the set of all primes, we have that $\sqrt[\pi]{H} = G$. Thus, $(\sqrt[\pi]{H})' = G'$, which is the central $\mathbb{Z}$ of G and also the center of H. On the other hand $\sqrt[\pi]{H'}$ is the full center of G, and it is isomorphic to $\mathbb{Q}$. Clearly, the two are not the same.

On the other hand, the second result, pertaining to the minimal π-powered group, still holds.

Lemma 4.3.10. Suppose G is a π-torsion-free nilpotent group and $\hat{G}^{\pi}$ is a minimal π-powered group containing G. Then, $\widehat{\gamma_i(G)}^{\pi}$ is canonically isomorphic to $\gamma_i(\hat{G}^{\pi})$.

Proof. Since $\hat{G}^{\pi}$ is π-powered, Theorem 4.1.20 tells us that $\gamma_i(\hat{G}^{\pi})$ is also π-powered. We already know that $\gamma_i(G) \leq \gamma_i(\hat{G})$, and thus, $\sqrt[\pi]{\gamma_i(G)} \leq \gamma_i(\hat{G}^{\pi})$. By Theorem 4.3.3, the left side becomes $\gamma_i(\hat{G})^\pi$. Thus, we have that:

$$\gamma_i(\hat{G})^\pi \leq \gamma_i(\hat{G}^\pi)$$

The proof for the other direction is also fairly similar and proceeds by inducting over the lower central series, starting from smaller members upwards. The mechanics of the proof are quite similar to that of Theorem 4.3.2. We begin by looking at $\gamma_c(G)$ as the image of the c-fold iterated left normed commutator map, and note that we can pull powers in and out of the commutators. For brevity, we omit the proof details. $\square$

4.4 Free powered Lie rings and powering functors for Lie rings

The final results of this section mirror those of the preceding section (Section 4.3). However, the proofs are much easier.

4.4.1 Construction of the free powered Lie ring

This section uses basic terminology from universal algebra. For background on the terminology, see Section A.2.4.

For any variety of algebras, we can talk of the free algebra in that variety on any set. In particular, we can talk of the free π-powered Lie ring on a set S. We already saw in Section 4.2 that π-powered Lie rings are the same as $\mathbb{Z}[\pi^{-1}]$-Lie algebras. Thus, the free π-powered Lie ring on S coincides with the free $\mathbb{Z}[\pi^{-1}]$-Lie algebras. Equivalently, the free $\mathbb{Z}[\pi^{-1}]$-Lie algebra on S is $\mathbb{Z}[\pi^{-1}] \otimes L$ where L is the free Lie algebra on S. We will denote the free π-powered Lie algebra on S as Lie algebra as $F(S, \pi)$ here to keep notation similar to the preceding section.

4.4.2 Free nilpotent and free powered nilpotent Lie rings

We begin with the definition.

Definition (Free π-powered nilpotent Lie ring)**.** Suppose S is a set, π is a set of primes, and c is a positive integer. The *free π-powered nilpotent Lie ring* of class c on S is defined as the quotient Lie ring $F(S, \pi)/\gamma_{c+1}(F(S, \pi))$ where $F(S, \pi)$ is the free π-powered Lie ring on S. Equivalently, this Lie ring, along with the set map to it from S, is the initial object in the category of Lie rings of nilpotency class at most c with set maps to them from S.

The functor sending a set to its free π-powered nilpotent Lie ring of class c is left adjoint to the forgetful functor from π-powered nilpotent Lie rings of class (at most) c to sets.

4.4.3 π-powered words and word maps

We can define π-powered words and π-powered class c words, and the corresponding word maps, in a manner analogous to Section 4.3.3. Due to the biadditivity of the Lie bracket, we can readily deduce the Lie ring analogues of results that took us some effort to deduce for groups. Further, we do not need the assumption of nilpotency.

Any π-powered word $w(g_1, g_2, \dots, g_n)$ can be written in the form $\frac{1}{m}v(g_1, g_2, \dots, g_n)$ where v is an ordinary word (a sum of Lie products) and m is a π-number. The same conclusion applies if we start with a π-powered class c word.

4.4.4 Localization and powering functors

For a set π of primes, the π-powering functor is a functor from the category of Lie rings to the category of π-powered Lie rings that is left adjoint to the forgetful functor from the category of π-powered Lie rings to the category of Lie rings. More explicitly, for a Lie ring L, the π-powering of L is a Lie ring K along with a homomorphism $\varphi : L \to K$ such that for any homomorphism $\theta : L \to N$ from L to a π-powered Lie ring N, there is a unique homomorphism $\alpha : K \to N$ such that $\theta = \alpha \circ \varphi$.

It turns out that the π-powering functor is the same as the functor that tensors with $\mathbb{Z}[\pi^{-1}]$ to change the base ring to $\mathbb{Z}[\pi^{-1}]$. Explicitly, the functor takes the $\mathbb{Z}$-Lie algebra L

and returns the $\mathbb{Z}[\pi^{-1}]$-Lie algebra $\mathbb{Z}[\pi^{-1}] \otimes_{\mathbb{Z}} L$.

For a prime set π, the π-*localization* functor refers to the powering functor for the set of primes *outside of* π.

4.4.5 Results about isoclinisms for π-powered Lie rings

We now state and prove a π-powered analogue of Theorem 2.2.2. Note that unlike the situation for groups, we do not restrict ourselves to the nilpotent case, because the proofs are straightforward without the assumption of nilpotency. However, if we wish, we *can* formulate the results in the context of π-powered class c Lie ring words. The proofs will remain similar.

Theorem 4.4.1. Suppose π is a set of primes and $w(g_1, g_2, \dots, g_n)$ is a π-powered word in n letters with the property that w evaluates to the zero element in *any* π-powered abelian Lie ring. Then, for any π-powered Lie ring L, the word map $w : L^n \to L$ obtained by evaluating w descends to a map:

$$\chi_{w,L} : (\mathrm{Inn}(L))^n \to L'$$

Proof. As discussed above, we can write $w = (1/m)v$ where m is a π-number and v is a Lie word (a sum of Lie products) and m is a π-number. Moreover, since w is guaranteed to be satisfied in any π-powered abelian Lie ring, so is v. Thus, v is satisfied in the vector space over the rationals generated by the n letters. So, v is satisfied in the free abelian Lie ring generated by the n letters, and therefore v is satisfied in any abelian Lie ring. Thus, Theorem 2.2.2 applies to the word v, and we obtain that the map descends to a map:

$$\chi_{v,L} : \mathrm{Inn}(L))^n \to L'$$

Since $w = (1/m)v$ and L' is π-powered by Lemma 4.2.8, we can obtain the map:

$$\chi_{w,L} : \operatorname{Inn}(L))^n \to L'$$

□

The next theorem is related to Theorem 2.2.3.

Theorem 4.4.2. Suppose π is a set of primes and (ζ, φ) is a homoclinism of π-powered Lie rings L_1 and L_2, where $\zeta : \operatorname{Inn}(L_1) \to \operatorname{Inn}(L_2)$ and $\varphi : L_1' \to L_2'$ are the component homomorphisms. Then for any π-powered word $w(g_1, g_2, \ldots, g_n)$ that is trivial in every π-powered abelian Lie ring (as described above), we have:

$$\chi_{w,L_2}(\zeta(x_1), \zeta(x_2), \ldots, \zeta(x_n)) = \varphi(\chi_{w,L_1}(x_1, x_2, \ldots, x_n))$$

for all $x_1, x_2, \ldots, x_n \in \operatorname{Inn}(G)$.

Any word w that is an iterated commutator (with any order of bracketing) satisfies this condition, and the theorem applies to such word maps.

Proof. We can write $w = (1/m)v$ where v is an ordinary word and m is a π-number. Moreover, since w is guaranteed to be satisfied in any π-powered abelian Lie ring, so is v. Thus, v is satisfied in the vector space over the rationals generated by the n letters. So, v is satisfied in the free abelian Lie ring generated by the n letters, and therefore v is satisfied in any abelian Lie ring. Thus, Theorem 2.2.2 applies to the word v, and we obtain:

$$\chi_{v,L_2}(\zeta(x_1), \zeta(x_2), \ldots, \zeta(x_n)) = \varphi(\chi_{v,L_1}(x_1, x_2, \ldots, x_n))$$

Dividing both sides by m, we obtain:

$$\chi_{w,L_2}(\zeta(x_1), \zeta(x_2), \ldots, \zeta(x_n)) = \varphi(\chi_{w,L_1}(x_1, x_2, \ldots, x_n))$$

as desired. $\square$

CHAPTER 5

BAER CORRESPONDENCE

5.1 Baer correspondence: the basic setup

The *Baer correspondence* was introduced by Reinhold Baer in [3]. We will review the correspondence in this section, and study it in further detail in the next two sections (Sections 5.2 and 5.3). This paves the way for the section after that (Section 5.4), which contains a novel contribution of this thesis, that we call the *Baer correspondence up to isoclinism.* This is relatively straightforward to prove and understand. It sets the stage for the next few sections, where we discuss the *Lazard correspondence* (introduced by Lazard in [30]) and our variation of it, namely the *Lazard correspondence up to isoclinism.*

Many of the ideas described in this section are similar to, and build upon, ideas in Section 1.3, where we describe the abelian Lie correspondence.

5.1.1 Baer Lie groups and Baer Lie rings

We begin with some definitions. These definitions are not standard, and there may be somewhat different meanings in other sources that use these words.

Definition (Baer Lie group)**.** A group G is termed a *Baer Lie group* if G is powered over the prime 2 (per Definition 4.1.3; explicitly, this means that every element of G has a unique square root) *and* G is nilpotent with nilpotency class at most 2.

Definition (Baer Lie ring)**.** A Lie ring L is termed a *Baer Lie ring* if L is powered over the prime 2 (i.e., its additive group is powered over 2 per Definition 4.1.3; explicitly, this means that every element has a unique half) *and* L is nilpotent with nilpotency class at most 2.

The Baer correspondence is a correspondence:

$$\text{Baer Lie groups} \leftrightarrow \text{Baer Lie rings}$$

A group and Lie ring that are in Baer correspondence have *the same underlying set.*

5.1.2 Construction from group to Lie ring

Consider a Baer Lie group G with multiplication denoted by juxtaposition and the identity element denoted by 1. We define a Baer Lie ring, denoted $\log G$ or $\log(G)$, as follows. The underlying set of $\log G$ is the same as the underlying set of G, and the operations are as follows.

- The addition on $\log(G)$ is defined as $x + y := \frac{xy}{\sqrt{[x,y]}}$ where $[x, y]$ denotes the group commutator. Note that because the group has class two, it does not matter whether we use the left action convention for the commutator $[x, y] = xyx^{-1}y^{-1}$ or the right action convention for the commutator $[x, y] = x^{-1}y^{-1}xy$: they both mean the same thing.

  Note that $[x, y] \in Z(G)$ (where $Z(G)$ denotes the center of G) because G has class at most two. G is 2-powered, so by Lemma 4.1.5, the center $Z(G)$ is also 2-powered. Thus, $\sqrt{[x, y]}$ is also in $Z(G)$. Thus, we can "divide" xy by this element unambiguously, without specifying whether the division is on the left or on the right.

  There are two alternative expressions for $x + y$ that are equal to the above and are sometimes more useful to use: $x+y = \sqrt{x}y\sqrt{x}$ and $x+y = \sqrt{xy^2x}$. For more on these expressions, see Section 5.1.6.

- The zero element of $\log(G)$ is defined as equal to the identity element 1 of G.

- The additive inverse $-x$ is defined as $-x := x^{-1}$.

- The Lie bracket $[x, y]_{\text{Lie}}$ is defined as the group commutator $[x, y]$. As remarked above, it does not matter whether we use the left action convention or the right action convention for the commutator.

Lemma 5.1.1. $\log G$ (as defined above, with the same underlying set as G), is a Baer Lie ring.

Proof. The proof requires showing the following:

1. Addition is associative
2. Addition is commutative
3. Identity and inverses work
4. The Lie bracket is additive in the first variable
5. The Lie bracket is additive in the second variable
6. The Lie bracket is alternating
7. The Lie bracket satisfies the Jacobi condition and gives a class two Lie ring
8. The Lie ring is 2-powered.

Proof of (1): We want to show that for every x, y, z in G (possibly equal, possibly distinct), we have:

$$(x + y) + z = x + (y + z)$$

We first consider the left side:

$$(x + y) + z = \frac{\frac{xy}{\sqrt{[x,y]}} \cdot z}{\sqrt{\left[\frac{xy}{\sqrt{[x,y]}}, z\right]}}$$

We know that for c central, $[a, bc] = [ac, b] = [a, b]$. Since the reciprocal of $\sqrt{[x, y]}$ is central, it can be dropped from inside commutator expressions, and we simplify to:

$$(x + y) + z = \frac{xyz}{\sqrt{[x, y]}\sqrt{[xy, z]}}$$

The square root operation is a homomorphism on the center, and we can thus rewrite it as:

$$(x + y) + z = \frac{xyz}{\sqrt{[x, y][xy, z]}} \tag{†}$$

Similarly, the right side of the associativity result we want to prove becomes:

$$x + (y + z) = \frac{xyz}{\sqrt{[x, yz][y, z]}} \tag{††}$$

Thus, to prove associativity, it suffices to show that the right sides of (†) and (††) are equal, which in turn reduces to proving that:

$$[x, y][xy, z] = [x, yz][y, z]$$

For a group of class two, the commutator map is a homomorphism in each of its coordinates (see Lemma A.3.2 for a proof of this and related statements). Thus, both sides simplify to:

$$[x, y][x, z][y, z]$$

and hence both sides are equal, completing the proof.

Proof of (2): We want to show that for any x, y in the group, $x + y = y + x$. The key ingredient to our proof is the observation that $[x, y]^{-1} = [y, x]$.

We have, by definition:

$$x + y = \frac{xy}{\sqrt{[x,y]}}$$

and:

$$y + x = \frac{yx}{\sqrt{[y,x]}}$$

It thus suffices to prove that:

$$\frac{xy}{\sqrt{[x,y]}} = \frac{yx}{\sqrt{[y,x]}}$$

which is equivalent to proving that:

$$\frac{xy}{\sqrt{[x,y]}} = yx\sqrt{[x,y]}$$

which in turn is equivalent to proving that:

$$xy = yx[x,y]$$

which is true by the definition of $[x,y]$.

Proof of (3): We have:

$$x + 1 = \frac{x1}{\sqrt{[x,1]}} = x$$

and:

$$1 + x = \frac{1x}{\sqrt{[1,x]}} = x$$

Thus, 1 is an identity element for the Lie ring addition.

We also have:

$$x + x^{-1} = \frac{xx^{-1}}{\sqrt{[x, x^{-1}]}} = 1$$

and:

$$x^{-1} + x = \frac{x^{-1}x}{\sqrt{[x^{-1}, x]}} = 1$$

Proof of (4) and (5): These follow from the corresponding facts for the commutator map in a group of class two.

Proof of (6): This follows from the general fact that $[x, y]^{-1} = [y, x]$.

Proof of (7): In fact, *all* Lie products $[[x, y], z]$ are zero, so the Jacobi identity is trivially satisfied.

Proof of (8): We have:

$$x + x = \frac{x^2}{\sqrt{[x, x]}} = x^2$$

In other words, the double of an element in the Lie ring is the same as its square in the group. Since the group is 2-powered, the Lie ring is also 2-powered. □

5.1.3 Construction from Lie ring to group

Suppose L is a Baer Lie ring with addition $+$ and Lie bracket $[\ ,\ ]$. We define a Baer Lie group $\exp(L)$ as follows. The underlying set of $\exp(L)$ is the same as the underlying set of L. The group operations are defined as follows:

- The group multiplication on $\exp(L)$ is defined as:

$$xy = x + y + \frac{1}{2}[x, y]$$

- The identity element for the group multiplication of $\exp(L)$ is defined as the element 0 of L.

- The inverse operation is defined as $x^{-1} := -x$.

Lemma 5.1.2. $\exp(L)$ (defined as above, with the same underlying set as L) is a Baer Lie group. Moreover, the group commutator in $\exp(L)$ coincides with the Lie bracket in L.

Proof. The proof requires showing the following:

1. Multiplication is associative.
2. The identity element and inverses work.
3. The commutator map in the group agrees with the Lie bracket.
4. The group has nilpotency class at most two.
5. The group is 2-powered.

Proof of (1): Let x, y, z be arbitrary (possibly equal, possibly distinct) elements of L.

To prove: $(xy)z = x(yz)$

Proof: We begin by simplifying the left side. We have:

$$(xy)z = \left(x + y + \frac{1}{2}[x,y]\right) + z + \frac{1}{2}\left[x + y + \frac{1}{2}[x,y], z\right]$$

We use the linearity of the Lie bracket, and also use that the Lie ring has nilpotency class two to simplify $[[x,y],z]$ to zero. The expression simplifies to:

$$(xy)z = x + y + z + \frac{1}{2}\left([x,y] + [x,z] + [y,z]\right)$$

Similarly, we can show that:

$$x(yz) = x + y + z + \frac{1}{2}\left([x,y] + [x,z] + [y,z]\right)$$

Thus, associativity holds.

Proof of (2): From the expression for group multiplication, we obtain that if $[x, y] = 0$, then $xy = x + y$. In particular, this means that:

$$x(0) = x + 0 = x$$

and:

$$(0)x = 0 + x = x$$

Thus, $x(0) = (0)x = x$, so 0 is an identity element for multiplication, and we obtain that the multiplication defined turns L into a monoid.

Further, we obtain that:

$$x(-x) = x + (-x) = 0$$

and:

$$(-x)x = (-x) + x = 0$$

Thus, $-x$ is a two-sided multiplicative inverse for x. L is thus a monoid where every element has a two-sided multiplicative inverse, hence is a group. Further, $-x = x^{-1}$ in this group for all x.

Proof of (3): We want to compute an explicit expression for the group commutator $[x, y]_{\text{Group}} = xyx^{-1}y^{-1} = (xy)(yx)^{-1}$ in terms of the Lie ring operations.

First, we use that $(yx)^{-1} = -(yx)$, so we get:

$$[x, y]_{\text{Group}} = (xy)(-(yx)) = (xy) + (-(yx)) + \frac{1}{2}[xy, -(yx)]$$

This simplifies to:

$$[x, y]_{\text{Group}} = x + y + \frac{1}{2}[x, y] - (y + x + \frac{1}{2}[y, x]) + \frac{1}{2}[x + y + \frac{1}{2}[x, y], -(y + x + \frac{1}{2}[y, x])]$$

Simplify using the fact that the Lie ring has class two, so that all Lie products of the form $[a, [b, c]]$ or $[[a, b], c]$ are zero. We get:

$$[x, y]_{\text{Group}} = [x, y]$$

Thus, the group commutator equals the Lie bracket. Note that the proof above is for the group commutator defined using the left action convention, but an analogous proof exists for the group commutator defined using the right action convention.

Proof of (4): This follows from (3) and the fact that the Lie ring has nilpotency class two.

Proof of (5): For any $x \in L$, x^2 with respect to the group structure is given by:

$$x^2 = x + x + \frac{1}{2}[x, x] = 2x$$

In other words, the squaring operation in the group coincides with the doubling operation in the Lie ring. The latter is bijective because the Lie ring is 2-powered. Hence, the former operation is also bijective. Therefore, the group is 2-powered. □

5.1.4 *Mutually inverse nature of the constructions*

We now show that exp and log are two-sided inverses of each other.

Lemma 5.1.3. The construction of the Baer Lie ring of a Baer Lie group and the construction of the Baer Lie group of a Baer Lie ring are two-sided inverses of each other. Explicitly:

1. Start with a Baer Lie group G. Then, $G = \exp(\log(G))$.

2. Start with a Baer Lie ring L. Then, $L = \log(\exp(L))$.

Proof. Note that the identity element and inverse map are the same for the group and Lie ring, and the Lie bracket for the Lie ring is the same as the commutator for the group, so the main thing to check is the interplay between the Lie ring addition and the group multiplication.

Proof of (1): We want to show that the "new" group multiplication coincides with the original group multiplication:

$$(x + y) + \frac{1}{2}[x, y] = xy$$

We begin by simplifying the left side. We begin by replacing $x + y$ by its expression in terms of the group multiplication, and obtain:

$$\frac{xy}{\sqrt{[x, y]}} + \frac{1}{2}[x, y]$$

This further simplifies to:

$$\frac{\frac{xy}{\sqrt{[x,y]}}\sqrt{[x, y]}}{\sqrt{\left[\frac{xy}{\sqrt{[x,y]}}, \sqrt{[x, y]}\right]}}$$

The lower denominator is the identity element because $\sqrt{[x, y]}$ is central on account of the group having class two and being 2-powered. The numerator simplifies to xy. This completes the proof.

Proof of (2): We want to show that the "new" Lie ring addition coincides with the original Lie ring addition. Explicitly, we want to show that:

$$\frac{xy}{\sqrt{[x,y]}} = x + y$$

We simplify the left side. Note that $\sqrt{[x,y]} = \frac{1}{2}[x,y]$ is central back in the Lie ring, so this becomes:

$(x + y + \frac{1}{2}[x,y]) - \frac{1}{2}[x,y]$

This simplifies to $x + y$, as desired. $\square$

5.1.5 Understanding the formulas in the Baer correspondence

Given two elements x and y in a Baer Lie group G, there are two possible products we can consider: xy and yx. The quotient of these products $(xy)/(yx)$ is the commutator $[x,y]$. Note that we get the same answer whether we use left or right quotients, because the elements xy and yx commute on account of the class being two.

The "average" of the two products can be thought of as an element z that is midway between xy and yx, i.e., we want z to satisfy:

$$\frac{xy}{z} = \frac{z}{yx}$$

If we rearrange and solve, we will get:

$$z = \frac{xy}{\sqrt{[x,y]}}$$

The Baer Lie ring construction sets $x + y$ to equal this "average" value and sets the Lie bracket $[x,y]$ to equal the "distance" between xy and yx. This agrees with our earlier statement made in Section 1.1.7 about Lie-type correspondences in general: "The addition operation of the Lie ring captures the abelian part of the group multiplication, whereas the Lie bracket captures the non-abelian part of the group multiplication."

5.1.6 Twisted multiplication of a 2-powered group

Suppose G is a 2-powered (not necessarily nilpotent) group. For any $u \in G$, denote by $\sqrt{u}$ the unique element $v \in G$ such that $v^2 = u$.[1]

The *twisted multiplication* on G has two somewhat different but related definitions. The two definitions are denoted as $*_1$ and $*_2$ below, and the reason for their equivalence is discussed below:

$$x *_1 y := \sqrt{x} y \sqrt{x}$$

$$x *_2 y := \sqrt{xy^2x} = \sqrt{(xy)(yx)}$$

The latter can be thought of as the "mean" between xy and yx, and more explicitly, it is the unique solution z to:

$$z^{-1}xy = z(yx)^{-1}$$

For any $x, y \in G$, we have:

$$x^2 *_1 y^2 = (x *_2 y)^2 = xy^2x$$

Thus, the square map establishes an isomorphism between $(G, *_2)$ and $(G, *_1)$.

As proved in [18], G acquires the structure of a gyrocommutative gyrogroup (and in particular, the structure of a loop) under either of these equivalent operations. Explicitly:

- The identity element for $*_1$ equals the identity element for $*_2$, and both are equal to the identity element for G as a group.

1. The typical case of interest is where G is a finite group, in which case being 2-powered is equivalent to being an odd-order group. However, none of the statements here rely on finiteness.

- The inverse map for $*_1$ is the same as the inverse map for $*_2$, and both are equal to the inverse map for G as a group.
- In terms of $*_2$, the gyroautomorphism $\operatorname{gyr}([x, y])$ is defined to be conjugation in G by $\sqrt{xy^2x}x^{-1}y^{-1} = (\sqrt{xy^2x})^{-1}xy$. Note that the conjugation element can be thought of as the "mean deviation", i.e., it is the distance between either of xy and yx and the "mean" between them, in a manner similar to that described in Section 5.1.5.

The connection of the twisted multiplication with the Baer correspondence is as follows: given a Baer Lie group, the addition operation in the corresponding Baer Lie ring coincides with the twisted multiplication (in fact, it coincides with *both* $*_1$ and $*_2$). Explicitly, for a Baer Lie group, the Lie ring addition has the following equivalent forms:

$$x + y = \frac{xy}{\sqrt{[x, y]}} = \sqrt{x}y\sqrt{x} = \sqrt{xy^2x}$$

5.1.7 Preservation of homomorphisms and isomorphism of categories

In Section 1.3.2, we made a number of observations leading to the conclusion that the category of abelian groups is isomorphic to the category of abelian Lie rings, with the isomorphisms given explicitly by the log and exp functors.

The analogous conclusion also holds for the Baer correspondence. However, the reasoning behind these steps is somewhat different from the abelian case. In the abelian case, the only conceptual distinction between the group side and Lie ring side was that the latter had a trivial Lie bracket operation. Other than that, the operations were the same. In the Baer case, the group operations and Lie ring operations are defined somewhat differently. The reason that the correspondence works is that *any formula commutes with any homomorphism.* For instance, if $w(x, y)$ is the word describing the Lie ring addition in terms of the group operations (including powering operations), then for any group homomorphism φ:

$$\varphi(w(x,y)) = w(\varphi(x), \varphi(y))$$

In the case of the Baer correspondence, the formula in question is:

$$w(x,y) = \frac{xy}{\sqrt{[x,y]}}$$

and the assertion becomes:

$$\varphi\left(\frac{xy}{\sqrt{[x,y]}}\right) = \frac{\varphi(x)\varphi(y)}{\sqrt{[\varphi(x), \varphi(y)]}}$$

Since the Lie ring operations are defined in terms of the group operations, a homomorphism of groups preserves the Lie ring operations, and therefore gives a homomorphism of Lie rings. In the opposite direction, since the group operations are defined in terms of the Lie ring operations, a homomorphism of Lie rings preserves the group operations, and therefore gives a homomorphism of groups. Explicitly, in this case, if φ is a Lie ring homomorphism between Baer Lie rings, then the assertion is that:

$$\varphi\left(x + y + \frac{1}{2}[x,y]\right) = \varphi(x) + \varphi(y) + \frac{1}{2}[\varphi(x), \varphi(y)]$$

The explicit statements are below:

- log defines a functor from Baer Lie groups to Baer Lie rings: Suppose G_1 and G_2 are Baer Lie groups and $\varphi : G_1 \to G_2$ is a group homomorphism. Then, there exists a unique Lie ring homomorphism $\log(\varphi) : \log(G_1) \to \log(G_2)$ that has the same underlying set map as φ. *Reason*: The Lie ring operations are defined as formal expressions in terms of the group operations and the square root operation, and this expression is preserved under homomorphisms.

- exp defines a functor from Baer Lie rings to Baer Lie groups: Suppose L_1 and L_2 are Baer Lie rings and $\varphi : L_1 \to L_2$ is a Lie ring homomorphism. Then, there exists a unique group homomorphism $\exp(\varphi) : \exp(G_1) \to \exp(G_2)$ that has the same underlying set map as φ. *Reason*: The group operations are defined as formal expressions in terms of the Lie ring operations and the halving operation, and this expression is preserved under homomorphisms.

- The log and exp functors are two-sided inverses of each other: This has four parts:
  - For every Baer Lie group G, $G = \exp(\log(G))$. This is part of Lemma 5.1.3.
  - For every Baer Lie ring L, $L = \log(\exp(L))$. This is part of Lemma 5.1.3.
  - For every group homomorphism $\varphi : G_1 \to G_2$ of Baer Lie groups, $\exp(\log(\varphi)) = \varphi$. This follows immediately from the fact that both taking log and taking exp preserve the underlying set map.
  - For every Lie ring homomorphism $\varphi : L_1 \to L_2$ of Baer Lie rings, $\log(\exp(\varphi)) = \varphi$. This follows immediately. This following immediately from the fact that both taking log and taking exp preserve the underlying set map.

The upshot is that the Baer correspondence defines an isomorphism of categories over the category of sets between the category of Baer Lie groups and the category of Baer Lie rings. Here, by "category of Baer Lie groups" we mean the full subcategory[2] of the category of groups where the objects are the Baer Lie groups. Similarly, by "category of Baer Lie rings" we mean the full subcategory of the category of Lie rings where the objects are Baer Lie rings.

Note that all steps of this reasoning can be repeated for the Lazard correspondence. To avoid repetition, we will omit the details and instead refer back to this section as needed.

2. Full subcategory means that all morphisms of the big category (in this case, the category of groups) between objects of the subcategory (in this case, Baer Lie groups) are morphisms in the subcategory.

5.1.8 *Consequences for the Baer correspondence of being an isomorphism of categories*

We have established above that the Baer correspondence defines an isomorphism of categories. Mimicking the steps in Section 1.3, we obtain the following:

- The Baer correspondence preserves endomorphism monoids. Explicitly, if G is a Baer Lie group and $L = \log(G)$, then $\mathrm{End}(G)$ and $\mathrm{End}(L)$ are isomorphic monoids, and define the same collection of set maps. The reasoning mimicks Section 1.3.4.
- The Baer correspondence also preserves automorphism groups. Again, the reasoning mimicks Section 1.3.4.
- We can define the Baer correspondence *up to isomorphism* (mimicking Section 1.3.5). This is a correspondence:

Isomorphism classes of Baer Lie groups $\leftrightarrow$ Isomorphism classes of Baer Lie rings

5.2 Baer correspondence: additional remarks

5.2.1 *Subgroups, quotients, and direct products*

In Section 1.3.7, we noted that the abelian Lie correspondence between an abelian group and an abelian Lie ring gives rise to a correspondence between all subgroups of the group and all subrings of the Lie ring.

A related result holds for the Baer correspondence, but there are more caveats. The important caveat is that the 2-powered groups do *not* form a sub*variety* of the variety of groups. Therefore, the Baer Lie groups do not form a subvariety of the variety of groups. Let us examine subgroups, quotients, and direct products separately:

- *Subgroups*: A subgroup of a Baer Lie group need not be a Baer Lie group. For instance, the group $\mathbb{Q}$ of rational numbers is a Baer Lie group, but its subgroup $\mathbb{Z}$ is not a Baer Lie group.
- *Quotients*: A quotient group of a Baer Lie group need not be a Baer Lie group. For instance, the group $\mathbb{Q}$ of rational numbers is a Baer Lie group, but its quotient group $\mathbb{Q}/\mathbb{Z}$ is not a Baer Lie group.
- *Direct products*: An arbitrary direct product of Baer Lie groups is a Baer Lie group.

Similar observations hold for Baer Lie rings:

- *Subrings*: A subring of a Baer Lie ring need not be a Baer Lie ring. For instance, the abelian Lie ring with additive group $\mathbb{Q}$ but its subring with additive group $\mathbb{Z}$ is not a Baer Lie ring.
- *Quotient rings*: A quotient ring of a Baer Lie ring need not be a Baer Lie ring. For instance, the abelian Lie ring with additive group $\mathbb{Q}$ is a Baer Lie ring, but the quotient ring with additive group $\mathbb{Q}/\mathbb{Z}$ is not a Baer Lie ring.
- *Direct products*: An arbitrary direct product of Baer Lie rings is a Baer Lie ring.

Due to the above considerations, we need to impose some restrictions on the nature of the subgroup and nature of the quotient group in order to use the Baer correspondence to obtain a correspondence between subgroups and subrings, or between quotient groups and quotient rings.

Call a subgroup H of a Baer Lie group G a *Baer Lie subgroup* if H is 2-powered. In particular, this means that H is a Baer Lie group in its own right. Note also that for a normal subgroup H of G, H is a Baer Lie subgroup if and only if the quotient group G/H is a Baer Lie group (this follows from the two-out-of-three theorem, Theorem 4.1.27). In this case, we say that G/H is a *Baer Lie quotient group* of G.

Call a subring M of a Baer Lie ring L a *Baer Lie subring* if M is 2-powered. In particular, this means that M is a Baer Lie ring in its own right. Note also that for an ideal I of L, I is a Baer Lie subring if and only if the quotient ring L/I is a Baer Lie ring (this follows from Theorem 4.2.1). In these equivalent cases, we will say that I is a *Baer Lie ideal* of L and L/I is a *Baer Lie quotient ring* of L.

- *Baer Lie subgroups correspond to Baer Lie subrings*: Suppose a Baer Lie ring L is in Baer correspondence with a Baer Lie group G, i.e., $L = \log(G)$ and $G = \exp(L)$. Then, for every Baer Lie subgroup H of G, $\log(H)$ is a subring of L, and the inclusion map of $\log(H)$ in L is obtained by applying the log functor to the inclusion map of H in G. In the opposite direction, for every Baer Lie subring M of L, $\exp(M)$ is a subgroup of G, and the inclusion map of $\exp(M)$ in G is obtained by applying the exp functor to the inclusion map of M in L. The Baer correspondence thus gives rise to a correspondence:

$$\text{Baer Lie subgroups of } G \leftrightarrow \text{Baer Lie subrings of } L$$

- *Quotient groups by normal Baer Lie subgroups correspond to quotient rings by Baer Lie ideals*: Suppose a Baer Lie ring L is in Baer correspondence with a Baer Lie group G. Then, for every normal Baer Lie subgroup H of G, $\log(G/H)$ is a quotient Lie ring of L, and the quotient map $L \to \log(G/H)$ is obtained by applying the log functor to the quotient map $G \to G/H$. In the opposite direction, for every Baer Lie ideal I of L, $\exp(L/I)$ is a quotient group of G, and the quotient map $G \to \exp(L/I)$ is obtained by applying the exp functor to the quotient map $L \to L/I$. The Baer correspondence thus gives rise to correspondences:

$$\text{Normal Baer Lie subgroups of } G \leftrightarrow \text{Baer Lie ideals of } L$$

$$\text{Baer Lie quotient groups of } G \leftrightarrow \text{Baer Lie quotient rings of } L$$

- *Direct products correspond to direct products*: Suppose I is an indexing set, and $G_i, i \in I$ is a collection of Baer Lie groups. For each $i \in I$, let $L_i = \log(G_i)$. Then, the external direct product $\prod_{i \in I} L_i$ is in Baer correspondence with the external direct product $\prod_{i \in I} G_i$. Moreover, the projection maps from the direct product to the individual direct factors are in Baer correspondence. Also, the inclusion maps of each direct factor in the direct product are in Baer correspondence.

5.2.2 Twisted subgroups and subrings

We introduce the notion of *twisted subgroup* of a group. Our definition differs somewhat from the definition found in the literature (see, for instance, [18]) in that our definition requires twisted subgroups to be closed under taking inverses. The condition is not stated in [18] because that paper, and the other related literature, are interested primarily in finite groups, where the condition is redundant.

Definition (Twisted subgroup)**.** A subset K of a group G is termed a *twisted subgroup* if it satisfies the following three conditions:

1. For any $x, y \in K$ (possibly equal, possibly distinct), $xyx \in K$.
2. The identity element of G is in K.
3. For any $x \in K$, $x^{-1} \in K$.

Note that Conditions (1) and (2) imply closure under taking positive powers, so if every element of K has finite order in G, condition (3) is redundant.

We will call a twisted subgroup K of a group G *powered* over a set of primes π if the map $x \mapsto x^p$ is a bijection from K to itself for every $p \in \pi$.

We had earlier defined the addition in a Baer Lie group as follows:

$$x + y = \frac{xy}{\sqrt{[x, y]}}$$

As described in Section 5.1.6, we can rewrite this as:

$$x + y = \sqrt{x}y\sqrt{x}$$

It follows that under the Baer correspondence, we have a correspondence:

2-powered twisted subgroups of the Baer Lie group $\leftrightarrow$ 2-powered additive subgroups of the Baer Lie ring

5.2.3 Characteristic subgroups and subrings

In Section 5.2.1, we noted that the Baer correspondence between a Baer Lie group G and a Baer Lie ring L induces a correspondence:

Baer Lie subgroups of G $\leftrightarrow$ Baer Lie subrings in L

Recall that a Baer Lie subgroup of a Baer Lie group is simply a 2-powered subgroup. Similarly, a Baer Lie subring of a Baer Lie ring is simply a 2-powered subring.

In Section 5.1.8, we noted that the Baer correspondence preserves automorphisms groups, i.e., $\text{Aut}(G)$ and $\text{Aut}(L)$ define the same collection of permutations on the underlying set. Thus, the above correspondence preserves the property of being invariant under automorphisms, and we obtain a correspondence:

Characteristic Baer Lie subgroups of G $\leftrightarrow$ Characteristic Baer Lie subrings of L

Note that, combined with the fact that normal Baer Lie subgroups of G correspond with Baer Lie ideals of L, this tells us that any characteristic Baer Lie subring of L (i.e., any 2-powered characteristic subring of L) is an ideal of L. Note that this is a nontrivial statement about the structure of L, since there do exist Lie rings that have characteristic subrings that are not ideals.

Conjecture 4.1.28 (respectively, Conjecture 4.2.10) stated that for a prime set π, any characteristic subgroup (respectively, characteristic Lie subring) in a π-powered nilpotent group (respectively, π-powered nilpotent Lie ring) must be π-powered. We can consider restricted versions of Conjectures 4.1.28 and 4.2.10 to the case of Baer Lie groups and Baer Lie rings respectively. If both restricted conjectures are true, then we have a correspondence:

$$\text{Characteristic subgroups of } G \leftrightarrow \text{Characteristic subrings of } L$$

Analogous remarks to the above remarks for characteristic subgroups and subrings apply to the case of fully invariant subgroups and subrings. Note that the conjecture that would be necessary for fully invariant subgroups and subrings is implied by the conjecture for characteristic subgroups.

5.2.4 The p-group case

Let p be an odd prime. We will use the term *p-group* for a group (not necessarily finite) in which the order of every element is a power of p. We will use the term *p-Lie ring* for a Lie ring whose additive group is a p-group. The Baer correspondence restricts to a correspondence:

$$p\text{-groups of nilpotency class (at most) two} \leftrightarrow p\text{-Lie rings of nilpotency class (at most) two}$$

The square root operation in this case corresponds to a powering operation. Explicitly, if g is an element of a p-group G, the order of g is a prime power p^k. $\sqrt{g}$ equals $g^{(p^k+1)/2}$. In particular, it is a positive integral power of g.

Thus, *every* subset of a p-group that is closed under taking positive powers is also closed under taking square roots. In particular, *every* subgroup of a p-group is 2-powered, and *every* twisted subgroup of a p-group is 2-powered.

Thus, in the case of p-groups for odd primes p, the correspondences discussed in the preceding sections are particularly easy. The correspondence between 2-powered subgroups and 2-powered subrings becomes a correspondence:

$$\text{Subgroups of } G \leftrightarrow \text{Subrings of } L$$

We also obtain correspondences:

- Normal subgroups of $G \leftrightarrow$ Ideals of L
- Quotient groups of $G \leftrightarrow$ Quotient rings of L
- Characteristic subgroups of $G \leftrightarrow$ Characteristic subrings of L
- Fully invariant subgroups of $G \leftrightarrow$ Fully invariant subrings of L

The correspondence between 2-powered twisted subgroups and 2-powered additive subgroups of the Lie ring becomes a correspondence:

$$\text{Twisted subgroups of } G \leftrightarrow \text{Subgroups of the additive group of } L$$

5.2.5 Relation between the Baer correspondence and the abelian Lie correspondence

In an earlier section (Section 1.3), we introduced the abelian Lie correspondence:

$$\text{Abelian groups} \leftrightarrow \text{Abelian Lie rings}$$

In the preceding section (Section 5.1), we introduced the Baer correspondence:

$$\text{Baer Lie groups} \leftrightarrow \text{Baer Lie rings}$$

We used the same symbols (log and exp) to describe the functors for both correspondences. This leads to a potential for ambiguity: what happens if a group happens to be both an abelian group *and* a Baer Lie group? It turns out that in this case, the two correspondences agree. Explicitly:

- Suppose G is a 2-powered abelian group, i.e., G is *both* an abelian group and a Baer Lie group. Then, the two definitions of $\log G$ (based on the abelian Lie correspondence and Baer correspondence respectively) agree with each other.

- Suppose L is a 2-powered abelian Lie ring, i.e., L is *both* an abelian Lie ring and a Baer Lie ring. Then, the two definitions of $\exp L$ (using the abelian Lie correspondence and Baer Lie correspondence) agree with each other.

- Suppose G_1 and G_2 are 2-powered abelian groups and $\varphi : G_1 \to G_2$ is a homomorphism of groups. Then, the two definitions of $\log(\varphi)$ (based on the abelian Lie correspondence and Baer correspondence respectively) agree.

- Suppose L_1 and L_2 are 2-powered abelian Lie rings and $\varphi : L_1 \to L_2$ is a homomorphism of Lie rings. Then, the two definitions of $\exp(\varphi)$ (based on the abelian Lie correspondence and Baer correspondence respectively) agree.

Every time we introduce a new correspondence between groups and Lie rings, we will attempt to verify whether it is compatible with existing correspondences. Checking compatibility will reduce to the question of checking whether the formulas agree with each other in the case of overlap. For illustrative purposes, consider the proof that for a 2-powered abelian Lie ring L, the two definitions of $\exp L$ agree. The definitions of group multiplication in terms of the Lie ring operations:

$x+y$ for the abelian Lie correspondence, $\quad x+y+\frac{1}{2}[x,y]$ for the Baer Lie correspondence

These formulas agree for a 2-powered abelian group.

5.2.6 Abelian subgroups, abelian quotient groups, center and derived subgroup

Suppose a group G is in Baer correspondence with a Lie ring L. We know that G and L have the same underlying set, and the commutator map in G coincides with the Lie bracket in L. From this, we can deduce the following:

1. The abelian subgroups of G are in abelian Lie correspondence with the abelian subrings of L, and this abelian Lie correspondence arises by restricting the Baer correspondence between G and L.

   $$\text{Abelian subgroups of } G \leftrightarrow \text{Abelian subrings of } L$$

   Note that for the 2-powered abelian subgroups and 2-powered abelian subrings, this coincides with the Baer correspondence.

   The correspondence also restricts to a correspondence:

   $$\text{Abelian normal subgroups of } G \leftrightarrow \text{Abelian ideals of } L$$

   and to a subcorrespondence:

   $$\text{Abelian characteristic subgroups of } G \leftrightarrow \text{Abelian characteristic subrings of } L$$

   Finally, the correspondence gives rise to a correspondence:

   $$\text{Quotient groups of } G \text{ by abelian normal subgroups} \leftrightarrow \text{Quotient rings of } L \text{ by abelian ideals}$$

   Note, however, that the instances of this last correspondence are *not* instances of the Baer correspondence. They do, however, form instances of the divided Baer correspondence described in Section 5.3.4.

2. For a subset S of the common underlying set of G and L, the subgroup generated by S in G is abelian if and only if the subring generated by S in L is abelian, and if so, the subgroup and subring are in abelian Lie correspondence.

3. The abelian quotient groups of G are in abelian Lie correspondence with the abelian quotient Lie rings of L. Explicitly:

$$\text{Abelian quotient groups of } G \leftrightarrow \text{Abelian quotient Lie rings of } L$$

   We obtain a correspondence between the corresponding kernels. Explicitly, the Baer correspondence between G and L restricts to a correspondence via identification of the underlying sets:

$$\text{Subgroups of } G \text{ containing } G' \leftrightarrow \text{Subrings of } L \text{ containing } L'$$

   Note, however, that each individual instance of this correspondence is *not* an instance of the Baer correspondence. Rather, it would be an instance of the generalization of the Baer correspondence described in Section 5.3.2.

4. The center $Z(G)$ is in abelian Lie correspondence as well as in Baer correspondence with the center $Z(L)$. Note that the claim has two parts:

   (a) $Z(G)$ and $Z(L)$ have the same underlying set: This follows from the fact that the commutator map of G coincides with the Lie bracket map of L, so the set of elements whose commutator with every element of G is the identity element coincides with the set of elements whose Lie bracket with every element of L is the zero element.

   (b) Both $Z(G)$ and $Z(L)$ are 2-powered, so that we can apply the Baer correspondence: This follows from Lemmas 4.1.5 and 4.2.3.

5. The inner automorphism group $G/Z(G)$ is in abelian Lie correspondence as well as in Baer correspondence with the inner derivation Lie ring $L/Z(L)$. This follows from the preceding point about $Z(G)$ being in correspondence with $Z(L)$ and the observations made regarding subgroups and quotients in Section 5.2.1.

6. The derived subgroup G' is in abelian Lie correspondence as well as in Baer correspondence with the derived subring L'. Note that the claim has two parts:

   (a) G' and L' have the same underlying set: The commutator map in G coincides with the Lie bracket map in L, so the set of commutators in G coincides with the set of elements in L that can be expressed as Lie brackets. We know that both G' is an abelian group and L' is an abelian Lie ring, because both G and L have class two. By point (2) above, G' and L' are in abelian Lie correspondence and have the same underlying set.

   (b) G' and L' are both 2-powered: This follows from Theorem 4.1.20 and Lemma 4.2.8 respectively.

7. The abelianization $G^{\text{ab}} = G/G'$ is in abelian Lie correspondence as well as in Baer correspondence with the abelianization $L^{\text{ab}} = L/L'$. This follows from the preceding point and the observations regarding subgroups and quotients in Section 5.2.1.

8. The abelian subgroups of G that contain G' and are contained in $Z(G)$ are in abelian Lie correspondence with the abelian subgroups of L that contain L' and are contained in $Z(L)$. Moreover, the corresponding quotient group is in abelian Lie correspondence with the corresponding quotient ring.

5.2.7 Cyclic subgroups, preservation of element orders, and the parallels with one-parameter subgroups

We noted in Section 5.2.6 that given a group G and a Lie ring L that are in Baer correspondence, we obtain a correspondence, with each instance also an instance of the abelian Lie correspondence:

$$\text{Abelian subgroups of } G \leftrightarrow \text{Abelian subrings of } L$$

In particular, we get a correspondence:

$$\text{Cyclic subgroups of } G \leftrightarrow \text{Cyclic subrings of } L$$

Another way of framing this is that the additive group of L and the group G have the same cyclic subgroup structure. In other words, the map $\exp : L \to G$ restricts to an isomorphism on cyclic subgroups of the additive group of L. Some of the generalizations of the Baer correspondence, including all those described in the next section, continue to have this property, so that the remarks of the next paragraph apply to these generalizations.

For any element of the common underlying set, its order as an element of the additive group of L is the same as its order as an element of G. In the case that the common underlying set of G and L is finite, this translates to the requirement that for every positive integer d, the number of elements of G of order d equals the number of elements of the additive group of L as order d. In particular, we obtain that the order *statistics* of G (information about how many elements are there of any given order) coincide with the order statistics of some abelian group. When considering whether a group G can participate in a potential generalization of the Baer correspondence, this condition serves as a potential filter.

The Baer correspondence for cyclic subgroups and subrings is closely related to the correspondence between one-dimensional subspaces of the real Lie algebra and one-parameter subgroups of the real Lie group under the Lie correspondence described in Section 1.1.3 (we did not describe one-parameter subgroups there).

5.2.8 Inner automorphisms and inner derivations

Supose G is a Baer Lie group and L is the corresponding Baer Lie ring. Under the Baer correspondence, $Z(G)$ is in Baer correspondence (and hence also in abelian Lie correspondence) with $Z(L)$, and the quotient group $G/Z(G) \cong \mathrm{Inn}(G)$ is in Baer correspondence (and hence also in abelian Lie correspondence) with the quotient Lie ring $L/Z(L) \cong \mathrm{Inn}(L)$. The former gives the inner automorphisms of the group G (that are hence also automorphisms of L). The latter gives the inner derivations of L.

Consider an element $x \in G$ with image $\overline{x}$ in the common underlying set of $G/Z(G)$ and $L/Z(L)$. We would like to understand the relationship between these two set maps from L to L:

- The inner automorphism corresponding to $\overline{x}$, i.e., the map $g \mapsto xgx^{-1}$, now viewed as a automorphism *of* L as a Lie ring. As noted in Section 5.1.8, the automorphisms of L as a Lie ring coincide with the automorphisms of G as a group. We will denote this map as Ad_x.
- The inner derivation corresponding to $\overline{x}$, i.e., the map $g \mapsto [x, g]$ where $[\ ,\ ]$ denotes the Lie bracket. We will denote this map as ad_x. Derivations and inner derivations are discussed in more detail in the Appendix, Sections A.1.7 and A.1.8.

We first work out the set map Ad_x in terms of the Lie ring operations.

$$\mathrm{Ad}_x(g) = xgx^{-1} = \left(x + g + \frac{1}{2}[x, g]\right) x^{-1}$$

This simplifies to:

$$\mathrm{Ad}_x(g) = x + g + \frac{1}{2}[x, g] + (-x) + \left[\left(x + g + \frac{1}{2}[x, g]\right), -x\right]$$

This simplifies to:

$$\mathrm{Ad}_x(g) = g + [x, g]$$

or equivalently:

$$\mathrm{Ad}_x(g) = g + \mathrm{ad}_x(g)$$

If we view both Ad_x and ad_x as elements of the ring $\mathrm{End}_{\mathbb{Z}}(L)$ of endomorphisms of the underlying *additive group* of L, then we can write the above relationship as:

$$\mathrm{Ad}_x = 1 + \mathrm{ad}_x$$

The expression for Ad_x in terms of ad_x is a truncated form of the power series for the exponential function. It turns out that this is not a coincidence. We will see in Section 6.6.9 that for the Malcev and Lazard correspondences, $\mathrm{Ad}_x = \exp(\mathrm{ad}_x)$.

5.3 Generalizations of the Baer correspondence: relaxing the definitions

In the construction of the Baer Lie ring and Baer Lie group from one another, we did not use the existence of unique square roots in the whole group or Lie ring. Rather, we only made use of the fact that we be able to make sense of the expression $\sqrt{[x, y]}$ when going from groups to Lie rings and of the expression $\frac{1}{2}[x, y]$ when going from Lie rings to groups, and further, that the outputs of these expressions land in the respective centers.

5.3.1 Generalization that allows for division within the lower central series

This generalization is a correspondence:

Groups of nilpotency class (at most) two where the derived subgroup is 2-powered $\leftrightarrow$ Lie rings of nilpotency class (at most) two where the derived subring is 2-powered

Note that this correspondence has the advantage of including as subcorrespondences *both* the abelian Lie correspondence *and* the Baer correspondence.

This correspondence behaves nicely in a number of ways:

- *Isomorphism of categories*: We can define log and exp functors and obtain an isomorphism of categories between the full subcategories of the category of groups and category of Lie rings as described above. We can then deduce consequences similar to those described for the Baer correspondence in Section 5.1.8.

- *Subgroups and subrings*: A subgroup of a group in this subcategory need not be in the subcategory. However, if we do restrict to subgroups that satisfy the condition for being in the category, we can deduce results analogous to the results stated for subgroups in Section 5.2.1. Note in particular that the correspondence between subgroups and subrings here includes two subcorrespondences:

$$\text{Abelian subgroups} \leftrightarrow \text{Abelian subrings}$$

$$\text{Baer Lie subgroups} \leftrightarrow \text{Baer Lie subrings}$$

- *Direct products*: Direct products on the group side correspond with direct products on the Lie ring side. The statement is similar to that for the abelian Lie correspondence (as described in Section 1.3.7) and the Baer correspondence (as described in Section 5.2.1).

However, the categories in question are *not* well-behaved with respect to the relation between subgroups and quotients. Explicitly, it is possible to have a group in the category and a normal subgroup that is also in the category, but such that the quotient group is not in the category. For instance, consider the case that $G = UT(3, \mathbb{Q})$ and H is a copy of $\mathbb{Z}$ in the center. Then, both G and H are objects of the category, and H is normal in G, but the quotient group G/H is not an object of the category.

5.3.2 Generalization that allows for division starting in the lower central series and ending in the upper central series

This generalization is a correspondence:

Groups of nilpotency class (at most) two where every element of the derived subgroup has a unique square root in the center $\leftrightarrow$ Lie rings of nilpotency class (at most) two where every element of the derived subring has a unique half in the center.

Note that the "unique square root in the center" clause could be interpreted in two ways: one could understand it to mean that there is a unique square root in the whole group that happens to be in the center, or one could understand it to mean that there is a unique square root among the elements in the center. However, for nilpotent groups, these are equivalent. If every element of the derived subgroup has a unique square root among elements of the center, then in particular the identity element has a unique square root among elements in the center, so the center is 2-torsion-free. Thus. by Theorem 4.1.14, the whole group is 2-torsion-free, so the squaring map is injective on the whole group.

Similarly, both ways of interpreting "unique half in the center" on the Lie ring side are equivalent to each other.

Note also that by Lemma 4.1.5, the condition on the group side can be reformulated as "group of nilpotency class (at most) two where every element of the derived subgroup has a unique square root in the whole group." A similar reformulation is possible on the Lie ring side by Lemma 4.2.3.

The correspondence is nice in a number of ways:

- *Isomorphism of categories*: We can define log and exp functors and obtain an isomorphism of categories between the full subcategories of the category of groups and category of Lie rings as described above. We can then deduce consequences similar to those described for the Baer correspondence in Section 5.1.8.
- *Subgroups and subrings*: A subgroup of a group in this subcategory need not be in

the subcategory. However, if we do restrict to subgroups that satisfy the condition for being in the category, we can deduce results analogous to the results stated for subgroups in Section 5.2.1.

- *Direct products*: Direct products on the group side correspond with direct products on the Lie ring side. The statement is similar to that for the abelian Lie correspondence (as described in Section 1.3.7) and the Baer correspondence (as described in Section 5.2.1).

However, the categories in question are *not* well-behaved with respect to the relation between subgroups and quotients. Explicitly, it is possible to have a group in the category and a normal subgroup that is also in the category, but such that the quotient group is not in the category. For instance, consider the case that $G = UT(3, \mathbb{Q})$ and H is a copy of $\mathbb{Z}$ in the center. Then, both G and H are objects of the category, and H is normal in G, but the quotient group G/H is not an object of the category.

5.3.3 Incomparability of the generalizations

Neither of the two preceding generalizations contains the other. Explicitly:

- Any abelian group with 2-torsion would be covered under the first generalization (described in Section 5.3.1) but not the second (described in Section 5.3.2).
- An example of a group that would be covered under the second generalization but not the first is the group $UT(3, \mathbb{Z}) *_{\mathbb{Z}} \mathbb{Q}$ where $*$ denotes the central product where we identify the center of $UT(3, \mathbb{Z})$ with a copy of $\mathbb{Z}$ in $\mathbb{Q}$.

There are generalizations that are strictly more general than both the above generalizations. We consider one such generalization below.

5.3.4 The divided Baer correspondence: a generalization that uses additional structure

This generalization of the Baer correspondence involves specifying additional structure on the Lie ring and on the group. *We use new terminology in this section. However, the results of this section are not necessary for our main results, and the terminology used here is not required for our main results.*

Definition (Baer-divided Lie group)**.** A *Baer-divided Lie group* is a group G of nilpotency class at most two equipped with an alternating $\mathbb{Z}$-bilinear map $\{,\} : G \times G \to G$ (i.e., the map is a homomorphism in each coordinate holding the other coordinate fixed, and $\{x, x\} = 1$ for all $x \in G$) such that the following hold:

1. $\{x, y\}^2 = [x, y]$ for all $x, y \in G$, where $[x, y]$ denotes the group commutator.
2. $\{\{x, y\}, z\}$ is the identity element of G for all $x, y, z \in G$.

Definition (Baer-divided Lie ring)**.** A *Baer-divided Lie ring* is a Lie ring L (with Lie bracket denoted $[\ ,\ ]$) equipped with an alternating $\mathbb{Z}$-bilinear map $\{,\} : L \times L \to L$ such that the following hold:

1. $2\{x, y\} = [x, y]$ for all $x, y \in L$.
2. $\{,\}$ also defines a Lie bracket on the additive group of L, and the corresponding Lie ring has nilpotency class two.

In particular, the original Lie ring L with Lie bracket $[\ ,\ ]$ is also a Lie ring of nilpotency class at most two.

We can now define the *divided Baer correspondence* as a correspondence:

$$\text{Baer-divided Lie groups} \leftrightarrow \text{Baer-divided Lie rings}$$

In the direction from the group to the Lie ring, the correspondence uses the formula:

$$x + y := \frac{xy}{\{x, y\}}$$

and:

$$[x, y] = [x, y]_{\text{Group}}$$

In the direction from the Lie ring to the group, the correspondence uses the formula:

$$xy := x + y + \{x, y\}$$

In other words, the roles of $\frac{1}{2}[x, y]$ and $\sqrt{[x, y]}$ are taken over by the operation $\{x, y\}$ (of the group or the Lie ring). The key difference is that this operation is an *additional structure specified* rather than being purely dependent on the group or Lie ring as an abstract structure.

The Baer correspondence and the generalizations of it described earlier can be reframed in terms of the divided Baer correspondence as follows:

1. In the case of the Baer correspondence, as well as in the generalization described in Section 5.3.2, there is a *unique* possibility for $\{x, y\}$. In fact, in the Baer correspondence as well as the generalization, the uniqueness is at the level of *elements*: every element of the form $[x, y]$ has a unique square root or half. Note that there could be situations that fall outside this generalization where there is a unique possibility for $\{x, y\}$, even though individual elements in the derived subgroup (respectively, derived subring) have non-unique halves, as discussed in the example of $UT(3, \mathbb{Z}[1/2]) \times \mathbb{Z}/2\mathbb{Z}$ below.

2. In the case of the generalization described in Section 5.3.1, the possibility for $\{x, y\}$ need not be unique. Nonetheless, there is a particular *canonical* choice we can make

for $\{x, y\}$, namely the unique option available *within* the deried subgroup or derived subring.

Below, we describe some examples of the divided Baer correspondence.

1. The case $G = UT(3, \mathbb{Q})/\mathbb{Z}$ and $L = NT(3, \mathbb{Q})/\mathbb{Z}$: G is the group described as Example (3) in the counterexample list in Section 4.1.13 and L is the Lie ring described in Example (3) in the counterexample list in Section 4.2.6.

   In this case, G is not a Baer Lie group and L is not a Baer Lie ring, because neither G nor L is 2-powered. However, we can give G the structure of a Baer-divided Lie group as follows. Note that $Z(G) = G'$ is isomorphic to the subgroup $\mathbb{Q}/\mathbb{Z}$ in G, and $G/Z(G) = G/G'$ is isomorphic to $\mathbb{Q} \times \mathbb{Q}$. The commutator map $G/Z(G) \times G/Z(G) \to G'$ can be described as the composite of the maps:

$$(\mathbb{Q} \times \mathbb{Q}) \times (\mathbb{Q} \times \mathbb{Q}) \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$$

   where the map on the left is given by:

$$((a_1, b_1), (a_2, b_2)) \mapsto a_1b_2 - a_2b_1$$

   and the map $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ is the quotient map.

   There is a canonical choice of half for this map, namely, the composite:

$$(\mathbb{Q} \times \mathbb{Q}) \times (\mathbb{Q} \times \mathbb{Q}) \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$$

   where the first map is:

$$((a_1, b_1), (a_2, b_2)) \mapsto \frac{1}{2}(a_1b_2 - a_2b_1)$$

Note that we circumvent the problem of non-unique halves in the derived subgroup or subring by performing the halving in an intermediate group (namely $\mathbb{Q}$) through which we factor the map.

Similar observations hold on the Lie ring side.

2. The case $G = UT(3, \mathbb{Z}[1/2]) \times \mathbb{Z}/2\mathbb{Z}$ and $L = NT(3, \mathbb{Z}[1/2]) \times \mathbb{Z}/2\mathbb{Z}$: Note that this case actually falls under the earlier generalization described in Section 5.3.1. One interesting feature of this example is that although in general the choice of half is non-unique when the center has 2-torsion, in this case, there is a unique choice of divided Baer structure. Explicitly, each element of the derived subgroup has two halves: a half inside the first direct factor, and a half that has a nontrivial second coordinate. However, a linear choice of $\{,\}$ requires that we choose each half inside the first direct factor. Similar observations hold on the Lie ring side.

3. The case where G and L are as follows:

$$G = \langle a, b, c \mid a^4 = b^4 = c^4 = 1, ab = ba, ac = ca, [b, c] = a^2\rangle$$

$$L = \langle a, b, c \mid 4a = 4a = 4c = 0, [a, b] = 0, [a, c] = 0, [b, c] = 2a\rangle$$

In this case, $Z(G) = \langle a\rangle$ and $G' = \langle a^2\rangle$. $Z(G)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ and G' is the unique subgroup of order two. We can define $\{,\}$ as $\{b, c\} = a$ with the rest of the definition following from that. Note that this is not the unique choice of $\{\ ,\ \}$, because we could choose $\{b, c\} = a^{-1}$ as well. However, it is a choice that works.

A similar construction works for L, and the divided Baer correspondence between G and L works as expected.

5.3.5 *Category-theoretic perspective on the divided Baer correspondence*

The Baer-divided Lie groups form a category as follows:

- The objects of the category are Baer-divided Lie groups.
- For Baer-divided Lie groups G_1 and G_2, the morphisms from G_1 to G_2 are group homomorphisms $\varphi : G_1 \to G_2$ satisfying the additional condition $\varphi(\{x, y\}) = \{\varphi(x), \varphi(y)\}$ for all $x, y \in G_1$. Note that in the case that $\{\ ,\ \}$ is defined canonically in terms of the group operations, the additional condition is satisfied for *all* group homomorphisms.

We can similarly define a category of Baer-divided Lie rings. The divided Baer correspondence defines an isomorphism of categories between the category of Baer-divided Lie groups and the category of Baer-divided Lie rings.

There is a natural forgetful functor from the category of Baer-divided Lie groups to the category of groups. This functor forgets the $\{\ ,\ \}$-structure and simply stores the underlying group structure. This forgetful functor is faithful but not full: there may well be homomorphisms between groups that do not preserve the $\{\ ,\ \}$-structure. The functor is not injective or surjective on objects. It is not injective because there exist groups with multiple possibilities for $\{\ ,\ \}$. It is not surjective, even to the subcategory of groups of nilpotency class two, because there exist such groups for which there is no possible $\{\ ,\ \}$-structure.

The following are true.

- If G is a Baer Lie group, or more generally, a group that fits the generalization described in Section 5.3.2, then the functor is injective to G, i.e., there is a unique Baer-divided Lie group structure on G. Further, if G_1 and G_2 are two such groups, then all homomorphisms between them are realized as Baer-divided Lie group homomorphisms, so the functor behaves as a full functor if we restrict to such groups.
- If G fits the generalization described in Section 5.3.1, then the functor need not be injective to G, but there does exist a canonical choice of Baer-divided Lie group structure

on G. In other words, if we restrict attention to the subcategory of groups described in Section 5.3.1, we can obtain a functor from this subcategory to the category of Baer-divided Lie groups that is a one-sided inverse to the forgetful functor.

Analogous observations hold on the Lie ring side.

5.3.6 The case of finite p-groups

Note that for odd primes p, p-groups of class two and p-Lie rings of class two fall in the domain of the Lazard correspondence, and we do not need to rely on any of the generalizations. The case $p = 2$ is interesting. In this case, the following are true:

- The generalization described in Section 5.3.1 applies only to abelian 2-groups and abelian 2-Lie rings, and not to any others.
- The generalization described in Section 5.3.2 does not apply to any nontrivial 2-groups or nontrivial 2-Lie rings, because the center is nontrivial and hence is not 2-powered.
- The divided Baer correspondence generalization applies to some but not all 2-groups of class two. Explicitly, a necessary but not sufficient condition for a group G to be the underlying group of a Baer-divided Lie group is that $G' \subseteq \mho^1(Z(G))$, where $\mho^1(Z(G))$ denotes the set of squares of elements in $Z(G)$. A similar necessary but not sufficient condition exists on the Lie ring side.

5.4 Baer correspondence up to isoclinism

The concept of "Baer correspondence up to isoclinism" is a novel contribution of this thesis. Many of the results in this section are based on joint work with John Wiltshire-Gordon.

5.4.1 Motivation

In Section 5.2.6, we noted that if G and L are in Baer correspondence, the subgroups of G that contain G' and are contained in $Z(G)$ are in abelian Lie correspondence with the subrings of L that contain L' and are contained in $Z(L)$. Further, for each such subgroup and subring in correspondence, the associated quotient group and quotient ring are also in abelian Lie correspondence. In other words, we can build the group G as a central extension of groups, and the Lie ring L as a central extension of Lie rings, where the central subgroup of G is in abelian Lie correspondence with the central subring of L, and the quotient group of G is in abelian Lie correspondence with the quotient ring of L.

We describe two extreme cases below.

1. The case where the subgroup is $Z(G)$ and the subring is $Z(L)$. We can depict this case as follows:

$$\begin{array}{ccccccccc} 0 \to & Z(G) \to & G \to & G/Z(G) \to & 1 \\ & \downarrow^{\log} & \downarrow^{\log} & \downarrow^{\log} & \\ 0 \to & Z(L) \to & L \to & L/Z(L) \to & 0 \end{array}$$

   Note that the log connecting G and L arises from the Baer correspondence. The log connecting $Z(G)$ with $Z(L)$, and the log connecting $G/Z(G)$ with $L/Z(L)$, can be viewed as arising both from the Baer correspondence and from the abelian Lie correspondence, as described in Section 5.2.6.

2. The case where the subgroup is G' and the subring is L'. We can depict this case as follows:

$$\begin{array}{ccccccccc} 0 & \to & G' & \to & G & \to & G/G' \to & 1 \\ & & \downarrow^{\log} & & \downarrow^{\log} & & \downarrow^{\log} & \\ 0 & \to & L' & \to & L & \to & L/L' \to & 0 \end{array}$$

An analogous observation to the note in point (1) above applies here, with $Z(G)$, $Z(L)$, $G/Z(G)$, and $L/Z(L)$ replaced by G', L', G/G', and L/L' respectively.

Our aim is to generalize the Baer correspondence to a situation where the middle downward arrow (connecting G with L) is missing, but we still have an abelian Lie correspondence between the central subgroup and central subring, an abelian Lie correspondence between the quotient group and quotient ring, and a condition to the effect that the commutator map on the group side looks the same as the Lie bracket map on the Lie ring side.

5.4.2 Definition of the correspondence

The Baer correspondence up to isoclinism is a correspondence that we will define between the following two sets:

Equivalence classes up to isoclinism of groups of nilpotency class at most two $\leftrightarrow$ Equivalence classes up to isoclinism of Lie rings of nilpotency class at most two

Suppose G is a group of nilpotency class at most two and L is a Lie ring of nilpotency class at most two. A *Baer correspondence up to isoclinism* between G and L is a pair (ζ, φ) where:

- ζ is an isomorphism from the abelian group $\mathrm{Inn}(G)$ to the abelian group that is the additive group $\exp(\mathrm{Inn}(L))$ of $\mathrm{Inn}(L)$, and
- φ is an isomorphism from the abelian group G' to the abelian group that is the additive group $\exp(L')$ of L',

such that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Inn}(G) \times \mathrm{Inn}(G) & \stackrel{\zeta \times \zeta}{\to} & \exp(\mathrm{Inn}(L)) \times \exp(\mathrm{Inn}(L)) \\ \downarrow^{\omega_G} & & \downarrow^{\exp(\omega_L)} \\ G' & \stackrel{\varphi}{\to} & \exp(L') \end{array}$$

where ω_G is the map $\mathrm{Inn}(G) \times \mathrm{Inn}(G) \to G'$ obtained from the commutator map on G, and ω_L is the map $\mathrm{Inn}(L) \times \mathrm{Inn}(L) \to L'$ obtained from the Lie bracket on L. We had introduced the notation for the maps ω_G and ω_L in Sections 2.1 and 2.2.

We say that G and L are *in Baer correspondence up to isoclinism* if there exists a Baer correspondence up to isoclinism between G and L.

The following are easy to verify. All the groups and Lie rings referred to below are of nilpotency class at most two. The proofs of all the assertions below rely on a similar commutative diagram setup to the setup used in Section 2.1.3 to prove that a composite of homoclinisms is a homoclinism.

- If G_1 and G_2 are isoclinic groups, and G_1 and L are in Baer correspondence up to isoclinism, then G_2 and L are also in Baer correspondence up to isoclinism.
- If L_1 and L_2 are isoclinic Lie rings, and G and L_1 are in Baer correspondence up to isoclinism, then G and L_2 are also in Baer correspondence up to isoclinism.
- If G_1 and G_2 are groups and L is a Lie ring such that G_1 is in Baer correspondence up to isoclinism with L and G_2 is also in Baer correspondence up to isoclinism with L, then G_1 and G_2 are isoclinic.
- If L_1 and L_2 are Lie rings and G is a group such that G is in Baer correspondence up to isoclinism with L_1 and G is in Baer correspondence up to isoclinism with L_2, then L_1 and L_2 are isoclinic Lie rings.

In other words, the definition we gave above establishes a correspondence between *some* equivalences classes up to isoclinism of groups and *some* equivalence classes up to isoclinism of Lie rings. However, it is not yet clear that the correspondence applies to *every* equivalence class up to isoclinism of groups and to *every* equivalence class up to isoclinism of Lie rings. Essentially, we need to show two things:

1. For every group G of nilpotency class at most two, there exists a Lie ring L of nilpotency class at most two such that G is in Baer correspondence up to isoclinism with L.

2. For every Lie ring L of nilpotency class at most two, there exists a group G of nilpotency class at most two such that G is in Baer correspondence up to isoclinism with L.

(1) is relatively easy to show: we can take the associated graded Lie ring of a group. (2) is harder to show. We will now discuss some ideas related to group extension theory that will help us establish both (1) and (2) in a better way.

5.4.3 Exterior square for an abelian group

Suppose G is an abelian group. Then, the following are canonically isomorphic:

1. The exterior square $G \wedge_{\mathbb{Z}} G$ of G as an abelian group.

2. The exterior square $G \wedge G$ of G as a group (as defined in section 3.4.1). The map in the forward direction $G \wedge_{\mathbb{Z}} G \to G \wedge G$ is as follows. Note that the commutator map in a class two group is $\mathbb{Z}$-bilinear, so that the map $G \times G \to G \wedge G$ is $\mathbb{Z}$-bilinear. Thus, it gives rise to a homomorphism $G \wedge_{\mathbb{Z}} G \to G \wedge G$.

3. The Schur multiplier $M(G)$ of G as a group.

4. The exterior square $G \wedge G$ of G as an abelian Lie ring. The exterior square is itself an abelian Lie ring with the same additive group structure. We have already described this map in Section 3.5.3.

5. The Schur multiplier $M(G)$ of G as an abelian Lie ring.

We first note the equivalence of (2) with (3) and also the equivalence of (4) with (5). For the equivalence of (2) and (3), note the canonical short exact sequence, introduced in Section 3.4.1:

$$0 \to M(G) \to G \wedge G \to [G, G] \to 1$$

Since G is abelian, $[G, G]$ is trivial and we get an isomorphism $M(G) \cong G \wedge G$.

Similarly, the equivalence of (4) with (5) follows from the analogous canonical short exact sequence for Lie rings introduced in Section 3.5.1.

It remains to show that the canonical map from (1) to (2) is an isomorphism and the canonical map from (1) to (4) is an isomorphism.

To see this, we can rely on the explicit presentations for the exterior square provided in Section 3.8.4 (for groups) and 3.9.3 (for Lie rings) to confirm that in the case that the group (respectively Lie ring) is abelian, its exterior square as a group (respectively Lie ring) agrees with its exterior square as an abelian group.

In order to better keep track of whether we are thinking of G as an abelian group or as an abelian Lie ring, it may sometimes help to use the log and exp functors of the abelian Lie correspondence (as described in Section 1.3) to go back and forth between the descriptions. With this language, we can rewrite the above results in the form:

- For any abelian group G, $\log(G \wedge G)$ is canonically isomorphic to $\log G \wedge \log G$, where the $\wedge$ on the left represents the exterior square as a group and the $\wedge$ on the right represents the exterior square as a Lie ring.
- For any abelian Lie ring L, $\exp(L \wedge L)$ is canonically isomorphic to $\exp L \wedge \exp L$ where the $\wedge$ on the left represents the exterior square as a Lie ring and the $\wedge$ on the right represents the exterior square as a group.

5.4.4 Description of central extensions for an abelian group

Suppose A and G are abelian groups. Recall from Section 3.1.5 that $H^2(G; A)$, termed the *second cohomology group for trivial group action* of G on A, is a group whose elements correspond with the central extensions with central subgroup A and quotient group G.

We are now assuming that G is abelian. Hence, all the extension groups have nilpotency class at most two. Further, $G^{\text{ab}} = G$ and $M(G) = G \wedge G$ as discussed. Thus, the short exact sequence described in Section 3.6.4 simplifies to:

$$0 \to \operatorname{Ext}^1_{\mathbb{Z}}(G; A) \to H^2(G; A) \to \operatorname{Hom}(G \wedge G, A) \to 0 \tag{5.1}$$

The short exact sequence splits (but not necessarily canonically) and we get:

$$H^2(G; A) \cong \operatorname{Ext}^1_{\mathbb{Z}}(G; A) \oplus \operatorname{Hom}(G \wedge G, A)$$

We will now proceed to explain the meaning of the short exact sequence in this context.

Description of the left map of the sequence

The map:

$$\operatorname{Ext}^1_{\mathbb{Z}}(G; A) \to H^2(G; A)$$

can be interpreted as follows. The underlying set of the group on the left is canonically identified with the set of all *abelian* group extensions with subgroup A and quotient group G. The group on the right is the group whose elements are all the *central* extensions with central subgroup A and quotient group G. Every abelian group extension is a central extension, and there is therefore a canonical injective set map from $\operatorname{Ext}^1_{\mathbb{Z}}(G; A)$ to $H^2(G; A)$. This set map turns out to be a *group homomorphism* based on the way the group structures on $\operatorname{Ext}^1_{\mathbb{Z}}(G; A)$ and $H^2(G; A)$ are defined. Delving into the group structure on $\operatorname{Ext}^1_{\mathbb{Z}}(G; A)$ will be too much of a diversion from our goal here, so we skip it.

The image of the map is described as precisely the set of those cohomology classes whose representative 2-cocycles are *symmetric*, i.e., any 2-cocycle f in that cohomology class satisfies the property that $f(x, y) = f(y, x)$ for all $x, y \in G$. This can be easily deduced from the discussion in Section 3.3.3.

Description of the right map of the sequence

The map:

$$H^2(G; A) \to \mathrm{Hom}(G \wedge G, A)$$

can be described as follows. For any group extension E, the commutator map $E \times E \to E$ descends to a set map:

$$\omega_{E,G} : G \times G \to A$$

Our earlier definition of $\omega_{E,G}$ defined it as a map to $[E, E]$, but $[E, E]$ lies in the image of A (under the inclusion of A in E), so it can be viewed as a map to A.

Note that the image of the map is in A *because* G is abelian. Further, $\omega_{E,G}$ is bilinear, because the image of the map is central. It thus defines a group homomorphism $G \wedge G \to A$.

The homomorphism above can also be described in terms of the how it operates at the level of 2-cocycles (this description requires understanding the explicit description of the second cohomology group using the bar resolution, as given in Section 3.3). Explicitly, the map:

$$H^2(G; A) \to \mathrm{Hom}(G \wedge G, A)$$

arises from a homomorphism:

$$Z^2(G; A) \to \mathrm{Hom}(G \wedge G, A)$$

given by:

$$f \mapsto \mathrm{Skew}(f)$$

where $\mathrm{Skew}(f)$ is the map $(x, y) \mapsto f(x, y) - f(y, x)$.

Intuitively, this is because the commutator of two elements represents the distance between their products in both possible orders, i.e., $[x, y]$ is the quotient $(xy)/(yx)$. Whether we use left or right quotients does not matter because the group has class two.

Based on the discussion in Section 3.6.2, the homomorphism:

$$H^2(G; A) \to \mathrm{Hom}(G \wedge G, A)$$

classifies extensions *up to isoclinism of group extensions.* In other words, the fibers for this map are precisely the equivalence classes up to isoclinism of group extensions.

5.4.5 Description of central extensions for an abelian Lie ring

Suppose A and L are abelian Lie rings. Recall that $H^2_{\mathrm{Lie}}(L; A)$, called the *second cohomology group for trivial Lie ring action*, is a group whose elements correspond to the congruence classes of central extensions with central subring A and quotient Lie ring L.

We are now assuming that L is abelian. Hence, $L^{\mathrm{ab}} = L$ and $M(L) = L \wedge L$. The short exact sequence of Section 3.7.4 simplifies to:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(L; A) \to H^2_{\mathrm{Lie}}(L; A) \to \mathrm{Hom}(L \wedge L, A) \to 0 \tag{5.2}$$

The short exact sequence splits *canonically*, and we get a canonical isomorphism:

$$H^2_{\mathrm{Lie}}(L; A) \cong \mathrm{Ext}^1_{\mathbb{Z}}(L; A) \oplus \mathrm{Hom}(L \wedge L, A)$$

Note that L being abelian is crucial to the splitting being canonical. We will understand the splitting in more detail, but first we need to explain what the maps are.

Description of the left map of the sequence

The map:

$$\mathrm{Ext}^1_{\mathbb{Z}}(L; A) \to H^2_{\mathrm{Lie}}(L; A)$$

can be described as follows. The group on the left is canonically identified with the *abelian* Lie rings arising as extensions with subring A and quotient ring L. The group on the right is canonically identified with the *central* extensions with subring A and quotient ring L. Every abelian Lie ring extension is a central extension, and there is therefore a canonical injective set map from $\mathrm{Ext}^1_{\mathbb{Z}}(L; A)$ to $H^2_{\mathrm{Lie}}(L; A)$. This set map turns out to be a *group homomorphism* based on the way the group structures on $\mathrm{Ext}^1_{\mathbb{Z}}(L; A)$ and $H^2_{\mathrm{Lie}}(L; A)$ are defined. Delving into the group structure on $\mathrm{Ext}^1_{\mathbb{Z}}(L; A)$ will be too much of a diversion from our goal here, so we skip it.

Description of the right map of the sequence

The map:

$$H^2_{\mathrm{Lie}}(L; A) \to \mathrm{Hom}(L \wedge L, A)$$

is defined as follows. For any extension Lie ring M, consider the Lie bracket $M \times M \to M$. This descends to a $\mathbb{Z}$-bilinear map:

$$\omega_M : L \times L \to A$$

Note that the image is in A because L is abelian. The map can be viewed as a homomorphism from $L \wedge L$ to A, and hence as an element of $\mathrm{Hom}(L \wedge L, A)$.

Note also that, per the discussion in Section 3.7.2, this homomorphism classifies the extension *up to isoclinism of Lie ring extensions.* In other words, the fibers of this map are precisely the equivalence classes up to isoclinism of Lie ring extensions.

Canonical splitting

We will now describe how the short exact sequence below splits:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(L; A) \to H^2_{\mathrm{Lie}}(L; A) \to \mathrm{Hom}(L \wedge L, A) \to 0$$

We can describe the splitting either by specifying the projection $H^2_{\mathrm{Lie}}(L; A) \to \mathrm{Ext}^1_{\mathbb{Z}}(L; A)$ or by specifying the inclusion $\mathrm{Hom}(L \wedge L, A) \to H^2_{\mathrm{Lie}}(L; A)$. We do both.

The projection:

$$H^2_{\mathrm{Lie}}(L; A) \to \mathrm{Ext}^1_{\mathbb{Z}}(L; A)$$

is defined as follows. For any extension Lie ring M, map it to the extension Lie ring that is *abelian* as a Lie ring and has the same additive group as M. In other words, keep the additive structure intact, but "forget" the Lie bracket.

The inclusion:

$$\mathrm{Hom}(L \wedge L, A) \to H^2_{\mathrm{Lie}}(L; A)$$

is defined as follows. Given a bilinear map $b : L \times L \to A$, define the extension Lie ring as a Lie ring M whose additive group is $L \oplus A$, and where the Lie bracket is:

$$[(x_1, y_1), (x_2, y_2)] = [0, b(x_1, x_2)]$$

In other words, we use the direct sum for the additive structure, and use the bilinear map to define the Lie bracket.

In light of this, we can think of the direct sum decomposition as follows:

$$H^2_{\mathrm{Lie}}(L; A) \cong \mathrm{Ext}^1_{\mathbb{Z}}(L; A) \oplus \mathrm{Hom}(L \wedge L, A)$$

The projection onto the first component stores the additive structure of the Lie ring, while destroying, or forgetting, the Lie bracket. The projection onto the second component preserves the Lie bracket while replacing the additive structure with a direct sum of L and A. Note also that the latter projection is equivalent to passing to the associated graded Lie ring. The associated graded Lie ring is discussed in more detail in the Appendix, Sections A.4.3, A.4.4, and A.4.5.

5.4.6 The Baer correspondence up to isoclinism for extensions

Suppose A and G are abelian groups. Denote by L the abelian Lie ring whose additive group is G. In other words, $L = \log G$ under the abelian Lie correspondence described in Section 1.3.

We abuse notation regarding A, using the same letter A to denote the abelian group and the abelian Lie ring, which might more properly be written as $\log A$ when viewed as a Lie ring. We engage in this abuse because, throughout this document, we deal with central extensions, so that the base of the extention is always abelian. We do not abuse notation when dealing with G and L, because the distinction will be helpful when we describe our later generalization, the Lazard correspondence up to isoclinism, in Section 7.7.

We have discussed above two short exact sequences:

$$0 \to \operatorname{Ext}^1_{\mathbb{Z}}(G; A) \to H^2(G; A) \to \operatorname{Hom}(G \wedge G, A) \to 0$$

and

$$0 \to \operatorname{Ext}^1_{\mathbb{Z}}(L; A) \to H^2_{\text{Lie}}(L; A) \to \operatorname{Hom}(L \wedge L, A) \to 0$$

We have canonical isomorphisms between the left terms of the exact sequences and between the right terms of the exact sequences:

$$\begin{array}{ccccccccc} 0 & \to & \operatorname{Ext}^1_{\mathbb{Z}}(G;A) & \to & H^2(G;A) & \to & \operatorname{Hom}(G \wedge G, A) & \to & 0 \\ & & \downarrow & & & & \downarrow & & \\ 0 & \to & \operatorname{Ext}^1_{\mathbb{Z}}(L;A) & \to & H^2_{\text{Lie}}(L;A) & \to & \operatorname{Hom}(L \wedge L, A) & \to & 0 \end{array}$$

We now try to understand both component isomorphisms in greater detail.

The isomorphism of the Ext^1 groups on the left side, and its relation to the abelian Lie correspondence

We have a canonical isomorphism of groups:

$$\operatorname{Ext}^1_{\mathbb{Z}}(G;A) \cong \operatorname{Ext}^1_{\mathbb{Z}}(L;A)$$

This is because, although we use different symbols for G and L, they both have the same underlying additive group, and the Ext^1 computation uses only the underlying additive group.

The elements of $\operatorname{Ext}^1_{\mathbb{Z}}(G;A)$ correspond to the extension groups with subgroup A and quotient group G *where the extension group is abelian.* The elements of $\operatorname{Ext}^1_{\mathbb{Z}}(L;A)$ correspond to the extension Lie rings with subring A and quotient Lie ring L *where the extension Lie ring is abelian.* The isomorphism above therefore gives a correspondence:

Group extensions with subgroup A and quotient group G such that the extensions are abelian groups $\leftrightarrow$ Lie ring extensions with subring A and quotient ring L such that the extensions are abelian Lie rings

For each group extension and Lie ring extension that are in bijection (in other words, each pair of elements in the two isomorphic groups that are in bijection with each other), the corresponding extension group is in abelian Lie correspondence with the corresponding extension Lie ring.

The isomorphism of the Hom groups on the right side, and its relation to the Baer correspondence up to isoclinism

We have a canonical isomorphism:

$$\operatorname{Hom}(G \wedge G, A) \cong \operatorname{Hom}(L \wedge L, A)$$

We reviewed the meanings of the two groups in Sections 5.4.4 and 5.4.5. The group $\operatorname{Hom}(G \wedge G, A)$ classifies the central extensions with central subgroup A and quotient group G up to isoclinism of extension. The group $\operatorname{Hom}(L \wedge L, A)$ classifies the central extensions with central subring A and quotient Lie ring L up to isoclinism of the extension.

The two Hom groups are isomorphic because, since $L = \log G$, Section 5.4.3 tells us that the additive group of $L \wedge L$ is isomorphic to $G \wedge G$ as an abelian group. Thus, the homomorphism groups can also be identified with one another.

The isomorphism gives a correspondence:

Equivalence classes up to isoclinism of Lie ring extensions with central subring A and quotient Lie ring $L \leftrightarrow$ Equivalence classes up to isoclinism of group extensions with central subgroup A and quotient group G

Any particular instance of this bijection (i.e., an equivalence class of Lie ring extensions and an equivalence class of group extensions that are in bijection with each other) is termed a *Baer correspondence up to isoclinism for extensions*.

We now state an important lemma that relates the Baer correspondence up to isoclinism for extensions with the Baer correspondence up to isoclinism.

Lemma 5.4.1. Supose A and G are abelian groups and $L = \log G$ is the corresponding abelian Lie ring. Suppose E is a group extension with central subgroup A and quotient group G. Suppose N is a Lie ring extension with central subring $\log A$ (which we denote as A via abuse of notation) and quotient Lie ring L. Suppose further than the equivalence class up to isoclinism of the group extension E corresponds, via the above bijection, to the equivalence class of the Lie ring extension N. Then, the group E is in Baer correspondence up to isoclinism with the Lie ring N.

Proof. We have the following map induced by the commutator map in E:

$$\omega_{E,G} : G \times G \to A$$

Similarly, we have the following map induced by the Lie bracket map in N:

$$\omega_{N,L} : L \times L \to A$$

The extensions being in correspondence up to isoclinism means that $\omega_{N,L} = \log(\omega_{E,G})$, in the sense that the underlying set map of $\omega_{N,L}$ coincides with the underlying set map of $\omega_{E,G}$. Note also that the images of these maps need not be all of A. The image of the first map generates a subgroup that can be identified with E', whereas the image of the second map generates a subgroup that can be identified with the additive group of N'. Both maps coincide, so E' and N' are in abelian Lie corespondence.

The image of $Z(E)$ in G coincides with the normal subgroup $\{x \in G \mid \omega_{E,G}(x, y) = 0 \; \forall \; y \in G\}$. Similarly, the image of $Z(N)$ in L coincides with the ideal $\{x \in L \mid \omega_{N,L}(x, y) = 0 \; \forall \; y \in L\}$. The underlying sets coincide, so the normal subgroup and ideal are in abelian Lie correspondence. Thus, the quotient group of G by the image of $Z(E)$ in G is in abelian Lie correspondence with the quotient group of L by the image of $Z(N)$ in L. Thus, $E/Z(E)$ is in abelian Lie correspondence with $N/Z(N)$. Thus, the descended maps:

$$\omega_E : E/Z(E) \times E/Z(E) \to E'$$

and

$$\omega_N : N/Z(N) \times N/Z(N) \to N'$$

are in correspondence. $\square$

Relation between the middle groups

We have demonstrated the existence of canonical isomorphisms between the left groups and between the right groups in the two short exact sequences:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{Ext}^1_{\mathbb{Z}}(G;A) & \to & H^2(G;A) & \to & \mathrm{Hom}(G \wedge G, A) & \to & 0 \\ & & \downarrow & & & & \downarrow & & \\ 0 & \to & \mathrm{Ext}^1_{\mathbb{Z}}(L;A) & \to & H^2_{\mathrm{Lie}}(L;A) & \to & \mathrm{Hom}(L \wedge L, A) & \to & 0 \end{array}$$

As described in Sections 5.4.4 and 5.4.5, both short exact sequences split. Therefore, it is possible to find an isomorphism $H^2(G;A) \to H^2_{\mathrm{Lie}}(L;A)$ that establishes an isomorphism of the short exact sequences:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{Ext}^1_{\mathbb{Z}}(G;A) & \to & H^2(G;A) & \to & \mathrm{Hom}(G \wedge G, A) & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \mathrm{Ext}^1_{\mathbb{Z}}(L;A) & \to & H^2_{\mathrm{Lie}}(L;A) & \to & \mathrm{Hom}(L \wedge L, A) & \to & 0 \end{array}$$

Note, however, that the middle isomorphism is not canonical. In fact, choosing a middle isomorphism is equivalent to choosing a splitting of the top sequence. This is because the bottom sequence splits canonically, as described in Section 5.4.5. We will return to a discussion of this in Sections 5.4.8 and 5.4.9.

5.4.7 The Baer correspondence up to isoclinism for groups: filling the details

We are now in a position to flesh out the remaining details of the Baer correspondence up to isoclinism, which we defined in Section 5.4.2:

Equivalence classes up to isoclinism of groups of nilpotency class at most two $\leftrightarrow$
Equivalence classes up to isoclinism of Lie rings of nilpotency class at most two

There are two pending facts we need to establish:

1. For every group G of nilpotency class at most two, there exists a Lie ring L of nilpotency class at most two such that G is in Baer correspondence up to isoclinism with L.
2. For every Lie ring L of nilpotency class at most two, there exists a group G of nilpotency class at most two such that G is in Baer correspondence up to isoclinism with L.

We had already noted in Section 5.4.2 that (1) can be achieved by using the associated graded Lie ring for the group. We will now provide a better way to think about both (1) and (2). We will begin with (1).

Explicit construction from the group to the Lie ring

We are given a group G of nilpotency class at most two, and we need to find a Lie ring L of nilpotency class at most two such that L and G are in Baer correspondence up to isoclinism.

(a) Consider G as a central extension:

$$0 \to Z(G) \to G \to G/Z(G) \to 1$$

Consider the equivalence class up to isoclinism of this extension.

(b) Based on the discussion in Section 5.4.6, this equivalence class corresponds to an equivalence class up to isoclinism of Lie ring extensions with central subring $\log(Z(G))$ and quotient Lie ring $\log(G/Z(G))$. Let L be any extension Lie ring in this equivalence class.

(c) By Lemma 5.4.1, L and G are in Baer correspondence up to isoclinism.

Note that in this direction, one *can* make a canonical choice of L based on G, namely, one can take the associated graded ring for the central series $0 \le Z(G) \le G$. Note that this choice of L will be the same for all G in the equivalence class up to isoclinism. The ability to make a canonical choice here is related to the canonical splitting of the short exact sequence for Lie ring extensions with abelian quotient group, as discussed in Section 5.4.5.

Explicit construction from the Lie ring to the group

We are given a Lie ring L of nilpotency class at most two, and we need to find a group G of nilpotency class at most two such that L and G are in Baer correspondence up to isoclinism.

(a) Consider L as a central extension:

$$0 \to Z(L) \to L \to L/Z(L) \to 0$$

Consider the equivalence class up to isoclinism of this extension.

(b) Based on the discussion in Section 5.4.6, this equivalence class corresponds to an equivalence class up to isoclinism of group extensions with central subgroup $\exp(Z(L))$ and quotient group $\exp(L/Z(L))$. Let G be any extension group in this equivalence class.

(c) By Lemma 5.4.1, L and G are in Baer correspondence up to isoclinism.

Preservation of order

In both directions, the constructions preserve the orders. In other words, if we start with a finite group and use the construction in the direction from groups to Lie rings, the Lie ring that we obtain has the same order as the group that we started with. Similarly, if we start with a finite Lie ring and use the construction in the direction from Lie groups to groups, the group that we obtain has the same order as the Lie ring that we started with.

This does not imply that *every* group and every Lie ring that are in Baer correspondence up to isoclinism must have the same order. Rather, we are saying that the answer to the existence question continues to be affirmative even after we impose the condition that the orders have to be equal.

In particular, given a a finite 2-group of nilpotency class 2, we can find a finite 2-Lie ring (i.e., a Lie ring whose additive group is a finite 2-group) of nilpotency class 2 such that the group and Lie ring are in Baer correspondence up to isoclinism. Similarly, given a finite 2-Lie ring of nilpotency class 2, we can find a finite 2-group of nilpotency class 2 such that the group and Lie ring are in Baer correspondence up to isoclinism.

5.4.8 Relating the Baer correspondence and the Baer correspondence up to isoclinism

If a Baer Lie group G is in Baer correspondence with a Baer Lie ring L, then G and L are in Baer correspondence up to isoclinism (as defined in Section 5.4.2). Explicitly, the Baer correspondence between G and L can be used to define an isomorphism ζ between $\mathrm{Inn}(G)$ and the additive group of $\mathrm{Inn}(L)$, and also an isomorphism φ between G' and the additive group of L', satisfying the compatibility condition for being a Baer correspondence up to isoclinism.

Another way of framing this is that if we restrict attention to Baer Lie groups and Baer Lie rings, then the Baer correspondence up to isoclinism can be *refined* to a correspondence that works up to isomorphism, namely the usual Baer correspondence up to isomorphism. In fact, it can be refined even further to obtain the strict Baer correspondence between individual groups and Lie rings, as has been done in the previous two sections (Sections 5.1 and 5.2).

We now turn to how the Baer correspondence relates to the Baer correspondence up to isoclinism for group extensions. Let G and A be abelian groups, and let $L = \log G$ be the abelian Lie ring with additive group G. In Section 5.4.6, we worked out the following relation between the universal coefficient theorem short exact sequences, where the downward maps are isomorphisms:

$$\begin{array}{ccccccccc} 0 & \to & \operatorname{Ext}^1_{\mathbb{Z}}(G;A) & \to & H^2(G;A) & \to & \operatorname{Hom}(G \wedge G, A) & \to & 0 \\ & & \downarrow & & & & \downarrow & & \\ 0 & \to & \operatorname{Ext}^1_{\mathbb{Z}}(L;A) & \to & H^2_{\text{Lie}}(L;A) & \to & \operatorname{Hom}(L \wedge L, A) & \to & 0 \end{array}$$

We had also noted in Section 5.4.5 that the second short exact sequence splits canonically, i.e.,:

$$H^2_{\text{Lie}}(L;A) \cong \operatorname{Ext}^1_{\mathbb{Z}}(L;A) \oplus \operatorname{Hom}(L \wedge L, A)$$

Thus, as observed in Section 5.4.6, specifying an isomorphism between the middle groups such that the diagram commutes is equivalent to specifying a splitting of the first short exact sequence.

Now, consider the case that G and A are both 2-powered abelian groups. In that case, by Lemma 4.1.12, all the extensions with central subgroup A and quotient group G are themselves 2-powered, and are therefore Baer Lie groups. Similarly, all the extension Lie rings with central subring A and quotient Lie ring L are Baer Lie rings. Further, the Baer correspondence establishes a bijection between the group extensions and Lie ring extensions in such a manner that the diagram commutes. Equivalently, it provides a canonical splitting of the top row. Explicitly, we now obtain a commutative diagram with the middle isomorphism filled in:

$$\begin{array}{ccccccccc}
0 & \to & \mathrm{Ext}^1_{\mathbb{Z}}(G;A) & \to & H^2(G;A) & \to & \mathrm{Hom}(G \wedge G, A) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mathrm{Ext}^1_{\mathbb{Z}}(L;A) & \to & H^2_{\mathrm{Lie}}(L;A) & \to & \mathrm{Hom}(L \wedge L, A) & \to & 0
\end{array}$$

Equivalently, we have an explicit splitting:

$$H^2(G;A) \cong \mathrm{Ext}^1_{\mathbb{Z}}(G;A) \oplus \mathrm{Hom}(G \wedge G, A)$$

We will now discuss explicitly how this splitting works.

5.4.9 *Cocycle-level description of the Baer correspondence*

Suppose G and A are abelian groups (we will soon restrict to the case that one or both of G and A is 2-powered). Consider the following two short exact sequences. The first is the short exact sequence relating the coboundary, cocycle and cohomology groups, originally described in Section 3.3.4:

$$0 \to B^2(G;A) \to Z^2(G;A) \to H^2(G;A) \to 0$$

The second is the universal coefficient theorem short exact sequence, originally described in Section 3.6.4 and described specifically for abelian G in Section 5.4.4:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(G;A) \to H^2(G;A) \to \mathrm{Hom}(G \wedge G, A) \to 0$$

The first short exact sequence need not split. An example where it does not split was discussed in Section 3.3.4. The second short exact sequence does always split but the splitting need not be canonical (see Section 3.6.4).

The right parts of these short exact sequences give surjective homomorphisms, which we can compose:

$$Z^2(G; A) \to H^2(G; A) \to \mathrm{Hom}(G \wedge G, A)$$

As we discussed in Section 5.4.4, the composite of these maps is the skew map. Explicitly, the composite is the map $f \mapsto \mathrm{Skew}(f)$, that sends a function f to the function:

$$\mathrm{Skew}(f) = (x, y) \mapsto f(x, y) - f(y, x)$$

Note that the function $\mathrm{Skew}(f)$ is a $\mathbb{Z}$-bilinear map $G \times G$ to A, which can be interpreted as a homomorphism $G \wedge G \to A$.

Now, suppose that G and A are both 2-powered abelian groups. In that case, there is a canonical splitting of the composite map, given as follows:

$$f \mapsto \frac{1}{2} f$$

In other words, a $\mathbb{Z}$-bilinear map $f : G \times G \to A$ is sent to $\frac{1}{2} f : G \times G \to A$. Note that any $\mathbb{Z}$-bilinear map is a 2-cocycle (in general, any n-linear map is a n-cocycle) so this works.

In particular, *both* the short exact sequences split, and we get canonical direct sum decompositions:

$$Z^2(G; A) \cong B^2(G; A) \oplus H^2(G; A), \text{ splitting is } H^2(G; A) \to Z^2(G; A)$$

$$H^2(G; A) \cong \mathrm{Ext}^1_{\mathbb{Z}}(G; A) \oplus \mathrm{Hom}(G \wedge G, A), \text{ splitting is } \mathrm{Hom}(G \wedge G, A) \to H^2(G; A)$$

Note that the first short exact sequence need not split for all G and A (see the discussion in Section 3.3.4) and the existence of a splitting is itself a piece of information. The second short exact sequence does split for all G and A, but the splitting is not in general canonical, as discussed in Section 3.6.4, so the case where G and A are both 2-powered is special in that we obtain a *canonical* splitting.

The splitting map $\mathrm{Hom}(G \wedge G, A) \to H^2(G; A)$ is the same as the one arising from the Baer correspondence. Explicitly, as noted in Section 5.4.6, specifying the splitting map $\mathrm{Hom}(G \wedge G, A) \to H^2(G; A)$ is equivalent to specifying an isomorphism of $H^2(G; A)$ and $H^2_{\mathrm{Lie}}(L; A)$ such that the diagram below commutes:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{Ext}^1_{\mathbb{Z}}(G; A) & \to & H^2(G; A) & \to & \mathrm{Hom}(G \wedge G, A) & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \mathrm{Ext}^1_{\mathbb{Z}}(L; A) & \to & H^2_{\mathrm{Lie}}(L; A) & \to & \mathrm{Hom}(L \wedge L, A) & \to & 0 \end{array}$$

This isomorphism can be described in an alternative way. Let E be an extension group corresponding to an element of $H^2(G; A)$. Let $N = \log(E)$ via the Baer correspondence. We can relate two short exact sequences via a log functor.

$$\begin{array}{cccc} 0 \to & A \to & E \to & G \to & 1 \\ & \downarrow^{\log} & \downarrow^{\log} & \downarrow^{\log} & \\ 0 \to & A \to & N \to & L \to & 0 \end{array}$$

Note that we abuse notation again, using the same letter A for A as a group and as a Lie ring.

Then, the element of $H^2_{\mathrm{Lie}}(L; A)$ that corresponds to the second row is the same as the image of the element of $H^2(G; A)$ under the isomorphism described earlier.

5.4.10 Relaxation of the 2-powered assumption

We consider what can be said when the assumption that both G and A are 2-powered is relaxed.

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(G; A) \to H^2(G; A) \to \mathrm{Hom}(G \wedge G, A) \to 0$$

Note that if the group $\mathrm{Hom}(G \wedge G, A)$ itself is 2-powered, then the preceding construction can still be carried out, and we can obtain a splitting of the short exact sequence. The correspondence between the extension group and the extension Lie ring need no longer be an instance of the Baer correspondence. However, it will continue to be an instance of the *divided* Baer correspondence described in Section 5.3.4. Note in particular that this includes the case where the group A alone is 2-powered. It will also include the case where the group G alone is 2-powered.

In the case that $\mathrm{Hom}(G \wedge G, A)$ is not 2-powered, the preceding method for obtaining a splitting will not work. However, we know that the short exact sequence must still split. For some choices of G and A, it is possible to obtain an automorphism-invariant splitting, even though such a splitting does not arise from the Baer correspondence or any of its generalizations described here.

5.4.11 Inner automorphisms and inner derivations in the context of the correspondence up to isoclinism

Many aspects of the relationship between inner automorphisms and inner derivations described in Section 5.2.8 continue to be valid, with suitable modification, for the Baer correspondence up to isoclinism.

Suppose G is a group of nilpotency class two and L is a Lie ring of nilpotency class two such that G and L are in Baer correspondence up to isoclinism. In particular, this means that the groups $G/Z(G) \cong \mathrm{Inn}(G)$ and $L/Z(L) \cong \mathrm{Inn}(L)$ are in abelian Lie correspondence up to isomorphism.

The adjoint action of G on L is defined as follows:

$$\mathrm{Ad} : G \to \mathrm{Aut}(L)$$

For any $u \in G$, define Ad_u as follows. Denote by $\overline{u}$ the image of u in $G/Z(G)$. Denote by x an element of L such that the image of x in $L/Z(L)$ corresponds to the element $\overline{u}$

under the abelian Lie correspondence between $L/Z(L)$ and $G/Z(G)$. We define Ad_u as the following automorphism of L:

$$\mathrm{Ad}_u(g) = g + [x, g]$$

It can easily be verified that Ad_u is an automorphism of L. It can also be verified that $\mathrm{Ad}_{uv} = \mathrm{Ad}_u \mathrm{Ad}_v$, making Ad a homomorphism.

More conceptually, we can write the description as follows:

$$\mathrm{Ad}_u = 1 + \mathrm{ad}_x$$

where the images of u and x modulo the respective centers are in abelian Lie correspondence.

5.5 Examples of the Baer correspondence up to isoclinism

In the case that G and A are odd-order abelian groups, the *original* Baer correspondence works. To obtain finite examples where the Baer correspondence works only up to isoclinism, we need to look at 2-groups. Further, our examples must be cases where the quotient $\mathrm{Hom}(G \wedge G, A)$ is nontrivial, so that there is at least some non-abelian extension.[3]

5.5.1 Extensions with quotient the Klein four-group and center cyclic of order two

The smallest sized example is: $A = \mathbb{Z}_2$ is the cyclic group of order 2 and $G = V_4$ is the Klein four-group, isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

3. The abelian extensions can be put in correspondence based on the correspondence between abelian groups and abelian Lie rings, which, although not strictly part of the Baer correspondence as have defined it, falls under the generalization described in Section 5.3.1

The short exact sequences discussed in Sections 5.4.4 and 5.4.5, along with the canonical isomorphisms discussed in Section 5.4.6, give the following:

$$\begin{array}{ccccccccc}
0 & \to & \mathrm{Ext}^1(V_4;\mathbb{Z}_2) & \to & H^2(V_4;\mathbb{Z}_2) & \to & \mathrm{Hom}(V_4 \wedge V_4, \mathbb{Z}_2) & \to & 0 \\
 & & \downarrow & & & & \downarrow & & \\
0 & \to & \mathrm{Ext}^1(V_4;\mathbb{Z}_2) & \to & H^2_{\mathrm{Lie}}(V_4;\mathbb{Z}_2) & \to & \mathrm{Hom}(V_4 \wedge V_4, \mathbb{Z}_2) & \to & 0
\end{array}$$

Recall that both short exact sequences split, and, as per the discussion in Section 5.4.5, the Lie ring short exact sequence splits canonically (with the splitting separating out the addition and Lie bracket parts).

It turns out that:

- $\mathrm{Ext}^1(V_4;\mathbb{Z}_2)$ is itself isomorphic to V_4, the Klein four-group.
- $(V_4 \wedge V_4)$ is isomorphic to $\mathbb{Z}_2$, and thus, $\mathrm{Hom}(H_2(V_4;\mathbb{Z}),\mathbb{Z}_2)$ is isomorphic to $\mathbb{Z}_2$.
- Thus, both of the second cohomology groups (the group and Lie ring side) are isomorphic to the elementary abelian group of order eight.

On the group side, we have the following eight extensions (eight being the order of the cohomology group):

(a) Elementary abelian group of order eight (1 time).

(b) $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ (3 times).

(c) D_8 (3 times).

(d) Q_8 (1 time).

(a) and (b) together form the image of Ext^1 (total size 4) while (c) and (d) form the non-identity coset of that image.

On the Lie ring side, the eight extensions (eight being the order of the cohomology group) are:

(a) Abelian Lie ring, additive group elementary abelian of order eight (1 time)

(b) Abelian Lie ring, additive group direct product of $\mathbb{Z}_4$ and $\mathbb{Z}_2$ (3 times).

(c) The niltriangular matrix Lie ring (3×3 strictly upper triangular matrices) over the field of two elements. (1 time)

(d) The semidirect product of $\mathbb{Z}_4$ and $\mathbb{Z}_2$ as Lie rings. (3 times).

(a) and (b) together form the image of Ext^1 (total size 4) while (c) and (d) form the non-identity coset of that image.

Note that there is no canonical bijection between the set of eight group extensions and the set of eight Lie ring extensions, but we can naturally correspond the images of Ext^1 in both. The problem arises when attempting an element-to-element identification of the non-identity cosets in the two cases. In other words, we have a correspondence at a coset level:

$$\{D_8, D_8, D_8, Q_8\} \leftrightarrow \{\text{The four non-abelian Lie ring extensions}\}$$

But there is no clear-cut way of making sense of *which* Lie ring extension to correspond to *which* group. This is an example of a situation where the Baer correspondence up to isoclinism does not seem to have any natural refinement to a correspondence up to isomorphism.

Note that in this case, it so happens that we can use an automorphism-invariance criterion and get a unique automorphism-invariant bijection. This would map the niltriangular matrix Lie ring to the quaternion group and the semidirect product of $\mathbb{Z}_4$ and $\mathbb{Z}_2$ to the dihedral group. However, this does not give a meaningful bijection at the level of elements. For instance, as described in Section 5.2.7, one feature that holds in all generalizations described so far for the Baer correspondence is that the correspondence restricts to isomorphism between cyclic subgroups and cyclic subrings. In particular, the rder statistics of the group (i.e., the multiset of the orders of the elements) in the group must match the order statistics of the additive group of the Lie ring. However, the order statistics of D_8 do not match the order statistics of any abelian group of order 8. The same is true for Q_8.

5.5.2 *Extensions with quotient the Klein four-group and center cyclic of order four*

We consider a slight variation of the preceding example. We set $G = V_4$ as before, but now set $A = \mathbb{Z}_4$, so A is the cyclic group of order four. The extension groups and extension Lie rings are all of order 16.

It turns out that:

- $\operatorname{Ext}^1(V_4; \mathbb{Z}_4)$ is itself isomorphic to V_4, the Klein four-group.
- $(V_4 \wedge V_4)$ is isomorphic to $\mathbb{Z}_2$, and thus, $\operatorname{Hom}(H_2(V_4; \mathbb{Z}), \mathbb{Z}_4)$ is isomorphic to $\mathbb{Z}_2$.
- Thus, both of the second cohomology groups (the group and Lie ring side) are isomorphic to the elementary abelian group of order eight.

On the group side, we have the following eight extensions (eight being the order of the cohomology group):

(a) $\mathbb{Z}_4 \oplus V_4$ (1 time).

(b) $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ (3 times).

(c) The group $M_{16} = M_4(2)$, given by the presentation $\langle a, x \mid a^8 = x^2 = 1, xax^{-1} = a^5 \rangle$ (3 times). This group has ID (16,6) in the SmallGroups library used in GAP and Magma.

(d) The group $D_8 *_{\mathbb{Z}_2} \mathbb{Z}_4 = Q_8 *_{\mathbb{Z}_2} \mathbb{Z}_4$ (1 time). This group has ID (16,13) in the SmallGroups library used in GAP and Magma.

(a) and (b) together form the image of Ext^1 (total size 4) while (c) and (d) form the non-identity coset of that image.

On the Lie ring side, we have the following eight extensions (eight being the order of the cohomology group):

(a) Abelian Lie ring with additive group $\mathbb{Z}_4 \oplus V_4$ (1 time).

(b) Abelian Lie ring with additive group $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ (3 times).

(c) Lie ring with presentation $\langle a, x \mid 8a = 2x = 0, [a, x] = 4a \rangle$ (3 times).

(d) Lie ring with presentation $\langle a, x, y \mid 4a = 2x = 4y = 0, 2a = 2y, [a, x] = 2a, [a, y] = [x, y] = 0 \rangle$ (1 time).

(a) and (b) together form the image of Ext^1 (total size 4) while (c) and (d) form the non-identity coset of that image.

We can naturally correspond the images of Ext^1 in both. We also have a correspondence at a coset level:

The four non-abelian group extensions $\leftrightarrow$ The four non-abelian Lie ring extensions

In general, we cannot refine this to a canonical bijection at the level of individual extensions. However, in this case, there does exist an automorphism-invariant splitting, under which the type (c) for groups corresponds to the type (c) for Lie rings, and the type (d) for groups corresponds to the type (d) for Lie rings. The splitting here is somewhat nicer than the splitting in the preceding example because for each group and Lie ring in correspondence, we can obtain a bijection between the group and the Lie ring that preserves the cyclic subgroup structure, similar to the description in Section 5.2.7.

CHAPTER 6

THE MALCEV AND LAZARD CORRESPONDENCES

6.1 Adjoint groups and the exponential and logarithm maps

6.1.1 Remarks on the approach followed from this point onward

Many of the identities that we will obtain in this section and the subsequent sections are *formal* identities. They make sense in a wide array of situations, if appropriately interpreted. Below, we outline our typical logic flow.

- Some of our identities start off as identities involving infinite series that make sense over the reals, or over real Lie groups. In those contexts, the identities may have specific interpretations related to differential equations, although those interpretations do not concern us directly.

- Our identities are valid *formally* in a noncommutative (but associative) power series algebra over $\mathbb{Q}$. Note that we need to use power series algebras because the identities involve infinite series.

- As a result, our identities are valid in free nilpotent associative $\mathbb{Q}$-algebras of nilpotency class c, where the identities get truncated to expressions of finite length. We therefore get identities involving the truncated expressions of finite length with the assumption about nilpotency class.

- We notice that the truncated expressions, for which the identity is valid, have only a finite number of coefficients, that in turn have only a finite number of prime divisors of their denominators. Typically, the truncated expression to class c uses only the primes that are less than or equal to c. Denote this prime set by π_c.

- We then notice that our identities (in truncated form) are valid in free nilpotent (associative) $\mathbb{Z}[\pi_c^{-1}]$-algebras of nilpotency class c.

- We conclude that our identities (in truncated form) are valid in all nilpotent (associative) $\mathbb{Z}[\pi_c^{-1}]$-algebras of nilpotency class at most c, on account of our being able to express such algebras as quotients of the free nilpotent $\mathbb{Z}[\pi_c^{-1}]$-algebras of nilpotency class c.

6.1.2 Some background on adjoint groups and algebra groups

An associative (not necessarily unital) ring N is termed a *radical ring* if for every $x \in N$ there exists $y \in N$ such that $x + y + xy = 0$.

For any radical ring N, we define the *adjoint group* corresponding to N as the set $1 + N$, i.e., the set of formal symbols:

$$\{1 + x \mid x \in N\}$$

equipped with the multiplication:

$$(1 + x)(1 + y) = 1 + (x + y + xy)$$

The identity element for this adjoint group is $1+0$ (simply denoted as 1). For any $x \in N$, the inverse of $1+x$ is the element $1+y$ where y is an element satisfying $x+y+xy = 0$. Such an element exists by the assumption that N is radical. The uniqueness and two-sidedness of inverses follows from group theory.[1]

An *algebra group* over a field F is defined as a group arising as the adjoint group corresponding to an associative algebra N over F that is also a radical ring.

Suppose G is an algebra group over a field F corresponding to a radical ring N that is an associative algebra over F. A subgroup H of G is termed an *algebra subgroup* if $H = 1 + M$ for a subalgebra M of N (note that M must also be a radical ring for H to be a subgroup).

1. Specifically, if every element of a monoid has a right inverse, then every element has a two-sided inverse and the two-sided inverse is unique.

The following facts about algebra groups can be easily checked.

1. An associative ring in which every element is nilpotent is a radical ring. In particular, an associative ring that is itself nilpotent is a radical ring.

   The proof of this assertion relies on the observation that if $x^n = 0$, then the element $y = \sum_{i=1}^{n-1}(-1)^i x^i = -x + x^2 - x^3 + \cdots + (-1)^{n-1}x^{n-1}$ satisfies $x + y + xy = 0$. Secretly, the expression above relies on expanding $(1-(-x)^n)(1-(-x))$ as a power series in x.

2. Suppose K is a field extension of a field F. Then, any K-algebra group naturally acquires the structure of a F-algebra group. In particular, any algebra group over a field of characteristic zero is a $\mathbb{Q}$-algebra group. Similarly any algebra group over a field of characteristic p is a $\mathbb{F}_p$-algebra group.

3. It is possible to have two non-isomorphic $\mathbb{F}_p$-algebras N_1 and N_2 such that the algebra group corresponding to N_1 is isomorphic (as an abstract group) to the algebra group corresponding to N_2. In fact, we can construct examples of non-isomorphic associative algebras over $\mathbb{F}_2$ whose corresponding algebra groups are both isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

4. Suppose N is a radical $\mathbb{F}_p$-algebra where p is a prime number. Then, we have $(1+x)^p = 1 + x^p$ for all $x \in N$. In other words, the p^{th} power map in the algebra and the algebra group correspond to each other.

5. A finite $\mathbb{F}_p$-algebra N is radical if and only if every element of N is nilpotent. One direction was already established in (1). For the reverse direction, note that if $1 + x$ has finite order p^k, then $1 + x^{p^k} = (1+x)^{p^k} = 1$, so $x^{p^k} = 0$, and thus, x is nilpotent.

6. For any field F and a positive integer n, consider the group $UT(n, F)$ of upper triangular unipotent matrices over F. $UT(n, F)$ is the algebra group corresponding to

$NT(n, F)$, the strictly upper triangular matrices over F, where we view $NT(n, F)$ as an *associative* F-algebra with the usual addition and multiplication of matrices.

7. Any $\mathbb{F}_q$-algebra group $G = 1 + N$ of order q^m is isomorphic to an algebra subgroup of the algebra group $UT(m + 1, q) = UT(m + 1, \mathbb{F}_q)$. The proof idea is to consider G as a multiplicative subgroup of the ring $N + \mathbb{F}_q$ (the *unitization* of N) and then consider the action of G on the underlying vector space of $N + \mathbb{F}_q$ by multiplication. This action is faithful, and defines an injective homomorphism $G \to GL(m + 1, \mathbb{F}_q)$. By Sylow's theorem, G can be conjugated to a subgroup inside any p-Sylow subgroup of $GL(m+1, q)$ (where p is the underlying prime of q). $UT(m+1, q)$ is one such p-Sylow subgroup.

6.1.3 *Exponential map inside an associative ring: the torsion-free case*

Suppose R is an associative unital ring. For now, assume that the additive group of R is torsion-free (we will later relax the assumption). An element $x \in R$ is termed *exponentiable* if the following sum makes sense, and if so the sum is termed the *exponential* of x:

$$\exp(x) = e^x = \sum_{m=0}^{\infty} \frac{x^m}{m!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

The notations $\exp(x)$ and e^x are both used. The exp notation is more helpful when the argument to the function is complicated and cumbersome to write in a superscript.

Here, $x^0 = 1$, and $x^m/m!$ is the unique element $y \in R$ such that $m!y = x^m$. Note that uniqueness follows from our assumption that R is torsion-free.

For the sum to make sense, we need two conditions:

- x is nilpotent, i.e., there exists a natural number n such that $x^n = 0$. The smallest such n is the *nilpotency* of x.

- For all positive integers $m < n$, $m!$ divides x^m, i.e., there exists an element $y \in R$

(unique by the torsion-free assumption) such that $m!y = x^m$.

If both the above conditions hold, then we can rewrite:

$$e^x = \sum_{m=0}^{n-1} \frac{x^m}{m!}$$

For an element $x \in R$, we say that x is *logarithmable* if there exists a positive integer n such that $(x-1)^n = 0$, *and* the following can be computed:

$$\log x := (x-1) - \frac{(x-1)^2}{2} + \frac{(x-1)^3}{3} - \cdots + \frac{(-1)^n (x-1)^{n-1}}{n}$$

Explicitly, x is logarithmable if the following two conditions hold:

- x is *unipotent*, or equivalently, $x - 1$ is nilpotent, i.e., there exists a natural number n such that $(x-1)^n = 0$. The smallest such n is termed the *unipotency* of x.
- For all positive integers $m < n$, m divides $(x-1)^m$, i.e., there exists an element $y \in R$ such that $my = (x-1)^m$.

The following can be deduced from formal manipulation:

- If $x \in R$ is exponentiable and e^x is logarithmable, then $\log(e^x) = x$.
- If $x \in R$ is logarithmable and $\log x$ is exponentiable, then $e^{\log x} = x$.

This follows from the fact that the identities hold formally on account of these being the usual Taylor series for the exponential and logarithm functions that are inverses of each other.

6.1.4 Exponential to and logarithm from the adjoint group

Suppose N is an associative (but not necessarily commutative and generally *not* unital) ring whose additive group is torsion-free and x is a nilpotent element of N satisfying the following two conditions:

- x is nilpotent, i.e., there exists a natural number n such that $x^n = 0$. The smallest such n is the *nilpotency* of x.
- For all positive integers $m < n$, $m!$ divides x^m, i.e., there exists an element $y \in R$ (unique by the torsion-free assumption) such that $m!y = x^m$.

Then, we can make sense of the element e^x as an element of the adjoint group $1 + N$. Explicitly:

$$e^x := 1 + \left(x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots \frac{x^{n-1}}{(n-1)!} \right)$$

Similarly, for an element $1 + x, x \in N$, we say that $1 + x$ is *logarithmable* if the following two conditions hold:

- x is nilpotent, i.e., there exists a natural number n such that $x^n = 0$. The smallest such n is the *nilpotency* of x.
- For all positive integers $m < n$, m divides x^m, i.e., there exists an element $y \in R$ (unique by the torsion-free assumption) such that $my = x^m$.

We then define $\log(1 + x)$ as an element of N:

$$\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots + \frac{(-1)^n x^{n-1}}{n-1}$$

We have observations similar to those in Section 6.1.3:

- If $x \in N$ is exponentiable and e^x is logarithmable, then $\log(e^x) = x$.
- If $x \in N$ is logarithmable and $\log x$ is exponentiable, then $e^{\log x} = x$.

Note that this notion of exponential differs slightly from the preceding definition in that the exponential of an element is now no longer in the ring but rather in its adjoint group. However, we can embed N inside its unitization $R = N + \mathbb{Z}$ and both the definitions would then agree.[2] In fact, via this method, we can deduce all results here from the results of Section 6.1.3 without redoing any of the work.

6.1.5 The exponential and logarithm as global maps

Suppose N is an associative ring whose additive group is torsion-free and in which *every* element is exponentiable (to the adjoint group) and *every* element of the adjoint group is logarithmable. Then, the exponential can be defined as a *global* set map:

$$\exp : N \to 1 + N$$

In this case, the logarithm is also a global map:

$$\log : 1 + N \to N$$

and further, the two maps are inverses of each other.

The following are some cases where these hypotheses are satisfied:

- The case that N is a nilpotent $\mathbb{Q}$-algebra. This will be the case that interests us the most in the beginning.
- The case that N is a torsion-free $\mathbb{Z}[\pi_c^{-1}]$-algebra of nilpotency class at most c where π_c is the set of all primes less than or equal to c. Many of our generalizations will apply to this case. (See the next subsection regarding relaxation to the non-torsion-free case).

6.1.6 Truncated exponentials and the case of torsion

So far, we have considered the definition of exponential and logarithm in the context of torsion-free additive groups. The torsion-free assumption is significant because it guarantees

2. Note that the definition of "unitization" depends on what commutative unital ring we are considering N as an algebra over. The default assumption is to treat it as an algebra over $\mathbb{Z}$, in which case the unitization is $N + \mathbb{Z}$. If, howevever, we are viewing N as an algebra over a field F, the unitization is $N + F$.

that all the summands of the form $x^n/n!$ or x^n/n are *uniquely defined* if they exist. We now consider whether this torsion-free assumption can be relaxed somewhat.

In the case that an element x satisfies $x^n = 0$ for some natural number n, we can truncate the exponential series and get:

$$e^x = 1 + \left(x + \frac{x^2}{2!} + \cdots + \frac{x^{n-1}}{(n-1)!} \right)$$

Similarly, we can truncate the logarithm series and get:

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots + \frac{(-1)^n x^{n-1}}{n-1}$$

Thus, we can relax the *torsion-free* assumption to the assumption that the ring is π-torsion-free where π is the set of all primes strictly less than the nilpotency. Alternatively, if N is a nilpotent associative ring of nilpotency class c (explicitly, this means that $x_1 x_2 \ldots x_c x_{c+1} = 0$ for all $x_1, x_2, \ldots, x_c, x_{c+1} \in N$) that is π_c-torsion-free where π_c is the set of primes less than or equal to c, then we can make unique sense of the terms $x^m/m!$ and x^m/m used in the definitions of the exponential and logarithm maps.

In particular, if N is a $\mathbb{Z}[\pi_c^{-1}]$-algebra of nilpotency class at most c, then the exponential and logarithm maps make sense globally.

There is, however, a small caveat. Namely, the process of truncating the exponential map involves a choice, even though the choice we have made is a canonical choice. Consider again the infinite series for the exponential:

$$e^x = 1 + \left(x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots \right)$$

The m^{th} term of the summation is $\frac{x^m}{m!}$. In the case that $m \geq n$, the numerator is the zero element of N. We are therefore trying to make sense of the computation:

$$\frac{0}{m!}$$

A canonical candidate for the answer is 0. However, if N has p-torsion for some prime p less than or equal to m, this is not the *unique* candidate for the answer. Our decision to truncate the exponential implicitly involves making the canonical choice of the answer of 0 for all terms $x^m/m!$, even though this choice is not uniquely fixed.

Despite the non-uniqueness of these choices, all the formal manipulations involving exponentials and logarithms continue to be valid. A quick explanation for this is as follows: all the proofs for these manipulations involve using the existing (truncated) expressions and then applying the operations of addition, subtraction, multiplication, and composition. None of these operations is capable of introducing new primes into the denominators. Thus, we do not ever need to confront the non-uniqueness of division by larger primes when mimicking the proofs that work over the rational numbers.

6.1.7 Exponential and logarithm maps preserve abelian and cyclic subgroup structures

The following lemmas follow from manipulation similar to the formal manipulation used when dealing with power series over the reals. We therefore omit the proofs.

Lemma 6.1.1. Suppose c is a positive integer and π_c is the set of primes less than or equal to c. Suppose N is an associative $\mathbb{Z}[\pi_c^{-1}]$-algebra of nilpotency class less than or equal to c. Suppose $x, y \in N$ are elements such that $xy = yx$. Then, the exponential map $\exp : N \to 1 + N$ satisfies the condition that:

$$\exp(x + y) = \exp(x)\exp(y)$$

Lemma 6.1.2. Suppose c is a positive integer and π_c is the set of primes less than or equal to c. Suppose N is an associative $\mathbb{Z}[\pi_c^{-1}]$-algebra of nilpotency class less than or equal to c. Suppose $x \in N$ and $n \in \mathbb{Z}$. Then, the exponential map $\exp : N \to 1 + N$ satisfies the condition that:

$$\exp(nx) = (\exp(x))^n$$

This follows from the preceding lemma, combined with a proof by induction.

6.2 Free nilpotent groups and the exponential and logarithm

6.2.1 Free associative algebra and free nilpotent associative algebra

The notation and results here follow Khukhro's book [29], Chapters 9 and 10. For brevity, we omit some proofs and provide citations to Khukhro.

For this and the next few subsections, c is a fixed but arbitrary positive integer. The algebraic structures F, A, and L are all dependent on c. However, to keep the notation as uncluttered as possible, we will not use c as an explicit parameter to these.

Denote by $\mathcal{A}$ the free associative $\mathbb{Q}$-algebra on a generating set $S = \{x_1, x_2, \dots\}$ The generating set may have any cardinality. By the well-ordering principle, we will index the generating set by a well-ordered set.

The algebra $\mathcal{A}$ is naturally a *graded* associative algebra. Explicitly, the i^{th} graded component of $\mathcal{A}$ is the $\mathbb{Q}$-subspace generated by all products of length i of elements from the generating set. Formally, $\mathcal{A}$ has the following direct sum decomposition as a vector space:

$$\mathcal{A} = \bigoplus_{i=1}^{\infty} \mathcal{A}_i$$

and further:

$$\mathcal{A}_i \mathcal{A}_j \subseteq \mathcal{A}_{i+j}$$

For any positive integer i, we can define an ideal:

$$\mathcal{A}^i = \bigoplus_{j=i}^{\infty} \mathcal{A}_j$$

For any positive integer c, define the associative algebra:

$$A = \mathcal{A}/\mathcal{A}^{c+1}$$

A can be described as the free nilpotent associative algebra of class c on the same generating set S. Explicitly, this means that all products in A of length more than c become zero.

Based on the discussion in Sections 6.1.4 and 6.1.5, the exponential and logarithm map are globally defined, i.e., we have global maps:

$$\exp : A \to 1 + A, \log : 1 + A \to A$$

that are inverses of each other. Explicitly:

$$\begin{aligned} \exp(x) &= 1 + \left(x + \frac{x^2}{2!} + \cdots + \frac{x^c}{c!}\right) \\ \log(1+x) &= x - \frac{x^2}{2} + \cdots + \frac{(-1)^{c-1}x^c}{c} \end{aligned}$$

6.2.2 *Free Lie algebra and free nilpotent Lie algebra*

Denote by $\mathcal{L}$ the Lie subring of $\mathcal{A}$ generated by the free generating set S. Note that $\mathcal{L}$ is *only* a Lie ring, *not* a $\mathbb{Q}$-Lie algebra. $\mathbb{Q}\mathcal{L}$ is the $\mathbb{Q}$-Lie algebra generated by S in $\mathcal{A}$.

By [29], Theorem 5.39, $\mathcal{L}$ is the free Lie ring on S, and $\mathbb{Q}\mathcal{L}$ is the free $\mathbb{Q}$-Lie algebra on S. Further, for every prime set π, $\mathbb{Z}[\pi^{-1}]\mathcal{L}$ is the free π-powered Lie ring on S.

We can define L in the following equivalent ways:

- $L = \mathcal{L}/\gamma_{c+1}(\mathcal{L}) = \mathcal{L}/(\mathcal{L} \cap \mathcal{A}^{c+1})$.
- L is the Lie subring generated by the image of S inside A, i.e., it is the Lie subring generated by the freely generating set inside A.

Denote by $1 + A$ the adjoint group to A.

Denote by F the subgroup of $1 + A$ generated by the elements e^{x_i}, $x_i \in S$.

Lemma 6.2.1. $1 + A$ is a rationally powered group.

Proof. The maps $\log : 1 + A \to A$ and $\exp : A \to 1 + A$ are inverses of each other. We know that A is a $\mathbb{Q}$-algebra, and Lemma 6.1.2 tells us that the map $\exp : A \to 1 + A$ preserves the cyclic subgroup structure (i.e., $\exp(nx) = (\exp(x))^n$ for any $n \in \mathbb{Z}$). Thus, $1 + A$ is also rationally powered. $\square$

Theorem 6.2.2. 1. For each x_i in the generating set S, choose an element $y_i \in A$ that has no homogeneous degree one component. Then, the subgroup of $1+A$ generated by the elements $1 + x_i + y_i$ is a free nilpotent group of class c on the generating set $\{1 + x_i + y_i \mid i \in I\}$.

2. The subgroup F of $1 + A$ generated by the elements e^{x_i}, $x_i \in S$ is a free nilpotent group of class c on the generating set $e^{x_i}, x_i \in S$. Thus, it is canonically isomorphic to the free nilpotent group of class c on S.

3. For any prime set σ, the subgroup $\sqrt[\sigma]{F}$ of $1 + A$ (where F is defined as in part (2)) is a free σ-powered nilpotent group of class c on the generating set $e^{x_i}, x_i \in S$.

Proof. Proof of (1): See [29], Theorem 9.2.

Proof of (2): This follows from (1), setting

$$y_i = \sum_{j=2}^{c} \frac{x_i^j}{j!}$$

Proof of (3): By (2), we obtain that $\hat{F}^\sigma$ is the free σ-powered free class c nilpotent group on the set $e^{x_i}, x_i \in S$. We also know that the group $1 + A$ is rationally powered, hence in particular it is torsion-free and σ-powered. Thus, $\hat{F}^\sigma$ is canonically isomorphic to $\sqrt[\sigma]{F}$ inside $1 + A$. This proves the result. $\square$

6.3 Baker-Campbell-Hausdorff formula

We use the same notation as in the preceding section (Section 6.2).

6.3.1 Introduction

Consider the case of a generating set $\{x_1, x_2\}$ of size two. A is the free associative algebra of class c generated by $\{x_1, x_2\}$. L is the Lie subring of A generated by the elements x_1 and x_2. Note that A is powered over all primes on account of being a $\mathbb{Q}$-algebra, and further, every element of A is nilpotent, in fact, $u^{c+1} = 0$ for all $u \in A$. Thus, for all $u \in A$, it makes sense to consider the element $e^u \in 1 + A$ defined as follows:

$$e^u = 1 + \left(u + \frac{u^2}{2!} + \frac{u^3}{3!} + \cdots + \frac{u^c}{c!}\right)$$

The Baker-Campbell-Hausdoroff formula for class c is a formal expression $H_c(x_1, x_2)$ with the property that:

$$e^{H_c(x_1,x_2)} = e^{x_1}e^{x_2}$$

It is not *a priori* obvious that $H_c(x_1, x_2)$ exists, but [29], Section 9.2 demonstrates that $H_c(x_1, x_2)$ exists, *and moreover, that* $H_c(x_1, x_2) \in \mathbb{Q}L$, i.e., it is in the $\mathbb{Q}$-Lie subalgebra generated by x_1 and x_2.

It is easy to see that in the Baker-Campbell-Hausdorff formula for class c, truncating to products of length $c-1$ and lower gives the Baker-Campbell-Hausdorff formula for class $c-1$. Equivalently, the Baker-Campbell-Hausdorff formula for class c can be obtained by adding a degree c term to the Baker-Campbell-Hausdorff formula for class $c-1$.

We can thus define an infinite Baker-Campbell-Hausdorff formula as follows:

$$H(x_1, x_2) = t_1(x_1, x_2) + t_2(x_1, x_2) + \dots$$

where each $t_i(x_1, x_2)$ is in the i^{th} homogeneous component of $\mathbb{Q}\mathcal{L}$, with the further property that if we truncate the summation to:

$$H_c(x_1, x_2) = t_1(x_1, x_2) + t_2(x_1, x_2) + \dots + t_c(x_1, x_2)$$

then for $A = \mathcal{A}/\mathcal{A}^{c+1}$, we have:

$$e^{H_c(x_1,x_2)} = e^{x_1}e^{x_2}$$

6.3.2 *Computational procedure for the Baker-Campbell-Hausdorff formula*

The following procedure can be used to compute the Baker-Campbell-Hausdorff formula. The procedure as described here is incomplete, because it only gives the formula inside the associative algebra, but does not express it in terms of Lie products. There are closed-form expressions using Lie products, but these are extremely messy to work with, so we provide only the conceptual outline for obtaining $H(x_1, x_2)$ as an expression in terms of x_1 and x_2 in the associative algebra. See [29], Sections 5.3 and 9.9 for more more details, and see [9] for the most efficient known computational procedure.

First, we begin by considering the product:

$$e^{x_1}e^{x_2} = \sum_{k=0}^{\infty}\sum_{l=0}^{\infty}\frac{x_1^k}{k!}\frac{x_2^l}{l!}$$

Subtract 1 and obtain:

$$w = e^{x_1}e^{x_2} - 1 = \sum_{k,l \geq 0, 0 < k+l} \frac{x_1^k x_2^l}{k!l!}$$

We have a formal power series:

$$\log(1+w) = w - \frac{w^2}{2} + \frac{w^3}{3} - \dots$$

It can also be formally verified that:

$$e^{\log(1+w)} = 1 + w = 1 + (e^{x_1}e^{x_2} - 1) = e^{x_1}e^{x_2}$$

Thus, $H(x_1, x_2) = \log(1+w)$. Formally:

$$H(x_1, x_2) = \sum_{k,l \geq 0, 0 < k+l} \frac{x_1^k x_2^l}{k!l!} - \frac{1}{2}\left(\sum_{k,l \geq 0, 0 < k+l} \frac{x_1^k x_2^l}{k!l!}\right)^2 + \frac{1}{3}\left(\sum_{k,l \geq 0, 0 < k+l} \frac{x_1^k x_2^l}{k!l!}\right)^3 - \dots$$

The above calculation gives the full Baker-Campbell-Hausdorff formula. If we are interested in the class c Baker-Campbell-Hausdorff formula, we can use truncated versions of both the exponential and the logarithm power series.

6.3.3 Homogeneous terms of the Baker-Campbell-Hausdorff formula

The infinite Baker-Campbell-Hausdorff formula has the form:

$$H(x_1, x_2) = t_1(x_1, x_2) + t_2(x_1, x_2) + \dots$$

where $t_i(x_1, x_2)$ is the homogeneous component of degree i. The first few homogeneous components are given below:

The case $i = 1$ is obvious. The case $i = 2$ is derived in the Appendix, Section B.1.1. The

Table 6.1: Truncations of the Baker-Campbell-Hausdorff formula

i	$t_i(x_1, x_2)$	$H_i(x_1, x_2)$
1	$x_1 + x_2$	$x_1 + x_2$
2	$\frac{1}{2}[x_1, x_2]$	$x_1 + x_2 + \frac{1}{2}[x_1, x_2]$
3	$\frac{1}{12}([x_1, [x_1, x_2]] - [x_2, [x_1, x_2]])$	$x_1 + x_2 + \frac{1}{2}[x_1, x_2] + \frac{1}{12}([x_1, [x_1, x_2]] - [x_2, [x_1, x_2]])$
4	$-\frac{1}{24}[x_2, [x_1, [x_2, x_2]]]$	$H_3(x_1, x_2) - \frac{1}{24}[x_2, [x_1, [x_2, x_2]]]$

case $i = 3$ is derived in the Appendix, Section B.1.2.

For explicit descriptions of higher degree terms of the Baker-Campbell-Hausdorff formula, see [9].

6.3.4 Universal validity of the Baker-Campbell-Hausdorff formula

The Baker-Campbell-Hausdorff formula is valid wherever it makes sense. Explicitly, the following holds. Note that Lemma 6.1.1 can be viewed as a special case of this theorem (or rather, of Theorem 6.3.4, the generalization to $\mathbb{Z}[\pi_c^{-1}]$-algebras).

Theorem 6.3.1. Suppose R is a nilpotent $\mathbb{Q}$-algebra. Then, the Baker-Campbell-Hausdorff formula is valid for any $x, y \in R$:

$$e^{H(x,y)} = e^x e^y$$

where we make sense of the exponentials as expressions in the adjoint group $1 + R$, which can be viewed as a multiplicative subgroup inside the unitization $\mathbb{Q} \oplus R$.

Proof. Denote by c the nilpotency class of R. Let A be the free nilpotent $\mathbb{Q}$-algebra of class c on two generators x_1 and x_2. There is a unique $\mathbb{Q}$-algebra homomorphism $\theta : A \to R$ that sends x_1 to x and x_2 to y. The existence of this homomorphism is guaranteed by A being the *free* class c nilpotent $\mathbb{Q}$-algebra on two generators.

It is useful to extend θ to a homomorphism between the unitizations:

$$\varphi : \mathbb{Q} \oplus A \to \mathbb{Q} \oplus R$$

where φ acts as the identity map on the first coordinate and acts as θ on the second coordinate. φ is a $\mathbb{Q}$-algebra homomorphism satisfying $\varphi(x_1) = x$ and $\varphi(x_2) = y$.

We now use the fact that the corresponding identity holds in A, and the fact that homomorphisms preserve all formulas, to obtain the identity for x and y. Explicitly, we know that:

$$e^{H_c(x_1,x_2)} = e^{x_1}e^{x_2}$$

Apply φ to both sides:

$$\varphi(e^{H_c(x_1,x_2)}) = \varphi(e^{x_1}e^{x_2})$$

$\mathbb{Q}$-algebra homomorphisms commute with exponentiation and with products, so this becomes:

$$e^{\varphi(H_c(x_1,x_2))} = e^{\varphi(x_1)}e^{\varphi(x_2)}$$

$\mathbb{Q}$-algebra homomorphism also commute with H_c, and we get:

$$e^{H_c(\varphi(x_1),\varphi(x_2))} = e^{\varphi(x_1)}e^{\varphi(x_2)}$$

We had set $\varphi(x_1) = x$ and $\varphi(x_2) = y$, so we get:

$$e^{H_c(x,y)} = e^x e^y$$

as desired. $\square$

6.3.5 *Formal properties of the Baker-Campbell-Hausdorff formula*

Below are some important properties of the Baker-Campbell-Hausdorff formula:

1. The i^{th} homogeneous component $t_i(x_1, x_2)$ of the Baker-Campbell-Hausdorff formula is symmetric if i is odd and skew-symmetric if i is even. Explicitly:

$$t_i(x_1, x_2) = (-1)^{i-1} t_i(x_2, x_1)$$

2. The Baker-Campbell-Hausdorff formula is associative, i.e., we have the following formal identity:

$$H(H(x_1, x_2), x_3) = H(x_1, H(x_2, x_3))$$

   Equivalently, for every positive integer c, the following identity holds in class c:

$$H_c(H_c(x_1, x_2), x_3) = H_c(x_1, H_c(x_2, x_3))$$

   Note that by "holds in class c" we mean that we *truncate* the formula to all Lie products of degree at most c, and set all higher degree Lie products to be zero.

3. The Baker-Campbell-Hausdorff formula satisfies:

$$H(x, 0) = H(0, x) = x$$

   Equivalently, for every positive integer c, we have:

$$H_c(x, 0) = H_c(0, x) = x$$

   Note that in this case, explicit truncation to class c is not necessary.

4. The Baker-Campbell-Hausdorff formula satisfies:

$$H(x, -x) = H(-x, x) = 0$$

Equivalently, for every positive integer c, we have:

$$H_c(x, -x) = H_c(-x, x) = 0$$

Note that in this case, explicit truncation to class c is not necessary.

6.3.6 Universal validity of the formal properties of the Baker-Campbell-Hausdorff formula

Note that the universal validity being alluded to here differs in spirit from the universal validity that was alluded to in Section 6.3.4. The universal validity alluded to earlier was the universal validity of the Baker-Campbell-Hausdorff formula in relation with the exponential map in an *associative* algebra. The universal validity alluded to here is in *Lie* algebras.

Theorem 6.3.2. Suppose N is a nilpotent $\mathbb{Q}$-Lie algebra of nilpotency class c for some positive integer c. Then, the following hold for all $x, y, z \in N$:

$$\begin{aligned} H_c(H_c(x,y),z) &= H_c(x, H_c(y,z)) \\ H_c(x,0) &= x \\ H_c(0,x) &= x \\ H_c(x,-x) &= 0 \\ H_c(-x,x) &= 0 \end{aligned}$$

Proof. All identities except the first are obvious from the expressions. We therefore concentrate on the first identity.

Denote by L the free Lie ring on the set $\{x_1, x_2, x_3\}$. Then, $\mathbb{Q}L$ is the free $\mathbb{Q}$-Lie algebra on $\{x_1, x_2, x_3\}$. Consider the unique $\mathbb{Q}$-algebra homomorphism $\varphi : \mathbb{Q}L \to N$ defined as follows: $\varphi(x_1) = x$, $\varphi(x_2) = y$, and $\varphi(x_3) = z$.

We know that $H_c(H_c(x_1, x_2), x_3) = H_c(x_1, H_c(x_2, x_3))$ by the formal associativity of the Baker-Campbell-Hausdorff formula. The homomorphism φ is a homomorphism of $\mathbb{Q}$-Lie algebras, hence it preserves the identity, and we obtain that:

$$H_c(H_c(x, y), z) = H_c(x, H_c(y, z))$$

□

6.3.7 *Primes in the denominator for the Baker-Campbell-Hausdorff formula*

The lemma below allows us to restrict the Baker-Campbell-Hausdorff formula to $\mathbb{Z}[\pi_c^{-1}]L$ where π_c is the set of primes less than or equal to c.

Lemma 6.3.3. It is possible to express the Baker-Campbell-Hausdorff formula $H_c(x, y)$ in a manner where all primes that appear as divisors of denominators of the coefficients are less than or equal to c.

Proof. The Baker-Campbell-Hausdorff formula is obtained from the class c exponential and logarithm formulas using the operations of addition, subtraction, multiplication, and composition. The class c exponential and logarithm formulas use only the primes less than or equal to c, and the operations of addition, subtraction, multiplication and composition cannot introduce new prime divisors into the denominators, so the Baker-Campbell-Hausdorff formula does not have any other primes in its denominator.

Note that the above only demonstrates the result for the *associative* expression for the Baker-Campbell-Hausdorff formula. However, [29], Theorem 5.39[3] demonstrates that we can rewrite the expression as a sum of basic Lie products in a manner that does not use any new prime divisors in the denominator. □

A somewhat stronger result is true: Suppose p is a prime. Then, the largest k such that p^k divides one or more of the denominators in the coefficients for $H_c(x_1, x_2)$ is at most $\left\lfloor \frac{c-1}{p-1} \right\rfloor$. This is derived in the Appendix, Section B.1.3. Note that this would immediately imply the preceding lemma, but it has additional significance.

6.3.8 Universal validity assuming powering over the required primes

Below, we present results analogous to those described in Sections 6.3.4 and 6.3.6, but with the base ring taken to be $\mathbb{Z}[\pi_c^{-1}]$ instead of $\mathbb{Q}$, where π_c is the set of primes less than or equal to c.

Theorem 6.3.4. Suppose c is a positive integer, π_c is the set of all primes less than or equal to c, and R is an associative $\mathbb{Z}[\pi^{-1}]$-algebra that is nilpotent of nilpotency class at most c. Then, the Baker-Campbell-Hausdorff formula is valid for any $x, y \in R$:

$$e^{H_c(x,y)} = e^x e^y$$

where we make sense of the exponentials as expressions in the adjoint group $1 + R$, which can be viewed as a multiplicative subgroup inside the unitization $\mathbb{Z}[\pi^{-1}] \oplus R$.

Proof. Let A be the free nilpotent associative $\mathbb{Q}$-algebra of class c on the two generators x_1 and x_2 and let B be the $\mathbb{Z}[\pi^{-1}]$-subalgebra generated by x_1 and x_2. Clearly, B is the

3. It would be helpful to read the surrounding discussion in Section 5.3

free $\mathbb{Z}[\pi^{-1}]$-algebra on x_1 and x_2. There is a natural homomorphism $\theta : B \to R$ of $\mathbb{Z}[\pi^{-1}]$-algebras that sends x_1 to x and x_2 to y. The existence of this homomorphism is guaranteed by B being the *free* class c nilpotent $\mathbb{Z}[\pi^{-1}]$-algebra on two generators. Further, θ extends uniquely to a homomorphism $\varphi : \mathbb{Z}[\pi^{-1}] \oplus B \to \mathbb{Z}[\pi^{-1}] \oplus R$ between the unitizations of B and R as $\mathbb{Z}[\pi^{-1}]$-algebras.

Note that the Baker-Campbell-Hausdorff formula is valid for the elements $x_1, x_2 \in A$, i.e., we have:

$$e^{H_c(x_1,x_2)} = e^{x_1}e^{x_2}$$

Both sides of the identity and all intermediate calculations happen inside B, because the exponential map as well as the Baker-Campbell-Hausdorff formula all involve division only by the primes in π_c (by Lemma 6.3.3). Thus, the above identity holds in B.

We now apply φ to both sides and obtain the conclusion. The details are analogous to those of Theorem 6.3.1. The main difference is that the homomorphism φ is now a $\mathbb{Z}[\pi^{-1}]$-algebra homomorphism rather than a $\mathbb{Q}$-algebra homomorphism. The reason it commutes with the formulas is that all the formulas involved make sense over $\mathbb{Z}[\pi^{-1}]$. $\square$

Theorem 6.3.5. Suppose c is a positive integer and π_c is the set of all primes less than or equal to c. Suppose N is a nilpotent $\mathbb{Z}[\pi^{-1}]$-Lie algebra of nilpotency class c. Then, the following hold for all $x, y, z \in N$:

$$\begin{aligned}
H_c(H_c(x,y),z) &= H_c(x,H_c(y,z)) \\
H_c(x,0) &= x \\
H_c((0,x) &= x \\
H_c(x,-x) &= 0 \\
H_c(-x,x) &= 0
\end{aligned}$$

Proof. All identities except the first one are obvious from the expressions. We therefore concentrate on proving the first identity.

Denote by L the free Lie ring on the set $\{x_1, x_2, x_3\}$. Then, $\mathbb{Z}[\pi^{-1}]L$ is the free $\mathbb{Z}[\pi^{-1}]$-Lie algebra on the set $\{x_1, x_2, x_3\}$. Consider the unique $\mathbb{Z}[\pi^{-1}]$-algebra homomorphism $\varphi : \mathbb{Z}[\pi^{-1}]L \to N$ defined by the conditions $\varphi(x_1) = x$, $\varphi(x_2) = y$, $\varphi(x_3) = z$.

We know that $H_c(H_c(x_1, x_2), x_3) = H_c(x_1, H_c(x_2, x_3))$ by the formal associativity of the Baker-Campbell-Hausdorff formula. Lemma 6.3.3 tells us that this identity holds inside $\mathbb{Z}[\pi^{-1}]L$. The homomorphism $\varphi : \mathbb{Z}[\pi^{-1}]L \to N$ is a homomorphism of $\mathbb{Z}[\pi^{-1}]$-algebras, hence it preserves the identity, and we obtain that:

$$H_c(H_c(x,y),z) = H_c(x,H_c(y,z))$$

□

6.4 The inverse Baker-Campbell-Hausdorff formulas

6.4.1 Brief description of the formulas

There are two inverse Baker-Campbell-Hausdorff formulas. The first inverse Baker-Campbell-Hausdorff formula is a formula to compute:

$$h_1(x, y) = \exp(\log x + \log y)$$

The second inverse Baker-Campbell-Hausdorff formula is a formula to compute:

$$h_2(x, y) = \exp([\log x, \log y])$$

We will now provide a few important details regarding the formulas that will help understand the correspondence. However, we do not attempt to be comprehensive here. More information about the inverse Baker-Campbell-Hausdorff formula is in [29], Section 10.1. Lemma 10.7 in particular establishes the key nature of the formula. For an explicit description of the first few terms for both h_1 and h_2, as well as an efficient computation strategy, see [9].

6.4.2 Origin of the formulas

We follow the notation of Section 6.2. The highlights of the notation follow: $\mathcal{A}$ is the free associative $\mathbb{Q}$-algebra on a generating set $S = \{x_1, x_2, \dots\}$. $\mathcal{L}$ is the Lie subring (not the $\mathbb{Q}$-Lie subalgebra, but just the $\mathbb{Z}$-Lie subalgebra) of $\mathcal{A}$ generated by S. c is a fixed positive integer. We denote by $\mathcal{A}_c$ the c^{th} graded component in the natural gradation of $\mathcal{A}$, and we denote by $\mathcal{A}^c$ the sum of all graded components at and beyond c. Define $A = \mathcal{A}/\mathcal{A}^{c+1}$ and define L to be the Lie subring of A generated by S.[4] By Theorem 6.2.2, the set $\{e^{x_i} \mid x_i \in S\}$ generates a free nilpotent group of class c and is a freely generating set for it. We denote

4. Note that the S viewed as a subset inside A is the image of the S viewed as a subset of $\mathcal{A}$.

this group as F.

Corollary 9.22 in Khukhro's book ([29]) states that $\sqrt{F}$ is a free rationally powered nilpotent group of nilpotency class c. This is a consequence of Theorem 4.3.3. Further, Theorem 10.4 of [29] states that $\sqrt{F} = e^{\mathbb{Q}L}$. Thus, every element of $e^{\mathbb{Q}L}$ can be expressed in terms of the elements e^{x_i} using group operations as well as taking roots.

The first inverse Baker-Campbell-Hausdorff formula expresses $e^{x_1+x_2}$ as a word in terms of e^{x_1} and e^{x_2} using the group operations and taking roots. Explicitly, the first inverse Baker-Campbell-Hausdorff formula in class c is a formula $h_{1,c}$ such that:

$$e^{x_1+x_2} = h_{1,c}(e^{x_1}, e^{x_2})$$

Note importantly that the element $e^{x_1+x_2}$ need not lie inside F, but it does lie inside $\sqrt{F}$.

Similarly, the second inverse Baker-Campbell-Hausdorff formula expresses $e^{[x_1,x_2]}$ as a word in terms of e^{x_1} and e^{x_2} using the group operations and taking roots. The second inverse Baker-Campbell-Hausdorff formula in class c is a formula $h_{2,c}$ such that:

$$e^{[x_1,x_2]} = h_{2,c}(e^{x_1}, e^{x_2})$$

Here, $[x_1, x_2]$ denotes the Lie bracket of x_1 and x_2 inside L. Inside A, this can be viewed as the expression $x_1x_2 - x_2x_1$. However, the latter does not make sense as an expression inside L.

6.4.3 Formal properties of the inverse Baker-Campbell-Hausdorff formulas

- As with the original Baker-Campbell-Hausdorff formula, both the inverse Baker-Campbell-Hausdorff formulas can be truncated to class c for any positive integer c. We will denote the truncations as $h_{1,c}$ and $h_{2,c}$ respectively.

- The class $c+1$ inverse Baker-Campbell-Hausdorff formula is obtained by taking the class c inverse Baker-Campbell-Hausdorff formula and multiplying by a suitable product of iterated commutators, each of length $c+1$. Note that the precise nature of the terms depends on whether we multiply on the left or the right.[5]

- For $h_1(x_1, x_2)$, the degree one term is $x_1 x_2$ and the degree two term is $[x_1, x_2]^{-1/2}$, the reciprocal of the square root of the group commutator.
- For $h_2(x_1, x_2)$, there is no degree one term, and the degree two term is the group commutator $[x_1, x_2]$.

6.4.4 Universal validity of Lie ring axioms for inverse Baker-Campbell-Hausdorff formulas

We begin by establishing the universal validity over rationally powered nilpotent groups.

Theorem 6.4.1. Suppose G is a rationally powered nilpotent group of nilpotency class c. Then, the following are true for all $x, y, z \in G$:

5. Technically, the new term that needs to be inserted is the same whether on the left or on the right, because it is central and therefore commutes with the rest of the expression. However, the choice of whether previous terms were inserted on the left or the right affects the precise choice of the term being inserted at a given stage, so in that sense, it does matter whether the higher degree terms are being inserted on the left or the right.

$$
\begin{aligned}
h_{1,c}(h_{1,c}(x,y),z) &= h_{1,c}(x,h_{1,c}(y,z)) \\
h_{1,c}(x,1) &= x \\
h_{1,c}(1,x) &= x \\
h_{1,c}(x,x^{-1}) &= 1 \\
h_{1,c}(x^{-1},x) &= 1 \\
h_{1,c}(x,y) &= h_{1,c}(y,x) \\
h_{2,c}(x,h_{1,c}(y,z)) &= h_{1,c}(h_{2,c}(x,y),h_{2,c}(x,z)) \\
h_{2,c}(h_{1,c}(x,y),z) &= h_{1,c}(h_{2,c}(x,z),h_{2,c}(y,z)) \\
h_{2,c}(x,x) &= 1 \\
h_{1,c}(h_{1,c}(h_{2,c}(h_{2,c}(x,y),z),h_{2,c}(h_{2,c}(y,z),x)),h_{2,c}(h_{2,c}(z,x),y)) &= 1
\end{aligned}
$$

Proof. Let $S = \{x_1, x_2, x_3\}$ and use the setup of Section 6.4.2. F is therefore a free nilpotent group of class c with freely generating set comprising e^{x_1}, e^{x_2}, e^{x_3}. There is therefore a unique group homomorphism from F to G sending e^{x_1} to x, e^{x_2} to y, and e^{x_3} to z. By Theorem 4.3.3 and the fact that G is rationally powered, this extends to a unique group homomorphism from $\sqrt{F}$ to G. All the above identites hold for $\sqrt{F}$ because of the Lie ring structure on L. The identities are preserved under homomorphisms, therefore they also hold in G (the proof details are similar to those for Theorems 6.3.1 and 6.3.2). □

6.4.5 Universal validity of Lie ring axioms: the π_c-powered case

Denote by π_c the set of all primes less than or equal to c. Theorem 10.22 of Khukhro's book [29] states that for any prime set $\sigma \supseteq \pi_c$, we have $\sqrt[\sigma]{F} = e^{\mathbb{Z}[\sigma^{-1}]L}$. In particular, this means that $\sqrt[\pi_c]{F} = e^{\mathbb{Z}[\pi_c^{-1}]L}$. Therefore, both the formulas $h_{1,c}$ and $h_{2,c}$ (which describe elements of e^L and hence elements of $e^{\mathbb{Z}[\pi_c^{-1}]L}$) can be written using p^{th} roots only for the primes p

that are in π_c.

We will later see, in Lemma 7.1.2, that a slightly stricter bound applies to $h_{2,c}$, though the bound here is tight for $h_{1,c}$. However, we do not need the stricter bound for our present purpose.

Based on this, we can formulate a π_c-powered version of the preceding theorem.

Theorem 6.4.2. Suppose G is a π_c-powered nilpotent group of nilpotency class c. Then, the following are true for all $x, y, z \in G$:

$$\begin{aligned}
h_{1,c}(h_{1,c}(x,y),z) &= h_{1,c}(x,h_{1,c}(y,z)) \\
h_{1,c}(x,1) &= x \\
h_{1,c}(1,x) &= x \\
h_{1,c}(x,x^{-1}) &= 1 \\
h_{1,c}(x^{-1},x) &= 1 \\
h_{1,c}(x,y) &= h_{1,c}(y,x) \\
h_{2,c}(x,h_{1,c}(y,z)) &= h_{1,c}(h_{2,c}(x,y),h_{2,c}(x,z)) \\
h_{2,c}(h_{1,c}(x,y),z) &= h_{1,c}(h_{2,c}(x,z),h_{2,c}(y,z)) \\
h_{2,c}(x,x) &= 1 \\
h_{1,c}(h_{1,c}(h_{2,c}(h_{2,c}(x,y),z),h_{2,c}(h_{2,c}(y,z),x)),h_{2,c}(h_{2,c}(z,x),y)) &= 1
\end{aligned}$$

Proof. Let $S = \{x_1, x_2, x_3\}$ and use the setup of Section 6.4.2. F is therefore a free nilpotent group of class c with freely generating set comprising e^{x_1}, e^{x_2}, e^{x_3}. There is therefore a unique group homomorphism from F to G sending e^{x_1} to x, e^{x_2} to y, and e^{x_3} to z. By Theorem 4.3.3 and the fact that G is π_c-powered, this extends to a unique group homomorphism from

$\sqrt[\pi c]{F}$ to G. All the above identities hold inside $\sqrt[\pi c]{F}$, therefore, they also hold in G. $\square$

6.5 The Malcev correspondence

6.5.1 The class c Malcev correspondence

The class c Malcev correspondence is a correspondence:

Rationally powered nilpotent groups of nilpotency class at most $c \leftrightarrow$ Rationally powered nilpotent Lie rings of nilpotency class at most c (i.e., nilpotent $\mathbb{Q}$-Lie algebras)

The class c Malcev correspondence has a number of features similar to the abelian Lie correspondence (described in Section 1.3) and the Baer correspondence (described in Sections 5.1 and 5.2). To avoid repetition, we refer to relevant sections for the earlier correspondences where helpful.

Given a rationally powered nilpotent Lie ring L of nilpotency class at most c, the *Malcev Lie group* for L, denoted $\exp(L)$, is a rationally powered nilpotent group of nilpotency class at most c defined as follows:

- The underlying set of $\exp(L)$ is the same as the underlying set of L.
- The group operation of $\exp(L)$ is defined as follows: $xy = H_c(x, y)$ where H_c is the class c Baker-Campbell-Hausdorff formula, and the operations in the formula are interpreted over L.
- The identity element $1 \in \exp(L)$ of the group is the same as the zero element $0 \in L$.
- The inverse map is defined as $x^{-1} := -x$.

Conversely, given a rationally powered nilpotent group G of nilpotency class at most c, the *Malcev Lie ring* for G, denoted $\log(G)$, is a rationally powered nilpotent Lie ring of nilpotency class at most c defined as follows:

- The underlying set of $\log(G)$ is the same as the underlying set of G.

- The Lie ring addition is defined using the first inverse Baker-Campbell-Hausdorff formula in terms of the group operations. Explicitly, we define $x + y := h_{1,c}(x, y)$, where $h_{1,c}$ is the first inverse Baker-Campbell-Hausdorff formula for class c, and the operations in the formula are interpreted over G.

- The Lie bracket is defined using the second inverse-Baker-Campbell-Hausdorff formula in terms of the group operations. Explicitly, we define $[x, y] := h_{2,c}(x, y)$, where $h_{2,c}$ is the inverse Baker-Campbell-Hausdorff formula for class c, and the operations in the formula are interpreted over G.

- The zero element $0 \in \log(G)$ is defined to be the identity element $1 \in G$.

- The negation map in $\log(G)$ is defined to be the same as the inverse map in the group, i.e., $-x := x^{-1}$.

6.5.2 Why the class c Malcev correspondence works

The class c Malcev correspondence works in the direction from Lie rings to groups due to Theorem 6.3.2. It works in the reverse direction due to Theorem 6.4.1. The fact that the two directions are inverses of each other (i.e., applying the correspondence in one direction and then in the other direction returns to the original object) also follows from the original setup of the formulas.

6.5.3 Description of the Malcev correspondence (combining all possibilities for nilpotency class)

The class c Malcev correspondences for different values of c are related in the following manner. Suppose $c_1 \leq c_2$. Then, the class c_1 Malcev correspondence is a subcorrespondence of the class c_2 Malcev correspondence. Explicitly, this means that the subcategory (on the group side and the Lie ring side respectively) for the class c_1 Malcev correspondence is a full subcategory of the subcategory (on the group and the Lie ring side respectively) for the class c_2 Malcev correspondence. Further, the exp and log functors for the class c_1 Malcev correspondence are obtained by restricting to that subcategory the exp and log functors for the class c_2 Malcev correspondence.

Thus, as we increase the value of c, both sides of the correspondence become larger. We can thus consider a combined correspondence for all classes. This is the *Malcev correspondence*. The Malcev correspondence is a correspondence:

Rationally powered nilpotent groups $\leftrightarrow$ Rationally powered nilpotent Lie rings

6.5.4 The Malcev correspondence as an isomorphism of categories over Set

We can use reasoning analogous to that used for the Baer correspondence in Section 5.1.7 to deduce that the Malcev correspondence defines an isomorphism of categories over the category of sets between the following two categories: the category of rationally powered nilpotent groups and the category of rationally powered nilpotent Lie rings. We can also deduce some immediate consequences similar to those deduced for the Baer correspondence in Section 5.1.8.

6.6 The global Lazard correspondence

Remark about the "global" and "3-local" terminology

Although the terms "Lazard Lie group" and "Lazard Lie ring" are reasonably standard, the prefix adjectives "global" and "3-local" are not standard. Some sources, such as Khukhro's book [29], use the term "Lazard correspondence" only for the global Lazard correspondence, and do not describe the 3-local Lazard correspondence. Others, including Lazard's original paper [30], describe the 3-local Lazard correspondence.

We will separate the two ideas because the statements and proofs are easier to understand in the global class case, and due to considerations of space and complexity, we provide complete proofs only for the global class case. We begin by understanding the global class case of the Lazard correspondence.

6.6.1 Definitions of global class Lazard Lie group and global class Lazard Lie ring

Definition (Global class c Lazard Lie group)**.** Suppose G is a nilpotent group and c is a positive integer. Denote by π_c the set of all primes less than or equal to c. We say that G is a *global class c Lazard Lie group* if the following two conditions are satisfied:

- The nilpotency class of G is at most equal to c.
- G is π_c-powered, i.e., G is powered over all primes less than or equal to c.

We say that G is a global Lazard Lie group if G is a global class c Lazard Lie group for some positive integer c. Equivalently, G is a global Lazard Lie group if it is powered over all primes less than or equal to its nilpotency class.

Definition (Global class c Lazard Lie ring)**.** Suppose L is a nilpotent Lie ring and c is a positive integer. Denote by π_c the set of all primes less than or equal to c. We say that L is a *global class c Lazard Lie ring* if the following two conditions are satisfied:

1. The nilpotency class of L is at most equal to c.
2. L is π_c-powered, i.e., L is powered over all primes less than or equal to c.

We say that L is a global Lazard Lie ring if L is a global class c Lazard Lie ring for some positive integer c. Equivalently, L is a global Lazard Lie ring if L is powered over all primes less than or equal to its nilpotency class.

6.6.2 Possibilities for the set of values of c for a global class c Lazard Lie group

We re-examine the two conditions for a group G to be a "global class c Lazard Lie group":

1. The nilpotency class of G is at most equal to c.

2. G is powered over all primes less than or equal to c.

Condition (1) becomes weaker as we increase c. Condition (2), on the other hand, becomes *stronger* as we increase c. Overall, therefore, being a global class c Lazard Lie group is neither stronger nor weaker than being a global class $(c+1)$ Lazard Lie group.

For instance, an abelian group with 2-torsion is a global class 1 Lazard Lie group, but not a global class 2 Lazard Lie group. On the other hand, a finite non-abelian p-group of class two for odd p (such as the unitriangular group $UT(3,p)$, which is a non-abelian group of order p^3 and exponent p) is a global class 2 Lazard Lie group, but not a global class 1 Lazard Lie group. Thus, neither condition implies the other.

We now turn to what we *can* say about the set of possible values c for which a given group is a global class c Lazard Lie group.

Suppose G is a nilpotent group. Denote by c_0 the nilpotency class of G. Let p_0 be the smallest prime such that G is *not* powered over p_0, if there exists such a prime (G is rationally powered if and only if no such p_0 exists). There are four possibilities:

- $c_0 \geq p_0$: In this case, G is *not* a global class c Lazard Lie group for any value of c.

- $c_0 = p_0 - 1$: In this case, G is a global class c_0 Lazard Lie group, but is not a global class c Lazard Lie group for any other value of c.

- $c_0 < p_0 - 1$: In this case, G is a global class c Lazard Lie group for all c satisfying $c_0 \leq c \leq p_0 - 1$.

- G is rationally powered: In this case, G is a global class c Lazard Lie group for all c satisfying $c_0 \leq c$.

The upshot is that the set of values c for which G is a global class c Lazard Lie group is either empty or a single value or a contiguous (possibly finite and possibly infinite) subsegment of the nonnegative integers.

Analogous remarks apply for the case of nilpotent Lie rings.

6.6.3 *The global class c Lazard correspondence*

The global class c Lazard correspondence is a correspondence:

$$\text{Global class } c \text{ Lazard Lie groups} \leftrightarrow \text{Global class } c \text{ Lazard Lie rings}$$

The global class c Lazard correspondence operates in a manner quite similar to the class c Malcev correspondence. We describe it explicitly below.

Given a global class c Lazard Lie ring L, the corresponding global class c Lazard Lie ring $\exp(L)$ is defined as follows:

- The underlying set of $\exp(L)$ is the same as the underlying set of L.
- The group operation of $\exp(L)$ is defined as follows: $xy = H_c(x, y)$ where H_c is the class c Baker-Campbell-Hausdorff formula, and the Lie brackets in the formula are interpreted as Lie brackets in L. The reason this makes sense is that we have assumed that L powered over all primes less than or equal to c, and by Lemma 6.3.3, these are the only primes that appear as divisors of the denominators in $H_c(x, y)$.
- The identity element $1 \in \exp(L)$ of the group is the same as the zero element $0 \in L$.
- The inverse map is defined as $x^{-1} := -x$.

In the reverse direction, given a global class c Lazard Lie group G of nilpotency class c, the *Lazard Lie ring* for G is a rationally powered nilpotent Lie ring $\log(G)$ of nilpotency class c defined as follows:

- The underlying set of $\log(G)$ is the same as the underlying set of G.
- The Lie ring addition is defined using the first inverse Baker-Campbell-Hausdorff formula $h_{1,c}$ in terms of the group operations. Note that, as explained in Section 6.4.5, the formula for $h_{1,c}$ makes sense in a π_c-powered nilpotent group of nilpotency class at most c.
- The Lie bracket is defined using the second inverse-Baker-Campbell-Hausdorff formula in terms of the group operations. Note that, as explained in Section 6.4.5, the formula for $h_{2,c}$ makes sense in a π_c-powered nilpotent group of nilpotency class at most c.
- The zero element of $\log(G)$ is defined to be the identity element of G.
- The negation map in the Lie ring is defined to be the same as the inverse map in the group, i.e., $-x := x^{-1}$.

The forward direction (from Lie rings to groups) works because of Theorem 6.3.5. The reverse direction works due to Theorem 6.4.2. The directions are reverses of each other due to the formal properties of the formulas.

6.6.4 The global class one Lazard correspondence is the abelian Lie correspondence

The global class one Lazard correspondence is the abelian Lie correspondence described in Section 1.3:

$$\text{Abelian groups} \leftrightarrow \text{Abelian Lie rings}$$

6.6.5 The global class two Lazard correspondence is the Baer correspondence

Recall the definition of Baer Lie group from Section 5.1.1: a 2-powered group of nilpotency class at most two. This agrees with the definition of a global class 2 Lazard Lie group. Similarly, the definition of Baer Lie ring in Section 5.1.1 agrees with the definition of a global class 2 Lazard Lie ring.

The class two Baker-Campbell-Hausdorff formula, stated in Section 6.3.3 and worked out in the Appendix, Section B.1.1, is:

$$H_2(x, y) = x + y + \frac{1}{2}[x, y]$$

This is precisely the same as the formula in the direction from Lie rings to groups in the Baer correspondence. Similarly, the class two inverse Baker-Campbell-Hausdorff formulas are:

$$x + y = \frac{xy}{\sqrt{[x, y]}}$$

$$[x, y]_{\text{Lie}} = [x, y]_{\text{Group}}$$

These are precisely the same as the formulas in the direction from groups to Lie rings in the Baer correspondence.

Thus, the Baer correspondence is the same as the global class two Lazard correspondence.

6.6.6 Interaction of global Lazard correspondences for different classes

In Section 6.6.2, we noted that a given global Lazard Lie group may be a global class c Lazard Lie group for multiple values of c. The analogous observation applies to Lie rings. This leads to potential for ambiguity regarding which global class c Lazard correspondence we are referring to.

It turns out that the global class c Lazard correspondences for different values of c agree with each other wherever both are applicable. Explicitly, the following are true:

- Suppose G is a group of nilpotency class exactly c_0, and p_0 is the smallest prime for which G is not powered (see below for the case that G is rationally powered). Suppose that $c_0 \leq p_0 - 1$. Then, for each c satisfying $c_0 \leq c \leq p_0 - 1$, G is a global class c Lazard Lie group. Therefore, for each such c, we can consider a definition of $\log(G)$ based on the global class c Lazard correspondence. All these definitions coincide.

  In the case that G is rationally powered and has class exactly c_0, we can consider a definition of $\log(G)$ based on the global class c Lazard correspondence for all $c \geq c_0$. All the definitions coincide.

- Suppose L is a Lie ring of nilpotency class exactly c_0, and p_0 is the smallest prime for which L is not powered (see below for the case that L is rationally powered). Suppose that $c_0 \leq p_0 - 1$. Then, for each c satisfying $c_0 \leq c \leq p_0 - 1$, L is a global class c Lazard Lie ring. Therefore, for each such c, we can consider a definition of $\exp(L)$ based on the global class c Lazard correspondence. All these definitions coincide.

  In the case that L is rationally powered and has class exactly c_0, we can consider a definition of $\exp(L)$ based on the global class c Lazard correspondence for all $c \geq c_0$. All the definitions coincide.

Thus, we can define the global Lazard correspondence as the union of all the global class c Lazard correspondences. We now make a brief philosophical remark regarding why this behaves a little worse than the correspondences discussed earlier.

An observation people make early on in their study of algebraic structures is that whereas intersections behave nicely with respect to presrving closure and important structural attributes, unions rarely do. For instance, an intersection of subgroups is a subgroup, but a union of two subgroups is not a subgroup unless one of them contains the other. In general, unions are not guaranteed to preserve closure except in situations where they are unions of ascending chains or of directed sets.

We encounter a similar type of problem dealing with the global Lazard correspondence, albeit the problem is now at a higher level of abstraction. Each of the individual global class c Lazard correspondences behaves very nicely, just as the Baer correspondence and the abelian Lie correspondence do. However, when we combine the correspondences, we are dealing with heterogeneous types of objects, and we need to be more careful. In particular, the combined correspondence does not behave well with respect to direct products. Also, it does not behave well with respect to the relation between subgroups and quotient groups: the normal subgroups that are in the category are not the same as the normal subgroups for which the quotient groups are in the category. We will return to these in more detail in Section 6.6.8.

6.6.7 Isomorphism of categories

We follow here the general template outlined in Section 1.3.9.

Each global class c Lazard correspondence defines an isomorphism of categories over the category of sets[6] between the full subcategory of the category of groups comprising the global class c Lazard Lie groups and the full subcategory of the category of Lie rings comprising the global class c Lazard Lie rings. The functor from Lie rings to groups is the exp functor and the functor from groups to Lie rings is the log functor.

The global Lazard correspondence can be viewed as an isomorphism of categories over the category of sets between the full subcategory of the category of groups comprising all the global Lazard Lie groups, and the full subcategory of the category of Lie rings comprising all the global Lazard Lie rings.

The set of objects involved in the global Lazard correspondence is the union of the sets of objects involved in each of the global class c Lazard correspondences. The set of morphisms,

6. This means that the functors in both directions preserve the underlying set.

however, is strictly larger, because the new correspondence includes morphisms between global class c Lazard Lie groups for different values of c. For instance, an inclusion of $\mathbb{Z}$ in $UT(3, \mathbb{Q})$ is a morphism in the category on the group side, because $\mathbb{Z}$ is a global class 1 Lazard Lie group and $UT(3, \mathbb{Q})$ is a global class 2 Lazard Lie group.

We can deduce a number of immediate consequences of the isomorphism of categories similar to those in Section 5.1.8.

6.6.8 Subgroups, quotients, and direct products

We describe how subgroups, quotient groups, and direct products interact with the global class c Lazard correspondence.

Subgroups

Suppose G is a global class c Lazard Lie group and $L = \log(G)$ is the corresponding global class c Lazard Lie ring. Then, the global class c Lazard correspondence gives a bijective correspondence:

Global class c Lazard Lie subgroups of $G \leftrightarrow$ Global class c Lazard Lie subrings of L

The global Lazard correspondence gives a bijective correspondence:

Global Lazard Lie subgroups of $G \leftrightarrow$ Global Lazard Lie subrings of L

The latter correspondence is somewhat more general than the former, because it includes subgroups (respectively, subrings) that are global Lazard Lie groups (respectively, global Lazard Lie rings) for smaller nilpotency class values. In particular, it includes all abelian subgroups and abelian subrings, as well as all Baer Lie subgroups and Baer Lie subrings. These may not qualify for the earlier correspondence because they may not be powered over *all* the primes less than or equal to c. For instance, any copy of $\mathbb{Z}$ inside $UT(3, \mathbb{Q})$ is part of the latter correspondence but not the former.

Quotient groups

Suppose G is a global class c Lazard Lie group and $L = \log(G)$ is the corresponding global class c Lazard Lie ring. We have a correspondence:

Global class c Lazard Lie groups that are quotient groups of $G \leftrightarrow$ Global class c Lazard Lie rings that are quotient Lie rings of L

We also obtain correspondences between the corresponding kernels:

Global class c Lazard Lie groups that are normal subgroups of $G \leftrightarrow$ Global class c Lazard Lie rings that are ideals of L

Note that the equivalence relies on Theorem 4.1.27 and Lemma 4.2.1. These show that in a π_c-powered nilpotent group (respectively, π_c-powered nilpotent Lie ring) a normal subgroup (respectively, ideal) is π_c-powered if and only if the quotient group (respectively, quotient Lie ring) is π_c-powered. Here, we take π_c to be the set of all primes less than or equal to c.

We also have a correspondence:

Global Lazard Lie groups that are quotient groups of $G \leftrightarrow$ Global Lazard Lie rings that are quotient Lie rings of L

This gives rise to another correspondence:

Normal subgroups of G for which the quotient group is a global Lazard Lie group $\leftrightarrow$ Ideals of L for which the quotient Lie ring is a global Lazard Lie ring

Note, however, that these normal subgroups are *not necessarily the same as* the normal subgroups that are also global Lazard Lie groups. For instance, consider the global class two Lazard Lie group (i.e., the Baer Lie group) $G = UT(3, \mathbb{Q})$. A subgroup H isomorphic to $\mathbb{Z}$ inside the center of G is a normal subgroup that is a global class one Lazard Lie group. However, G/H is not a global Lazard Lie group, because it has class two but has 2-torsion in the center. On the other hand, consider the subgroup K of G such that $K/Z(G)$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$ inside $G/Z(G) \cong \mathbb{Q} \times \mathbb{Q}$. K is a normal subgroup that is not a global Lazard Lie group, but the quotient group G/K is a global Lazard Lie group.

Direct products

Suppose $G_i, i \in I$, are all global class c Lazard Lie groups for the same value of c. Then, the external direct product $\prod_{i \in I} G_i$ is also a global class c Lazard Lie group. Moreover, $\log(\prod_{i \in I} G_i) = \prod_{i \in I} \log(G_i)$.

On the other hand, it may happen that G_1 is a global class c_1 Lazard Lie group, G_2 is a global class c_2 Lazard Lie group, and the direct product $G_1 \times G_2$ is not a global class c Lazard Lie group for any value of c. For instance, this happens if $G_1 = \mathbb{Z}/2\mathbb{Z}$ (with $c_1 = 1$) and $G_2 = UT(3, \mathbb{Q})$ (with $c_2 = 2$).

6.6.9 *Inner derivations and inner automorphisms*

Suppose G is a global class c Lazard Lie group and L is the corresponding global class c Lazard Lie ring. The group $G/Z(G) \cong \mathrm{Inn}(G)$ is in global class $c-1$ Lazard correspondence with the Lie ring $L/Z(L) \cong \mathrm{Inn}(L)$. In particular, $G/Z(G)$ and $L/Z(L)$ have the same underlying set.

For any x in the common underlying set of G and L, denote by $\overline{x}$ its image in the common underlying set of $G/Z(G)$ and $L/Z(L)$. We have two set maps of interest from L to itself induced by x:

- The automorphism of L arising from the inner automorphism of G given by conjugation by x, i.e., the map $g \mapsto xgx^{-1}$. We denote this as Ad_x.
- The inner derivation of L given as $g \mapsto [x, g]$. We denote this as ad_x.

We then have the relationship:

$$\mathrm{Ad}_x = \exp(\mathrm{ad}_x)$$

where the exponentiation occurs inside the ring $\mathrm{End}_{\mathbb{Z}}(L)$ of the additive group of L.

Deducing the result would require us to return to the free group scenario, obtain the result in that scenario where the group and Lie ring are both subsets in an associative ring, and then apply homomorphisms. We are not using this result for our main proofs, so we skip the proof. Interested readers may look at Lemma 3.3 of George Glauberman's paper [19].

This relationship continues to be valid in the general case (the 3-local case) that we discuss in the next section.

6.6.10 The case of adjoint groups

In Section 6.1, we introduced the general idea of the adjoint group of a radical ring. Suppose N is a nilpotent associative ring of nilpotency class c (this means that any product of length $c+1$ or more is zero) and $1+N$ is the corresponding adjoint group. We can view N as a Lie ring by using the same additive structure and defining:

$$[x, y] := xy - yx$$

N as a Lie ring also has nilpotency class at most c (although the nilpotency class as a Lie ring could be smaller). The following turn out to be true.

- The adjoint group $1+N$ is a nilpotent group of nilpotency class at most c. Note that this is true regardless of whether N is powered over any primes.

- Suppose the additive group of N is powered over the set π_c of all primes less than or equal to c. Then, the Lie ring N and the group $1+N$ are in global class c Lazard correspondence *up to isomorphism*. Moreover, the isomorphism is given by the set maps $\exp : N \to 1 + N$ and $\log : 1 + N \to N$ described in Section 6.1 (specifically, see Section 6.1.6). This follows quite directly from the analytical framework described in Section 6.1.

6.6.11 *The case of the niltriangular matrix Lie ring and the unitriangular matrix group*

The material discussed here builds on Section 1.1.6 in the introduction.

Suppose R is a commutative associative unital ring and n is a positive integer. We define $UT(n, R)$ as the group of $n \times n$ upper triangular matrices with 1s on the diagonal, with the group operation being the usual matrix multiplication. we define $NT(n, R)$ as the Lie ring of $n \times n$ strictly upper triangular matrices, with the Lie bracket defined as $[x, y] = xy - yx$ where the multiplication here is matrix multiplication. We had considered groups of the form $UT(n, R)$ and $NT(n, R)$ (in the case $n = 3$) when describing counterexamples to naively plausible statements about powering and divisibility in Sections 4.1.13 and 4.2.6.

The following turn out to be true for any positive integer c. Denote by π_c the set of all primes less than or equal to c.

1. The group $UT(c+1, R)$ is a group of nilpotency class c and the Lie ring $NT(c+1, R)$ is a Lie ring of nilpotency class c.

2. The group $UT(c+1, R)$ is the adjoint group to the radical ring $NT(c+1, R)$, based on the definitions in Section 6.1.

3. If the additive group of R is π_c-powered, the additive group of $NT(c+1, R)$ is also π_c-powered, and the group $UT(c+1, R)$ is also π_c-powered. This follows from (2) and the discussion in Section 6.6.10.

4. If the equivalent conditions for (3) hold, then the group $UT(c+1, R)$ is in global class c Lazard correspondence *up to isomorphism* with $NT(c+1, R)$. The logarithm and

exponential maps used to describe the bijection of sets are the usual matrix logarithm and exponential maps. This follows by combining (2) and the discussion in Section 6.6.10.

Particular cases of interest for the above scenario are:

- R is a field of characteristic zero. Note that in this case, we get an instance of the class c Malcev correspondence.
- R is a field of characteristic p, where $p > c$.
- R is a local ring of characteristic p^k, where p is the underlying prime and $p > c$. For instance, the case $c = 2$ and $R = \mathbb{Z}/9\mathbb{Z}$.

6.7 The general definition of the Lazard correspondence: 3-local case

6.7.1 Definition of local nilpotency class

This is the general version of the Lazard correspondence.

Definition (k-local nilpotency class)**.** Suppose G is a group and k is a positive integer (we are generally interested in $k \geq 2$). The *k-local nilpotency class* of G is the supremum over all subgroups H of G with generating set of size at most k of the nilpotency class of H. Note that if any subgroup of G with generating set of size at most k is non-nilpotent, *or* if there is no common finite upper bound on the nilpotency classes of all such subgroups, then the k-local nilpotency class is ∞.

We say that G is a group of k-local nilpotency class (at most) c if the k-local nilpotency class of G is finite and less than or equal to c.

Definition (k-local nilpotency class of a Lie ring)**.** Suppose L is a Lie ring and k is a positive integer (we are generally interested in $k \geq 2$). The *k-local nilpotency class* of L is the supremum over all Lie subrings M of L with generating set of size at most k of the nilpotency class of M. Note that if any Lie subring of L with generating set of size at most k is non-nilpotent, *or* if there is no common finite upper bound on the nilpotency classes of all such subgroups, then the k-local nilpotency class is ∞.

We say that L is a Lie ring of k-local nilpotency class (at most) c if the k-local nilpotency class of L is finite and less than or equal to c.

6.7.2 Definition of Lazard Lie group and Lazard Lie ring, and the correspondence

We can now define Lazard Lie group and Lazard Lie ring.

Definition (Lazard Lie group)**.** Suppose G is a group and c is a positive integer. G is termed a *class c Lazard Lie group* if *both* the following conditions are satisfied:

1. The 3-local nilpotency class of G is at most c.
2. G is powered over all primes less than or equal to c.

Definition (Lazard Lie ring)**.** Suppose L is a Lie ring and c is a positive integer. L is termed a *class c Lazard Lie ring* if *both* the following conditions are satisfied:

1. The 3-local nilpotency class of L is at most c.
2. L is powered over all primes less than or equal to c.

The (3-local) class c Lazard correspondence is a correspondence:

$$\text{(3-local) class } c \text{ Lazard Lie groups} \leftrightarrow \text{(3-local) class } c \text{ Lazard Lie rings}$$

Note that the "(3-local)" qualifier may be specified on occasions where there is potential for confusion with the global class c Lazard correspondence. However, by default, in this section and later, if we just say *class c Lazard* (followed by any of the terms *correspondence*, *Lie group*, and *Lie ring*), we are referring to the 3-local case.

This correspondence works in a manner analogous to the global class c Lazard correspondence, and the remarks made in the preceding section (Section 6.6) about the global Lazard correspondence apply to the (3-local) Lazard correspondence. For brevity, we will not repeat the observations.

Note that the *formulas* use only 2 elements at a time. So one might naively expect that a "2-local" condition would suffice. However, the associativity condition for groups, and correspondingly, many of the Lie ring identities (associativity of addition, distributivity, and the Jacobi identity), reference three arbitrary elements at a time. This is why we need to impose the "3-local" condition. With this caveat, the reasoning is similar to that for the global class c Lazard correspondence. All the other remarks made in the previous section also apply. We had touched on the significance of the numbers 2 and 3 in an introductory section (Section 1.1.11) and we are now making use of the observations made at the time.

6.7.3 Divergence between the 3-local and global class cases

For $c = 1, 2, 3$, the global class c Lazard correspondence coincides with the class c Lazard correspondence. The cases $c = 1$ and $c = 2$ are obvious: if every 3-generated subgroup (respectively Lie subring) is abelian, the whole group (respectively, Lie ring) is abelian. Similarly, if every 3-generated subgroup (respectively Lie subring) has class at most two, the whole group (respectively, Lie ring) has class at most two. This is because the class two condition involves checking the triviality of $[[x, y], z]$, and this expression uses only three elements. The case $c = 3$ is more interesting, because it is not immediate. However, providing details of this case would distract us from our main goal, so we omit it. The case of $c = 3$ for Lie rings is discussed in the Appendix, Section B.2.1.

The global class c Lazard correspondence becomes strictly weaker than the class c Lazard correspondence for $c \geq 4$, as demonstrated by Lazard in [30]. For more about the relationship between local and global nilpotency, see the literature on Engel conditions and local nilpotency. In particular, the paper [41] by Pilgrim and the paper [42] by Plotkin provide a summary of the known results relating local and global nilpotency.

6.7.4 The p-group case of the Lazard correspondence

Recall that a p-group is a group in which the order of every element is a power of p. We use the term *p-Lie ring* for a Lie ring whose additive group is a p-group.

The *global* Lazard correspondence is a correspondence:

p-groups of nilpotency class at most $p-1 \leftrightarrow p$-Lie rings of nilpotency class at most $p-1$

The Lazard correspondence (including the 3-local case) is a correspondence:

p-groups of 3-local nilpotency class at most $p-1 \leftrightarrow p$-Lie rings of 3-local nilpotency class at most $p-1$.

CHAPTER 7

GENERALIZING THE LAZARD CORRESPONDENCE TO A CORRESPONDENCE UP TO ISOCLINISM

7.1 The Lie bracket and group commutator in terms of each other: prime bounds

7.1.1 Group commutator formula in terms of the Lie bracket

For reasons that will become clear later, we will work with the class $(c+1)$ Baker-Campbell-Hausdorff formula instead of the class c Baker-Campbell-Hausdorff formula, where c is a positive integer. This is purely a matter of notation, and its main advantage is that later results that use the results here can do so directly without needing to increase or decrease the values by one.

In the usual Lazard correspondence, there is an explicit formula for the group commutator of two elements in terms of Lie brackets. In fact, there is an infinite series, which can be obtained from the Baker-Campbell-Hausdorff formula series, whose truncations give the formula for the group commutator. We will now describe how this formula is obtained.

Note that the explicit expressions here are sensitive to whether we use the left or right action convention for computing the group commutator. We will use the left action convention.

$$[x, y]_{\text{Group}} = (xy)(yx)^{-1}$$

Inverses in the group correspond to taking the negative in the Lie ring, so this becomes:

$$[x, y]_{\text{Group}} = (xy)(-(yx))$$

We now need to apply the Baker-Campbell-Hausdorff formula to expand each piece.

We have the following in the class $(c+1)$ case:

$$xy = x + y + t_2(x, y) + t_3(x, y) + \cdots + t_{c+1}(x, y)$$
$$yx = y + x + t_2(y, x) + t_3(y, x) + \cdots + t_{c+1}(y, x)$$

We thus get the following expression for $[x, y]_{\text{Group}}$.

$$(x + y + t_2(x, y) + t_3(x, y) + \cdots + t_{c+1}(x, y))$$
$$-(y + x + t_2(y, x) + t_3(y, x) + \cdots + t_{c+1}(y, x))$$
$$+t_2(xy, -(yx)) + t_3(xy, -(yx)) + \cdots + t_{c+1}(xy, -(yx))$$

Based on the symmetry and skew symmetry properties deduced in the preceding section, we obtain the following, where c' is the largest even number less than or equal to $c+1$:

$$[x, y]_{\text{Group}} = 2(t_2(x, y)+t_4(x, y)+\cdots+t_{c'}(x, y))+t_2(xy, -(yx))+t_3(xy, -(yx))+\cdots+t_{c+1}(xy, -(yx))$$

It is also the case that $t_{c+1}(xy, -(yx)) = 0$. This is because when we expand these out, all the degree c terms in the product are iterated products with each piece equal to $(x + y)$ or $-(x + y)$, and all higher degree terms are anyway zero. Thus, the group commutator simplifies to:

$$[x, y]_{\text{Group}} = 2(t_2(x, y)+t_4(x, y)+\cdots+t_{c'}(x, y))+t_2(xy, -(yx))+t_3(xy, -(yx))+\cdots+t_c(xy, -(yx))$$

Denote this formula of x and y by $M_{c+1}(x, y)$. In other words:

$$[x, y]_{\text{Group}} = M_{c+1}(x, y)$$

Note that in the case that we are using the Lazard correspondence up to isomorphism, such as the case where we are using the exponential and logarithm maps inside an associative ring of class $c + 1$, M_{c+1} can be interpreted as follows:

$$e^{M_{c+1}(x,y)} = [e^x, e^y]_{\text{Group}}$$

The distinction between this and the earlier interpretation is that with the earlier intepretation, we identified x and e^x as the same element, whereas now, we are treating them as different elements. The latter interpretation makes sense when we are describing the exponential and logarithm maps inside an associative ring.

Note that the explicit formula M_{c+1} is sensitive to whether we are using the left action convention or the right action convention, but the existence of a formula of the sort is not, and the general properties of the prime divisors of denominators for the formula are not. The corresponding formula with the right action convention would expand the product $(yx)^{-1}(xy)$ instead of $(xy)(yx)^{-1}$, and the steps would be fairly similar. The results from this point onward do not depend on the choice of action convention (left versus right).

We are now in a position to prove a lemma.

Lemma 7.1.1. In the formula $M_{c+1}(x, y)$ for the group commutator $[x, y]_{\text{Group}}$ in terms of Lie ring operations (addition and Lie bracket) in class $c + 1$, all prime divisors of the denominators are less than or equal to c.

Proof. We divide into cases:

- $c = 1$, so that $c + 1 = 2$: In this case, we can work the formula out and we get that $[x, y]_{\text{Group}} = [x, y]$. This satisfies the condition, since there are no prime factors of the denominator.

- c is even, so that $c + 1$ is odd: In this case, the formula above shows that we use terms only up to t_c, and do not use t_{c+1}. Thus, we can only get the primes less than or equal to c.

- c is odd and at least 3, so that $c + 1$ is even and greater than 2: In this case, $c + 1$ is composite. We know from the formula that we only use primes less than or equal to $c + 1$. Since $c + 1$ is composite, this means we only use primes less than or equal to c.

$\square$

It is also possible to construct an infinite series expression whose truncations give the group commutator formulas for various choices of 3-local nilpotency class.

The importance of these observations is as follows. We can make sense of the formula for $M_{c+1}(x, y)$ for certain Lie rings that are *not* Lazard Lie rings. Specifically, we can make sense of this formula for Lie rings of 3-local nilpotency class $(c + 1)$ which are uniquely divisible by primes strictly *less* than $c + 1$, but not by $c + 1$ itself. This case is of interest (i.e., it conveys nontrivial information) when $c + 1$ itself is a prime number. We will build on the results here in Sections 7.3.4 and 7.7.

The procedure outlined above has been used to compute M_{c+1} for small values of c in the Appendix. The case $c = 2$ is described in Section B.1.4 and the case $c = 3$ is described in Section B.1.5.

7.1.2 Inverse Baker-Campbell-Hausdorff formula: bound on denominators

We want to prove a similar result for the bounds on prime powers of denominators for the formula h_2 that describes the Lie bracket of the Lie ring in terms of group commutators.

The result follows from Theorem 6.4 in [9], but we provide a minimalistic proof below that builds on Lemma 7.1.1.

Lemma 7.1.2. In the formula $h_{2,c+1}(x,y)$ for the Lie bracket $[x,y]_{\text{Lie}}$ in terms of group commutators, all prime divisors of the denominators in the exponents are less than or equal to c.

Proof. Recall that $M_{c+1}(x,y)$ expresses the group commutator in terms of the Lie bracket and its iterations, whereas $h_{2,c+1}(x,y)$ expresses the Lie bracket in terms of the group commutator and its iterations. These formulas are therefore "inverses" of each other in the following sense. Denote by $(h_{2,c+1} \circ M_{c+1})(x,y)$ the formula that substitutes, in each of the commutators appearing in the expression for $h_{2,c+1}$, the formula for M_{c+1}, and then expands group products of these commutators as Lie ring expressions using the class $(c+1)$ Baker-Campbell-Hausdorff formula. Then:

$$(h_{2,c+1} \circ M_{c+1})(x,y) \equiv [x,y]_{\text{Lie}},$$

where the equality is considered modulo $\mathcal{A}^{c+2}$ where $\mathcal{A}$ is the free associative $\mathbb{Q}$-algebra with generators x and y. Replacing $c+1$ by c above, we obtain:

$$(h_{2,c} \circ M_c)(x,y) \equiv [x,y]_{\text{Lie}} \pmod{\mathcal{A}^{c+1}}$$

Thus, we get that:

$$(h_{2,c} \circ M_c)(x,y) \equiv [x,y]_{\text{Lie}} + \chi_{c+1}(x,y) \pmod{\mathcal{A}^{c+2}}$$

where χ_{c+1} is a $\mathbb{Q}$-linear combination of weight $c+1$ Lie products. Note that since χ_{c+1} is obtained by composing and manipulating terms from $h_{2,c}$, M_c, and the class c Baker-Campbell-Hausdorff formula, all the prime divisors appearing in its denominators are less than or equal to c.

We also have that:

$$M_{c+1}(x,y) = M_c(x,y) + \xi_{c+1}(x,y)$$

where, by Lemma 7.1.1, all the prime divisors of denominators appearing in the expression for ξ_{c+1} are less than or equal to c. It follows that:

$$(h_{2,c} \circ M_{c+1})(x,y) \equiv [x,y]_{\text{Lie}} + \chi_{c+1}(x,y) + \xi_{c+1}(x,y)$$

It now follows that:

$$h_{2,c+1}(x,y) = h_{2,c}(x,y)(\tilde{\chi}_{c+1}(x,y)\tilde{\xi}_{c+1}(x,y))^{-1}$$

where $\tilde{\chi}$ and $\tilde{\xi}$ denote the same expressions as those used for χ and ξ but interpreting the Lie brackets as commutators. This works because the $(c+1)$-fold iterated commutator coincides with the $(c+1)$-fold iterated Lie bracket in class $c+1$. In other words, the set map:

$$(x_1, x_2, \ldots, x_{c+1}) \mapsto [[\ldots[x_1, x_2], x_3], \ldots, x_c], x_{c+1}]$$

is the same whether we interpret the brackets on the right as group commutators or as Lie brackets: this follows immediately from the formula M_{c+1}.

In particular, note that the only prime divisors that appear in the denominators of the exponents on the right are primes less than or equal to c, completing the proof. $\square$

The case $c = 2$ (so that $c+1 = 3$) has been worked out in the Appendix, Section B.1.6. Readers interested in understanding the proof via a concrete illustration are advised to read this.

7.2 Lazard correspondence, commutativity relation, and central series

7.2.1 The commutativity relation and the upper central series

We begin with an important lemma.

Lemma 7.2.1. Suppose G is a (3-local) class c Lazard Lie group and $L = \log(G)$ is its Lazard Lie ring. Then, for elements $x, y \in G$, the commutator $[x, y]$ is the identity element of G if and only if the Lie bracket $[x, y]$ is zero. In other words, x and y commute as group elements if and only if they commute as Lie ring elements.

Proof. In Section 7.1.1, we described a formula M_{c+1} for the group commutator in terms of the Lie bracket. The formula makes it clear that if the Lie bracket is zero, the group commutator is the identity element.

In Section 6.4, we described a formula $h_{2,c+1}$ for the Lie bracket in terms of the group commutator. The formula makes it clear that if the group commutator is the identity element, then the Lie bracket is zero. $\square$

It is possible to prove one direction directly from the Baker-Campbell-Hausdorff formula rather than referencing the above sections. The idea behind a direct proof would be to show that if the Lie bracket $[x, y]$ is 0, then $xy = x + y = yx$, so that the group commutator is zero.

We now show that the Lazard correspondence relates the upper central series of the Lie ring with the upper central series of the group.

Theorem 7.2.2. Suppose G is a (3-local) class c Lazard Lie group and $L = \log(G)$ is its Lazard Lie ring. Then the following are true:

1. $\log(Z(G)) = Z(L)$ (this is an instance of the 3-local class c Lazard correspondence)

2. $\log(G/Z(G)) = L/Z(L)$ (this is an instance of the 3-local class c Lazard correspondence)

3. For all positive integers i, we have $\log(Z^i(G)) = Z^i(L)$ and $\log(G/Z^i(G)) = L/Z^i(L)$. where Z^i denotes the i^{th} member of the upper central series (for G or L respectively).

4. For all positive integers $i > j$, $\log(Z^i(G)/Z^j(G)) = Z^i(L)/Z^j(L)$ where Z^i, Z^j denote the i^{th} and j^{th} members of the lower central series (for G or L respectively).

Note that since we are in general using the 3-local class c Lazard correspondence, the global class of G and L may be greater than c. Thus, the result is potentially of interest even for $i \geq c$.

Proof. Proof of (1): The fact that $\log(Z(G)) = Z(L)$ follows immediately from the preceding lemma (Lemma 7.2.1). By Lemmas 4.1.5 and 4.2.3, $Z(G)$ and $Z(L)$ are both π_c-powered, so this is an instance of the 3-local class c Lazard correspondence.

Proof of (2): This follows from (1) and from facts for the 3-local class c Lazard correspondence similar to those for the global Lazard correspondence described in Section 6.6.8. Thus, $\log(G/Z(G)) = L/Z(L)$.

Proof of (3): We obtain this by induction using (1) and (2).

Proof of (4): This follows from (3), using reasoning similar to that in (2). □

7.2.2 The commutator map and the lower central series

We begin with a lemma.

Lemma 7.2.3. Suppose G is a 3-local class c Lazard Lie group and $L = \log(G)$ is its Lazard Lie ring. Suppose H is a π_c-powered normal subgroup of G and $I = \log(H)$ is the corresponding π_c-powered ideal of L. Then, $[G,H]$ is a π_c-powered normal subgroup of G, $[L,I]$ is a π_c-powered ideal of L, and $[L,I] = \log([G,H])$.

Proof. $[G,H]$ is normal by basic group theory, and it is π_c-powered by Lemma 4.1.22. $[L,I]$ is a π_c-powered ideal by basic Lie ring theory. Thus, $\log([G,H])$ is a 3-local class c Lazard Lie subring of L, and $\exp([L,I])$ is a 3-local class c Lazard Lie subgroup of G. It therefore suffices to show that a generating set for $[G,H]$ is inside $[L,I]$ and that a generating set for $[L,I]$ is inside $[G,H]$.

Proof that $\log([G,H]) \subseteq [L,I]$: It suffices to show that every element of the form $[g,h]$, for $g \in G, h \in H$, is in $[L,I]$. This follows from the formula $[g,h] = M_{c+1}(g,h)$ described in Section 7.1.1. In particular, we use Lemma 7.1.1 to argue that the expression is in $[L,I]$.

Proof that $[L,I] \subseteq \log([G,H])$: It suffices to show that every element of the form $[x,y]$, for $x \in L$, $y \in I$, is in $[G,H]$. This follows from the formula $[x,y] = h_{2,c+1}(x,y)$ described as the second inverse Baker-Campbell-Hausdorff formula in Section 6.4. In particular, we use Lemma 7.1.2 to argue that the expression is in $[G,H]$. □

We now show that the Lazard correspondence relates the lower central series of the Lie ring with the lower central series of the group.

Theorem 7.2.4. Suppose G is a 3-local class c Lazard Lie group and $L = \log(G)$ is its Lazard Lie ring. Then, the following hold.

1. For all positive integers i, $\log(\gamma_i(G)) = \gamma_i(L)$ where γ_i denotes the i^{th} member of the lower central series (for G or L respectively).

2. For all positive integers $i < j$, $\log(\gamma_i(G)/\gamma_j(G)) = \gamma_i(L)/\gamma_j(L)$. In particular, setting $i = 1$, $\log(G/\gamma_j(G)) = L/\gamma_j(L)$.

Proof. Proof of (1): This follows by inducting on Lemma 7.2.3. The base case $i = 1$ is given.

For the inductive step from i to $i+1$, set $H = \gamma_i(G)$ and $I = \gamma_i(L)$.

Proof of (2): This follows from (1). $\square$

7.3 The Malcev and Lazard correspondence in the free case

7.3.1 Setup

We use the same notation as in Section 6.2.1. The notation is reviewed below for convenience. Denote by $\mathcal{A}$ the free associative $\mathbb{Q}$-algebra on a generating set $S = \{x_1, x_2, \dots\}$. The generating set may have any cardinality. By the well-ordering principle, we will index the generating set by a well-ordered set. For a positive integer c, define $A := \mathcal{A}/\mathcal{A}^{c+1}$. A can be described as the free nilpotent associative algebra of class c on the same generating set S. Explicitly, this means that all products in A of length more than c become zero.

Denote by $\mathcal{L}$ the Lie subring of $\mathcal{A}$ generated by the free generating set S. Note that $\mathcal{L}$ is *only* a Lie ring, *not* a $\mathbb{Q}$-Lie algebra. $\mathbb{Q}\mathcal{L}$ is the $\mathbb{Q}$-Lie algebra generated by S in $\mathcal{A}$.

We can define L in the following equivalent ways:

- $L = \mathcal{L}/\gamma_{c+1}(\mathcal{L}) = \mathcal{L}/(\mathcal{L} \cap \mathcal{A}^{c+1})$.
- L is the Lie subring generated by the image of S inside A, i.e., it is the Lie subring generated by the freely generating set inside A.

Denote by F the group generated by the elements e^{x_i}, x_i varying over the generating set S of L. As per Theorem 6.2.2, F is a free nilpotent group with e^{x_i} forming a freely generating set.

We can define an exponential map

$$\exp : L \to 1 + A$$

by:

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^c}{c!}$$

We can also define a logarithm map:

$$\log : F \to A$$

by:

$$\log x = (x-1) - \frac{(x-1)^2}{2} + \frac{(x-1)^3}{3} - \cdots + \frac{(-1)^c(x-1)^c}{c}$$

We might naively hope that $\exp(L) = F$ and $\log(F) = L$. This, however, is not the case. A somewhat weaker version of the statement *is* true, as described in Section 6.4.5 (the original proof is in Khukhro's book [29], Theorem 10.22), and we recall that below, because we will be using it extensively in some of our proofs. Denote by π_c the set of all primes less than or equal to c. Then, for any prime set $\sigma \supseteq \pi_c$, $\sqrt[\sigma]{F} = \exp(\mathbb{Z}[\sigma^{-1}]L)$. In particular, both of these hold:

- $\sqrt[\pi_c]{F} = \exp(\mathbb{Z}[\pi_c^{-1}]L)$
- $\sqrt{F} = \exp(\mathbb{Q}L)$

7.3.2 Interpretation as correspondences up to isomorphism

In Section 1.3.5, we had described the abelian Lie correspondence *up to isomorphism.* This differs from the abelian Lie correspondence in the important sense that the group and the Lie ring need not have the same underlying set. Instead, we are given a set map (denoted exp) from the Lie ring to the group and a set map (denoted log) from the group to the Lie ring that play the role of identifying the sets with each other. We noted in Section 1.3.9 that this notion of relaxing *up to isomorphism* applies to all the similarly defined correspondences in this document. In Section 5.1.8, we noted that the notion applies to the Baer correspondence.

The notion of a correspondence up to isomorphism also applies to the Malcev correspondence and the Lazard correspondence. In both cases, we need to specify a set map from the Lie ring to the group (customarily denoted exp) and a set map from the group to the Lie ring (customarily denoted log) that play the role of identifying the sets.

Using the same notation as in Section 7.3.1, we obtain the following correspondences up to isomorphism:

- The Lie ring $\mathbb{Q}L$ and the group $\sqrt{F}$ are in class c Malcev correspondence up to isomorphism. The exp and log maps defining the correspondence coincide with the exp and log maps defined in Section 7.3.1. This is not a coincidence: the terminology exp and log that we introduced in the abstract setting was specifically *chosen* based on this setup.
- For any prime set σ containing π_c, the Lie ring $\mathbb{Z}[\sigma^{-1}]L$ and the group $\sqrt[\sigma]{F}$ are in global class c Lazard correspondence up to isomorphism. The exp and log maps defining the correspondence coincide with the exp and log maps defined in Section 7.3.1.
- In particular, the Lie ring $\mathbb{Z}[\pi_c^{-1}]L$ and the group $\sqrt[\pi_c]{F}$ are in global class c Lazard correspondence up to isomorphism, with the same exp and log maps.

7.3.3 Restriction of the Malcev correspondence to groups and Lie rings that lack adequate powering

We continue using the same notation as above: L is a free nilpotent Lie ring of class c on the generating set S, and F is a free nilpotent group of class c on the generating set e^S, which is in canonical bijection with S. We had already noticed that L and F are not in Lazard correspondence with one another. We will now take a closer look at the statement.

Any element of L can be written as a sum involving the x_is and Lie products involving the x_is. Consider, for instance, the case that $|S| = 2$ and the generating set is $\{x_1, x_2\}$.

Consider the element $x_1 + x_2$ of L. Then, to find $e^{x_1+x_2}$, we can use the inverse Baker-Campbell-Haudorff formula, and obtain:

$$e^{x_1+x_2} = h_{1,c}(e^{x_1}, e^{x_2})$$

The formula $h_{1,c}$ involves taking p^{th} roots for primes $p \in \pi_c$. Therefore, even though the elements e^{x_1} and e^{x_2} are in F, the element $e^{x_1+x_2}$ is not in F if $c \geq 2$.

Consider a more complicated element of L.

$$z = x_1 + x_2 + 3[x_1, x_2]$$

We can compute e^z by splitting z as a sum $(x_1 + x_2) + 3[x_1, x_2]$, then splitting $x_1 + x_2$ as a sum again, and also $h_{2,c}$ to compute $e^{[x_1,x_2]}$. The final formula is:

$$e^z = h_{1,c}(h_{1,c}(e^{x_1}, e^{x_2}), (h_{2,c}(e^{x_1}, e^{x_2}))^3)$$

Once again, we are guaranteed that $e^z \in \sqrt[\pi_c]{F}$. However, it will not in general be in F itself.

There do exist some elements of L whose exponential is in F. For instance, all the elements of the generating set S have exponentials in F. Other examples also exist. For instance, in the case $c = 2$, the exponential of $[x_1, x_2]$ is $[e^{x_1}, e^{x_2}]$ and is inside F. The subset of L comprising those elements whose exponential is in F is a generating set for L as a Lie ring (because in particular it contains S) and therefore in particular it is *not* a subring of L.

Suppose now that we consider the Lie ring $\mathbb{Z}[\sigma^{-1}]L$ and the group $\sqrt[\sigma]{F}$, where σ is a subset of π_c that does not include all the primes in π_c. Note that the whole Lie ring $\mathbb{Z}[\sigma^{-1}]L$ is not in Lazard correspondence with the whole group $\sqrt[\sigma]{F}$. In particular, $\exp(\mathbb{Z}[\sigma^{-1}]L)$ is not contained in $\sqrt[\sigma]{F}$, and $\log(\sqrt[\sigma]{F})$ is not contained in $\mathbb{Z}[\sigma^{-1}]L$.

It might still be the case, however, that there are subrings of $\mathbb{Z}[\sigma^{-1}]L$ that are in Lazard correspondence with certain subgroups of $\sqrt[\sigma]{F}$. The naive intuition is that, as long as the formulas involved require division only by the primes in σ and not by any of the other primes in π_c, the correspondence should work.

We will now establish a few important results of this sort.

7.3.4 Lazard correspondence between derived subgroup and derived subring

The following result is an extremely important first step both in defining and in establishing important aspects of the Lazard correspondence up to isoclinism.

We will perform our calculuations in class $c+1$. This will make it easier to use our results directly in later sections. However, it will be a slight departure from the preceding discussion. For clarity, we use subscripts to remind ourselves of the class we are operating in.

Let c be a positive integer and π_c be the set of all primes less than or equal to c. Let S be a set. The algebra $A = A_{c+1}$, the Lie ring $L = L_{c+1}$, and the group $F = F_{c+1}$ are defined the same way as in Sections 7.3.1 and 7.3.2, but replacing c by $c+1$. In particular, A is a free $\mathbb{Q}$-algebra on S of nilpotency class $c+1$, L is the Lie subring of A_{c+1} generated by S, and D is the group generated by $e^{x_i}, x_i \in S$.

Let K be the group $\sqrt[\pi_c]{F}$ and N be the group $\mathbb{Z}[\pi_c^{-1}](L)$. As shown in Theorem 6.2.2, K is a free π_c-powered class $(c+1)$ group on e^S (and therefore canonically isomorphic to the free π_c-powered class $(c+1)$ group on S), and N is a free π_c-powered class $(c+1)$ Lie ring on S.

Before proceeding, we note a few basic facts that we will repeatedly use in the course of our proofs.

- $\sqrt{F} = \sqrt{K}$ is the free $\mathbb{Q}$-powered group on e^S.
- $\mathbb{Q}N = \mathbb{Q}L$ is the free $\mathbb{Q}$-powered Lie ring on S.

Our eventual goal will be to show that the exponential and logarithm map establish a Lazard corespondence between $[N, N]$ and $[K, K]$. We will begin by establishing some preliminaries.

Lemma 7.3.1. With notation as above, the following are true:

1. $[N, N]$ is a global class c Lazard Lie ring, i.e., it is a π_c-powered Lie ring of nilpotency class at most c.

2. $[K, K]$ is a global class c Lazard Lie group, i.e., it is a π_c-powered group of nilpotency class at most c.

3. Under the exponential map from A to $1 + A$, $\exp([N, N])$ is a π_c-powered subgroup of $1 + A$ (in fact, it is a subgroup of $\sqrt{F}$). Moreover, the exponential and logarithm maps establish a Lazard correspondence up to isomorphism between $[N, N]$ and $\exp([N, N])$.

4. Under the logarithm map from $1 + A$ to A, $\log([K, K])$ is a π_c-powered Lie subring of A (in fact, it is a Lie subring of $\mathbb{Q}L$). Moreover, the exponential and logarithm maps establish a Lazard correspondence up to isomorphism between $\log([K, K])$ and $[K, K]$.

Proof. We prove the parts one by one.

1. $[N, N]$ is a global class c Lazard Lie ring:

    - $[N, N]$ is π_c-powered: This follows from the fact that N is π_c-powered and Lemma 4.2.8.

    - $[N, N]$ has nilpotency class at most c: In fact, since N has nilpotency class $c + 1$, $[N, N]$ has nilpotency class at most $\lfloor (c + 1)/2 \rfloor$, which is less than or equal to c.

2. $[K, K]$ is a global class c Lazard Lie group:

    - $[K, K]$ is π_c-powered: The follows from the fact that K is π_c-powered and Theorem 4.1.20.

- $[K, K]$ has nilpotency class at most c: In fact, since K has nilpotency class $c+1$, $[K, K]$ has nilpotency class at most $\lfloor (c+1)/2 \rfloor$, which is less than or equal to c.

3. This follows directly from (1) and applying the global Lazard correspondence between *subrings and subgroups* described in Section 6.6.8, to the Lazard correspondence between $\mathbb{Q}L$ and $\sqrt{F}$.

4. This follows directly from (2) and applying the global Lazard correspondence between *subrings and subgroups* described in Section 6.6.8, to the Lazard correspondence between $\mathbb{Q}L$ and $\sqrt{F}$.

$\square$

Lemma 7.3.2. With notation as above, the following are true (recall that $Z(\sqrt{K})$ is the center of $\sqrt{K} = \sqrt{F}$):

1. Under the exponential map $\exp : \mathbb{Q}L = \mathbb{Q}N \to \sqrt{F} = \sqrt{K}$ (which in turn is obtained from the exponential map $\exp : A \to 1 + A$), we have $\exp(N) \subseteq KZ(\sqrt{K})$.

2. Under the logarithm map $\log : \sqrt{F} = \sqrt{K} \to \mathbb{Q}L = \mathbb{Q}N$ (which in turn is obtained from the logarithm map $\log : 1 + A \to A$), we have $\log(K) \subseteq N + Z(\mathbb{Q}N)$.

3. Under the exponential map $\exp : \mathbb{Q}L = \mathbb{Q}N \to \sqrt{F} = \sqrt{K}$ (which in turn is obtained from the exponential map $\exp : A \to 1 + A$), we have $K \subseteq \exp(N)Z(\sqrt{K})$.

4. Under the logarithm map $\log : \sqrt{F} = \sqrt{K} \to \mathbb{Q}L = \mathbb{Q}N$ (which in turn is obtained from the logarithm map $\log : 1 + A \to A$), we have $N \subseteq \log(K) + Z(\mathbb{Q}N)$.

Proof. Consider the quotient map $A \to A/A^{c+1}$. This map factors out the products of length $c+1$ and the quotient is therefore the free nilpotent associative algebra of nilpotency class c on S. Based on the setup described in Section 6.2, the image of F under the quotient map is F_c (the class c version of F) and the image of L under the quotient map is L_c (the class c version of L). Denote by K_c and N_c the images of K and N under the quotient map. Then, $K_c = \sqrt[\pi_c]{F_c}$ and $N_c = \mathbb{Z}[\pi_c^{-1}]L_c$, so that K_c and N_c are in global class c Lazard correspondence up to isomorphism.

Proof of (1): For $x \in N$, denote by $\overline{x}$ the image of x in N_c. Then, $\exp(\overline{x}) = \overline{\exp(x)} \in K_c$, so $\exp(x)$ can be written in the form $g + a$ where $g \in K$ and a is in the $(c+1)^{th}$ graded component of A. This can be rewritten as $g(1 + g^{-1}a)$. The element $1 + g^{-1}a$ is an element of $\sqrt{F} = \sqrt{K}$, and $g^{-1}a$ is in the $(c+1)^{th}$ graded component of A, so that $1 + g^{-1}a \in Z(\sqrt{F}) = Z(\sqrt{K})$.

Proof of (2): For $g \in K$, denote by $\overline{g}$ the image of g in K_c. Then, $\log(\overline{x}) = \overline{\log(x)} \in N_c$, so $\log x$ can be written in the form $x + a$ where $x \in N$ and a is in the $(c+1)^{th}$ graded component of A, so that $a \in Z(\mathbb{Q}L) = Z(\mathbb{Q}N)$.

Proof of (3): For $g \in K$, part (2) says that we can write $\log g = x + a$ where a is central. Exponentiating both sides, we obtain that $g = e^x e^a$, with $e^a \in Z(\sqrt{K})$.

Proof (4): For $x \in N$, part (1) says that we can write $e^x = gu$ where $g \in K$ and $u \in Z(\sqrt{K})$. Taking logarithms both sides, and using the centrality of u, we obtain that $x = \log g + \log u$, with $\log u \in Z(\mathbb{Q}N)$. $\square$

Theorem 7.3.3 (Lazard correspondence between derived subgroup and derived subring)**.** With notation as above, the derived subgroup $[K, K]$ and the derived subring $[N, N]$ are in Lazard correspondence up to isomorphism. Moreover, this Lazard correspondence arises as a restriction of the Malcev correspondence between $\sqrt{F} = \hat{K}$ and $\mathbb{Q}N = \mathbb{Q}L$ described in Section 7.3.2.

Before we begin the proof, we make a few remarks. First, note that K and N are very close to being in Lazard correspondence themselves. If we had inverted all primes in π_{c+1}, then we would have obtained the Lazard correspondence. This also means that if $c + 1$ is composite, then K and N *are* in Lazard correspondence. In that case, the result follows from Theorem 7.2.4.

The case of interest is where $c+1$ is prime, so that K and N are not in Lazard correspondence themselves. In other words, when we compute e^u for some $u \in N$, we do obtain an element of $\sqrt{K}$ but not necessarily an element of K. We want to show that if the element of N that we start with is in $[N, N]$, then computing the exponential gives an element in $[K, K]$, and that every element of $[K, K]$ can be obtained in this fashion.

We are now in a position to begin the proof.

Proof. By Lemma 7.3.1, it suffices to show that $\exp([N, N]) = [K, K]$, or equivalently, that $\log([K, K]) = [N, N]$. We can show this in two steps: showing that $[K, K] \subseteq \exp([N, N])$ and showing that $[N, N] \subseteq \log([K, K])$.

1. Proof that $[K, K] \subseteq \exp([N, N])$: Lemma 7.3.1 established that $\exp([N, N])$ is a group. Thus, it suffices to show that a generating set of $[K, K]$ is in $\exp([N, N])$. Specifically, it suffices to show that for all $g, h \in K$, $[g, h] \in \exp([N, N])$.

   By Lemma 7.3.2 (part (3)), $g = e^x u$ and $h = e^y v$ where $x, y \in N$ and $u, v \in Z(\sqrt{K})$. Thus, $[g, h] = [e^x, e^y] = e^{M_{c+1}(x,y)}$. By Lemma 7.1.1, M_{c+1} uses only division by primes in π_c, so that $[g, h] \in \exp([N, N])$.

2. Proof that $[N, N] \subseteq \log([K, K])$: We showed in Lemma 7.3.1 that $\log([K, K])$ is a Lie ring. Thus, it suffices to show that a generating set of $[N, N]$ is in $\log([K, K])$. Specifically, it suffices to show that for $x, y \in N$, $[x, y] \in \log([K, K])$.

   By Lemma 7.3.2 (part (4)), $x = \log g + s$ and $y = \log k + t$ where $g, k \in K$ and $s, t \in Z(\mathbb{Q}N)$. Thus, $[x, y] = [\log g, \log k] = \log(h_{2,c+1}(g, k))$. By Lemma 7.1.2, $h_{2,c+1}(g, k) \in [K, K]$, so $[x, y] \in \log([K, K])$.

$\square$

In later applications of the result, we will use the result in its *abstract* form, i.e., instead of treating K and N as subsets inside $\mathbb{Q} + A$ as we did above, we will treat them as the abstract free π_c-powered group and Lie ring respectively of class $c + 1$.

Lemma 7.3.4. Continuing notation from the preceding theorem (Theorem 7.3.3), let $K_1 = K/\gamma_c(K)$ and $N_1 = N/\gamma_c(N)$. Let R be the π_c-powered normal subgroup of K containing $\gamma_c(K)$ while J is a π_c-powered ideal of N containing $\gamma_c(N)$. Let $R_1 = R/\gamma_c(K)$ and $J_1 = J/\gamma_c(N)$. Further, suppose that $R_1 = \exp(J_1)$ with respect to the Lazard correspondence given by the usual logarithm and exponential map between N_1 and K_1. Then, the following are true:

1. Under the exponential map $\exp : \mathbb{Q}L = \mathbb{Q}N \to \sqrt{F} = \sqrt{K}$ (which in turn is obtained from the exponential map $\exp : A \to 1 + A$), we have $\exp(J) \subseteq RZ(\sqrt{K})$.

2. Under the logarithm map $\log : \sqrt{F} = \sqrt{K} \to \mathbb{Q}L = \mathbb{Q}N$ (which in turn is obtained from the logarithm map $\log : 1 + A \to A$), we have $\log(R) \subseteq J + Z(\mathbb{Q}N)$.

3. Under the exponential map $\exp : \mathbb{Q}L = \mathbb{Q}N \to \sqrt{F} = \sqrt{K}$ (which in turn is obtained from the exponential map $\exp : A \to 1 + A$), we have $R \subseteq \exp(J)Z(\sqrt{K})$.

4. Under the logarithm map $\log : \sqrt{F} = \sqrt{K} \to \mathbb{Q}L = \mathbb{Q}N$ (which in turn is obtained from the logarithm map $\log : 1 + A \to A$), we have $J \subseteq \log(R) + Z(\mathbb{Q}N)$.

Proof. The proof is analogous to the proof of Lemma 7.3.2. $\square$

Theorem 7.3.5. Continuing notation from Lemma 7.3.4, the Lazard correspondence between $[K, K]$ and $[N, N]$ restricts to a Lazard correspondence between $R \cap [K, K]$ and $J \cap [N, N]$.

Before we begin the proof, note that R and J are not themselves necessarily in Lazard correspondence. They *would be* in Lazard correspondence if $c+1$ were composite, because in that case, $\pi_c = \pi_{c+1}$. We want to show here that even though R and J may themselves fail to be in Lazard correspondence, their respective intersections with $[K,K]$ and $[N,N]$ are in Lazard correspondence.

Proof. We prove the result in several steps:

1. $R \cap [K,K]$ is a global class c Lazard Lie group: By Lemma 7.3.1, $[K,K]$ is a global class c Lazard Lie group. In particular, it is π_c-powered and has nilpotency class at most c. R is given to be π_c-powered. Thus, $R \cap [K,K]$ is π_c-powered, and its nilpotency class is at most c. Note that the only bound we have on the nilpotency class of R is $c+1$, but bounding the class of $[K,K]$ is sufficient to bound the class of $R \cap [K,K]$.

2. $J \cap [N,N]$ is a global class c Lazard Lie ring: By Lemma 7.3.1, $[N,N]$ is a global class c Lazard Lie ring. In particular, it is π_c-powered and has nilpotency class at most c. J is π_c-powered. Thus, $J \cap [N,N]$ is π_c-powered, and its nilpotency class is at most c. Note that the only bound we have on the nilpotency class of J is $c+1$, but bounding the class of $[N,N]$ is sufficient to bound the class of $J \cap [N,N]$.

3. $\exp(J \cap [N,N]) \subseteq R \cap [K,K]$: We know that $\exp([N,N]) = [K,K]$, so $\exp(J \cap [N,N]) \subseteq [K,K]$. In addition, $\exp(J \cap [N,N]) \subseteq \exp(J)$. By Lemma 7.3.4 (part (1)), we obtain that $\exp(J \cap [N,N]) \subseteq RZ(\sqrt{K})$, and hence $\exp(J \cap [N,N]) \subseteq RZ(\sqrt{K}) \cap [K,K]$. We will show that $RZ(\sqrt{K}) \cap [K,K] = R \cap [K,K]$, completing the proof.

   Consider an element $g \in RZ(\sqrt{K}) \cap [K,K]$. Then, $g = uv$ with $u \in R$ and $v \in Z(\sqrt{K})$. We obtain that $v = u^{-1}g$. Since both R and $[K,K]$ are subgroups of K, we obtain that $v \in K$, so $v \in Z(\sqrt{K}) \cap K$, so that $v \in Z(K)$. But $Z(K) = \gamma_c(K)$ (both are precisely the elements in K that have the form $1 + a$ with a a homogeneous degree $c+1$ element of A), so $v \in \gamma_c(K) \subseteq R$. Thus, $g = uv \in R$, so that $g \in R \cap [K,K]$ as desired.

4. $\log(R\cap[K,K]) \subseteq J\cap[N,N]$: We know that $\log([K,K]) = [N,N]$, so $\log(R\cap[K,K]) \subseteq [N,N])$. In addition, $\log(R\cap[K,K]) \subseteq \log(R)$. By Lemma 7.3.4 (part (2)), we obtain that $\log(R\cap[K,K]) \subseteq J+Z(\mathbb{Q}N)$, and hence $\log(R\cap[K,K]) \subseteq (J+Z(\mathbb{Q}N))\cap[N,N]$. We will now show that $(J + Z(\mathbb{Q}N)) \cap [N,N] = J \cap [N,N]$, completing the proof.

   Consider an element $x \in (J + Z(\mathbb{Q}N)) \cap [N,N]$. Then, $x = y + z$ with $y \in J$ and $z \in Z(\mathbb{Q}N)$. We obtain that $z = x - y$. Since both J and $[N,N]$ are subrings of N, we obtain that $z \in N$, so $z \in Z(\mathbb{Q}N) \cap N$, so $z \in Z(N)$. We have $Z(N) = \gamma_c(N)$, so $z \in \gamma_c(N) \subseteq J$. Thus, $x = y + z \in J$, so $x \in J \cap [N,N]$ as desired.

□

Theorem 7.3.6. Continuing notation from the preceding theorem (Theorem 7.3.3), the Lazard correspondence between $[K,K]$ and $[N,N]$ restricts to a Lazard correspondence between $[K,R]$ and $[N,J]$.

Proof. 1. $[K,R]$ is a global class c Lazard Lie group and $[N,J]$ is a global class c Lazard Lie ring: This requires verifying that both $[K,R]$ and $[N,J]$ are π_c-powered, and both have class at most c. We break this down further:

   - $[K,R]$ is a π_c-powered group: This follows from Lemma 4.1.22.
   - $[N,J]$ is a π_c-powered Lie ring: This follows from N and J both being π_c-powered, and the additivity of the Lie bracket.
   - $[K,R]$ has nilpotency class at most c: $[K,R]$ is a subgroup of $[K,K]$, which has nilpotency class at most c as established in Theorem 7.3.3.
   - $[N,J]$ has nilpotency class at most c: $[N,J]$ is a subring of $[N,N]$, which has nilpotency class at most c as established in Theorem 7.3.3.

2. $\exp([N,J])$ is a group with which $[N,J]$ is in global class c Lazard correspondence up to isomorphism via exp, and $\log([K,R])$ is a Lie ring that is in global class c

Lazard correspondence with it via exp: These follow from Step (1) and the fact that the exponential and logarithm maps establish correspondences between global class c Lazard Lie subgroups and global class c Lazard Lie subrings.

3. $[K, R] \subseteq \exp([N, J])$ and $[N, J] \subseteq \log([K, R])$: We show both parts:

    - $[K, R] \subseteq \exp([N, J])$: In Step (2), we established that $\exp([N, J])$ is a group. Thus, it suffices to show that every commutator between an element of K and an element of R is in $\exp([N, J])$. Explicitly, given $g \in K$ and $h \in R$, we need to show that $[g, k] \in \exp([N, J])$.

      By Lemma 7.3.2 (part (3)) and Lemma 7.3.4 (part (3)), $g = e^x u$ and $h = e^y v$ where $x \in N$, $y \in J$ and $u, v \in Z(\sqrt{K})$. Thus, $[g, h] = [e^x, e^y] = e^{M_{c+1}(x,y)}$. By Lemma 7.1.1, M_{c+1} uses only division by primes in π_c, so that $[g, h] \in \exp([N, J])$.

    - $[N, J] \subseteq \log([K, R])$: In Step (2), we established that $\log([K, R])$ is a Lie ring. Thus, it suffices to show that a generating set of $[N, J]$ is in $\log([K, R])$. Specifically, it suffices to show that for $x \in N$ and $y \in J$, $[x, y] \in \log([K, R])$.

      By Lemma 7.3.2 (part (4)) and Lemma 7.3.4 (part (4)), $x = \log g + s$ and $y = \log k + t$ where $g \in K$, $k \in R$, and $s, t \in Z(\mathbb{Q}N)$. Thus, $[x, y] = [\log g, \log k] = \log(h_{2,c+1}(g, k))$. By Lemma 7.1.2, $h_{2,c+1}(g, k) \in [K, R]$, so $[x, y] \in \log([K, R])$.

Combining these, we obtain the result. □

7.4 Homology of powered nilpotent groups

7.4.1 Hopf's formula variant for Schur multiplier of powered nilpotent group

So far, we have studied the extension theory and homology theory of groups *qua* groups. We now consider the extension theory and homology theory in the context of π-powered groups.

For the results presented throughout this section, π is *any* set of primes. Later, we will apply the results to the case where $\pi = \pi_c$ is the set of all primes less than or equal to c, but the results for this section are not restricted to such sets of primes.

It turns out that, in the nilpotent case, the Schur multiplier, Schur covering group, exterior square, and all related constructions *qua* group are the same as the corresponding constructions *qua* π-powered group. This is specific to the nilpotent case.

Lemma 7.4.1. Suppose G is a π-powered nilpotent group. Then, the following hold:

1. All the homology groups $H_i(G;\mathbb{Z})$, $i > 0$, are π-powered abelian groups.

2. The Schur multiplier $M(G)$, which is $H_2(G;\mathbb{Z})$, is a π-powered abelian group.

Proof. Proof of (1): This follows from May and Ponto's text, [34], Theorem 6.1.1, implication (iii) $\implies$ (iv), setting $Z = K(G, 1)$ and T as the complement of π in the set of primes. The result appeared earlier in [25], Theorem 2.9. However, the notation and surrounding explanation in May and Ponto's text are easier to follow.

Proof of (2): This follows immediately from (1). □

Lemma 7.4.2. Suppose G is a π-powered nilpotent group. Every Schur covering group of G is π-powered. Since Schur covering groups exist and are by definition initial objects in the category of central extensions of G with homoclinisms, there exist initial objects in the category of extensions of G with homoclinisms that are π-powered.

Proof. By the preceding lemma (Lemma 7.4.1), $M(G) = H_2(G;\mathbb{Z})$ is π-powered. Consider a Schur covering group E of G. E is a central extension of the form:

$$0 \to M(G) \to E \to G \to 1$$

By Lemma 4.1.12, E is also π-powered. By definition, any Schur covering group gives an inital object in the category of central extensions of G with homoclinisms, so the last part of the statement follows.

Schur covering groups exist by Theorem 3.6.3, so the final sentence follows. □

We are now in a position to prove results that establish analogues of Hopf's formula (discussed in Section 3.6.9):

Theorem 7.4.3. Suppose π is a set of primes and G is a π-powered nilpotent group. Express G in the form $G \cong F/R$ where F is a free π-powered group. Then, the following are true.

1. The group $E_1 = F/[F, R]$, with the natural quotient map $E_1 \to G$, is an initial object in the category of central extensions of G with homoclinisms.
2. The exterior square $G \wedge G$ is canonically isomorphic to the quotient group $[F, F]/[F, R]$.
3. The Schur multiplier $M(G)$ is canonically isomorphic to the quotient group $(R \cap [F, F])/[F, R]$:

$$M(G) \cong (R \cap [F, F])/[F, R] \tag{7.1}$$

Proof. Proof of (1): Let E_2 be a Schur covering group of G. By Lemma 7.4.2, E_2 is π-powered.

Consider the commutator map $\omega_1 : G \times G \to E_1$ and denote by Ω_1 the corresponding group homomorphism:

$$\Omega_1 : G \wedge G \to [E_1, E_1]$$

Consider also the extension:

$$0 \to A \to E_2 \xrightarrow{\mu} G \to 1$$

with the natural commutator map $\omega_2 : G \times G \to E_2$ and the corresponding commutator map homomorphism:

$$\Omega_2 : G \wedge G \to [E_2, E_2]$$

Our goal is to show that there there exists a unique homomorphism $\varphi : [E_1, E_1] \to [E_2, E_2]$ such that $\varphi \circ \omega_1 = \omega_2$, or equivalently, $\varphi \circ \Omega_1 = \Omega_2$.

The map $\nu : F \to G$ lifts to a map $\psi : F \to E_2$ on account of F being a free π-powered group and E_2 being a π-powered group (note that the lift is not necessarily unique). Explicitly, this means that $\mu \circ \psi = \nu$.

We know that $\nu(R)$ is trivial, so $\mu(\psi(R))$ is trivial. Thus, $\psi(R)$ lands inside the kernel of μ, which is the image of A in E_2. Thus, $\psi(R)$ is a central subgroup of E_2. Therefore, $\psi([F, R]) = [\psi(F), \psi(R)]$ is trivial.

Thus, ψ descends to a homomorphism $\theta : E_1 \to E_2$, where $E_1 = F/[F, R]$ as defined above, with the property that $\mu \circ \theta = \overline{\nu}$. The condition $\mu \circ \theta = \overline{\nu}$ can be interpreted as saying that θ is a homomorphism between the central extensions $(E_1, \overline{\nu})$ and (E_2, μ). Denote by $\varphi : E_1' \to E_2'$ the restriction of θ to E_1'. Thus, by Lemma 3.4.1, φ defines a homoclinism of the central extensions.

Now, we know that (E_2, μ) is an initial object in the category, so there is a homoclinism from it to any other object in the category. Composing with the above gives a homoclinism from $(E_1, \overline{\nu})$ to any central extension of G. By Lemma 3.4.2, this homoclinism is unique. Finally, Lemma 3.4.3 establishes from this that $(E_1, \overline{\nu})$ defines an initial object in the category of central extensions of G with homoclinisms.

Proof of (2): By definition, $G \wedge G$ is isomorphic to the derived subgroup $[E_1, E_1]$ on account of E_1 being an initial object in the category of central extensions with homoclinisms.

$[E_1, E_1]$ is canonically isomorphic to $[F, F]/[F, R]$.

Proof of (3): The Schur multiplier is the kernel of the map $[E_1, E_1] \to [G, G]$, or equivalently, it is the kernel of the map $[F, F]/[F, R] \to [F, F]/(R \cap [F, F])$. The kernel works out to $(R \cap [F, F])/[F, R]$. $\square$

7.4.2 Hopf's formula variant for Schur multiplier of powered nilpotent group: class one more version

Suppose π is a set of primes and G is a π-powered nilpotent group of nilpotency class c. Suppose G can be expressed in the form F/R where F is a free π-powered nilpotent group of class $c+1$ and R is a normal subgroup of F. Then:

$$M(G) \cong (R \cap [F, F])/([F, R]) \tag{7.2}$$

Also:

$$G \wedge G \cong [F, F]/[F, R] \tag{7.3}$$

Our application of these results, in Section 7.7, will combine these results with the results of Section 7.3. In that section, we use the letter K for the free group, and R for the normal subgroup that is being factored out. Therefore, in our application of the above theorem, the letter K will appear instead of the letter F.

7.4.3 Remark on powered Schur multipliers and powered Schur covering groups

It is possible to define concepts of Schur multiplier, Schur covering group, and exterior square, all *within the variety of π-powered groups*. In other words, we can mimic the steps of Section 3.4, replacing "group" by π-powered group", and obtain corresponding notions of

π-powered exterior square and π-powered Schur multiplier. We can also define π-powered Schur covering group.

The results of Sections 7.4.1 and 7.4.2 tell us that for nilpotent groups, the π-powered Schur multiplier coincides with the usual Schur multiplier and the π-powered exterior square coincides with the usual exterior square.

7.4.4 Results about isoclinisms for π-powered central extensions

The results here follow from the results of Section 4.3.8 using reasoning similar to the way the results in Section 3.4.9 follow from the results in Section 2.1.6. Note that we restrict our statements to π-powered class c nilpotent groups and π-powered class c words. Note that although the result is stated for π-powered class c words, it also applies to π-powered words in general, because a π-powered class c word can be viewed as an equivalence class of π-powered words that are equal in any π-powered class c group.

Lemma 7.4.4. Suppose $c \geq 1$ and π is a set of primes. Suppose G is a π-powered group and $w(g_1, g_2, \dots, g_n)$ is a π-powered class c word in n letters with the property that w evaluates to the identity element in every π-powered abelian group. The following are true.

1. For every π-powered central extension E of G such that E has class at most c, w can be used to define a set map $\chi_{w,E} : G^n \to [E, E]$.
2. For any homoclinism between π-powered central extensions E_1 and E_2, with the central extension specified via a homomorphism $\varphi : [E_1, E_1] \to [E_2, E_2]$, we have that:

$$\varphi \circ \chi_{w,E_1} = \chi_{w,E_2}$$

Proof. Proof of (1): This is similar to the proof of Theorem 4.3.6. Alternatively, we can deduce it from the *result* of Theorem 4.3.6 by noting that the map factors as follows:

$$G^n \to (E/Z(E))^n \to [E, E]$$

Proof of (2): This is similar to the proof of Theorem 4.3.7. Alternatively, we can deduce it from the *result* of Theorem 4.3.7 by factoring through $E/Z(E)$. $\square$

We can now prove the theorem.

Theorem 7.4.5. Suppose π is a set of primes. Suppose G is a π-powered nilpotent group and $w(g_1, g_2, \dots, g_n)$ is a π-powered word in n letters with the property that w evaluates to the identity element in every π-powered abelian group. Then, there exists a set map $X_w : G^n \to G \wedge G$ with the property that for any π-powered central extension E of G, $\Omega_{E,G} \circ X_w = \chi_{w,E}$.

Proof. Set c to be one more than the nilpotency class of G, and treat w as a π-powered class c word. Apply Part (1) of Lemma 7.4.4 to the case where the extension E_0 is an initial object in the category of central extensions of G, *and* E_0 is π-powered (this is possible by Lemma 7.4.2). The rest of the proof is analogous to Theorem 3.4.5. $\square$

7.5 Homology of powered Lie rings

This section develops the Lie ring analogues of the results in Section 7.4. One key difference is that whereas the results of the previous section were restricted to nilpotent groups, some of the results in this section apply in full generality to all Lie rings.

7.5.1 Hopf's formula for powered Lie rings

We now establish the Lie ring analogues of the results describe in Section 7.4.1.

Lemma 7.5.1. Suppose L is a π-powered Lie ring. Then, the following hold:

1. All the homology groups $H_i(L;\mathbb{Z})$, $i > 0$, are π-powered abelian groups.

2. The Schur multiplier $M(L)$, which is $H_2(L;\mathbb{Z})$, is a π-powered abelian group.

Proof. Proof of (1): This is a direct consequence of how we define cohomology, and follows from the fact that the universal enveloping algebra is the same except in degree zero whether taken over $\mathbb{Z}$ or $\mathbb{Z}[\pi^{-1}]$, and the homology groups are defined in terms of the universal enveloping algebra.

Proof of (2): This follows immediately from (1). □

Lemma 7.5.2. Suppose L is a π-powered Lie ring. Every Schur covering Lie ring of L is π-powered. Since Schur covering Lie rings exist and are by definition initial objects in the category of extensions of L with homoclinisms, there exist initial objects in the category of extensions of L with homoclinisms that are π-powered.

Proof. By the preceding lemma (Lemma 7.5.1), $M(L)$ is π-powered. Consider a Schur covering Lie ring N of L. N is a central extension of the form:

$$0 \to M(L) \to N \to L \to 1$$

By Lemma 4.2.1, N is also π-powered. By definition, any Schur covering Lie ring gives an inital object in the category of central extensions of L with homoclinisms, so the last part of the statement follows.

Schur covering Lie rings exist by Theorem 3.7.3, so the final sentence follows. □

We are now in a position to prove results that establish analogues of Hopf's formula (discussed in Section 3.6.9):

Theorem 7.5.3. Suppose π is a set of primes and L is a π-powered Lie ring. Express L

in the form $L \cong F/R$ where F is a free π-powered Lie ring. Then, the following are true.

1. The Lie ring $N_1 = F/[F, R]$, with the natural quotient map $N_1 \to L$, is an initial object in the category of central extensions of L with homoclinisms.

2. The exterior square $L \wedge L$ is canonically isomorphic to the quotient Lie ring $[F, F]/[F, R]$.

3. The Schur multiplier $M(L)$ is canonically isomorphic to the quotient Lie ring $(R \cap [F, F])/[F, R]$:

$$M(L) \cong (R \cap [F, F])/[F, R] \tag{7.4}$$

Proof. Proof of (1): Let N_2 be a Schur covering Lie ring of L. By Lemma 7.5.2, N_2 is π-powered.

Consider the commutator map $\omega_1 : L \times L \to N_1$ and denote by Ω_1 the corresponding Lie ring homomorphism:

$$\Omega_1 : L \wedge L \to [N_1, N_1]$$

Consider also the extension:

$$0 \to A \to N_2 \xrightarrow{\mu} L \to 1$$

with the natural commutator map $\omega_2 : L \times L \to N_2$ and the corresponding commutator map homomorphism:

$$\Omega_2 : L \wedge L \to [N_2, N_2]$$

Our goal is to show that there there exists a unique homomorphism $\varphi : [N_1, N_1] \to [N_2, N_2]$ such that $\varphi \circ \omega_1 = \omega_2$, or equivalently, $\varphi \circ \Omega_1 = \Omega_2$.

The map $\nu : F \to L$ lifts to a map $\psi : F \to N_2$ on account of F being a free pi-powered Lie ring and N_2 being a π-powered Lie ring (note that the lift is not necessarily unique). Explicitly, this means that $\mu \circ \psi = \nu$.

We know that $\nu(R)$ is trivial, so $\mu(\psi(R))$ is trivial. Thus, $\psi(R)$ lands inside the kernel of μ, which is the image of A in N_2. Thus, $\psi(R)$ is a central Lie subring of N_2. Therefore, $\psi([F, R]) = [\psi(F), \psi(R)]$ is trivial.

Thus, ψ descends to a homomorphism $\theta : N_1 \to N_2$, where $N_1 = F/[F, R]$ as defined above, with the property that $\mu \circ \theta = \overline{\nu}$. The condition $\mu \circ \theta = \overline{\nu}$ can be interpreted as saying that θ is a homomorphism between the central extensions $(N_1, \overline{\nu})$ and (N_2, μ). Denote by $\varphi : N_1' \to N_2'$ the restriction of θ to N_1'. Thus, by Lemma 3.5.4, φ defines a homoclinism of the central extensions.

Now, we know that (N_2, μ) is an initial object in the category, so there is a homoclinism from it to any other object in the category. Composing with the above gives a homoclinism from $(N_1, \overline{\nu})$ to any central extension of L. By Lemma 3.5.5, this homoclinism is unique. Finally, Lemma 3.5.6 establishes from this that $(N_1, \overline{\nu})$ defines an initial object in the category of central extensions of L with homoclinisms.

Proof of (2): By definition, $L \wedge L$ is isomorphic to the derived subring $[N_1, N_1]$ on account of N_1 being an initial object in the category of central extensions with homoclinisms. $[N_1, N_1]$ is canonically isomorphic to $[F, F]/[F, R]$.

Proof of (3): The Schur multiplier is the kernel of the map $[N_1, N_1] \to [L, L]$, or equivalently, it is the kernel of the map $[F, F]/[F, R] \to [F, F]/(R \cap [F, F])$. The kernel works out to $(R \cap [F, F])/[F, R]$. $\square$

7.5.2 Hopf's formula variant for Schur multiplier of powered nilpotent Lie ring: class one more version

Suppose π is a set of primes and L is a π-powered nilpotent Lie ring of nilpotency class c. Suppose L can be expressed in the form F/R where F is a free π-powered nilpotent Lie ring of class $c+1$ and R is an ideal of F. Then:

$$M(L) \cong (R \cap [F,F])/([F,R]) \tag{7.5}$$

Also:

$$L \wedge L \cong [F,F]/[F,R] \tag{7.6}$$

Our application of these results, in Section 7.7, will combine these results with the results of Section 7.3. In that section, we used the letter N for the free Lie ring, and J for the ideal is being factored out. Therefore, in our application of the above theorem, the letter N will appear instead of the letter F, and the letter J will appear instead of the letter R.

7.5.3 Sidenote on powered Schur multipliers and powered Schur covering Lie rings

It is possible to define concepts of Schur multiplier, Schur covering group, and exterior square, all *within the variety of π-powered Lie rings*. In other words, we can mimic the steps of Section 3.5, replacing "Lie ring" by π-powered Lie ring", and obtain corresponding notions of π-powered exterior square and π-powered Schur multiplier. We can also define π-powered Schur covering Lie ring.

The results of Sections 7.5.1 and 7.5.2 tell us that the π-powered Schur multiplier coincides with the usual Schur multiplier and the π-powered exterior square coincides with the usual exterior square.

7.5.4 Results about isoclinisms for π-powered central extensions of Lie rings

The results here follow from the results of Section 4.3.8 using reasoning similar to the way the results in Section 3.4.9 follow from the results in Section 2.1.6. Unlike the corresponding section for groups (Section 7.4.4), we do not restrict ouselves to the nilpotent case. However, we *can* formulate all our results for the nilpotent setting. The proofs remain similar.

Lemma 7.5.4. Suppose π is a set of primes. Suppose L is a π-powered Lie ring and $w(g_1, g_2, \ldots, g_n)$ is a π-powered Lie ring word in n letters with the property that w evaluates to the zero element in every abelian Lie ring. The following are true.

1. For every central extension N of L, w can be used to define a set map $\chi_{w,N} : L^n \to [N, N]$.
2. For any homoclinism between central extensions N_1 and N_2, with the central extension specified via a homomorphism $\varphi : [N_1, N_1] \to [N_2, N_2]$, we have that:

$$\varphi \circ \chi_{w,N_1} = \chi_{w,N_2}$$

Proof. Proof of (1): This is similar to the proof of Theorem 4.4.1. Alternatively, we can deduce it from the *result* of Theorem 4.4.1 by noting that the map factors as follows:

$$L^n \to (N/Z(N))^n \to [N, N]$$

Proof of (2): This is similar to the proof of Theorem 4.4.2. Alternatively, we can deduce it from the *result* of Theorem 4.4.2 by factoring through $N/Z(N)$. ☐

We can now prove the theorem.

Theorem 7.5.5. Suppose π is a set of primes. Suppose L is a π-powered Lie ring and $w(g_1, g_2, \dots, g_n)$ is a π-powered Lie ring word in n letters with the property that w evaluates to the identity element in every abelian Lie ring. Then, there exists a set map $X_w : L^n \to L \wedge L$ with the property that for any central extension N of L, $\Omega_{N,L} \circ X_w = \chi_{w,N}$.

Proof. Apply Part (1) of Lemma 7.5.4 to the case where the extension N_0 is an initial object in the category of central extensions of L and such that N_0 is π-powered. Such an extension exists by Lemma 7.5.2. The rest of the proof is analogous to the proof of Theorem 3.5.8. □

7.6 Commutator-like and Lie bracket-like maps

This section describes maps that can be used to compute a "commutator-like" expression for Lie rings whose nilpotency class is one more than desired (or the 3-local variant thereof), and correspondingly, a "Lie bracket-like" expression for groups whose nilpotency class is one more than desired (or the 3-local variant thereof). We use the formula M_{c+1} (introduced in Section 7.1.1) to express the group commutator as a π_c-powered word that makes use of the Lie bracket. We use the formula $h_{2,c+1}$ (the second inverse Baker-Campbell-Hausdorff formula) to express the Lie bracket as a π_c-powered word that makes use of the group commutator.

For simplicity, we will restrict our definitions to situations where the groups and Lie rings involved are *globally* nilpotent, but without any restriction on their global nilpotency class. This will allow us to apply the theorems stated about nilpotent groups and Lie rings. It is possible to relax these assumptions to some extent, but the ensuing greater generality will not be worth the additional cost in the complexity of proofs.

7.6.1 Commutator-like map for Lie ring whose class is one more

Suppose c is a natural number and π_c is the set of primes less than or equal to c.

Suppose L is a π_c-powered nilpotent Lie ring such that the inner derivation Lie ring $L/Z(L)$ is a 3-local class c Lazard Lie ring. We can define a set map:

$$\omega_L^{\text{Group}} : \text{Inn}(L) \times \text{Inn}(L) \to [L, L]$$

The set map is defined as follows:

$$\omega_L^{\text{Group}}(x, y) := M_{c+1}(\tilde{x}, \tilde{y})$$

where M_{c+1} is the formula for the group commutator in terms of the Lie bracket described in Section 7.1.1, and $\tilde{x}$, $\tilde{y}$ are elements of L that map to x and y respectively in $L/Z(L)$. Note that this is defined because of the following:

- The expression M_{c+1} makes sense because L is π_c-powered, and Lemma 7.1.1 shows that all prime divisors of the denominators of coefficients for M_{c+1} are in π_c.
- The output of the expression is independent of the choice of lifts, because the Lie bracket map descends to a map $L/Z(L) \times L/Z(L) \to [L, L]$, and M_{c+1} is obtained by using the Lie bracket and its iterations. See Theorem 4.4.1 for an explanation.

Further, in the case that L itself is a 3-local class c Lazard Lie ring, $\omega_L^{\text{Group}}(x, y)$ agrees with the commutator-induced map $\omega_G : \text{Inn}(G) \times \text{Inn}(G) \to G'$ where G is the Lazard Lie group for L. Recall that ω_G was originally defined in Section 2.1.1 along with the definition of isoclinism.

This again follows from the definition of M_{c+1} as introduced in Section 7.1.1.

We now show that the map ω^{Group} is an isoclinism-invariant.

Lemma 7.6.1. Suppose c is a natural number and π_c is the set of primes less than or equal to c. Suppose L_1 and L_2 are isoclinic π_c-powered Lie rings, such that $\text{Inn}(L_1) \cong \text{Inn}(L_2)$ is a 3-local class c Lazard Lie ring.

Suppose (ζ, φ) is an isoclinism from L_1 to L_2: ζ is the isomorphism $\mathrm{Inn}(L_1) \to \mathrm{Inn}(L_2)$ and φ is the isomorphism $L_1' \to L_2'$. Then:

$$\varphi(\omega_{L_1}^{\mathrm{Group}}(x, y)) = \omega_{L_2}^{\mathrm{Group}}(\zeta(x), \zeta(y))$$

Proof. Apply Theorem 4.4.2 to the word ω^{Group} and obtain the result. □

7.6.2 Lie bracket-like map for group whose class is one more

A special case of the map described here appeared in Theorem 5.1 of the 2008 paper [20] by George Glauberman. Glauberman's paper proves certain properties of the map that we do not prove in this section, but that follow from stronger results we will prove later in the course of establishing the global Lazard correspondence up to isoclinism. We discuss the relationship in more detail in Section 8.1.1.

Suppose c is a natural number and π_c is the set of primes less than or equal to c.

Suppose G is a π_c-powered nilpotent group such that the inner automorphism group $G/Z(G)$ is a 3-local class c Lazard Lie group. We can define a set map:

$$\omega_G^{\mathrm{Lie}} : G/Z(G) \times G/Z(G) \to [G, G]$$

The set map is defined as follows:

$$(x, y) \mapsto h_{2,c+1}(\tilde{x}, \tilde{y})$$

where $h_{2,c+1}$ is the formula for the Lie bracket in terms of the group commutator and its iterations. It is the second of the two inverse Baker-Campbell-Hausdorff formulas described in Section 6.4. Note that this is defined because:

- The expression $h_{2,c+1}$ makes sense because G is π_c-powered, and Lemma 7.1.2 shows that all prime divisors of the denominators of coefficients for $h_{2,c+1}$ are in π_c.

- The output of the expression is independent of the choice of lifts, because the commutator map descends to a map $G/Z(G) \times G/Z(G) \to [G, G]$, and $h_{2,c+1}$ is obtained by using the commutator map and its iterations. See Theorem 4.3.6 for an explanation.

Further, in the case that G itself is a 3-local class c Lazard Lie group, $\omega_G^{\mathrm{Lie}}(x, y)$ agrees with the definition of the Lie bracket-induced map $\omega_L : \mathrm{Inn}(L) \times \mathrm{Inn}(L) \to L'$ where L is the Lazard Lie ring for G. Recall that ω_L was defined in Section 2.2.1 where we introduced the definition of isoclinism and homoclinism for Lie rings.

This again follows from the definition of $h_{2,c+1}$.

We now show that ω_G^{Lie} is an isoclinism-invariant.

Lemma 7.6.2. Suppose c is a natural number and π_c is the set of primes less than or equal to c. Suppose G_1 and G_2 are isoclinic π_c-powered groups such that $\mathrm{Inn}(G_1) \cong \mathrm{Inn}(G_2)$ is a 3-local class c Lazard Lie group.

Suppose (ζ, φ) is an isoclinism from G_1 to G_2: ζ is the isomorphism $\mathrm{Inn}(G_1) \to \mathrm{Inn}(G_2)$ and φ is the isomorphism $G_1' \to G_2'$. Then:

$$\varphi(\omega_{G_1}^{\mathrm{Lie}}(x, y)) = \omega_{G_2}^{\mathrm{Lie}}(\zeta(x), \zeta(y))$$

Proof. Apply Theorem 4.3.7 to the word ω^{Lie} and obtain the result. Note that the c used in that theorem refers to a bound on the global class of G_1 and G_2, and may be a different value from the value of c used here. The fact of significance is that G_1 and G_2 are nilpotent, so the theorem can be applied. □

7.6.3 Commutator-like map for Lie ring extensions

In Section 7.6.1, we described a commutator-like map that can be defined for any π_c-powered Lie ring whose inner derivation Lie ring is nilpotent and of 3-local nilpotency class at most

c. We will now consider the corresponding notion for Lie ring *extensions*. Consider a central extension of Lie rings, with the following central extension short exact sequence:

$$0 \to A \to N \to L \to 0$$

The Lie bracket map in N descends to a $\mathbb{Z}$-bilinear map:

$$\omega_{N,L} : L \times L \to [N, N]$$

Suppose now that N is π_c-powered and that L has 3-local nilpotency class at most c. Then, we can define a commutator-like map:

$$\omega_{N,L}^{\text{Group}} : L \times L \to [N, N]$$

The map $\omega_{N,L}^{\text{Group}}$ can be defined as the map $\chi_{w,N}$ described in Lemma 7.5.4 where w is the word M_{c+1}.

$\omega_{N,L}^{\text{Group}}$ can be obtained by composing the quotient map $L \times L \to N/Z(N) \times N/Z(N)$ with the map ω_N^{Group} described in Section 7.6.1 (the Lie ring is now N instead of L).

7.6.4 Lie bracket-like map for group extensions

In Section 7.6.2, we described a Lie bracket-like map that can be defined for any π_c-powered nilpotent group whose inner automorphism group is of 3-local nilpotency class at most c. We will now consider the corresponding notion for Lie ring extensions. Consider a central extension of groups, with the following central extension short exact sequence:

$$0 \to A \to E \to G \to 1$$

The commutator map in E descends to a set map:

$$\omega_{E,G} : G \times G \to [E, E]$$

Suppose now that E is π_c-powered and that G has 3-local nilpotency class at most c. Then, we can define a Lie bracket-like map:

$$\omega_{E,G}^{\text{Lie}} : G \times G \to [E, E]$$

The map $\omega_{E,G}^{\text{Lie}}$ can be defined as the map $\chi_{w,N}$ described in Lemma 7.4.4 where w is the word M_{c+1}.

This map $\omega_{E,G}^{\text{Lie}}$ can be obtained by composing the quotient map $G \times G \to E/Z(E) \times E/Z(E)$ with the map ω_E^{Lie} described in Section 7.6.2 (the group is now E instead of G).

7.6.5 The commutator in terms of the Lie bracket: the central extension and exterior square version

Suppose c is a positive integer and L is a π_c-powered nilpotent Lie ring of 3-local nilpotency class at most c. Our goal is to define a set map:

$$\tilde{M}_{c+1}(x, y) : L \times L \to L \wedge L$$

where $L \wedge L$ is the exterior square of L as defined in Section 3.5.1 (and later explicitly in Section 3.9.3).

The definition of $\tilde{M}_{c+1}$ is as follows: it is the map X_w of Theorem 7.5.5 where $\pi = \pi_c$ and w is the word M_{c+1}. The word M_{c+1} satisfies the hypotheses of the theorem, so the theorem applies.

Using Theorem 7.5.5 again, the map $\omega_{N,L}^{\text{Group}}$ defined in Section 7.6.3 is related to the map $\tilde{M}_{c+1}$ defined in Section as follows:

$$\omega_{N,L}^{\text{Group}}(x,y) = \Omega_{N,L}(\tilde{M}_{c+1}(x,y))$$

where the maps are $\omega_{N,L}^{\text{Group}} : L \times L \to [N,N]$, $\Omega_{N,L} : L \wedge L \to [N,N]$, and $\tilde{M}_{c+1} : L \times L \to L \wedge L$.

7.6.6 The Lie bracket in terms of the commutator: the central extension and exterior square version

Suppose c is a positive integer and G is a π_c-powered nilpotent group of 3-local nilpotency class at most c. Our goal is to define a set map:

$$\tilde{h}_{2,c+1}(x,y) : G \times G \to G \wedge G$$

where $G \wedge G$ is the exterior square of G as defined in Section 3.4.1 (and later explicitly in Section 3.8.4).

The definition of $\tilde{h}_{2,c+1}$ is as follows: it is the map X_w of Theorem 7.4.5 where $\pi = \pi_c$, w is the word $h_{2,c+1}$, and the value c of the theorem is taken to be $c+1$. The word $h_{2,c+1}$ satisfies the hypotheses of the theorem, so the result applies.

Using Theorem 7.4.5 again, the map $\omega_{E,G}^{\text{Lie}}$ defined in Section 7.6.4 is related to the map $\tilde{h}_{2,c+1}$ as follows:

$$\omega_{E,G}^{\text{Lie}}(x,y) = \Omega_{E,G}(\tilde{h}_{2,c+1}(x,y))$$

where the maps are $\omega_{E,G}^{\text{Lie}} : G \times G \to [E,E]$, $\Omega_{E,G} : G \wedge G \to [E,E]$, and $\tilde{h}_{2,c+1} : G \times G \to G \wedge G$.

7.7 Lazard correspondence up to isoclinism

7.7.1 Definition of Lazard correspondence up to isoclinism

The Lazard correspondence up to isoclinism combines the idea of isoclinism with the idea of the Lazard correspondence.

Definition (3-local class $(c+1)$ Lazard correspondence up to isoclinism)**.** Suppose c is a positive integer and π_c is the set of all prime numbers less than or equal to c. Suppose G is a π_c-powered nilpotent group whose inner automorphism group and derived subgroup are both 3-local class c Lazard Lie groups, and L is a π_c-powered nilpotent Lie ring whose inner derivation Lie ring and derived subring are both 3-local class c Lazard Lie rings. A Lazard correspondence up to isoclinism from L to G is a pair of isomorphisms (ζ, φ) where ζ is an isomorphism from $\mathrm{Inn}(L)$ to $\log(\mathrm{Inn}(G))$ and φ is an isomorphism from L' to $\log(G')$ such that:

$$\varphi(\omega_L(x, y)) = \omega_G^{\mathrm{Lie}}(\zeta(x), \zeta(y))$$

This is equivalent to the requirement that:

$$\varphi(\omega_L^{\mathrm{Group}}(x, y)) = \omega_G(\zeta(x), \zeta(y))$$

The following are easy to verify for the 3-local class $(c+1)$ Lazard correspondence up to isoclinism. All the groups mentioned below are π_c-powered groups that have the property that their inner automorphism group and derived subgroup are both 3-local class c Lazard Lie groups, and all the Lie rings mentioned below are π_c-powered Lie rings that have the property that their inner derivation Lie ring and derived subring are both 3-local class c Lazard Lie rings.

- If G_1 and G_2 are isoclinic groups, and G_1 and L are in 3-local class $(c+1)$ Lazard correspondence up to isoclinism, then G_2 and L are also in 3-local class $(c+1)$ Lazard correspondence up to isoclinism. This follows from Lemma 7.6.2.

- If L_1 and L_2 are isoclinic Lie rings, and G and L_1 are in 3-local class $(c+1)$ Lazard correspondence up to isoclinism, then G and L_2 are in 3-local class $(c+1)$ Lazard correspondence up to isoclinism. This follows from Lemma 7.6.1.

- If G_1 and G_2 are groups and L is a Lie ring such that G_1 is in 3-local class $(c+1)$ Lazard correspondence up to isoclinism with L and G_2 is also in 3-local class $(c+1)$ Lazard correspondence up to isoclinism with L, then G_1 and G_2 are isoclinic.

- If L_1 and L_2 are Lie rings and G is a group such that G is in 3-local class $(c+1)$ Lazard correspondence up to isoclinism with L_1 and G is in 3-local class $(c+1)$ Lazard correspondence up to isoclinism with L_2, then L_1 and L_2 are isoclinic Lie rings.

In other words, the definition we gave above establishes a correspondence between *some* equivalences classes up to isoclinism of groups and *some* equivalence classes up to isoclinism of Lie rings. However, it is not yet clear that the correspondence applies to *every* equivalence class up to isoclinism of groups of the specified type and to *every* equivalence class up to isoclinism of Lie rings of the specified type. Ideally, we would like to demonstrate the following two facts:

1. For every π_c-powered group G whose inner automorphism group and derived subgroup are both 3-local class c Lazard Lie groups, there exists a π_c-powered Lie ring L whose inner derivation Lie ring and derived subring are both 3-local class c Lazard Lie rings such that G is in 3-local class $(c+1)$ Lazard correspondence up to isoclinism with L.

2. For every π_c-powered Lie ring L whose inner derivation Lie ring and derived subring are both 3-local class c Lazard Lie rings, there exists a π_c-powered group G whose inner automorphism group and derived subgroup are both 3-local class c Lazard Lie

groups, such that G is in 3-local class $(c+1)$ Lazard correspondence up to isoclinism with L.

Unfortunately, the full proofs of these results would require us to develop further machinery and notation that would take too much work. Therefore, we restrict attention to the global class case. The proofs in the 3-local case are analogous, but would require us to deal with a 3-local version of the free constructions that we used earlier, which would considerably complicate the presentation. For this reason, we restrict our proof to the global case.

7.7.2 *Global Lazard correspondence up to isoclinism*

We begin with a couple of lemmas about the structures between which we aim to establish the correspondence.

Lemma 7.7.1. Suppose c is a positive integer and π_c is the set of all primes less than or equal to c. Suppose G is a π_c-powered nilpotent group of nilpotency class at most $c+1$. Then, both $\operatorname{Inn}(G)$ and G' are global class c Lazard Lie groups, i.e., both $\operatorname{Inn}(G)$ and G' are π_c-powered groups of nilpotency class at most c.

Proof. We need to establish four facts:

1. $\operatorname{Inn}(G)$ has nilpotency class at most c: This is obvious from the condition on the nilpotency class of G.

2. $\operatorname{Inn}(G)$ is π_c-powered: This follows from Lemma 4.1.7.

3. G' has nilpotency class at most c: In fact, G' has nilpotency class at most $\lfloor (c+1)/2 \rfloor$, which in turn is at most c, but the naive bound of c can be established in a straightforward manner by looking at the lower central series of G and comparing with

that of G'. More explicitly, this follows from the fact that the lower central series is a strongly central series. See the Appendix, Section A.3.4 for more details.

4. G' is π_c-powered: This follows from Theorem 4.1.20.

$\square$

Lemma 7.7.2. Suppose c is a positive integer and π_c is the set of all primes less than or equal to c. Suppose L is a π_c-powered Lie ring of nilpotency class at most $c+1$. Then, both $\mathrm{Inn}(L)$ and L' are global class c Lazard Lie rings, i.e., both $\mathrm{Inn}(L)$ and L' are π_c-powered groups of nilpotency class at most c.

Proof. We need to establish four facts:

1. $\mathrm{Inn}(L)$ has nilpotency class at most c: This is obvious from the condition on the nilpotency class of L.

2. $\mathrm{Inn}(L)$ is π_c-powered: This follows from Theorem 4.2.4.

3. L' has nilpotency class at most c: In fact, L' has nilpotency class at most $\lfloor (c+1)/2 \rfloor$, which in turn is at most c, but the naive bound of c can be established very straightforwardly by looking at the lower central series of L and comparing with that of L'.

4. L' is π_c-powered: This follows from Lemma 4.2.8.

$\square$

We can now define the correspondence:

Definition (Global class $(c+1)$ Lazard correspondence up to isoclinism)**.** Suppose c is a positive integer and π_c is the set of (all) prime numbers less than or equal to c. Suppose

G is a π_c-powered group of nilpotency class at most $c+1$, and L is a π_c-powered Lie ring of nilpotency class at most $c+1$. A global class $(c+1)$ Lazard correspondence up to isoclinism from L to G is a pair of isomorphisms (ζ, φ) where ζ is an isomorphism from $\operatorname{Inn}(L)$ to $\log(\operatorname{Inn}(G))$ (note that this log uses the global Lazard correspondence) and φ is an isomorphism from L' to $\log(G')$ such that:

$$\varphi(\omega_L(x,y)) = \omega_G^{\text{Lie}}(\zeta(x), \zeta(y))$$

This is equivalent to the requirement that:

$$\varphi(\omega_L^{\text{Group}}(x,y)) = \omega_G(\zeta(x), \zeta(y))$$

The observations from Section 7.7.1 about the 3-local class $(c+1)$ Lazard correspondence up to isoclinism continue to apply here: the correspondence establishes a correspondence between *some* π_c-powered groups of class at most $c+1$ and *some* π_c-powered Lie rings of class at most $c+1$. However, it is not yet clear that the correspondence applies to *every* equivalence class up to isoclinism of groups of the specified type and to *every* equivalence class up to isoclinism of Lie rings of the specified type. Essentially, we need to establish two facts:

1. For every π_c-powered group G of nilpotency class at most $c+1$, there exists a π_c-powered Lie ring L of nilpotency class at most $c+1$ such that L and G are in global class $(c+1)$ Lazard correspondence up to isoclinism.

2. For every π_c-powered Lie ring L of nilpotency class at most $c+1$, there exists a π_c-powered group G of nilpotency class at most $c+1$ such that L and G are in global class $(c+1)$ Lazard correspondence up to isoclinism.

7.7.3 The Baer correspondence up to isoclinism is the case $c = 1$

If we set $c = 1$, then the global class $(c+1)$ Lazard correspondence up to isoclinism reduces to the Baer correspondence up to isoclinism, as described in Section 5.4. The general proof that we will now give follows steps very similar to the proof of the statement for the Baer correspondence. The key difference is that the group whose Schur multiplier and exterior square we are computing is no longer an abelian group. Therefore, we have to explicitly use the Lazard correspondence rather than the abelian Lie correspondence to move back and forth between the group and the Lie ring.

7.7.4 Global Lazard correspondence preserves Schur multipliers

For both groups and Lie rings, the Schur multiplier is the object that controls the equivalence class of the extension up to isoclinism. The first step in establishing the global Lazard correspondence up to isoclinism is therefore to establish that Schur multipliers are preserved under the global Lazard correspondence.

A particular case of this statement appeared as a conjecture in the paper [13] by Eick, Horn, and Zandi in September 2012, stated informally after Theorem 2 of the paper. Specifically, the authors conjectured that for a finite p-groups of nilpotency class at most $p-1$, the Schur multiplier of the group coincides with the Schur multiplier of its Lazard Lie ring. The authors proved the corresponding statement for p-groups of nilpotency class at most $p-2$ by noting that the central extensions of the group are in Lazard correspondence with the central extensions of the Lie ring.[1]

Theorem 7.7.3. Suppose c is a positive integer and π_c is the set of all primes less than or equal to c. Suppose G is a π_c-powered group of nilpotency class at most c and L is its

1. The authors write: "Based on various example computations, see also [7], we believe that Theorems 1 and 2 also hold for finite p-groups of class $p-1$. However, our proofs do not extend to this case." The reference [7] alluded to by the authors has not yet been published or made available online.

Lazard Lie ring under the global Lazard correspondence. Then:

1. The short exact sequences:

$$0 \to M(L) \to L \wedge L \to [L, L] \to 0$$

and

$$0 \to M(G) \to G \wedge G \to [G, G] \to 1$$

are canonically in Lazard correspondence.

2. $L \wedge L$ and $G \wedge G$ are in Lazard correspondence up to canonical isomorphism. Moreover, if we denote the isomorphism as a set map $\exp : L \wedge L \to G \wedge G$, we have $\exp(x \wedge y) = \tilde{h}_{2,c+1}(x, y)$ where $\tilde{h}_{2,c+1}$ is the adaptation of $h_{2,c+1}$ described in Section 7.6.6. Similarly, under the inverse set map $\log : G \wedge G \to L \wedge L$, we have $\log(x \wedge y) = \tilde{M}_{c+1}(x, y)$, where $\tilde{M}_{c+1}$ is the adaptation of M_{c+1} described in Section 7.6.5.

3. $M(L)$ and $M(G)$ are canonically isomorphic as abelian groups.

Note that these theorems are framed in terms of the Lazard correspondence *up to isomorphism* rather than the strict Lazard correspondence (in the sense of equality of sets). It does not make sense to do the latter here because a strict Lazard correspondence would require us to keep track of the strict definition of the sets. However, although our results are *up to isomorphism*, they are *up to canonical isomorphism*, which means that they commute with the isomorphisms induced by transitioning from a group to an isomorphic group.

Proof. Proof of (1): Denote by K_1 the free π_c-powered group of class c on the underlying set of G. Denote by R_1 the kernel of the natural homomorphism $K_1 \to G$.

Denote by K the free π_c-powered group of class $c+1$ on the underlying set G. Denote by R the kernel of the natural homomorphism $K \to G$. Note that $K_1 = K/\gamma_c(K)$, and R is the inverse image of R_1 under the projection map.

Denote by N_1 the free π_c-powered Lie ring of class c on the underlying set of L (which is identified with the underlying set of G). Denote by J_1 the kernel of the natural homomorphism $N_1 \to L$. Denote by N the free π_c-powered Lie ring of class $c+1$ on the underlying set of L. Denote by J the kernel of the natural homomorphism $N \to L$. Note that $N_1 = N/\gamma_c(N)$ and J is the inverse image of J_1 under the projection map.

From Theorem 7.3.3 (note that the notation of that theorem matches the notation here), the derived subgroup $[K, K]$ is in Lazard correspondence with the derived subring $[N, N]$. From Theorems 7.3.5 and 7.3.6 (again, note that the notation of that theorem matches the notation here), we see that this Lazard correspondence restricts to a Lazard correspondence between $[K, R]$ and $[N, J]$ and also to a Lazard correspondence between $R \cap [K, K]$ and $J \cap [N, N]$. Applying these to quotient groups, we obtain that:

- $[K, K]/[K, R]$ is canonically in Lazard correspondence with the quotient Lie ring $[N, N]/[N, J]$.
- $[K, K]/(R \cap [K, K])$ is canonically in Lazard correspondence with $[N, N]/(J \cap [N, N])$.
- $(R \cap [K, K])/[K, R]$ is canonically in Lazard correspondence with $(J \cap [N, N])/[N, J]$.

Moreover, these short exact sequences are also in Lazard correspondence:

$$0 \to (J \cap [N, N])/[N, J] \to [N, N]/[N, J] \to [N, N]/(J \cap [N, N]) \to 0$$

$$0 \to (R \cap [K, K])/[K, R] \to [K, K]/[K, R] \to [K, K]/(K \cap [R, R]) \to 1$$

By the discussion in Sections 7.4.2 and 7.5.2, these correspond respectively to the short exact sequences:

$$0 \to M(L) \to L \wedge L \to [L, L] \to 0$$

$$0 \to M(G) \to G \wedge G \to [G, G] \to 1$$

Proof of (2): The fact of isomorphism follows directly from (1). The assertions about M_{c+1} and $h_{2,c+1}$ follow from the fact that the Lazard correspondence between $[N, N]$ and $[K, K]$ arises as the restriction of the Lazard correspondence between $\mathbb{Q}N$ and $\sqrt{K}$, and under this correspondence, by definition, $e^{M_{c+1}(x,y)} = [e^x, e^y]$ (with the group commutator appearing on the right) and $[\log x, \log y] = \log(h_{2,c+1}(x, y))$ (with the Lie bracket appearing on the left) by the respective definitions of M_{c+1} and $h_{2,c+1}$.

Proof of (3): This follows from (1), and the observation that the Lazard correspondence coincides with the abelian Lie correspondence where they overlap, so $M(L)$ and $M(G)$ are isomorphic as abelian groups. $\square$

7.7.5 The global Lazard correspondence up to isoclinism for extensions

Suppose c is a positive integer and π_c is the set of all primes less than or equal to c. Suppose A is an abelian group and G is a global class c Lazard Lie group.

Denote by L the Lazard Lie ring of G.

We have the following short exact sequence (originally described in Section 3.6.4) for the central extensions with central subgroup A and quotient group G:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}; A) \to H^2(G; A) \to \mathrm{Hom}(M(G), A) \to 0$$

We also have the following short exact sequence (originally described in Section 3.7.4) for the central extensions with central subring A and quotient Lie ring L:

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}; A) \to H^2_{\mathrm{Lie}}(L; A) \to \mathrm{Hom}(M(L), A) \to 0$$

By Theorem 7.7.3, $M(L)$ and $M(G)$ are canonically isomorphic. Also, L^{ab} is canonically in abelian Lie correspondence with G^{ab}. Thus, the downward arrows below are canonical isomorphisms:

$$\begin{array}{ccccccccc}
0 & \to & \mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}; A) & \to & H^2(G; A) & \to & \mathrm{Hom}(M(G), A) & \to & 0 \\
 & & \downarrow & & & & \downarrow & & \\
0 & \to & \mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}; A) & \to & H^2_{\mathrm{Lie}}(L; A) & \to & \mathrm{Hom}(M(L), A) & \to & 0
\end{array}$$

The middle groups $H^2(G; A)$ and $H^2_{\mathrm{Lie}}(L; A)$ are isomorphic to each other, because both short exact sequences split. However, we *do not* in general have a *canonical* isomorphism between the middle groups.

The isomorphism of the Ext^1 groups on the left side, and its relation to the global class c Lazard correspondence

We have a canonical isomorphism of groups:

$$\mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}; A) \cong \mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}; A)$$

This is because the abelian group G^{ab} is in abelian Lie correspondence with the abelian Lie ring L^{ab}, so the additive groups are the same, and Ext^1 computation uses only the underlying additive group.

The elements of $\mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}; A)$ correspond to the extension groups with subgroup A and quotient group G for which the sub-extension with quotient group G' splits (as $G' \times A$) and the induced extension with subgroup A and quotient group G^{ab} gives an abelian group. As a result, all extensions corresponding to elements of $\mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}; A)$ have the property that the extension group is a global class c Lazard Lie group. Similarly, the extensions corresponding to elements of $\mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}; A)$ have the property that the extension group is a global class c Lazard Lie ring. We thus obtain a correspondence:

Group extensions with subgroup A and quotient group G that are in the image of $\operatorname{Ext}^1_{\mathbb{Z}}(G^{\text{ab}}; A) \leftrightarrow$ Lie ring extensions with subring A and quotient ring L that are in the image of $\operatorname{Ext}^1_{\mathbb{Z}}(L^{\text{ab}}; A)$

For each group extension and Lie ring extension that are in bijection (in other words, each pair of elements in the two isomorphic groups that are in bijection with each other), the corresponding extension group is in global class c Lazard correspondence with the corresponding extension Lie ring.

The isomorphism of the Hom groups on the right side, and its relation to the Lazard correspondence up to isoclinism

We have a canonical isomorphism:

$$\operatorname{Hom}(M(G), A) \cong \operatorname{Hom}(M(L), A)$$

We reviewed the meanings of the two groups in Sections 3.6.3 and 3.6.4 (for groups) and Sections 3.7.3 and 3.7.4 (for Lie rings). The group $\operatorname{Hom}(M(G), A)$ classifies the central extensions with central subgroup A and quotient group G up to isoclinism of extensions. The group $\operatorname{Hom}(M(L), A)$ classifies the central extensions with central subring A and quotient Lie ring L up to isoclinism of extensions.

The two Hom groups are isomorphic because, as established above (Theorem 7.7.3), the Schur multipliers $M(L)$ and $M(G)$ are canonically isomorphic.

The isomorphism gives a correspondence:

Equivalence classes up to isoclinism of group extensions with central subgroup A and quotient group $G \leftrightarrow$ Equivalence classes up to isoclinism of Lie ring extensions with central subring A and quotient Lie ring L

Any particular instance of this bijection (i.e., an equivalence class of Lie ring extensions and an equivalence class of group extensions that are in bijection with each other) is termed a *global class* $(c+1)$ *Lazard correspondence up to isoclinism for extensions.*

We now state an important lemma that relates the global class $(c+1)$ Lazard correspondence up to isoclinism for extensions with the global class $(c+1)$ Lazard correspondence up to isoclinism.

Theorem 7.7.4. Suppose A is an abelian group, G is a global class c Lazard Lie group, and $L = \log G$ is the corresponding global class c Lazard Lie ring. Suppose E is a group extension with central subgroup A and quotient group G. Suppose N is a Lie ring extension with central subring $\log A$ (which we denote as A via abuse of notation) and quotient Lie ring L. Suppose further that the equivalence class up to isoclinism of the group extension E corresponds, via the above bijection, to the equivalence class of the Lie ring extension N. Then, the following are true.

1. The group $[E, E]$ is in global class c Lazard correspondence with the Lie ring $[N, N]$.

2. The commutator-induced group homomorphism $\Omega_{E,G} : G \wedge G \to [E, E]$ is in global class c Lazard correspondence with the commutator-induced group homomorphism $\Omega_{N,L} : L \wedge L \to [N, N]$, where we use the canonical Lazard correspondence between $G \wedge G$ and $L \wedge L$ described in Theorem 7.7.3, and the Lazard correspondence between $[E, E]$ and $[N, N]$ described in part (1).

3. Explicitly, if $\varphi : [N, N] \to \log([E, E])$ describes the isomorphism of Step (1), then for all $x, y \in G$ (so that $x, y \in L$ as well because L and G have the same underlying set):

$$\varphi(\omega_{N,L}(x, y)) = \omega_{E,G}^{\text{Lie}}(x, y)$$

   Equivalently:

$$\varphi(\omega_{N,L}^{\text{Group}}(x,y)) = \omega_{E,G}(x,y)$$

4. The group E is in global class $(c+1)$ Lazard correspondence up to isoclinism with the Lie ring N.

Proof. Proof of (1) and (2): We have the following map induced by the commutator map in E:

$$\omega_{E,G} : G \times G \to [E,E]$$

Similarly, we have the following map induced by the Lie bracket map in N:

$$\omega_{N,L} : L \times L \to [N,N]$$

We can define $\omega_{E,G}^{\text{Lie}}$ in terms of $\omega_{E,G}$ as explained in Section 7.6.4. Consider the canonical isomorphism between $L \wedge L$ and $G \wedge G$ (described in Theorem 7.7.3) and denote the set map by $\exp : L \wedge L \to G \wedge G$.

In Section 3.6.3, we considered short exact sequences with surjective downward maps, where β_G is the element of $\text{Hom}(M(G), A)$ and β' is the morphism obtained by restricting β_G to its image, which we call B:

$$\begin{array}{ccccccccc}
0 & \to & M(G) & \to & G \wedge G & \to & [G,G] & \to & 1 \\
 & & \downarrow^{\beta'_G} & & \downarrow & & \downarrow^{\text{id}} & & \\
0 & \to & B & \to & [E,E] & \to & [G,G] & \to & 1
\end{array}$$

In Section 3.7.3, we considered a similar short exact sequence with surjective downward maps, where β_L is the element of $\text{Hom}(M(L), A)$ and β'_L is the morphism obtained by restricting β_L to its image, which we call B:

$$\begin{array}{ccccccccc}
0 & \rightarrow & M(L) & \rightarrow & L \wedge L & \rightarrow & [L,L] & \rightarrow & 1 \\
\downarrow & & \downarrow^{\beta'_L} & & \downarrow & & \downarrow & & \downarrow \\
0 & \rightarrow & B & \rightarrow & [N,N] & \rightarrow & [L,L] & \rightarrow & 1
\end{array}$$

Under the canonical isomorphism of $M(L)$ and $M(G)$, β_L and β_G are canonically identified, so that the subgroups B in both cases are the same, and β'_L and β'_G are canonically identified as well.

The left and right downward maps for the group short exact sequence are in Lazard correspondence respectively with the left and right downward maps for the Lie ring short exact sequence. Therefore, the middle maps for these sequences, which are determined uniquely up to isomorphism, are also in Lazard correspondence up to isomorphism.[2] In particular, $[E,E]$ and $[N,N]$ are in Lazard correspondence up to isomorphism and the maps $G \wedge G \rightarrow [E,E]$ and $L \wedge L \rightarrow [N,N]$ are in Lazard correspondence.

Proof of (3): The explicit description of the Lazard correspondence between $G \wedge G$ and $L \wedge L$ described in Theorem 7.7.3 gives us that, for $x, y \in L$ (so that $x, y \in G$ because L and G have the same underlying set):

$\exp(x \wedge y) = \tilde{h}_{2,c+1}(x,y)$

where the $x \wedge y$ on the left is interpreted as an element of $L \wedge L$.

Apply $\Omega_{E,G}$ to both sides and obtain:

$$\Omega_{E,G}(\exp(x \wedge y)) = \Omega_{E,G}(\tilde{h}_{2,c+1}(x,y))$$

The right side is $\omega^{\text{Lie}}_{E,G}(x,y)$, as described at the end of Section 7.6.6. We thus obtain:

$$\Omega_{E,G}(\exp(x \wedge y)) = \omega^{\text{Lie}}_{E,G}(x,y)$$

The left side involves composing the set map $\exp : L \wedge L \rightarrow G \wedge G$ and the group

2. To see this, we could apply exp to the diagram for Lie rings and note that that diagram is equivalent up to isomorphism with the diagram for groups.

homomorphism $\Omega_{E,G} : G \wedge G \to [E, E]$. By Part (2), this is equivalent to composing the map $\Omega_{N,L} : L \wedge L \to [N, N]$ with the Lazard correspondence up to isomorphism between $[N, N]$ and $[E, E]$. The statement of the theorem uses the symbol φ to denote the isomorphism $[N, N] \to \log([E, E])$ describing the correspondence, so we obtain:

$$\varphi(\Omega_{N,L}(x \wedge y)) = \omega^{\text{Lie}}_{E,G}(x, y)$$

$\Omega_{N,L}(x \wedge y) = \omega_{N,L}(x, y)$, and we obtain:

$$\varphi(\omega_{N,L}(x, y)) = \omega^{\text{Lie}}_{E,G}(x, y)$$

as desired.

The proof of the other identity is similar.

Proof of (4): The image of $Z(N)$ in L is precisely the set $\{x \in L \mid \omega_{N,L}(x, y) = 0 \forall\, y \in L\}$. The image of $Z(E)$ in G is precisely the set $\{x \in G \mid \omega_{E,G}(x, y) = 1\ \forall\, y \in G\}$. The condition $\omega_{E,G}(x, y) = 1$ implies that $\omega^{\text{Lie}}_{E,G}(x, y) = 0$ which in turn implies that $\omega_{N,L}(x, y) = 0$. Similarly, the condition that $\omega_{N,L}(x, y) = 0$ implies that $\omega^{\text{Group}}_{N,L}(x, y) = 1$ which in turn implies that $\omega_{E,G}(x, y) = 1$. The upshot is that the image of $Z(N)$ in L coincides with the image of $Z(E)$ in G.

Thus, the quotient of L by the image of $Z(N)$ in L is in strict Lazard correspondence with the quotient of G by the image of $Z(E)$ in G. The former is canonically isomorphic to $N/Z(N)$ and the latter is canonically isomorphic to $E/Z(E)$. Thus, $N/Z(N)$ is in Lazard correspondence with $E/Z(E)$. Finally, the maps $\omega_{N,L}$ and $\omega_{E,G}$ descend in the same way to maps ω_N and ω_E, and we obtain, for all $x, y \in \text{Inn}(N)$:

$$\varphi(\omega_N(x, y)) = \omega^{\text{Lie}}_{E}(x, y)$$

We thus obtain that N and E are in global class $(c + 1)$ Lazard correspondence up to isoclinism. $\square$

Relation between the middle groups

We have demonstrated the existence of canonical isomorphisms between the left groups and between the right groups in the two short exact sequences:

$$\begin{array}{ccccccccc} 0 & \to & \operatorname{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}; A) & \to & H^2(G; A) & \to & \operatorname{Hom}(G \wedge G, A) & \to & 0 \\ & & \downarrow & & & & \downarrow & & \\ 0 & \to & \operatorname{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}; A) & \to & H^2_{\mathrm{Lie}}(L; A) & \to & \operatorname{Hom}(L \wedge L, A) & \to & 0 \end{array}$$

As described in Sections 3.6.4 and 3.7.4, both short exact sequences split. Therefore, it is possible to find an isomorphism $H^2(G; A) \to H^2_{\mathrm{Lie}}(L; A)$ that establishes an isomorphism of the short exact sequences:

$$\begin{array}{ccccccccc} 0 & \to & \operatorname{Ext}^1_{\mathbb{Z}}(G; A) & \to & H^2(G; A) & \to & \operatorname{Hom}(G \wedge G, A) & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \operatorname{Ext}^1_{\mathbb{Z}}(L; A) & \to & H^2_{\mathrm{Lie}}(L; A) & \to & \operatorname{Hom}(L \wedge L, A) & \to & 0 \end{array}$$

Note, however, that the middle isomorphism is not canonical. In general, here, *neither* sequence splits canonically. This is in contrast with the Baer correspondence up to isoclinism, where the short exact sequence for Lie rings splits, as per Section 5.4.6. For the Baer correspondence up to isoclinism, specifying an isomorphism of the middle groups is equivalent to specifying a splitting of the short exact sequence corresponding to group extensions. For the global Lazard correspondence up to isoclinism, however, the analogous statement is not true.

7.7.6 The global Lazard correspondence up to isoclinism: filling the details

Suppose c is a positive integer and π_c is the set of all primes less than or equal to c.

We are now in a position to flesh out the remaining details of the global Lazard correspondence up to isoclinism, which we defined in Section 7.7.2:

Equivalence classes up to isoclinism of π_c-powered groups of nilpotency class at most $c+1$ $\leftrightarrow$ Equivalence classes up to isoclinism of π_c-powered Lie rings of nilpotency class at most $c+1$

There are two pending facts we need to establish:

1. For every π_c-powered group G of nilpotency class at most $c+1$, there exists a π_c-powered Lie ring L of nilpotency class at most $c+1$ such that G and L are in global class $(c+1)$ Lazard correspondence up to isoclinism.

2. For every π_c-powered Lie ring L of nilpotency class at most $c+1$, there exists a π_c-powered group G of nilpotency class at most $c+1$ such that G and L are in global class $(c+1)$ Lazard correspondence up to isoclinism.

Explicit construction from the group to the Lie ring

We are given a π_c-powered group G of nilpotency class at most $c+1$, and we need to find a π_c-powered Lie ring L of nilpotency class at most $c+1$ such that L and G are in global class $c+1$ Lazard correspondence up to isoclinism.

(a) Consider G as a central extension:

$$0 \to Z(G) \to G \to G/Z(G) \to 1$$

Consider the equivalence class up to isoclinism of this extension.

(b) Based on the discussion in Section 7.7.5, this equivalence class corresponds to an equivalence class up to isoclinism of Lie ring extensions with central subring $\log(Z(G))$ and quotient Lie ring $\log(G/Z(G))$. Let L be any extension Lie ring in this equivalence class.

(c) By Theorem 7.7.4, L and G are in global Lazard correspondence up to isoclinism.

Explicit construction from the Lie ring to the group

We are given a π_c-powered Lie ring L of nilpotency class at most $c+1$, and we need to find a π_c-powered group G of nilpotency class at most $c+1$ such that L and G are in global class $c+1$ Lazard correspondence up to isoclinism.

(a) Consider L as a central extension:

$$0 \to Z(L) \to L \to L/Z(L) \to 0$$

Consider the equivalence class up to isoclinism of this extension.

(b) Based on the discussion in Section 7.7.5, this equivalence class corresponds to an equivalence class up to isoclinism of group extensions with central subgroup $\exp(Z(L))$ and quotient group $\exp(L/Z(L))$. Let G be any extension group in this equivalence class.

(c) By Theorem 7.7.4, L and G are in global class $(c+1)$ Lazard correspondence up to isoclinism.

Preservation of order

In both directions, the constructions preserve the orders. In other words, if we start with a finite group and use the construction in the direction from groups to Lie rings, the Lie ring that we obtain has the same order as the group that we started with. Similarly, if we start with a finite Lie ring and use the construction in the direction from Lie groups to groups, the group that we obtain has the same order as the Lie ring that we started with.

This does not imply that *every* group and every Lie ring that are in global Lazard correspondence up to isoclinism must have the same order. Rather, we are saying that the answer to the existence question continues to be affirmative even after we impose the condition that the orders have to be equal.

In particular, given a a finite p-group of nilpotency class p, we can find a finite p-Lie ring (i.e., a Lie ring whose additive group is a finite p-group) of nilpotency class p such that the group and Lie ring are in global class p Lazard correspondence up to isoclinism. Similarly, given a finite p-Lie ring of nilpotency class p, we can find a finite p-group of nilpotency class p such that the group and Lie ring are in global class p Lazard correspondence up to isoclinism.

7.7.7 Relating the global Lazard correspondence and the global Lazard correspondence up to isoclinism

Suppose c is a positive integer and π_c is the set of all primes less than or equal to c. In Section 7.7.5, we considered the case where A is an abelian group and G is a global class c Lazard Lie group (i.e., a π_c-powered group of nilpotency class at most c) with Lazard Lie ring L. Recall the short exact sequences described in Section 7.7.5:

$$\begin{array}{ccccccccc} 0 & \to & \operatorname{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}};A) & \to & H^2(G;A) & \to & \operatorname{Hom}(M(G),A) & \to & 0 \\ & & \downarrow & & & & \downarrow & & \\ 0 & \to & \operatorname{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}};A) & \to & H^2_{\mathrm{Lie}}(L;A) & \to & \operatorname{Hom}(M(L),A) & \to & 0 \end{array}$$

We had noted at the time that both short exact sequences split, and therefore the middle groups are isomorphic. However, in general, neither splitting is canonical (the splitting on the Lie ring side is canonical for abelian L, as described in Section 5.4.5, but this is an exceptional situation). Moreover, in general, there is no canonical isomorphism between the middle groups.

Suppose now that A and G (and therefore also L) are powered over the set of all primes less than or equal to $c+1$. Note that in the case that $c+1$ is composite, this is always true, but it may also be true for specific choices of A and G even in the case that $c+1$ is prime. In this case, all the elements of $H^2(G;A)$ correspond to global class $(c+1)$ Lazard Lie groups and all the elements of $H^2_{\mathrm{Lie}}(L;A)$ correspond to global class $(c+1)$ Lazard Lie rings. Moreover, the global class $(c+1)$ Lazard correspondence induces an isomorphism between these groups that defines a canonical isomorphism of the short exact sequences:

$$\begin{array}{ccccccccc}
0 & \rightarrow & \mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}; A) & \rightarrow & H^2(G; A) & \rightarrow & \mathrm{Hom}(M(G), A) & \rightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \rightarrow & \mathrm{Ext}^1_{\mathbb{Z}}(L^{\mathrm{ab}}; A) & \rightarrow & H^2_{\mathrm{Lie}}(L; A) & \rightarrow & \mathrm{Hom}(M(L), A) & \rightarrow & 0
\end{array}$$

Note that in this situation, *both* short exact sequences split, *neither* splits canonically (unless $c = 1$), yet there is a canonical isomorphism between them.

Another way of framing this is that, wherever applicable, the global class $(c+1)$ Lazard correspondence *refines* the global class $(c+1)$ Lazard correspondence up to isoclinism.

CHAPTER 8

APPLICATIONS AND POSSIBLE EXTENSIONS

8.1 Applications and related results

The Lazard correspondence up to isoclinism can be used as an analytical framework for the study of previous extensions of the Lazard correspondence. Some of these are discussed in this section. For simplicity, we restrict our statements to the global Lazard correspondence up to isoclinism.

8.1.1 Relation with past work of Glauberman

A special case of the Lie bracket-like map for groups, described in Section 7.6.2, was described by Glauberman in Section 5 of his 2008 paper [20]. Theorem 5.1 of the paper demonstrated that the map is alternating and bilinear when viewed as a map from the Lazard Lie ring of the inner automorphsim group. Explicitly, the statement of Theorem 5.1 was as follows:

Theorem 8.1.1 (Theorem 5.1 of [20]). Suppose S has nilpotence class at most p and $Z = Z(S)$. Then the following assertions hold.

1. Both S/Z and S' have nilpotence class at most $p-1$.

2. Define addition (and bracket multiplication) on S/Z and S' as in Theorem 2.1 (of [20]). Then there exists an alternating bi-additive function f from $(S/Z) \times (S/Z)$ into S' such that, for all u, v in S,

   $$f(uZ, vZ) = 0 \text{ if and only if } uv = vu.$$

   Moreover, the image of f generates S' as an additive group.

Part (1) of the theorem is straightforward, and is a special case of Lemma 7.7.1. Part (2) of the Theorem describes the map ω_S^{Lie} described in Section 7.6.2. The statement of part (2) follows indirectly from the discussion in Section 7.7 as follows. The commutator map defines a map $(S/Z) \wedge (S/Z) \to S'$ from the exterior square of S/Z as a group. The Lie bracket map ω_S^{Lie} correspondingly defines a Lie ring map $\log(S/Z) \wedge \log(S/Z) \to \log(S')$. Here, $\log(S/Z) \wedge \log(S/Z)$ denotes the exterior square of $\log(S/Z)$ *as a Lie ring*. Essentially, this follows from Theorem 7.7.3 where $L = \log(S/Z)$ and $G = S/Z$ and part of the work done in the proof of Theorem 7.7.4.

The main way that our results are more general than Glauberman's is that our results establish the existence of a Lie ring that is a counterpart to the *whole* group (S in Glauberman's theorem) whose Lie bracket map realizes the map $\log(S/Z) \wedge \log(S/Z) \to \log(S')$. The crucial additional ingredient in our proof is the use of the surjectivity of the universal coefficient theorem short exact sequence (described in Section 3.7.4, and applied in Theorem 7.7.4) to demonstrate the existence of an appropriate Lie ring extension.

8.1.2 Correspondences between subgroups and subrings

The Lazard correspondence up to isoclinism is a correspondence between some equivalence classes *up to isoclinism* of groups and some equivalence classes *up to isoclinism* of Lie rings. This fact immediately constrains the utility of the correspondence to the study of attributes that are invariant under isoclinism. Explicitly, any attribute of a group that we wish to study using the Lazard correspondence up to isoclinism should be an attribute that is invariant under isoclinisms of groups. Keeping this in mind, we apply the Lazard correspondence up to isoclinism to relate subgroups of the group and subrings of the Lie ring.

In Section 2.1.8, we described some aspects of the subgroup structure that are invariant under isoclinism. In particular, we noted there that we have a correspondence between subgroups containing the center for the two groups. We discussed the similar situation for Lie rings in Section 2.2.5.

In Section 6.6.8, we described how the global Lazard correspondence gives a correspondence between some subgroups of the group and some subrings of the Lie ring. Explicitly, the correspondence is between the global Lazard Lie subgroups of the group and the global Lazard Lie subrings of the Lie ring.

The global Lazard correspondence up to isoclinism combines the above ideas to give a correspondence between some subgroups of the group and some subrings of the Lie ring. We now describe this correspondence.

Suppose c is a positive integer. Denote by π_c the set of primes that are less than or equal to c. Suppose G is a π_c-powered group of class $(c+1)$ and L is a π_c-powered Lie ring of class $(c+1)$, and suppose G and L are in global class $(c+1)$ Lazard correspondence. We have a correspondence:

π_c-powered subgroups of G containing $Z(G) \leftrightarrow \pi_c$-powered Lie subrings of L containing $Z(L)$

Further, if a subgroup H of G and a subring M of L correspond to each other by the correspondence above, then H and M are in global class c Lazard correspondence *up to isoclinism*. Even in the case that H is a global Lazard Lie group or M is a global Lazard Lie ring, H and M are not necessarily in global Lazard correspondence up to isomorphism.

The correspondence restricts to a correspondence between normal subgroups and ideals:

π_c-powered normal subgroups of G containing $Z(G) \leftrightarrow \pi_c$-powered ideals of L containing $Z(L)$

We can generalize the correspondence somewhat. For any $d \leq c$, denote by π_d the set of all primes less than or equal to d. We have a correspondence:

π_d-powered subgroups of G of class at most $(d+1)$ containing $Z(G) \leftrightarrow \pi_d$-powered Lie subrings of L of class at most $(d+1)$ containing $Z(L)$

This also restricts to a correspondence between normal subgroups and ideals:

π_d-powered normal subgroups of G of class at most $(d+1)$ containing $Z(G) \leftrightarrow \pi_d$-powered ideals of L of class at most $(d+1)$ containing $Z(L)$

8.1.3 Correspondence between abelian subgroups and abelian subrings

In Section 2.1.10 (respectively, Section 2.2.7), we noted that for two groups (respectively, two Lie rings) that are isoclinic, the abelian subgroups (respectively, abelian subrings) that contain the center are in correspondence. We now state similar results describing a correspondence between a group and a Lie ring that are in Lazard correspondence up to isoclinism. Suppose c is a positive integer. Denote by π_c the set of primes that are less than or equal to c. Suppose a group G is in global class $(c+1)$ Lazard correspondence up to isoclinism with a Lie ring L. Then, the following hold:

- The Lazard correspondence up to isoclinism establishes a correspondence between abelian subgroups of G containing $Z(G)$ and abelian subrings of L containing $Z(L)$.
- The Lazard correspondence up to isoclinism establishes a correspondence between the abelian subgroups of G that are self-centralizing and the abelian subrings of L that are self-centralizing.
- In the case that G and L are both finite, the Lazard correspondence up to isoclinism establishes a correspondence between abelian subgroups of maximum order in G and abelian subrings of maximum order in L.
- For each of the correspondences above, normal subgroups correspond with ideals.
- If G and L are both finite, then each of the correspondences above preserves index.

8.1.4 Normal subgroups that are global Lazard Lie groups

We begin with a lemma. We omit the proof because the lemma is straightforward.

Lemma 8.1.2. The following are equivalent for a group G.

1. Any two elements of G that are conjugate to each other commute.

2. Every element of G is contained in an abelian normal subgroup of G.

3. The normal closure of every element of G is abelian.

4. G is a union of abelian normal subgroups.

5. For all $x, y \in G$, $[[x, y], y] = 1$, i.e., G satisfies a 2-Engel condition.

Groups that satisfy the equivalent conditions of the lemma are termed *Levi groups* or *2-Engel groups*. We can now state the next lemma.

Lemma 8.1.3. Suppose G is a nilpotent group of nilpotency class two. Then, G is a Levi group.

We can now state an important result relating the nilpotency class of a group and the nilpotency class of normal closures of elements. The result follows from the above lemma and induction on the nilpotency class.

Lemma 8.1.4. Suppose G is a nilpotent group of nilpotency class $c + 1$ where $c \geq 1$. Then, the normal closure of any element of G is a nilpotent group of nilpotency class at most c. In other words, G is a union of normal subgroups each of which has nilpotency class at most c.

Proof. We prove the claim by induction on c. The base case $c = 1$ follows from the preceding lemma. We proceed to demonstrate the inductive step, assuming $c \geq 2$.

Let $x \in G$ and let H be the normal closure of x in G.

Denote by $\overline{x}$ the image of x in $G/Z(G)$. It is easy to verify that the normal closure of $\overline{x}$ in $G/Z(G)$ is the image of H in $G/Z(G)$. Denote this by $\overline{H}$. By assumption, $G/Z(G)$ has class c. Thus, by the inductive hypothesis, $\overline{H}$ has class at most $c-1$. Therefore, H has class at most c. $\square$

The relevance of this result to the global Lazard correspondence is as follows.

Lemma 8.1.5. Suppose c is a positive integer, π_c is the set of all primes less than or equal to c, and G is a π_c-powered group of nilpotency class at most $(c+1)$. Then, the following hold:

1. Every element of G is contained in a normal subgroup of G that is a global class c Lazard Lie group. Equivalently, G is a union of normal subgroups that are global class c Lazard Lie groups.
2. G is a union of normal subgroups that are global class c Lazard Lie groups such that all the subgroups contain the center of G.

Proof. *Proof of (1)*: We will show that for every element $g \in G$, g is contained in global class c Lazard Lie subgroup of G. By the preceding lemma (Lemma 8.1.4), the normal closure of g in G is a group of nilpotency class c. Denote this normal closure as H. Then, by Theorem 4.3.3, the subgroup $\sqrt[\pi_c]{H}$ is a π_c-powered normal subgroup of G. Thus, $\sqrt[\pi_c]{H}$ is a global class c Lazard Lie group that is a normal subgroup of G.

Proof of (2): We can replace each of the normal subgroups obtained for part (1) by its product with the center of G. $\square$

In Section 7.7, we showed that for a group G satisfying the hypotheses of the lemma above, we can find a Lie ring L such that G is in global class $(c+1)$ Lazard correspondence up to isoclinism with L. In Section 8.1.2, we showed that the π_c-powered normal subgroups of G that contain the center $Z(G)$ are in Lazard correspondence up to isoclinism with the

π_c-powered ideals of L that contain the center $Z(L)$. In particular, this means that there is a correspondence:

Normal subgroups of G containing the center that are global class c Lazard Lie groups $\leftrightarrow$
Ideals of L containing the center that are global class c Lazard Lie rings

Note, however, that even though the objects on both sides of the correspondence are in the domain of the global Lazard correspondence, the correspondence itself is only a global Lazard correspondence *up to isoclinism*.

This raises the following question:

> Given a π_c powered group G of nilpotency class $(c+1)$, is it possible to choose a π_c-powered Lie ring L such that, under the above correspondence, each of the corresponding objects are in global Lazard correspondence (not just up to isoclinism)?

In general, the answer to this question is *no*. We can see examples even for 2-groups of class two, such as the case where $c = 2$ and $G = D_8$. Our conclusion can be deduced from the discussion in Section 5.5.

8.1.5 Adjoint action

Many aspects of the relationship between inner automorphisms and inner derivations described in Section 6.6.9 continue to be valid, with suitable modification, for the global Lazard correspondence up to isoclinism (and also for the 3-local Lazard correspondence up to isoclinism). We will state our results for the global Lazard correspondence up to isoclinism, and mention at the end why the results generalize to the 3-local Lazard correspondence up to isoclinism.

Suppose c is a positive integer and π_c is the set of all primes less than or equal to c. Suppose G is a π_c-powered group of class at most $c+1$ and L is a π_c-powered Lie ring of class at most $c+1$ such that G and L are in global class $(c+1)$ Lazard correspondence up to isoclinism.

The adjoint action of G on L is defined as follows:

$$\mathrm{Ad} : G \to \mathrm{Aut}(L)$$

For any $u \in G$, define Ad_u as follows. Denote by $\overline{u}$ the image of u in $G/Z(G)$. Denote by x an element of L such that the image of x in $L/Z(L)$ corresponds to the element $\overline{u}$ under the global class c Lazard correspondence between $L/Z(L)$ and $G/Z(G)$. We define Ad_u as the following automorphism of L:

$$\mathrm{Ad}_u = \exp(\mathrm{ad}_x)$$

where exp is understood to mean the actual power series of exp, with the addition and multiplication happening inside $\mathrm{End}_{\mathbb{Z}}(L)$, the ring of endomorphisms of the underlying additive group of L. Explicitly:

$$\mathrm{Ad}_u = 1 + \mathrm{ad}_x + \frac{\mathrm{ad}_x^2}{2!} + \dots \frac{\mathrm{ad}_x^c}{c!}$$

Or even more explicitly:

$$\mathrm{Ad}_u(g) = g + [x, g] + \frac{1}{2!}[x, [x, g]] + \dots + \frac{1}{c!}[x, [x, \dots [x, g] \dots]]$$

where the x appears c times in the last iterated Lie bracket.

It can easily be verified that Ad_u is an automorphism of L (this follows, for instance, by noting that ad_x is a derivation of L satisfying the conditions of Proposition 2.5 in Alperin and Glauberman's paper [1]). It can also be verified that $\mathrm{Ad}_{uv} = \mathrm{Ad}_u \mathrm{Ad}_v$, making Ad a homomorphism. Note that both these verifications use only three elements at a time:

- The verification that Ad_u is an automorphism requires us to consider the effect of Ad_u

on an arbitrary Lie product $[g, h]$, and therefore involves three elements: x, g, and h.

- The verification that $\mathrm{Ad}_{uv} = \mathrm{Ad}_u \mathrm{Ad}_v$ requires us to consider an arbitrary element $g \in L$ and elements (say x and y) that correspond to u and v when considered modulo the center. Therefore, this involves three elements.

Thus, the proofs generalize to the 3-local case.

8.1.6 Adjoint group and unitriangular matrix group

In Section 6.6.10, we noted that for a nilpotent associative ring N of class c, its associated Lie ring and adjoint group $1 + N$ are both nilpotent. We further noted that if the additive group of N is π_c-powered where π_c is the set of primes less than or equal to c, then N (as a Lie ring) is in global class c Lazard correspondence with the adjoint group $1 + N$.

The result has an analogue for the global class $(c + 1)$ Lazard correspondence up to isoclinism, as follows. Suppose N is a nilpotent associative ring of nilpotency class $c+1$ (i.e., all products of length $c + 2$ or more are zero). Suppose further that the additive group of N is π_c-powered. Then, the Lie ring N and the adjoint group $1 + N$ are in global class $(c + 1)$ Lazard correspondence up to isoclinism.

We can therefore also obtain an analogue of the result described in Section 6.6.11. Explicitly, this says the following: if the additive group of a commutative associative unital ring R is π_c-powered, then $NT(c + 2, R)$, viewed as a Lie ring, is in global class $(c + 1)$ Lazard correspondence up to isoclinism with the group $UT(c + 2, R)$.

8.2 Possible extensions

8.2.1 Relaxing the π_c-powered assumption on the whole group

It is possible to reframe the existence result of the global class $(c+1)$ Lazard correspondence in a manner that replaces the assumption that the group itself is π_c-powered by the assumption that the inner automorphism group and derived subgroup are π_c-powered. Similarly, we can replace the assumption that the Lie ring itself is π_c-powered by the assumption that the inner derivation Lie ring and derived subring are both π_c-powered. We can ahow both results either by making modifications to the proofs or by first passing from the group to an isoclinic group that is π_c-powered.

Note that we *do* need to make the assumption of π_c-powering for *both* the inner automorphism group *and* the derived subgroup. If we assume only that the inner automorphism group is π_c-powered, it does follow from that that the derived subgroup is π_c-divisible, but the derived subgroup need not be π_c-torsion-free and therefore need not be π_c-powered. For instance, for $c \geq 2$, consider the group $G = UT(c+2, \mathbb{Q})/\mathbb{Z}$, where the subgroup $\mathbb{Z}$ being factored out is inside the central subgroup $\mathbb{Q}$. G is a global class $(c+1)$ group and $\mathrm{Inn}(G)$ is π_c-powered (in fact, it is rationally powered), but G' is not π_c-powered (in fact, it is not powered over any prime, because it contains $\mathbb{Q}/\mathbb{Z}$ as a subgroup).

8.2.2 3-local Lazard correspondence up to isoclinism: proof of existence

In Section 7.7, we *defined* the Lazard correspondence up to isoclinism in the 3-local setting, but we *proved existence* only in the global setting. We expect the results to hold in the 3-local setting. Explicitly, we expect the following results described in the outline to hold:

- For a Lie ring L, if both $\mathrm{Inn}(L)$ and L' are (3-local) Lazard Lie rings, then we can find a group G such that L is in (3-local) Lazard correspondence up to isoclinism with G.
- For a group G, if both $\mathrm{Inn}(G)$ and G' are (3-local) Lazard Lie groups, then we can find a Lie ring L such that L is in Lazard correspondence up to isoclinism with G.

We believe that proofs analogous to those presented in Section 7.7 of this thesis can be used to show the above. However, executing these proofs would require us to define a number of intermediate objects more generally, making the exercise of generalizing the proofs more difficult.

8.2.3 More results about primes appearing in denominators

The literature on the Baker-Campbell-Hausdorff formula and the Lazard correspondence includes a number of bounds on primes that appear in denominators in these formulas. Some of the relevant literature is discussed below.

- Theorem C of Easterfield's paper [11] provides bounds on the exponents of primes appearing in formulas for commutators between powers of elements. The paper does not explicitly discuss the Lazard correspondence or the Baker-Campbell-Hausdorff formula, but the results are closely related, and the relationship is elucidated further by Glauberman in his paper [19] on partial extensions of the Lazard correspondence.

- The paper [9], a paper describing a computationally effective version of the Lazard correspondence, provides bounds on the exponents of primes in denominators for the formula. The bounds for the inverse Baker-Campbell-Hausdorff formula are in Section 6 of the paper.

- Thomas Weigel's doctoral dissertation [48] contains strong bounds on the primes that appear in the denominators for formulas for M_d and $h_{2,d}$ where $d \leq 2c - 2$. These results are related to the results we describe in the Appendix, Section B.1.3.

8.2.4 Potential extension to a Lazard correspondence up to n-isoclinism

In the Appendix, Section A.5, we describe the notions of *isologism* and *homologism* for groups. Similar concepts can be defined for Lie rings (and in fact, for more general varieties of algebras). The corresponding generalization of the Schur multiplier is an abelian group termed the *Baer invariant*. The paper [31] by Leedham-Green and McKay is an important source of results about isologisms.

A particular form of isologism of interest to us is n-isoclinism for a positive integer n. The concepts of n-isoclinism and n-homoclinism are described in the Appendix, Section A.5.7 and also in [24] (for groups) and [40] (for Lie rings). Recall that an isoclinism between groups is an equivalence between their commutator structures. The commutator structure is precisely the structure that becomes trivial in all abelian groups. Thus, we can think of isoclinism as "equivalence modulo the subvariety of abelian groups." In a similar vein, n-isoclinism is an equivalence between the $(n+1)$-fold commutator structures, and we can think of it as "equivalence modulo the subvariety of groups of nilpotency class n." The corresponding generalization of the Schur multiplier is an abelian group termed the n-nilpotent multiplier. The n-nilpotent multiplier of a group G is denoted $M^{(n)}(G)$, and we use similar notation for Lie rings. Note that the Schur multiplier is the n-nilpotent multiplier for the case $n = 1$.

It may be possible to generalize the "global class $(c+1)$ Lazard correspondence up to isoclinism" to a "global class $(c+n)$ Lazard correspondence up to n-isoclinism" for some values of $n > 1$. Weigel's results, alluded to in Section 8.2.3, suggest that it may be possible to *define* the notion for some values of $n > 1$ (dependent on c).

However, there are important parts of the theory developed in Sections 3.6 and 3.7 that do not generalize in the expected manner. For instance, the paper [31] by Leedham-Green and McKay suggests that the approach that we have used in this thesis cannot be used to show existence. In particular, instead of the universal coefficient theorem short exact sequence described in Section 3.6.4, we obtain a long exact sequence. Specifically, the analogue of right exactness (the surjectivity of the right map) fails. For a more detailed discussion of the failure of surjectivity, see Section 2 of the paper by Leedham-Green and McKay.

8.2.5 Glauberman's partial extension

In his 2007 paper [19], George Glauberman described a generalization of the Lazard correspondence. His Theorem A and Theorem B are restated below.

Theorem 8.2.1 (Theorem A of [19])**.** Suppose p is a prime and S is a finite p-group. Then $[x, y]$ (in the Lie bracket sense) is well defined whenever x and y are elements of (possibly different) normal subgroups of S of nilpotence class at most $p-1$.

In addition, suppose A and B are normal subgroups of S of nilpotence class at most $p-1$. Define $+$ and $[\ ,\ ]$ on A and B as in the Lazard correspondence. Then:

(i) for each u in A and v in B, the elements $[u, v]$ and $[v, u]$ lie in $A \cap B$, and $[v, u] = [u, v]^{-1}$.

(ii) for each u, u' in A and v in B,

$$[u + u', v] = [u, v] + [u', v] \qquad \text{and} \qquad [[u, u'], v] = [[u, v], u'] + [u, [u', v]]$$

Theorem 8.2.2 (Theorem B of [19]). Suppose S is a finite p-group generated by a set $\mathcal{S}$ of normal subgroups N of S having nilpotence class at most $p-1$. Let $\mathfrak{U}$ be the set-theoretic union of the elements of $\mathcal{S}$. For each N in $\mathcal{S}$, define $+$ on N by Lazard's definition. For each $u, v \in \mathfrak{U}$, define $[u, v]$ as in Theorem A.

Let $E = \mathrm{End}(\mathcal{S})$ be the set of all mappings ϕ from $\mathcal{U}$ to $\mathcal{U}$ such that, for each N in $\mathcal{S}$, ϕ maps N into N and induces an endomorphism of N under $+$.

Define addition and multiplication on E by

$$(\phi + \phi')(x) = \phi(x) + \phi'(x) \qquad \text{and} \qquad (\phi\phi')(x) = \phi(\phi'(x))$$

For each $v \in \mathfrak{U}$, define a mapping $\operatorname{ad} v$ on $\mathfrak{U}$ by

$$(\operatorname{ad} v)(u) = [u, v]$$

Then:

(i) $\operatorname{ad} v$ lies in E for each v in $\mathfrak{U}$.

(ii) for each N in $\mathcal{S}$ and each $v, w \in N$, $\operatorname{ad}(v + w) = \operatorname{ad} v + \operatorname{ad} w$.

(iii) for $v, w \in \mathfrak{U}$:

$$[\operatorname{ad} v, \operatorname{ad} w] = \operatorname{ad}[w, v] = -\operatorname{ad}[v, w]$$

$$\operatorname{ad} v = \operatorname{ad} w \iff v \equiv w \pmod{Z(S)}$$

(iv) The additive subgroup $L(\mathcal{S})$ of E spanned by mappings $\operatorname{ad} v$ for v in $\mathfrak{U}$ is a Lie subring of E, and

(v) for $L(\mathcal{S})$ as in part (iv), each element ϕ of $L(\mathcal{S})$ satisfies

$$\phi([u, v]) = [\phi(u), v] + [u, \phi(v)] \; \forall u, v \in \mathfrak{U}$$

In the special case that S is a finite p-group of nilpotency class p, the existence of a collection $\mathcal{S}$ satisfying the hypotheses of the theorems is guaranteed by Lemma 8.1.5. We can also deduce that $L(\mathcal{S})$ is isomorphic to the Lazard Lie ring $\log(\operatorname{Inn}(S))$, regardless of the choice of $\mathcal{S}$. We also know that in this case there exists a Lie ring N that is in global class p Lazard correspondence up to isoclinism with S, and therefore, that $\operatorname{Inn}(N) \cong L(\mathcal{S})$.

Thus, in the case that S is a finite p-group of nilpotency class greater than p but admitting such a collection of normal subgroups $\mathcal{S}$, the Lie ring $L(\mathcal{S})$ can be thought of as our attempt to define $\log(\operatorname{Inn}(S))$, even though the latter does not exist.[1] This raises the question of whether we can define a generalization of the Lazard correspondence up to isoclinism that would guarantee the existence of a Lie ring N such that we can think of S and N as being related via that appropriate generalization, and such that $\operatorname{Inn}(N) \cong L(\mathcal{S})$.

1. In private correspondence, George Glauberman shared an example of a finite p-group S of class greater than p for which the isomorphism type of $L(\mathcal{S})$ is dependent on the choice of $\mathcal{S}$, i.e., different choices of $\mathcal{S}$ may yield different isomorphism types for $L(\mathcal{S})$. The example has not yet been published.

8.2.6 Possible generalization of the Kirillov orbit method

The Kirillov orbit method is a method used to compute the degrees of the irreducible representations of a finite Lazard Lie group. The following is the procedure for computing the degrees of irreducible representations of a finite group G:

- Denote by L the Lazard Lie ring corresponding to G.
- Denote by $\hat{L}$ the Pontryagin dual to L, viewed only as an additive group. Note that $\hat{L}$ is isomorphic to L, but there is no natural isomorphism.
- The natural action of G on L (called the *adjoint representation*, and described in Section 6.6.9) induces a natural action of G on $\hat{L}$ (called the *coadjoint representation*). The orbits under this action correspond to the irreducible representations. Moreover, the size of any orbit is the *square* of the degree of the irreducible representation to which it corresponds. Note that this is combinatorially consistent with the fact that the sum of squares of the degrees of irreducible representations of G equals the order of G (because the order of G equals the order of L, and this in turns equals the order of $\hat{L}$).

For a detailed discussion of the method, see the papers [21], [7], and [33].

In the Appendix, Section B.3, we show that if two finite groups are isoclinic, they have the same proportions of degrees of irreducible representations, and in particular, if they have the same order, then they have the same multiset of degrees of irreducible representations, and therefore they have isomorphic group algebras over the field of complex numbers.

In particular, suppose G_1 and G_2 are isoclinic and both are finite p-groups of the same order that are Lazard Lie groups. Denote by L_1 the Lazard Lie ring of G_1 and denote by $\hat{L_1}$ the Pontryagin dual to L_1. In order to find the degrees of irreducible representations of G_1, we consider its coadjoint representation (action on $\hat{L_1}$). Note that this action factors through the group $G_1/Z(G_1) \cong \mathrm{Inn}(G_1)$. In particular, since G_2 is isoclinic to G_1, we can also view the coadjoint action as an action of G_2 on $\hat{L_1}$. Moreover, the sizes of the orbits here are the squares of the degrees of irreducible representations of G_1, and hence also of G_2.

This has an important implication, namely, that if our goal behind using the Kirillov orbit method is solely to find the degrees of the irreducible representations rather than determine the actual irreducible representations, then we can use the Lazard Lie ring of any isoclinic group. This suggests that we might be able to generalize the method to the situation of the Lazard correspondence up to isoclinism.

In Section 8.1.5, we noted that if G and L are in global class $(c+1)$ Lazard correspondence up to isoclinism, then we can define an adjoint action of G on L. We can use this to obtain a *coadjoint action* of G on the Pontryagin dual $\hat{L}$.

This leads to the following conjecture.

Conjecture 8.2.3 (Kirillov orbit method for correspondence up to isoclinism)**.** Suppose p is a prime number, G is a finite p-group of nilpotency class p, and L is a finite p-Lie ring of nilpotency class p such that G and L are in global class p Lazard correspondence up to isoclinism, and such that G and L *have the same order*. Consider the coadjoint action of G on the Pontryagin dual $\hat{L}$ described above. The sizes of the orbits for this coadjoint action are the squares of the degrees of irreducible representations.

Note that, even if the conjecture were true, the method would be weaker than the actual Kirillov orbit method, because the actual Kirillov orbit method can be used to *find explicitly the characters of the irreducible representations.* However, this method can only provide the degrees of the irreducible representations. It cannot reveal the characters themselves because the characters are not invariant under isoclinism. In fact, this method can *only* reveal isoclinism-invariant information.

8.2.7 Other possibilities: the use of multiplicative Lie rings

In [17], Graham Ellis defined *multiplicative Lie rings*, which have been further considered in [4]. The theory of multiplicative Lie rings is powerful enough to encapsulate both the theory of groups and the theory of Lie rings. This theory is, however, relatively non-standard and not sufficiently well-developed in the literature, so we do not use this framework in the document. It would be a potentially interesting exercise to reformulate the results and proofs presented here in the language of multiplicative Lie rings.

Appendices

APPENDIX A

BACKGROUND MATERIAL

A.1 Background definitions and basic theory

A.1.1 *Rings and associativity*

A *ring* is an abelian group R (with the abelian group operation denoted additively) equipped with a $\mathbb{Z}$-bilinear operation $R \times R \to R$ called the ring multiplication. Here, "$\mathbb{Z}$-bilinear" is equivalent to the left and right distributivity laws. The multiplication operation of a ring may be denoted by an explicit multiplicative symbol such as $*$ or $\cdot$ but it will often be denoted by concatenation (also known as juxtaposition), i.e., we will denote by ab the image of (a, b).

An *associative* ring is a ring where the multiplication is associative. With the notation above, R is associative if the following holds:

$$(ab)c = a(bc) \; \forall \; a, b, c \in R$$

Note that we do *not* assume associativity as part of the definition of ring. Thus, our definition of ring includes associative rings, Lie rings, and other kinds of rings. The use of concatenation can be misleading in the non-associative case, because the string abc has two differing interpretations: $(ab)c$ versus $a(bc)$. When considering products of length more than two in a non-associative ring, we must take care to use parentheses to clarify the order of operations.

Note that when we use the term "commutative unital ring" we are by default referring to rings that are both commutative and associative and where the ring multiplication has an identity element, that we denote as 1.

A.1.2 Algebras over a commutative unital ring

Suppose R is a commutative (associative) unital ring. An *algebra over* R, also called a R-algebra, is a R-module A equipped with a R-bilinear operation $A \times A \to A$ called the multiplication or product. Note that any algebra over R is naturally also a ring. If the multiplication of A is associative, we say that A is an *associative algebra* over R. We can in fact define a ring as a $\mathbb{Z}$-algebra.

A.1.3 Structure constants and multilinear identities

Suppose R is a commutative (associative) unital ring and A, B, C are R-modules, with $f : A \times B \to C$ a R-bilinear map. Suppose $(a_i), (b_j), (c_k)$ form generating sets for A, B, and C as R-modules. We can find values $\lambda_{ij}^k \in R$, called the *structure constants* of f, such that the following holds for all i, j:

$$f(a_i, b_j) = \sum_k \lambda_{ij}^k c_k$$

Note that the structure constants need not be uniquely determined by the knowledge of f and the generating sets. However, in the case that C is a free R-module and the (c_k) form a freely generating set for C, the structure constants are uniquely determined by f and the choice of generating sets. The converse is always true: if we are given the structure constants and the generating sets, f is uniquely determined.

The typical case where we talk of structure constants is where A, B, and C are all free R-modules and each of the generating sets is a *freely generating set*. In this case, *every* possible tuple of values for λ_{ij}^k can be realized via a bilinear map. A further special case of this is where R is a field. In this case, all R-modules are free (explicitly, they are vector spaces over the field, and each generating set is a basis for the corresponding vector space).

In particular, given an algebra A over a commutative unital ring R such that the additive group of A is a free R-module, we can describe A by choosing a freely generating set for it and then using structure constants for the multiplication of A. In this case, we will call the structure constants for the multiplication of A the structure constants of A.

A.1.4 Lie rings and Lie algebras

A *Lie ring* is defined as an abelian group L equipped with a $\mathbb{Z}$-bilinear map $[\ ,\ ] : L \times L \to L$ called the *Lie bracket* satisfying the following conditions:

- *Alternating property*: $[x, x] = 0$ for all $x \in L$. It also follows from this that $[x, y] = -[y, x]$ for all $x, y \in L$. The latter condition is termed *skew symmetry*. The proof of the implication uses that $[\ ,\ ]$ is $\mathbb{Z}$-bilinear. Explicitly, the proof uses $\mathbb{Z}$-bilinearity to show that $[x, y] + [y, x] = [x + y, x + y] - [x, x] - [y, y]$, and we then note that the right side is zero by the alternating property.

  The converse implication does not hold, i.e., skew symmetry does not imply the alternating property, although it does so if L is 2-torsion-free. Explicitly, $[x, y] = -[y, x]$ for all x, y implies that $[x, x] = -[x, x]$ for all x, so $2[x, x] = 0$. In the case that L is torsion-free, this implies that $[x, x] = 0$.

- *Jacobi identity*: There are two versions, both of which are equivalent under skew symmetry (and hence under the alternating property):
  - *Left normed Jacobi identity*: $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ for all $x, y, z \in L$.
  - *Right normed Jacobi identity*: $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all $x, y, z \in L$.

Let R be a commutative (associative) unital ring. A *Lie algebra* over R is a R-module L equipped with a R-bilinear map $[\ ,\ ] : L \times L \to L$ called the *Lie bracket* satisfying the two conditions above, namely, the alternating property and the Jacobi identity.

Note in particular that any R-Lie algebra can naturally be viewed as a Lie ring. A Lie ring can be defined as a $\mathbb{Z}$-Lie algebra.

The following additional definitions are useful:

- *Subring of a Lie ring*: A subset S of a Lie ring is termed a *subring* (or *Lie subring*) if it is an additive subgroup of L and is closed under the Lie bracket, i.e., $[x, y] \in S$ for all $x, y \in S$.

- *Ideal of a Lie ring*: A subset I of a Lie ring L is termed an *ideal* if I is an additive subgroup of L and $[x, y] \in I$ for all $x \in I$, $y \in L$.

  Any ideal is a subring, but a subring need not be an ideal.

- *Homomorphism of Lie rings*: Given Lie ring L_1 and L_2, a *homomorphism* from L_1 to L_2 is a set map $\varphi : L_1 \to L_2$ that is a homomorphism between L_1 and L_2 as groups and such that $\varphi([x, y]) = [\varphi(x), \varphi(y)]$ for all $x, y \in L$.

- *Quotient Lie ring*: Given a Lie ring L and an ideal I of L, the quotient group L/I naturally inherits the structure of a Lie ring from L.

We can also define corresponding notions of subalgebra of a Lie algebra, ideal of a Lie algebra, homomorphism of Lie algebras, and quotient Lie algebra, all in the context of a R-Lie algebra for a commutative (associative) unital ring R.

There are analogues in Lie rings (and also in R-Lie algebras) of the four isomorphism theorems for groups.

A.1.5 The relationship between Lie rings and Lie algebras

Most of the basic ideas and definitions associated with Lie rings (that we can think of as $\mathbb{Z}$-Lie algebras) generalize to R-Lie algebras for any commutative (associative) unital ring R. In the Appendix, we discuss how the definitions for Lie rings relate to corresponding definitions for R-Lie algebras. However, all the definitions and results in the main document are framed in terms of Lie rings.

Many of the results in the main document generalize to Lie algebras. However, to correctly generalize the main results (which are about correspondences between groups and

Lie rings) we need to develop a concept of a group powered over an arbitrary commutative (associative) unital ring.

A.1.6 Verification of multilinear identities: associativity and the Jacobi identity

Suppose R is a commutative unital ring and M is a R-module. We use the term *R-multilinear identity* for an identity of the form:

$$F(x_1, x_2, \ldots, x_n) = 0$$

where $F : M \times M \times \cdots \times M \to M$ is R-linear in each coordinate. We say that the identity holds in M if the above holds for all $x_1, x_2, \ldots, x_n \in M$, i.e., F is identically the zero function.

For any commutative unital ring R and any R-algebra A, associativity of A is a R-multilinear identity (that may or may not hold for A). Similarly, the left-normed Jacobi identity for A is a R-multilinear identity (that may or may not hold for A).

For any R-multilinear identity being considered on a R-module M, the following are true:

- It suffices to verify the identity on a generating set for M as a R-module, i.e., it suffices to verify the identity for each x_i varying arbitrarily over a generating set for M as a R-module.
- In the case that M is a free R-module and the multilinear operation F is built from a R-bilinear operation $f : M \times M \to M$, the multilinear identity reduces to a polynomial condition in terms of the structure constants for f (this will be clearer from the examples below).

Suppose R is a commutative unital ring and A is a R-algebra with multiplication $*$, i.e., A is a R-module and $* : A \times A \to A$ is a R-bilinear map. The *associator* of $*$ is a R-trilinear function $a : A \times A \times A \to A$ defined as:

$$a(x, y, z) := ((x * y) * z) - (x * (y * z))$$

$*$ is associative if and only if a is the zero function. In order to verify that a is the zero function, it suffices to choose a generating set S for A as a R-module and then verify that $a(x, y, z) = 0$ for all $x, y, z \in S$.

In the case that A is a free R-module with freely generating set $e_i, i \in I$ and structure constants λ_{ij}^k for the multiplication, the associativity condition can be written as follows, for all $i, j, k, l \in I$:

$$\sum_{m \in I} \lambda_{ij}^m \lambda_{mk}^l = \sum_{m \in I} \lambda_{im}^l \lambda_{jk}^m$$

Suppose R is a commutative unital ring and L is a R-algebra with multiplication denoted by a bracket $[\ ,\ ]$. The left-normed and right-normed Jacobi identities respectively mean that the following R-trilinear functions are zero everywhere:

$$\begin{aligned} J_l(x, y, z) &= [[x, y], z] + [[y, z], x] + [[z, x], y] \\ J_r(x, y, z) &= [x, [y, z]] + [y, [z, x]] + [z, [x, y]] \end{aligned}$$

In order to verify either of these identities, it suffices to verify it on a generating set for L as a R-module. Explicitly, if S generates L as a R-module, then $J_l(x, y, z) = 0$ for all $x, y, z \in L$ if and only if $J_l(x, y, z) = 0$ for all $x, y, z \in S$. Similarly, $J_r(x, y, z) = 0$ for all $x, y, z \in L$ if and only if $J_r(x, y, z) = 0$ for all $x, y, z \in S$.

In the case that L is free as a R-module, the left-normed and right-normed Jacobi identities can be verified in terms of the structure constants. Explicitly, if $e_i, i \in I$ form a freely generating set for L, and λ_{ij}^k denote the structure constants, then the following hold:

- The left-normed Jacobi identity is equivalent to the condition that:

$$\sum_{m \in I} (\lambda_{ij}^m \lambda_{mk}^l + \lambda_{jk}^m \lambda_{mi}^l + \lambda_{ki}^m \lambda_{mj}^l) = 0$$

- The right-normed Jacobi identity is equivalent to the condition that:

$$\sum_{m \in I} (\lambda_{im}^l \lambda_{jk}^m + \lambda_{jm}^l \lambda_{ki}^m + \lambda_{km}^l \lambda_{ij}^m) = 0$$

A.1.7 Derivation of a ring and of an algebra

We define derivations for rings, and also for algebras for commutative unital rings.

Definition (Derivation)**.** Suppose A is a ring with multiplication denoted by $*$. A set map $d : A \to A$ is termed a *derivation* of A if it satisfies *both* these conditions:

- d is an endomorphism of the additive group of A.
- d satisfies the following condition, called the *Leibniz condition*:

$$d(x * y) = (d(x) * y) + (x * d(y)) \ \forall \ x, y \in R$$

Note that we typically do not use parentheses for the inputs to derivations if they are single letters, so the above is often written as:

$$d(x * y) = (dx * y) + (x * dy) \ \forall \ x, y \in R$$

The set of derivations of a ring forms a Lie ring, where the addition is pointwise, and the Lie bracket is defined as $[d_1, d_2] = d_1 \circ d_2 - d_2 \circ d_1$ (with $\circ$ denoting composition of set maps). For a ring A, we will denote the Lie ring of derivations of A by $\mathrm{Der}(A)$.

We now consider the definition of derivation for an algebra over a commutative unital ring.

Definition (Derivation of an algebra)**.** Suppose R is a commutative unital ring and A is a R-algebra. A set map $d : A \to A$ is termed a derivation of A as a R-algebra if d is a R-module endomorphism of A *and* satisfies the Leibniz condition (stated in the preceding definition).

The set of derivations of a R-algebra forms a R-Lie algebra.

A.1.8 Derivation of a Lie ring and of a Lie algebra

Suppose L is a Lie ring. For any $x \in L$, consider the set map $\mathrm{ad}_x : L \to L$ given by $\mathrm{ad}_x(y) = [x, y]$. ad_x is termed the *left adjoint map*, or simply the *adjoint map* corresponding to x.

It follows from the distributivity of the Lie bracket that ad_x is an additive group endomorphism, and the Jacobi identity along with skew symmetry give us that ad_x satisfies the Leibniz condition. Similarly, if L is a Lie algebra over a commutative unital ring R, then ad_x is a derivation in the R-algebra sense.

The derivations of the form ad_x are termed *inner derivations* of L. We can easily verify that two elements $x, y \in L$ satisfy $\mathrm{ad}_x = \mathrm{ad}_y$ if and only if $\mathrm{ad}_{x-y} = 0$, and the set of values $z \in L$ for which $\mathrm{ad}_z = 0$ is precisely the *center* of L (defined as the set $\{z \in L \mid [z, y] = 0 \ \forall \ y \in L\}$). We obtain the following:

- The inner derivations of L form an ideal inside $\mathrm{Der}(L)$. We will denote this ideal by $\mathrm{Inn}(L)$.

- The set map $x \mapsto \mathrm{ad}_x$ defines a Lie ring homomorphism from L to $\mathrm{Der}(L)$ with image $\mathrm{Inn}(L)$ and kernel $Z(L)$. Thus, by the first isomorphism theorem, $L/Z(L)$ is canonically isomorphic to $\mathrm{Inn}(L)$.

A.2 Abstract nonsense

A.2.1 Basic category theory: categories, functors, and natural transformations

We define here three foundational ideas of category theory: categories, functors, and natural transformations.

Definition of category

A *category* $\mathcal{C}$ is the following data:

- *Objects*: A collection $\mathrm{Ob}\,\mathcal{C}$ of objects.[1]
- *Morphisms*: For any objects $A, B \in \mathrm{Ob}\,\mathcal{C}$, a collection $\mathcal{C}(A, B)$ of morphisms. Every element in $\mathcal{C}(A, B)$ is termed a *morphism* from A (i.e., with source or domain A) to B (i.e., with target or co-domain B). The morphism sets for different pairs of objects are disjoint. Note that $f \in \mathcal{C}(A, B)$ is also written as $f : A \to B$. The collection $\mathcal{C}(A, B)$ is sometimes also denoted $\mathrm{Hom}_{\mathcal{C}}(A, B)$ or simply $\mathrm{Hom}(A, B)$.
- *Identity morphism*: For every object $A \in \mathrm{Ob}\,\mathcal{C}$, a distinguished morphism $\mathrm{id}_A \in \mathcal{C}(A, A)$. This is called the identity morphism of A.
- *Composition rule*: For $A, B, C \in \mathrm{Ob}\,\mathcal{C}$, a map, called *composition of morphisms*, from $\mathcal{C}(B, C) \times \mathcal{C}(A, B)$ to $\mathcal{C}(A, C)$. This map is denoted by $\circ$.

1. There are some set theory paradoxes due to which we are using the term “collection” rather than “set” here.

satisfying the following compatibility conditions:

- *Associativity of composition*: For $A, B, C, D \in \mathrm{Ob}\,\mathcal{C}$, with $f \in \mathcal{C}(A, B), g \in \mathcal{C}(B, C), h \in \mathcal{C}(C, D)$, we have $h \circ (g \circ f) = (h \circ g) \circ f$.

- *Identity behaves as an identity*: For $A, B \in \mathrm{Ob}\,\mathcal{C}$, with $f \in \mathcal{C}(A, B)$, we have $f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f$.

We will also use the following terms:

- For $A \in \mathrm{Ob}\,\mathcal{C}$, an *endomorphism* of A is defined as an element of $\mathcal{C}(A, A)$. The endomorphisms of A form a *monoid* under composition, denoted $\mathrm{End}_{\mathcal{C}}(A)$. The identity morphism Id_A is the identity element of this monoid.

- For $A, B \in \mathrm{Ob}\,\mathcal{C}$, an *isomorphism* from A to B is defined as an element $f \in \mathcal{C}(A, B)$ such that there exists an element $g \in \mathcal{C}(B, A)$ for which $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$.

- For $A \in \mathrm{Ob}\,\mathcal{C}$, an *automorphism* of A is defined an an endomorphism of A that is also an isomorphism. The automorphisms of A form a *group* under composition, denoted $\mathrm{Aut}_{\mathcal{C}}(A)$. The identity morphism Id_A is the identity element of this group. $\mathrm{Aut}_{\mathcal{C}}(A)$ is the subgroup of $\mathrm{End}_{\mathcal{C}}(A)$ comprising all the elements with two-sided inverses.

The categories that we will consider in this document include:

- The category of groups, where the morphisms are group homomorphisms. The notions of endomorphism, isomorphism, and automorphism in this case coincide with our usual notions. Similarly, we consider the category of Lie rings where the morphisms are Lie ring homomorphisms. Note that these are the default category structures on group and Lie rings respectively.

- The category of groups with homoclinisms, described in Section 2.1 (specifically, Section 2.1.4). The isomorphisms in this category are isoclinisms of groups. Similarly, we consider the category of Lie rings with homoclinisms in Section 2.2.

- The category of short exact sequences of groups, described in Section 3.1. Similarly, we consider the category of short exact sequences of Lie rings in Section 3.2.
- The category of central extensions of a group, described in Section 3.1.6. Similarly, we consider the category of central extensions of a Lie ring in Section 3.2.5.
- The category of central extensions of a group with homoclinisms, described in Section 3.4.3. Similarly, we consider the category of central extensions of a Lie ring with homoclinisms in Section 3.5.5.
- The category of π-powered groups for a prime set π, described in Section 4.1. Similarly, the category of π-powered Lie rings for a prime set π, described in Section 4.2.

Definition of functor

Suppose $\mathcal{C}, \mathcal{D}$ are categories. A *functor* (also called *covariant functor*) $\mathcal{F}$ from $\mathcal{C}$ to $\mathcal{D}$ comprises the following data:

- *Object level mapping*: A mapping $\mathcal{F} : \operatorname{Ob}\mathcal{C} \to \operatorname{Ob}\mathcal{D}$.
- *Morphism level mapping*: For any $A, B \in \mathcal{C}$, a mapping $\mathcal{F} : \mathcal{C}(A, B) \to \mathcal{D}(\mathcal{F}A, \mathcal{F}B)$.

satisfying the following conditions:

- *It preserves the identity morphism*: For any $A \in \mathcal{C}$, $\mathcal{F}(\mathrm{id}_A) = \mathrm{id}_{\mathcal{F}(A)}$.
- *It preserves composition*: For any $A, B, C \in \mathcal{C}$, and $f \in \mathcal{C}(A, B), g \in \mathcal{C}(B, C)$, we have $\mathcal{F}(g \circ f) = \mathcal{F}g \circ \mathcal{F}f$.

Suppose $\mathcal{C}, \mathcal{D}$ are categories. A *contravariant functor* $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ is defined by the following data:

- A mapping $\mathcal{F} : \operatorname{Ob}\mathcal{C} \to \operatorname{Ob}\mathcal{D}$.

- For every $A, B \in \operatorname{Ob}\mathcal{C}$, a mapping $\mathcal{F} : \mathcal{C}(A, B) \to \mathcal{D}(\mathcal{F}B, \mathcal{F}A)$.

satisfying the following conditions:

- It preserves the identity map: For any $A \in \operatorname{Ob}\mathcal{C}$, $\mathcal{F}(\mathrm{id}_A) = \mathrm{id}_{\mathcal{F}A}$.
- It preserves composition, albeit reversing the order of composition: For any $A, B, C \in \operatorname{Ob}\mathcal{C}$, and $f \in \mathcal{C}(A, B), g \in \mathcal{C}(B, C)$, we have $\mathcal{F}(g \circ f) = \mathcal{F}f \circ \mathcal{F}g$.

We use the following terminology for functors. As above, let $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ be a functor.

- $\mathcal{F}$ is *faithful* if the induced set map $\mathcal{C}(A, B) \to \mathcal{D}(\mathcal{F}A, \mathcal{F}B)$ is injective for all $A, B \in \operatorname{Ob}\mathcal{C}$.
- $\mathcal{F}$ is *full* if the induced set map $\mathcal{C}(A, B) \to \mathcal{D}(\mathcal{F}A, \mathcal{F}B)$ is surjective for all $A, B \in \operatorname{Ob}\mathcal{C}$.
- $\mathcal{F}$ is *essentially surjective on objects* if every object of $\mathcal{D}$ is isomorphic in $\mathcal{D}$ to some object in the image of $\mathcal{F}$.
- $\mathcal{F}$ is an *equivalence of categories* if it is full, faithful, and essentially surjective on objects. An equivalence of categories preserves many of the features we care about. In particular, it preserves the existence of initial objects and terminal objects, the nature of homomorphism sets, and the isomorphism types of endomorphism monoids and automorphism groups.
- $\mathcal{F}$ is an *isomorphism of categories* if it is full, faithful, and bijective on objects.

We will use functors in one important way. For each of the correspondences between suitably chosen groups and Lie rings, we will first identify full subcategories of the category of groups and the category of Lie rings respectively. Here, *full* subcategory means a subcategory where the inclusion functor into the whole category is a full functor. In other words, the full subcategory may not contain all the objects of the big category, but given two objects of the big category, it contains all the morphisms between them. Our correspondence will then explicitly describe functors exp and log between these full subcategories, where exp is from Lie rings to groups and log is from groups to Lie rings. The functors exp and log will turn out to be two-sided inverses of each other, and the full subcategories will therefore turn out to be isomorphic.

Section 1.3 describes all the details for the abelian Lie correspondence. Similar ideas apply to the Baer correspondence (described in Section 5.1.8), Malcev correspondence, global Lazard correspondence, and Lazard correspondence.

We also use the idea of equivalence of categories when relating two alternate descriptions of the category of central extensions of a group where the morphisms are homomorphisms of central extensions. There are two alternative definitions of this category, and these definitions do *not* define isomorphic categories. However, they do define *equivalent* categories. In fact, there is a forgetful functor from one category (that stores the short exact sequence) to the other category (that simply stores the quotient map of the short exact sequence) that serves as the equivalence of categories. For more details, see Section 3.1.6.

Apart from the above fairly foundational uses of functors, we do not use functors explicitly.

However, many of the constructions we use throughout the document are functorial, although we do not explicitly use that fact. Some examples are below.

- The exterior square of a group, described in Section 3.4.1, defines a functor from the category of groups to itself. In other words, given any homomorphism $\varphi : G_1 \to G_2$ of groups, there is an induced homomorphism $\varphi \wedge \varphi : G_1 \wedge G_1 \to G_2 \wedge G_2$ satisfying the conditions for being a functor.

- The Schur multiplier of a group, described in Section 3.4.1, defines a functor from the category of groups to itself (or, alternatively, to the category of abelian groups).

- The exterior square of a Lie ring, described in Section 3.5.1, defines a functor from the category of Lie rings to itself.

- The Schur multiplier of a Lie ring, described in Section 3.5.1, defines a functor from the category of Lie rings to the category of abelian groups.

- There are a number of free and forgetful functors we see. We discuss these a little later in the Appendix.

Definition of natural transformation

Given two functors $\mathcal{F}, \mathcal{G} : \mathcal{C} \to \mathcal{D}$, a *natural transformation* η from $\mathcal{F}$ to $\mathcal{G}$ associates to each $A \in \operatorname{Ob}\mathcal{C}$ a morphism $\eta_A : \mathcal{F}A \to \mathcal{G}A$ such that for every morphism $f \in \mathcal{C}(A, B)$ for $A, B \in \operatorname{Ob}\mathcal{C}$, we have:

$$\eta_B \circ \mathcal{F}(f) = \mathcal{G}(f) \circ \eta_A$$

Equivalently, the following diagram commutes:

$$\begin{array}{ccc} \mathcal{F}(A) & \overset{\mathcal{F}(f)}{\rightarrow} & \mathcal{F}(B) \\ \eta_A \downarrow & & \eta_B \downarrow \\ \mathcal{G}(A) & \overset{\mathcal{G}(f)}{\rightarrow} & \mathcal{G}(B) \end{array}$$

We call η a *natural isomorphism* if η_A is an isomorphism in $\mathcal{D}$ for each $A \in \operatorname{Ob}\mathcal{C}$.

We can also define an analogous concept of natural transformation between contravariant functors.

In our main proofs, we often use the term *canonical.* The definition of *canonical transformation* is similar to that of natural transformation, except that we impose the above condition only when f is an isomorphism. In other words, natural means that the transformation behaves well (in the sense of giving a commutative diagram) for *all* morphisms, whereas canonical means that the transformation behaves well for *isomorphisms.* A *canonical isomorphism* is a canonical transformation that is an isomorphism in every instance.

It turns out that most of the canonical constructions that we use in our main proofs are also natural. This is not hard to prove, but we do not demonstrate it because it is not necessary for our main proofs. We list below some important instances of this.

- In Section 3.4.1, we define the following short exact sequence associated with any group G:

  $$0 \to M(G) \to G \wedge G \to [G, G] \to 1$$

  All the groups appearing in the short exact sequence are functorial in G, and all the morphisms appearing in the short exact sequence are natural in G, i.e., they define natural transformation between the functors. Thus, we can view the short exact sequence itself as functorial in G, i.e., we can define a functor from the category of groups to the category of short exact sequences of groups that sends a group G to the above short exact sequence.

  A similar observation applies to the corresponding short exact sequence for Lie rings described in Section 3.5.1.

- In Section 3.6.4, we define the following short exact sequence associated with a group G and an abelian group A:

  $$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(G; A) \to H^2(G; A) \to \mathrm{Hom}(M(G), A) \to 0$$

  All the groups appearing in the short exact sequence are *contravariant* functors of G (holding A constant) and (covariant) functors of A (holding G constant). Further, the morphisms of the short exact sequence are natural transformations with respect to both G and A: they are natural transformations between the contravariant functors of G (holding A constant) and also between the covariant functors of A (holding G constant).

A similar observation applies to the corresponding short exact sequence for Lie ring extensions described in Section 3.7.4.

- In Section 3.3.4, we consider the following short exact sequence associated with a group G and an abelian group A:

$$0 \to B^2(G; A) \to Z^2(G; A) \to H^2(G; A) \to 0$$

  All the groups appearing in the short exact sequence are *contravariant* functors of G (holding A constant) and (covariant) functors of A (holding G constant). Further, the morphisms of the short exact sequence are natural transformations with respect to both G and A: they are natural transformations between the contravariant functors of G (holding A constant) and also between the covariant functors of A (holding G constant).

A.2.2 Initial objects, terminal objects, and zero objects

Suppose $\mathcal{C}$ is a category. We define the following:

- An *initial object* of $\mathcal{C}$ is an object A of $\mathcal{C}$ such that for every object B of $\mathcal{C}$, there is a unique morphism from A to B, i.e., there is a unique element of $\mathcal{C}(A, B)$. Any two initial objects must be isomorphic and have a unique isomorphism between them. A category may or may not have an initial object. For a category that has initial objects, we therefore abuse notation by talking of *the* initial object of the category.

- A *terminal object* of $\mathcal{C}$ is an object A of $\mathcal{C}$ such that for every object B of $\mathcal{C}$, there is a unique morphism from B to A, i.e., there is a unique element of $\mathcal{C}(B, A)$. Any two terminal objects must be isomorphic and have a unique isomorphism between them. A category may or may not have a terminal object. For a category that has terminal objects, we therefore abuse notation by talking of *the* terminal object of the category.

- A *zero object* of $\mathcal{C}$ is an object that is both an initial object and a terminal object. A category may or may not have a zero object. Any two zero objects must be isomorphic and have a unique isomorphism between them.

  Note that even if a category has an initial object and a terminal object, it may lack a zero object because the initial objects and terminal objects are not isomorphic. For instance, for the category of commutative unital rings, the initial object is $\mathbb{Z}$ and the terminal object is the zero ring, so there is no zero object. For a category that has terminal objects, we therefore abuse notation by talking of *the* terminal object of the category.

  For a category that has a zero object, we can define, between any two objects of the category, a morphism called the *zero morphism*. This is the morphism that is obtained by composing the map from the source object to the zero object and the map from the zero object to the target object. For instance, for the category of groups, the zero object is the trivial group, and the corresponding notion of zero morphism is the trivial homomorphism between any two groups.

The discussion in Sections 3.4.1 and 3.5.1 is motivated by the goal of finding an initial object in a category, namely, the category of central extensions of a particular group (or Lie ring) with the morphisms being homoclinisms of central extensions. We show that initial objects do exist for these categories, and these initial objects play an important role in the study of the categories.

A.2.3 Left and right adjoint functors

Suppose $\mathcal{C}, \mathcal{D}$ are categories and $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ are covariant functors. We say that $\mathcal{F}$ is left adjoint to $\mathcal{G}$, or equivalently, that $\mathcal{G}$ is right adjoint to $\mathcal{F}$, if there is a family of bijections:

$$\mathcal{D}(\mathcal{F}A, B) \cong \mathcal{C}(A, \mathcal{G}B)$$

for all $A \in \mathrm{Ob}\,\mathcal{C}$ and $B \in \mathrm{Ob}\,\mathcal{D}$, such that the bijection is natural (in the sense of being a natural transformation) in both the variables A and B. The use of the word "adjoint" here is in analogy with the idea of adjoint linear transformations with respect to an inner product.

A.2.4 Universal algebra

Universal algebra is a branch of mathematics that provides a unifying framework for the study of algebraic structures. Universal algebra is fairly general and it is ill-suited to proving deep facts about specific structures (such as advanced results in group theory or in ring theory). Nonetheless, basic vocabulary from universal algebra is useful in the study of specific algebraic structures.

The first concept we define is the concept of *signature*. A signature is a function from a fixed set (that we call the *operator domain*) to $\mathbb{N}_0$ (the set of nonnegative integers). The elements of the operator domain are the *operators* and the signature sends each operator to a nonnegative integer that is its *arity*. An *algebra* of a given signature is defined to be a set equipped with operations as follows: for each operator in the operator domain, there is a n-ary operation from the set to itself where n equals the arity of the operator. Note that a 0-ary operation is understood to mean a constant function.

An *identity* refers to a formal equality of two formal expressions that are constructed using operators in the operator domain, where the expressions make sense given what we know about the arities of the operations. An algebra is said to satisfy the identity if that identity holds for all choices of elements in that algebra.

Given a signature and a collection of identities, the collection of all algebras of the signature satisfying all the identities in the collection will be called a *variety of algebras*.

For instance, consider the signature with operator domain $\Omega = \{*\}$ where the arity of $*$ is 2. We will use infix notation to denote $*$, i.e., $*(x, y)$ will be denoted as $x * y$. An algebra with this signature is equivalent to a set with a binary operation, also called a *magma*.[2]

Then, associativity of $*$ is an identity. Explicitly, it is the identity:

$$(a * b) * c = a * (b * c)$$

The collection of all magmas that *satisfy the identity of associativity* is a *variety of algebras*. Algebras of this type are termed *semigroups*, and the variety of algebras is termed *the variety of semigroups*.

Groups also form a variety of algebras. The variety of groups has an operator domain with three operations:

- An operation $*$ of arity 2, called the *group multiplication* or *product* (denoted using infix notation)
- An operation e of arity 0, called the *identity element* or *neutral element*.[3]
- An operation $^{-1}$ of arity 1, called the *inverse map* (denoted using postfix superscript notation).

The identities that need to be universally satisfied are:

$$\begin{aligned} (a * b) * c &= a * (b * c) \quad \text{(Associativity)} \\ a * e = e * a &= a \quad \text{(Identity element)} \\ a * a^{-1} = a^{-1} * a &= a \quad \text{(Inverse map)} \end{aligned}$$

2. Historically, the term "groupoid" was used but that term now has a somewhat different meaning.

3. We use 1 to denote the identity element in this document, but it is more helpful to use the letter e here for pedagogical reasons.

The following notions can readily be defined in the context of algebras of a given signature:

- *Subalgebra* refers to a subset of the underlying set of the algebra that is closed under all the operations defined for the algebra structure.
- *Homomorphism of algebras* (between algebras of the same signature) refers to a set map between the algebras that commutes with all the algebra operations.
- Based on the definition of homomorphism, we can define *isomorphism*, *endomorphism*, and *automorphism*.
- *Direct product of algebras* (where all the algebras have the same signature) is defined as follows: we take the Cartesian product of the underlying sets, and define each of the operations coordinate-wise.

An important theorem about varieties of algebras is *Birkhoff's theorem*. The theorem states that a collection of algebras is a variety of algebras if and only if it is closed under taking subalgebras, homomorphic images, and direct products. One direction of the proof is easy: any variety of algebras is closed under taking subalgebras, homomorphic images, and direct products. The reverse direction is hard, and we omit the proof.

The following are some examples of varieties of algebras that we consider in this document:

- The variety of groups.
- The variety of Lie rings.
- The variety of abelian groups.
- The variety of associative rings.
- For a fixed commutative unital ring R, the variety of R-Lie algebras.
- For a fixed commutative unital ring R, the variety of associative R-algebras.

- For a fixed commutative unital ring R, the variety of R-modules.
- For a set π of primes, the variety of π-powered groups, described in Section 4.1.
- For a set π of primes, the variety of π-powered Lie rings, described in Section 4.2.
- The variety of groups of nilpotency class c, for some fixed positive integer c.
- The variety of Lie rings of nilpotency class c, for some fixed positive integer c.
- The variety of π-powered groups of nilpotency class c.
- The variety of π-powered Lie rings of nilpotency class c.

A.2.5 Universal algebra and category theory combined: free and forgetful functors

Every variety of algebras can naturally be interpreted as a *category*. The objects of the category are the algebras of the variety. The morphisms of the category are homomorphisms between the algebras of the variety. Note that the definition of homomorphism uses only the signature and *not* the identities.

The following are some immediate observations about the category corresponding to a particular variety of algebras:

- The notions of isomorphism, endomorphism, and automorphism defined in universal algebra coincide with the corresponding notions for the category.
- The terminal object has an underlying set of size one, and all the operations are defined in the unique manner possible.
- The category does have an initial object. If the variety has no 0-ary operations, the initial object of the variety has an empty underlying set. If the varety has 0-ary operations, the initial object has a nonempty underlying set.

- In general, the initial object and terminal object need not coincide, and therefore the zero object need not exist. Some varieties where they do coincide are the variety of groups, variety of Lie rings, variety of abelian groups, variety of R-modules for a commutative unital ring R, and variety of R-Lie algebras for a commutative unital ring R. A variety where they do not coincide is the variety of commutative unital rings. The initial object for this variety is $\mathbb{Z}$ and the terminal object is the zero ring.

Suppose $\mathcal{V}_1$ and $\mathcal{V}_2$ are two varieties of algebras such that the operator domain of $\mathcal{V}_2$ is a subset of the operator domain of $\mathcal{V}_1$, with the operators having the same arities, and every identity true in $\mathcal{V}_2$ is also true in $\mathcal{V}_1$. Formally, we say that the variety $\mathcal{V}_2$ is a *reduct* of $\mathcal{V}_1$.

In this case, there is a natural *forgetful functor* from the category corresponding to $\mathcal{V}_1$ to the category corresponding to $\mathcal{V}_2$. This functor is faithful: for any algebras A and B of $\mathcal{V}_1$, the set map $\mathrm{Hom}_{\mathcal{V}_1}(A, B) \to \mathrm{Hom}_{\mathcal{V}_2}(A, B)$ is injective. However, the functor is not necessarily *full* because the set map above need not be surjective. The functor also need not be *essentially surjective*: it is not necessary that every isomorphism type of algebra in $\mathcal{V}_2$ must arise from an isomorphism type of algebra in $\mathcal{V}_1$.

There is also a natural *free functor* from the category corresponding to $\mathcal{V}_2$ to the category corresponding to $\mathcal{V}_1$. This functor sends any algebra of $\mathcal{V}_2$ to the algebra of $\mathcal{V}_1$ "generated" by it, with all the identities of $\mathcal{V}_1$. The free functor is left adjoint to the forgetful functor.

Below are some cases of interest:

1. $\mathcal{V}_2$ is the variety with *no* operations and no identities, so that the corresponding category is the category of sets. In this case, the forgetful functor simply sends an algebra to its underlying set. The free functor sends a set to the *free algebra* of the variety $\mathcal{V}_1$ generated by the set.

2. The varieties $\mathcal{V}_1$ and $\mathcal{V}_2$ have the same operator domain, so the only difference is that $\mathcal{V}_1$ may have more identities than $\mathcal{V}_2$. In this case, we say that $\mathcal{V}_1$ is a subvariety of $\mathcal{V}_2$, and the forgetful functor from the category for $\mathcal{V}_1$ to the category for $\mathcal{V}_2$ is a

full functor in this case. An example is the case where $\mathcal{V}_1$ is the variety of groups of nilpotency class c (for some positive integer c) and $\mathcal{V}_2$ is the variety of all groups.

3. Cases other than (2) where the forgetful functor is still full, i.e., every homomorphism in $\mathcal{V}_2$ between two algebras of $\mathcal{V}_1$ defines a homomorphism in $\mathcal{V}_1$. For instance, the forgetful functor from the variety of groups to the variety of semigroups that "forgets" the identity element and inverse map is full: any homomorphism of semigroups between two groups is also a homomorphism of groups. Similarly, for a prime set π, the forgetful functor from the variety of π-powered groups to the variety of groups is a full functor: any homomorphism of groups between two π-powered groups is also a homomorphism of π-powered groups.

A.3 Foundational results for manipulations in nilpotent groups

A.3.1 Central series and nilpotency for groups and Lie rings

Suppose G is a group. A subgroup series:

$$G = K_1 \geq K_2 \geq \dots K_c \geq K_{c+1} = 1$$

is termed a *central series* if it satisfies the following conditions:

1. It is a normal series:[4] every K_i is normal in G.
2. For every i, K_i/K_{i+1} is contained in the center of G/K_{i+1}.

Equivalently, it should satisfy the condition that for every i:

$$[G, K_i] \subseteq K_{i+1}$$

4. Some people use the term "normal series" for a series where each term is normal in its predecessor, and use the term "strongly normal series" for a series satisfying the condition stated here.

Note that the notation above uses a descending series, but the series may also be described as an ascending series.

G is termed a *nilpotent group* if it has a central series. The *nilpotency class* of G is defined as the smallest c for which there exists a central series of length c (matching the above notation). We say that G is a group of nilpotency class (at most) c if the nilpotency class of G is less than or equal to c. We often drop the "(at most)" qualifier for nilpotency class and simply say "G is a group of nilpotency class c" to mean that G is a nilpotent group and its nilpotency class is at most c.

There is an ascending series termed the *upper central series* and a descending series termed the *lower central series*. Both of these can be defined for all groups. For each series, it reaches the other end in finitely many steps if and only if the group is nilpotent, and if so, its length is the nilpotency class of the group.

The *upper central series* of G is an ascending series $(Z^i(G))_{i\in\mathbb{N}_0}$ of subgroups of G defined as follows:

- $Z^0(G)$ is the trivial subgroup of G.
- For $i > 0$, $Z^i(G)$ is defined as the unique subgroup of G such that $Z^i(G)/Z^{i-1}(G) = Z(G/Z^{i-1}(G))$, where $Z(G/Z^{i-1}(G))$ denotes the center of $G/Z^{i-1}(G)$. In particular, $Z^1(G) = Z(G)$ is the center of G. The subgroup $Z^2(G)$ is termed the second center of G, and so on.

The upper central series reaches the whole group G in finitely many steps if and only if G is nilpotent. Further, if G has nilpotency class c, then $Z^c(G) = G$. More explicitly, if the nilpotency class of G is precisely c, then $Z^c(G) = G$ and $Z^i(G) \neq G$ for $i < c$. In fact, the upper central series is the *fastest ascending* central series possible.[5]

5. Technically, although we can define the upper central series for a non-nilpotent group, and this definition is useful, the upper central series is *not* a central series if the group is non-nilpotent.
We can also define a *transfinite* upper central series, where we define $Z^\alpha(G)$ for all ordinals α. However, we do not need to use the transfinite upper central series here, so we will not define it.

The *lower central series* of G is a descending series of subgroups $\gamma_i(G), i \in \mathbb{N}$, defined as follows:

- $\gamma_1(G) = G$
- For $i \in \mathbb{N}$, $\gamma_{i+1}(G) = [G, \gamma_i(G)] = [\gamma_i(G), G]$ is the commutator of the subgroups G and $\gamma_i(G)$.

The lower central series reaches the trivial subgroup in finitely many steps if and only if G is nilpotent. Further, if G has nilpotency class c, then $\gamma_{c+1}(G) = 1$. More explicitly, if the nilpotency class of G is precisely c, then $\gamma_{c+1}(G) = 1$ and $\gamma_{i+1}(G) \neq 1$ for $i < c$. In fact, the lower central series is the *fastest descending* central series possible.[6]

A.3.2 Witt's identity and the three subgroup lemma

Witt's identity (stated here with the right action convention) applies to any elements a, b, c in any group G. It says that:

$$[[a, b^{-1}], c]^b \cdot [[b, c^{-1}], a]^c \cdot [[c, a^{-1}], b]^a = 1$$

The three subgroup lemma follows directly from Witt's identity:

Lemma A.3.1 (Three subgroup lemma)**.** Suppose G is a group and A, B, and C are subgroups of G. Then, any two of these three statements implies the third:

- $[[A, B], C] = 1$

6. Technically, although we can define the lower central series for a non-nilpotent group, and this definition is useful, the lower central series is *not* a central series if the group is non-nilpotent.
The subgroup $\gamma_2(G)$, also denoted G', is the *derived subgroup* of G, and is sometimes also referred to as the *commutator subgroup* of G (note that the term "commutator subgroup" may also be used for a commutator of *two* subgroups). The quotient group $G/\gamma_2(G) = G/G'$ is denoted G^{ab} and is termed the *abelianization* of G.
We can also define a *transfinite* lower central series, where we define $\gamma_\alpha(G)$ for all ordinals α. However, we do not need to use the transfinite lower central series here, so we will not define it.

- $[[B, C], A] = 1$

- $[[C, A], B] = 1$

A.3.3 Commutator of element with products, and commutator as a homomorphism

The following computational result regarding the commutator of an element and a product is useful. The result has somewhat different explicit formulations depending on whether we use

With the *left action convention*, where we denote by ${}^x g$ the element xgx^{-1} and where we denote by $[x, y]$ the commutator $xyx^{-1}y^{-1}$, the result states that:

- $[x, yz] = [x, y]({}^y[x, z])$

- $[xy, z] = ({}^x[y, z])[x, z]$

With the *right action convention*, where we denote by g^x the element $x^{-1}gx$ and where we denote by $[x, y]$ the commutator $x^{-1}y^{-1}xy$,the result states that:

- $[x, yz] = [x, z][x, y]^z$

- $[xy, z] = ([x, z]^y)[y, z]$

Lemma A.3.2. 1. *Independent of the action convention*: Suppose G is a group of nilpotency class two. For any fixed $x \in G$, the commutator maps $y \mapsto [x, y]$ and $y \mapsto [y, x]$ are endomorphisms of G. Note that since the image of both endomorphisms is inside $[G, G]$, they can be viewed as homomorphisms to $[G, G]$.

2. *Formulation specific to the left action convention*: Suppose G is a group, H is a subgroup of G, and x is an element of G such that $[x, H] \subseteq C_G(H)$, or equivalently,

$[[x, h_1], h_2] = 1$ for all $h_1, h_2 \in H$. Then, the map $y \mapsto [x, y]$ is a homomorphism from H to G. Note that with the right action convention, the map may become an anti-homomorphism, and the corresponding statement for the right action convention would use $y \mapsto [y, x]$.

3. *Independent of the action convention*: Suppose G is a group of nilpotency class c. Consider the set map:

$$T : G \times G \times \cdots \times G \to G$$

where G occurs c times on the left, given by:

$$T(x_1, x_2, \dots, x_c) := [[\dots[[x_1, x_2], x_3], \dots, x_{c-1}], x_c]$$

Choose any i with $1 \le i \le c$ and fix the values of $x_j, j \neq i$. Then, T, viewed solely as a function of x_i, defines an endomorphism of G. The image of T is inside $\gamma_c(G)$, so viewed this way, T defines a homomorphism from G to $\gamma_c(G)$. In fact, T descends to a homomorphism from $G/Z^{c-1}(G)$ to $\gamma_c(G)$.

We will use the left action convention for our proofs, including proofs of the statements that are independent of the action convention.

Proof. Proof of (1): Showing that the map $y \mapsto [x, y]$ is an endomorphism is equivalent to showing that $[x, yz] = [x, y][x, z]$. This in turn follows from the identity $[x, yz] = [x, y]({}^y[x, z])$ and the assumption of class two allowing us to deduce that $[x, z] = {}^y[x, z]$. The proof for the other map is similar.

Proof of (2): This is similar to (1). Explicitly, we want to show that for $y, z \in H$, we have $[x, yz] = [x, y][x, z]$. This follows from the identity $[x, yz] = [x, y]({}^y[x, z])$ combined with the fact that, since $z \in H$, $[x, z] \in C_G(H)$ by assumption, so $[x, z]$ commutes with y.

Proof of (3): We prove the statement by induction on c. The base case $c = 2$ follows from (1). Suppose now that the statement is true for all smaller classes, and we want to prove it for class c.

By the inductive hypothesis, the map:

$$T_{c-1} : (x_1, x_2, \ldots, x_{c-1}) \mapsto [\ldots[x_1, x_2], \ldots, x_{c-1}] \mod \gamma_c(G)$$

satisfies all the hypotheses: it is a homomorphism in each coordinate holding the other coordinates fixed. Further, the image of the map is in $\gamma_{c-1}(G)/\gamma_c(G)$.

Now, note that the commutator map:

$$\gamma_{c-1}(G) \times G \to \gamma_c(G)$$

satisfies the condition that the image is in the center of G. In particular, by (2), we obtain that the commutator map is a homomorphism with respect to both coordinates. The map descends to the following map which is also a homomorphism in both coordinates:

$$U : \gamma_{c-1}(G)/\gamma_c(G) \times G \to \gamma_c(G)$$

We now see that:

$$T(x_1, x_2, \ldots, x_c) = U(T_{c-1}(x_1, x_2, \ldots, x_{c-1}), x_c)$$

The fact that both T_{c-1} and U are homomorphisms in each of their coordinates gives us that T is a homomorphism in each coordinate.

The proof of the statement that T descends to a map from $G/Z^{c-1}(G)$ follows from the three subgroup lemma, discussed in Section A.3.2. $\square$

A.3.4 Strongly central series

A descending series of subgroups:

$$G = G_1 \geq G_2 \geq G_3 \geq \cdots \geq G_n = 1 = G_{n+1} = G_{n+2} = \ldots$$

is termed a *strongly central series* if $[G_i, G_j] \leq G_{i+j}$ for any positive integers i and j.

Lemma A.3.3. For any group G and any positive integers i and j, we have that $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$. In particular, the lower central series of a nilpotent group is a strongly central series.

Proof. This follows from the three subgroup lemma and proof by induction. □

A.4 The use of grading

A.4.1 Graded ring

Suppose G is an abelian group with the group operation denoted additively. Suppose R is a commutative (associative) unital ring. A G-graded R-algebra is a R-algebra A whose additive group has a direct sum decomposition as a sum of R-submodules indexed by the group elements:

$$A = \bigoplus_{g \in G} A_g$$

such that for all $g, h \in G$, we have:

$$A_g A_h \subseteq A_{g+h}$$

An element of A that lies inside A_g for some $g \in G$ is termed a *homogeneous element.*

A G-graded *ring* is a G-graded $\mathbb{Z}$-algebra.

The following cases are of particular interest:

- A $\mathbb{Z}$-graded R-algebra is a R-algebra graded over the group of integers $\mathbb{Z}$.
- A $\mathbb{N}_0$-graded R-algebra is a $\mathbb{Z}$-graded R-algebra A where $A_i = 0$ for all $i < 0$.
- A $\mathbb{N}$-graded R-algebra a $\mathbb{Z}$-graded R-algebra A where $A_i = 0$ for all $i \leq 0$.

Generally, the term *graded R-algebra* is used for a $\mathbb{N}_0$-graded R-algebra, and the term *graded ring* is used for a $\mathbb{N}_0$-graded $\mathbb{Z}$-algebra. We will follow this convention for the rest of the appendix and in the main document.

A.4.2 Verification of multilinear identities for graded rings

A R-multilinear identity holds in a graded R-algebra A if and only if it holds in the case where all inputs are homogeneous elements. This is because the set of homogeneous elements forms a generating set for A as a R-module, and multilinear identities can be verified on a generating set, as described in Section A.1.6. In particular, this applies to verifying associativity and the Jacobi identity.

A.4.3 Associated graded Lie algebra for a Lie algebra

Suppose L is a Lie algebra over a commuative (associative) unital ring R. The *associated graded R-Lie algebra* for L is a graded R-Lie algebra defined as follows. The underlying R-module is:

$$\bigoplus_{i=1}^{\infty} \gamma_i(L)/\gamma_{i+1}(L)$$

where the i^{th} component is the direct summand $\gamma_i(L)/\gamma_{i+1}(L)$, where $\gamma_i(L)$ and $\gamma_{i+1}(L)$ are the i^{th} and $(i+1)^{th}$ members respectively of the lower central series of L. We now define the Lie bracket on the associated graded R-Lie algebra.

First, note that the Lie bracket restricts to the following R-bilinear maps:

$$\begin{aligned}
\gamma_i(L) \times \gamma_j(L) &\rightarrow \gamma_{i+j}(L) \\
\gamma_{i+1}(L) \times \gamma_j(L) &\rightarrow \gamma_{i+j+1}(L) \\
\gamma_i(L) \times \gamma_{j+1}(L) &\rightarrow \gamma_{i+j+1}(L)
\end{aligned}$$

As a result, we get a canonical R-bilinear map:

$$\gamma_i(L)/\gamma_{i+1}(L) \times \gamma_j(L)/\gamma_{j+1}(L) \to \gamma_{i+j}(L)/\gamma_{i+j+1}(L)$$

The Lie bracket on the associated graded R-Lie algebra of L is defined as the Lie bracket whose restriction to the bracket of the i^{th} graded component and the j^{th} graded component is the above map for all i and j. In order to show that this is a *Lie* bracket, we need to verify the Jacobi identity. Due to the multilinearity of the Jacobi identity, it suffices to verify it in the case that all three inputs are homogeneous (as explained in the preceding section, Section A.4.2), and in that case, it follows from the Jacobi identity in the original R-Lie algebra L.

Note in particular that if L is a nilpotent R-Lie algebra of nilpotency class at most c, then the direct sum above is the finite direct sum:

$$\bigoplus_{i=1}^{c} \gamma_i(L)/\gamma_{i+1}(L)$$

For the case that $R = \mathbb{Z}$, we are thinking of L simply as a Lie ring, and the corresponding associated graded $\mathbb{Z}$-Lie algebra will be called the *associated graded Lie ring.* Note that for any commutative unital ring R and any R-Lie algebra L, the following coincide:

- The associated graded Lie ring of L, viewed as a Lie ring (ignoring its structure as a

R-Lie algebra).

- The underlying Lie ring for the associated graded R-Lie algebra of L.

The definition of associated graded Lie ring can also be generalized to *any* strongly central series of a (nilpotent) Lie ring. Strongly central series for Lie rings are defined analogously to the definition for groups in Section A.3.4. In the context of this more general definition, the usual associated graded Lie ring is the associated graded Lie ring for the lower central series.

A.4.4 Associated graded Lie ring for a group

Suppose G is a group. The *associated graded Lie ring* for G is a graded Lie ring defined as follows. The additive group is:

$$\bigoplus_{i=1}^{\infty} \gamma_i(G)/\gamma_{i+1}(G)$$

where the i^{th} component is the direct summand $\gamma_i(G)/\gamma_{i+1}(G)$.

First, note that the Lie bracket restricts to the following $\mathbb{Z}$-bilinear maps:

$$\begin{aligned} \gamma_i(G) \times \gamma_j(G) &\rightarrow \gamma_{i+j}(G) \\ \gamma_{i+1}(G) \times \gamma_j(G) &\rightarrow \gamma_{i+j+1}(G) \\ \gamma_i(G) \times \gamma_{j+1}(G) &\rightarrow \gamma_{i+j+1}(G) \end{aligned}$$

As a result, we get a canonical $\mathbb{Z}$-bilinear map:

$$\gamma_i(G)/\gamma_{i+1}(G) \times \gamma_j(G)/\gamma_{j+1}(G) \rightarrow \gamma_{i+j}(G)/\gamma_{i+j+1}(G)$$

The Lie bracket on the associated graded Lie ring of G is defined as the Lie bracket whose restriction to the bracket of the i^{th} graded component and the j^{th} graded component is the above map for all i and j. In order to show that this is a *Lie* bracket, we need to verify the Jacobi identity. Due to the multilinearity of the Jacobi identity, it suffices to verify it in the case that all three inputs are homogeneous (as explained in the preceding section, Section A.4.2). The Jacobi identity in the homogeneous case follows from Witt's identity, described in Section A.3.2.

The definition of associated graded Lie ring can also be generalized to *any* strongly central series of a (nilpotent) Lie ring. Strongly central series were defined for groups in Section A.3.4. In the context of this more general definition, the usual associated graded Lie ring is the associated graded Lie ring for the lower central series.

A.4.5 Associated graded Lie ring as a functor

The associated graded Lie ring is functorial both for groups and for Lie rings. Explicitly, we can define a functor from the category of groups to the category of Lie rings such that its mapping on objects sends a group to its associated graded Lie ring. Similarly, we can define a functor from the category of Lie rings to itself such that its mapping on objects sends a Lie ring to its associated graded Lie ring.

We can think of taking the associated graded Lie ring as "flattening" the structure of the original object (the group or the Lie ring) thereby forgetting some aspects of the cohomology. Note, however, that taking the associated graded Lie ring *does* preserve the order and the nilpotency class. We discover that the following are true:

- If a group and Lie ring are in global class c Lazard correspondence, they define the same associated graded Lie ring.

- If two nilpotent groups are isoclinic to each other, then their associated graded Lie rings are isoclinic to each other. We can actually make a slightly stronger statement:

if two groups are isoclinic as central extensions with the same base and same quotient group, then their associated graded Lie rings are *isomorphic*. Here, "isoclinic as central extensions" is being used in the sense of Sections 3.6.2 and 3.6.3.

- If two Lie rings are isoclinic to each other, then their associated graded Lie rings are isoclinic to each other. We can actually make a slightly stronger statement: if two Lie rings are isoclinic as central extensions with the same base and same quotient Lie rings, then their associated graded Lie rings are isomorphic. Here, "isoclinic as central extensions" is being used in the sense of Sections 3.7.2 and 3.7.3.

- If a group and Lie ring are in global class $c+1$ Lazard correspondence up to isoclinism, then their associated graded Lie rings are isoclinic. We can make a slightly stronger statement: if a group and Lie ring are in global class $(c+1)$ Lazard correspondence up to isoclinism *as central extensions* (as described in Section 7.7.5), then their corresponding associated graded Lie rings are isomorphic.

In the case of class two, the associated graded Lie ring offers an essentially complete classification of the equivalence type up to isoclinism for the extension. This is because the "flattening" it does forgets only the abelian part of the group structure, and not the commutator structure. For higher class, however, although the associated graded Lie ring is invariant under taking isoclinisms of extensions, it is not a complete invariant, because passing to the associated graded Lie ring "flattens" out part of the commutator structure as well.

A.5 Homologism theory for arbitrary varieties

The material discussed in this section of the Appendix is used in Section 8.2.4 when discussing a potential extension of the Lazard correspondence up to isoclinism. It is not used elsewhere in the document, although it may help provide better perspective on the material elsewhere in the document as well.

For basic background material on varieties of algebras, see the Appendix, Sections A.2.4 and A.2.5.

The terms and concepts alluded to in this section can be found in the paper [31] by Leedham-Green and McKay. The concepts of n-isoclinism and n-homoclinism are also described in [24] (for groups) and [40] (for Lie rings).

A.5.1 Word maps: definition for an arbitrary variety of algebras

Suppose $\mathcal{V}$ is a variety of algebras. A *word* in n letters in $\mathcal{V}$ is defined as an element of the free algebra (with respect to the variety $\mathcal{V}$) in terms of the n letters. A word can be represented using an expression in terms of the n letters and the operations of the variety. Two expressions describe the same word if they are formally equal, i.e., their equality can be dedued from the formal identities of the variety. We will often abuse notation by conflating the concepts of the word with a formal expression used to describe the word.

Given a word w in n letters for the variety $\mathcal{V}$, and an algebra A in $\mathcal{V}$, w defines a set map $A^n \to A$ as follows. Denote by F the free algebra on the n letters, and denote the letters by $g_1, g_2, \ldots, g_n$. Then, for any tuple $(x_1, x_2, \ldots, x_n) \in A^n$, we can consider the unique homomorphism $\varphi : F \to A$ such that $\varphi(g_i) = x_i$. The image $\varphi(w)$ is the image of the tuple $(x_1, x_2, \ldots, x_n)$ under the word map. Abusing notation, we will use w to denote the word itself, the expression describing the word, *and* the word map, i.e., the image of the tuple $(x_1, x_2, \ldots, x_n)$ will be denoted $w(x_1, x_2, \ldots, x_n)$.

For some varieties, such as the variety of groups, there is a concept of a *reduced word expression*. Any element of the free group on n letters has a unique *reduced expression*, and the equality of two words can be determined by converting both of them to their corresponding reduced expressions and then checking for literal equality.

For the variety of groups, words involve group multiplication and inverse map operations, and a word in reduced form is an expression written as a product of the letters and their inverses, with no letter and its inverse occurring adjacent to one another. For instance, the following is an example word in two letters g_1 and g_2:

$$w(g_1, g_2) := g_1 g_2 g_1 g_2^2 g_1^{-1}$$

We say that a group G satisfies a word w in n letters (with respect to the variety of groups) if the image of the word map corresponding to w is the trivial subgroup of G, i.e., $w(x_1, x_2, \dots, x_n) = 1$ for all $x_1, x_2, \dots, x_n \in G$.

The concept generalizes to any *variety of algebras with zero*, i.e., a variety of algebra with a distinguished 0-ary operation called the *zero element*. Given a variety $\mathcal{V}$ with zero, an algebra A is said to *satisfy* a word w in n letters with respect to the variety $\mathcal{V}$ if $w(x_1, x_2, \dots, x_n)$ is the zero element of A for all $x_1, x_2, \dots, x_n \in A$. For the variety of groups, the zero element is the identity element.

A.5.2 Word maps and subvarieties of the variety of groups

To specify a subvariety of the variety of groups, we need to specify a set of identities that define the subvariety. Note that the set of identities we choose need not be an *exhaustive* list of identities satisfied in the subvariety, but it needs to be sufficient to generate all other identities satisfied in the subvariety.

An identity in the variety of groups has the form:

$$w_1(x_1, x_2, \dots, x_n) = w_2(x_1, x_2, \dots, x_n)$$

We can define a new word:

$$w(x_1, x_2, \dots, x_n) := w_1(x_1, x_2, \dots, x_n)(w_2(x_1, x_2, \dots, x_n))^{-1}$$

The identity can therefore be rewritten as:

$$w(x_1, x_2, \dots, x_n) = 1$$

Thus, any subvariety of the variety of groups can be described using a set of words, and a group is in the subvariety if and only if all the words are satisfied in the group.

A.5.3 Some examples of subvarieties of the variety of groups

The following are examples of subvarieties, each of which can be defined using *one* word. Note that for all these definitions, it does not matter whether we use the left or right convention for the commutator: both define the same variety.

- The variety of abelian groups: This can be defined using the commutator word $w(x_1, x_2) = [x_1, x_2]$.
- The variety of groups of nilpotency class at most c: This can be defined using the iterated commutator word $w(x_1, x_2, \dots, x_c, x_{c+1}) = [[\dots[x_1, x_2], \dots, x_c], x_{c+1}]$.
- The variety of groups of derived length at most ℓ: This can be defined using an iterated balanced commutator of length 2^ℓ. For instance, when $\ell = 2$, the commutator is $[[x_1, x_2], [x_3, x_4]]$.

A.5.4 Verbal and marginal subgroup corresponding to a subvariety

Suppose $\mathcal{V}$ is a subvariety of the variety of groups. For a group G, the $\mathcal{V}$-*verbal subgroup* of G is defined as the subgroup generated by the images of the word maps in G for all words that are satisfied in the subvariety $\mathcal{V}$. Equivalently, it is the smallest normal subgroup of G for which the quotient group is in $\mathcal{V}$.

Suppose C is a set of words that generates the variety $\mathcal{V}$, i.e., $\mathcal{V}$ is precisely the subvariety of the variety of groups comprising those groups that satisfy all the words in C. Then, the $\mathcal{V}$-verbal subgroup of G is the subgroup of G generated by the union of the images of the word maps for all words in C.

The $\mathcal{V}$-*marginal subgroup* of G is defined as follows. It is the set of elements x in G such that for every word w satisfied in $\mathcal{V}$, the following is true. Let n be the number of letters used in w. Then, we want:

$w(g_1, g_2, \dots, g_i, \dots, g_n) = w(g_1, g_2, \dots, xg_i, \dots, g_n) = w(g_1, g_2, \dots, g_i x, \dots, g_n) \; \forall \; g_1, g_2, \dots, g_n \in G, \; \forall \; i \in \{1, 2, \dots, n\}$

In other words, the marginal subgroup is the set of elements that do not affect the evaluation of any of the words that would become trivial in the variety.

Suppose C is a set of words that generates the variety $\mathcal{V}$, i.e., $\mathcal{V}$ is precisely the subvariety of the variety of groups comprising those groups that satisfy all the words in C. Then, we can define the $\mathcal{V}$-marginal subgroup as the set of elements of G that satisfy the above condition for the words in C alone.

Some examples of verbal and marginal subgroups are below.

- Consider the variety of abelian groups. The verbal subgroup of a group G corresponding to this variety is the derived subgroup G', and the marginal subgroup is the center $Z(G)$.
- Consider the variety of groups of nilpotency class at most c. The verbal subgroup of a group G corresponding to this variety is the lower central series member subgroup $\gamma_{c+1}(G)$. The marginal subgroup is the upper central series member $Z^c(G)$.

A.5.5 Homologism for a subvariety of the variety of groups

Suppose $\mathcal{V}$ is a subvariety of the variety of groups. For any group G, denote by $V^*(G)$ the $\mathcal{V}$-marginal subgroup and by $V(G)$ the $\mathcal{V}$-verbal subgroup.

For any word w satisfied in the variety $\mathcal{V}$, suppose w uses n_w letters. w defines a word map:

$$\beta_{w,G} : G^{n_w} \to G$$

By the definitions of marginal and verbal subgroup, the map descends to a set map:

$$\omega_{w,G} : (G/V^*(G))^{n_w} \to V(G)$$

A *homologism* of groups G_1 and G_2 with respect to $\mathcal{V}$ is a pair (ζ, φ) where $\zeta : G_1/V^*(G_1) \to G_2/V^*(G_2)$, $\varphi : V(G_1) \to V(G_2)$ are homomorphisms, and for every w satisfied in the variety $\mathcal{V}$, we have:

$$\omega_{w,G_2}(\zeta(x_1), \zeta(x_2), \ldots, \zeta(x_{n_w})) = \varphi(\omega_{w,G_1}(x_1, x_2, \ldots, x_{n_w})) \ \forall \ (x_1, x_2, \ldots, x_n) \in (G_1/V^*(G_1))^{n_w}$$

As with all the other definitions, it suffices to check this condition on a set of words that *generates* the variety rather than on all words satisfied in the variety.

A homologism is termed an *isologism* if both its component homomorphisms are isomorphisms, or equivalently, if there is an inverse map to it that is also a homologism.

For any subvariety $\mathcal{V}$ of the variety of groups, we can define the *category of groups with $\mathcal{V}$-homologisms*. The objects of this category are groups and the morphisms are $\mathcal{V}$-homologisms, with composition of homologisms defined via composition of the corresponding homomorphisms. The isomorphisms in this category are precisely the $\mathcal{V}$-isologisms. Further, a group is isomorphic to the trivial group in this category if and only if it is in the subvariety $\mathcal{V}$. Thus, the category of groups with $\mathcal{V}$-homologisms can be thought of as going "modulo" the subvariety $\mathcal{V}$, in so far as the "kernel" is precisely $\mathcal{V}$.

A.5.6 Relation between homologism categories for subvarieties

Consider two subvarieties $\mathcal{V}_1$ and $\mathcal{V}_2$ of the variety of groups. We can consider the category of groups with $\mathcal{V}_1$-homologisms as well as the category of groups with $\mathcal{V}_2$-homologisms. Suppose $\mathcal{V}_1$ is a subvariety within $\mathcal{V}_2$ (in other words, a group being in $\mathcal{V}_1$ is a *stronger* condition than the group being in $\mathcal{V}_2$).

We might naively expect that there is a natural forgetful functor of some sort from the category of groups to $\mathcal{V}_1$-homologisms and the category of groups with $\mathcal{V}_2$-homologisms. This, however, is not true. In Section 2.1.5, we discussed the situation in the case that $\mathcal{V}_1$ is the subvariety comprising only the trivial group (so that $\mathcal{V}_1$-homologisms can be identified with ordinary homomorphisms) and $\mathcal{V}_2$ is the subvariety of abelian groups (so that $\mathcal{V}_2$-homologisms are the same as homoclinisms). Using the same logic as we had used in Section 2.1.5, we obtain that a $\mathcal{V}_1$-homologism gives rise to a $\mathcal{V}_2$-homologism if and only if it sends the $\mathcal{V}_2$-marginal subgroup to within itself. In particular, any *surjective* $\mathcal{V}_1$-homologism induces a $\mathcal{V}_2$-homologism. Therefore, every $\mathcal{V}_1$-*isologism* induces a $\mathcal{V}_2$-isologism.

A.5.7 n-homoclinism and n-isoclinism

Suppose n is a positive integer. A n-homoclinism is defined as a homologism with respect to the subvariety of the variety of groups comprising groups of nilpotency class at most n. The subvariety is defined by the word $w(x_1, x_2, \dots, x_n, x_{n+1}) = [[\dots[x_1, x_2], \dots, x_n], x_{n+1}]$. The *category of groups with n-homoclinisms* is the category where the objects are groups and the homomorphisms are n-homoclinisms. A *n-isoclinism* is defined as an isomorphism in this category.

The concepts of n-isoclinism and c-homoclinism are also described in [24] (for groups) and [40] (for Lie rings).

A.5.8 Baer invariant and nilpotent multiplier

The Schur multiplier and exterior square are both defined based on the commutator structure, and their definitions can be viewed as arising from the choice of the subvariety of abelian groups and the notion of homoclinism. There exist generalizations of these to arbitrary subvarieties of the variety of nilpotent groups. The generalization of the Schur multiplier is termed the *Baer invariant*. Explicitly, for a subvariety $\mathcal{V}$ of the variety of groups, and any group G (not necessarily in $\mathcal{V}$), the *Baer invariant* of G for the subvariety $\mathcal{V}$ is an abelian group denoted $\mathcal{V}M(G)$. The definition is similar to that for the Schur multiplier in Section 3.4, but now using the word maps arising from words that define the subvariety $\mathcal{V}$ instead of the commutator word. Alternatively, it can be defined by generalizing Hopf's formula (described in Section 3.6.9) as follows. Interested readers are encouraged to read the paper [31] by Leedham-Green and McKay and the paper [24] by Hekster.

In the case that $\mathcal{V}$ is the subvariety comprising all the groups of nilpotency class at most n (where n is a fixed positive integer), the corresponding Baer invariant is termed the n-nilpotent multiplier and is denoted $M^{(n)}(G)$. In particular, the Schur multiplier $M(G)$ is the group $M^{(1)}(G)$, i.e., it is the 1-nilpotent multiplier.

We can deduce a formula for the n-nilpotent multiplier similar to Hopf's formula described in Section 3.6.9, and in fact, many sources use that formula as the *definition* of the n-nilpotent multiplier. Write G as a quotient F/R where F is a free group. Then:

$$M^{(n)}(G) = (R \cap \gamma_{n+1}(F))/\gamma_{n+1}(R, F)$$

Note that although it is not immediately obvious by looking at the expression, we can see via the three subgroup lemma that $M^{(n)}(G)$ as defined above is an abelian group, as expected.

Here, $\gamma_{n+1}(F)$ denotes the $(n+1)^{th}$ member of the lower central series of F, whereas $\gamma_{n+1}(R, F)$ is the $(n+1)^{th}$ member of the series given by $\gamma_1(R, F) = R$ and $\gamma_{i+1}(R, F) = [F, \gamma_i(R, F)]$. Note that in the case $n = 1$, this givees us the formula we are already familiar with:

$$M(G) = (R \cap [F, F])/[R, F]$$

Note in particular that if $G = F/\gamma_{c+1}(F)$ for some positive integer c (i.e., G is a free class c nilpotent group), we get:

$$M^{(n)}(G) = \gamma_{\max\{c,n\}+1}(F)/\gamma_{c+n+1}(F)$$

APPENDIX B

SUPPLEMENTARY PROOFS

B.1 Some computational proofs related to the Baker-Campbell-Hausdorff formula

B.1.1 Baker-Campbell-Hausdorff formula: class two: full derivation

In this case, we work with non-commuting variables x_1, x_2 such that $x_1^3 = x_1^2 x_2 = x_1 x_2 x_1 = x_1 x_2^2 = x_2 x_1^2 = x_2 x_1 x_2 = x_2^2 x_1 = x_2^3 = 0$. Thus:

$$\exp(x_1) = 1 + x_1 + \frac{x_1^2}{2}$$

$$\exp(x_2) = 1 + x_2 + \frac{x_2^2}{2}$$

We thus get:

$\exp(x_1)\exp(x_2) = \left(1 + x_1 + \frac{x_1^2}{2}\right)\left(1 + x_2 + \frac{x_2^2}{2}\right) = 1 + x_1 + \frac{x_1^2}{2} + x_2 + x_1x_2 + \frac{x_1^2 x_2}{2} + \frac{x_2^2}{2} + \frac{x_1 x_2^2}{2} + \frac{x_1^2 x_2^2}{4}$

We drop all products of degree three or more and rearrange the remaining terms to get:

$$\exp(x_1)\exp(x_2) = 1 + x_1 + x_2 + \frac{x_1^2}{2} + x_1x_2 + \frac{x_2^2}{2}$$

We thus get:

$$w = \exp(x_1)\exp(x_2) - 1 = x_1 + x_2 + \frac{x_1^2}{2} + x_1x_2 + \frac{x_2^2}{2}$$

Finally, we compute $\log(1 + w)$. We have:

$$\log(1 + w) = w - \frac{w^2}{2}$$

We note that w^2 is the same as the square of its linear part because the square of the degree two part, as well as products of the degree two and the linear part, are degree three or more and hence zero. Thus:

$\log(1+w) = x_1 + x_2 + \frac{x_1^2}{2} + x_1x_2 + \frac{x_2^2}{2} - (x_1+x_2)^2/2$

Simplifying, we get:

$\log(1+w) = x_1 + x_2 + \frac{x_1^2+2x_1x_2+x_2^2-(x_1+x_2)^2}{2}$

Now note that:

$(x_1+x_2)^2 = x_1^2 + x_1x_2 + x_2x_1 + x_2^2$

Plugging this in, we get:

$\log(1+w) = x_1 + x_2 + \frac{x_1^2+2x_1x_2+x_2^2-(x_1^2+x_1x_2+x_2x_1+x_2^2)}{2}$

Simplifying, we get:

$\log(1+w) = x_1 + x_2 + \frac{x_1x_2-x_2x_1}{2}$

Rewrite $x_1x_2 - x_2x_1 = [x_1, x_2]$ and we get the formula:

$x_1 + x_2 + \frac{1}{2}[x_1, x_2]$

B.1.2 Baker-Campbell-Hausdorff formula: class three: full derivation

Before proceeding to work out the formula in class three, we obtain a more concise description of w in terms of x_1 and x_2, thus saving steps on the initial computation. If we are working in class c, then:

$$w = \sum_{k,l\geq 0, 0<k+l\leq c} \frac{x_1^k x_2^l}{k!l!} = \sum_{n=1}^{c} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} x_1^k x_2^{n-k}$$

We now deduce the class three Baker-Campbell-Hausdorff formula:

$w = \exp(x_1)\exp(x_2) - 1 = (x_1+x_2) + \frac{1}{2!}(x_1^2 + 2x_1x_2 + x_2^2) + \frac{1}{3!}(x_1^3 + 3x_1^2x_2 + 3x_1x_2^2 + x_2^3)$

Since the class is three, we have $w^4 = 0$, hence we get:

$\log(1+w) = w - \frac{w^2}{2} + \frac{w^3}{3} = (x_1+x_2) + \frac{1}{2!}(x_1^2 + 2x_1x_2 + x_2^2) + \frac{1}{3!}(x_1^3 + 3x_1^2x_2 + 3x_1x_2^2 + x_2^3) - \frac{1}{2}((x_1+x_2) + \frac{1}{2!}(x_1^2 + 2x_1x_2 + x_2^2) + \frac{1}{3!}(x_1^3 + 3x_1^2x_2 + 3x_1x_2^2 + x_2^3))^2 + \frac{1}{3}((x_1+x_2) +$

$\frac{1}{2!}(x_1^2 + 2x_1x_2 + x_2^2) + \frac{1}{3!}(x_1^3 + 3x_1^2x_2 + 3x_1x_2^2 + x_2^3))^3$

The calculations for the degree one and degree two parts proceed exactly as they did in the class two case covered in the preceding section. We thus concentrate on the degree three part:

Degree three part $= \frac{1}{6}(x_1^3 + 3x_1^2x_2 + 3x_1x_2^2 + x_2^3) - \frac{1}{4}(x_1 + x_2)(x_1^2 + 2x_1x_2 + x_2^2) - \frac{1}{4}(x_1^2 + 2x_1x_2 + x_2^2) + \frac{1}{3}(x_1 + x_2)^3$

Instead of simplifying directly, we adopt the following procedure. We rewrite:

$x_1^2 + 2x_1x_2 + x_2^2 = (x_1 + x_2)^2 + [x_1, x_2]$

We similarly rewrite:

$x_1^3 + 3x_1^2x_2 + 3x_1x_2^2 + x_2^3 = (x_1 + x_2)^3 + 2x_1[x_1, x_2] + [x_1, x_2]x_1 + 2[x_1, x_2]x_2 + x_2[x_1, x_2]$

This can be further rewritten as:

$x_1^3 + 3x_1^2x_2 + 3x_1x_2^2 + x_2^3 = (x_1 + x_2)^3 + 3x_1[x_1, x_2] + 3[x_1, x_2]x_2 - [x_1, [x_1, x_2]] + [x_2, [x_1, x_2]]$

Now, we plug these into the expression

Degree three part $= \frac{1}{6}((x_1 + x_2)^3 + 3x_1[x_1, x_2] + 3[x_1, x_2]x_2 - [x_1, [x_1, x_2]] + [x_2, [x_1, x_2]]) - \frac{1}{4}(x_1 + x_2)((x_1 + x_2)^2 + [x_1, x_2]) - \frac{1}{4}((x_1 + x_2)^2 + [x_1, x_2])(x_1 + x_2) + \frac{1}{3}(x_1 + x_2)^3$

We rearrange to obtain:

Degree three part $= \left(\frac{1}{6} - \frac{1}{4} - \frac{1}{4} + \frac{1}{3}\right)(x_1 + x_2)^3 + \frac{1}{2}(x_1[x_1, x_2] + [x_1, x_2]x_2) - \frac{1}{6}([x_1, [x_1, x_2]] - [x_2, [x_1, x_2]]) - \frac{1}{4}(x_1 + x_2)[x_1, x_2] - \frac{1}{4}([x_1, x_2](x_1 + x_2))$

The $(x_1 + x_2)^3$ term has zero coefficient and disappears, and we are left with:

Degree three part $= \frac{1}{2}(x_1[x_1, x_2] + [x_1, x_2]x_2) - \frac{1}{6}([x_1, [x_1, x_2]] - [x_2, [x_1, x_2]]) - \frac{1}{4}x_1[x_1, x_2] - \frac{1}{4}x_2[x_1, x_2] - \frac{1}{4}[x_1, x_2]x_1 - \frac{1}{4}[x_1, x_2]x_2$

We now use that $x_2[x_1, x_2] = [x_1, x_2]x_2 + [x_2, [x_1, x_2]]$ and $[x_1, x_2]x_1 = x_1[x_1, x_2] - [x_1, [x_1, x_2]]$ to get:

Degree three part $= \frac{1}{2}(x_1[x_1, x_2] + [x_1, x_2]x_2) - \frac{1}{6}([x_1, [x_1, x_2]] - [x_2, [x_1, x_2]]) - \frac{1}{4}x_1[x_1, x_2] - \frac{1}{4}[x_1, x_2]x_2 - \frac{1}{4}[x_2, [x_1, x_2]] - \frac{1}{4}x_1[x_1, x_2] + \frac{1}{4}[x_1, [x_1, x_2]] - \frac{1}{4}[x_1, x_2]x_2$

Combining coefficients, we find that the coefficients on $x_1[x_1, x_2]$ and $[x_1, x_2]x_2$ are zero, and we are left with:

Degree three part $= -\frac{1}{6}([x_1,[x_1,x_2]] - [x_2,[x_1,x_2]]) + \frac{1}{4}([x_1,[x_1,x_2]] - [x_2,[x_1,x_2]])$

We simplify $1/4 - 1/6 = 1/12$ to get:

Degree three part $= \frac{1}{12}([x_1,[x_1,x_2]] - [x_2,[x_1,x_2]])$

Plug this back in to the formula, and get the overall formula:

$x_1 + x_2 + \frac{1}{2}[x_1,x_2] + \frac{1}{12}([x_1,[x_1,x_2]] - [x_2,[x_1,x_2]])$

B.1.3 Bounds on prime power divisors of the denominator

For a prime p and a natural number c, define $f(p,c)$ as follows. Consider the class c Baker-Campbell-Hausdorff formula. $f(p,c)$ is defined as the largest positive integer k such that p^k appears as a divisor of the denominator for one of the coefficients for the formula.

It turns out that:

$$f(p,c) \leq \left\lfloor \frac{c-1}{p-1} \right\rfloor$$

This was proved in Lazard's original paper ([30]). The proof sketch for the *associative* version of the formula is below. The result for the Lie version of the formula follows from Khukhro's text [29], Theorem 5.39 (see more generally the discussion in Sections 5.3 and 9.9 of the text).

Consider the ring of formal power series over $\mathbb{Q}$ in the two non-commuting variables x_1 and x_2.

Consider a p-adic valuation on $\mathbb{Q}$, i.e., a valuation $v_p : \mathbb{Q} \setminus \{0\} \to \mathbb{Z}$ that sends a rational number a/b to the integer k such that $a/(bp^k)$ in reduced form has no divisor of p for either the numerator or the denominator.

Extend the valuation to a value $1/(p-1)$ on the formal variables x_1, x_2. The valuation can then be extended to the whole ring. We then use multiplicativity to compute the valuation at various terms, for $n \leq c$:

$v_p(x_1^n/n!) = c/(p-1) - v_p(n!) \geq 1/(p-1)$

where we have used that $v_p(n!) \leq \lfloor (n-1)/(p-1) \rfloor$. Then, $v_p(\exp x_1 - 1) \geq 1/(p-1)$. Denote $w = \exp(x_1)\exp(x_2) - 1$. It is easy to see that $v_p(w) \geq 1/(p-1)$. The Baker-Campbell-Hausdorff formula is obtained by expanding

$\log(1+w)$

Note that $v_p(w^n/n) = nv_p(w) - v_p(c) \geq n/(p-1) - v_p(n!) \geq 1/(p-1)$. That is, $v_p(\log(1+w)) \geq 1/(p-1)$. For coefficients in degree n with $n \leq c$, we obtain:

$$v_p(\text{coefficient in degree n}) \geq 1/(p-1) - n/(p-1) = -(n-1)/(p-1)$$

Since the above holds for all $n \leq c$, we obtain that all the coefficients in degree $\leq c$ have prime power divisors of the denominator less than or equal to $(c-1)/(p-1)$. Thus, $f(p,c) \leq (c-1)/(p-1)$. Since $f(p,c)$ is an integer, we obtain that:

$$f(p,c) \leq \left\lfloor \frac{c-1}{p-1} \right\rfloor$$

B.1.4 Finding the explicit formula M_{c+1} for $c = 2$

In Section 7.1.1, we described the general approach for computing a formula M_{c+1} to describe the group commutator in terms of the Lie bracket for the class $(c+1)$ Lazard correspondence. The case $c = 1$ (and hence $c+1 = 2$) was discussed in detail in Section 5.1 (Lemma 5.1.2 says this explicitly). We consider the case $c = 2$, so that $c+1 = 3$. In other words, we are considering the class 3 Lazard correspondence.

We mimic the general procedure of Section 7.1.1.

The class three Baker-Campbell-Hausdorff formula gives us that:

$$\begin{aligned} xy &= x + y + \frac{1}{2}[x, y] + \frac{1}{12}([x, [x, y]] - [y, [x, y]]) \\ yx &= y + x + \frac{1}{2}[y, x] + \frac{1}{12}([y, [y, x]] - [x, [y, x]]) \end{aligned}$$

We will denote the degree i part as t_i, as in the discussion of the Baker-Campbell-Hausdorff formula. In other words, we have:

$$\begin{aligned} xy &= t_1(x, y) + t_2(x, y) + t_3(x, y) \\ yx &= t_1(y, x) + t_2(y, x) + t_3(y, x) \end{aligned}$$

Here:

$$t_1(x, y) = t_1(y, x) = x + y = y + x$$

$$t_2(x, y) = -t_2(y, x) = \frac{1}{2}[x, y]$$

$$t_3(x, y) = t_3(y, x) = \frac{1}{12}([x, [x, y]] - [y, [x, y]]) = \frac{1}{12}([y, [y, x]] - [x, [y, x]])$$

Thus:

$$[x, y]_{\text{Group}} = (xy)(-(yx))$$

becomes:

$t_1(x,y)+t_2(x,y)+t_3(x,y)-(t_1(y,x)+t_2(y,x)+t_3(y,x))+$

$t_2(xy,-(yx))+t_3(xy,-(yx))$

Based on the relationships above, this simplifies to:

$[x,y]_{\text{Group}} = 2t_2(x,y)+t_2(xy,-(yx))+t_3(xy,-(yx)) \qquad (*)$

We now expand each of the other terms. We have:

$t_2(xy,-(yx)) = \frac{1}{2}\left[t_1(x,y)+t_2(x,y)+t_3(x,y),-(t_1(y,x)+t_2(y,x)+t_3(y,x))\right]$

Expanding this out, we obtain:

$t_2(xy,-(yx)) = \frac{1}{2}[t_1(x,y),-t_2(y,x)]+\frac{1}{2}[t_2(x,y),-t_1(y,x)]$

$= [t_1(x,y),t_2(x,y)] = \frac{1}{2}[x+y,[x,y]] \qquad (**)$

On the other hand:

$t_3(xy,-(yx)) = t_3(t_1(x,y)+t_2(x,y)+t_3(x,y),-(t_1(y,x)+t_2(y,x)+t_3(y,x))$

$= t_3(t_1(x,y),-t_1(y,x)) = 0 \qquad (***)$

Plugging (**) and (***) into (*), we obtain that:

$[x,y]_{\text{Group}} = 2t_2(x,y)+\frac{1}{2}[x+y,[x,y]]$

This simplifies to:

$$[x,y]_{\text{Group}} = [x,y]+\frac{1}{2}[x+y,[x,y]]$$

Thus, we get:

$$M_3(x,y) = [x,y]+\frac{1}{2}[x+y,[x,y]]$$

Note that the formula would look somewhat different if we used the right action convention for the group commutator. Explicitly, the formula with the right action convention, which would be the formula for the group commutator $x^{-1}y^{-1}xy$, would be:

$$x^{-1}y^{-1}xy = [x,y]-\frac{1}{2}[x+y,[x,y]]$$

B.1.5 Finding the explicit formula M_{c+1} for $c = 3$

The steps here are very similar to the steps for the preceding example, so we go over the steps very briefly. We have:

$$\begin{aligned} xy &= t_1(x,y) + t_2(x,y) + t_3(x,y) + t_4(x,y) \\ yx &= t_1(y,x) + t_2(y,x) + t_3(y,x) + t_4(y,x) \end{aligned}$$

Here:

$$t_1(x,y) = t_1(y,x) = x + y = y + x$$

$$t_2(x,y) = -t_2(y,x) = \frac{1}{2}[x,y]$$

$$t_3(x,y) = t_3(y,x) = \frac{1}{12}([x,[x,y]] - [y,[x,y]]) = \frac{1}{12}([y,[y,x]] - [x,[y,x]])$$

$$t_4(x,y) = -t_4(y,x) = -\frac{1}{24}[y,[x,[x,y]]]$$

Based on the above relationships, we get:

$[x,y]_{\text{Group}} = (xy)(-(yx)) = 2(t_2(x,y) + t_4(x,y)) + t_2(xy, -(yx)) + t_3(xy, -(yx)) + t_4(xy, -(yx))$

The last expression $t_4(xy, -(yx))$ is 0 based on general reasons. We thus get:

$[x,y]_{\text{Group}} = 2(t_2(x,y) + t_4(x,y)) + t_2(xy, -(yx)) + t_3(xy, -(yx))$

We simplify the pieces separately. We have:

$t_2(xy, -(yx)) = \frac{1}{2}[t_1(x,y) + t_2(x,y) + t_3(x,y) + t_4(x,y), -(t_1(y,x) + t_2(y,x) + t_3(y,x) +$

$t_4(y, x))]$

Note that any pair involving t_4 becomes zero, so this becomes:

$t_2(xy, -(yx)) = \frac{1}{2}[t_1(x, y) + t_2(x, y) + t_3(x, y), -t_1(x, y) + t_2(x, y) - t_3(x, y)]$

Note that $[t_1(x, y), t_3(x, y)]$ and $[t_3(x, y), t_1(x, y)]$ cancel. Also, the products $[t_i(x, y), t_j(x, y)]$ are zero for $i + j \geq 5$, and also for $i = j$. Thus, the only products that survive are $[t_1(x, y), t_2(x, y)]$ and $[t_2(x, y), -t_1(x, y)]$, and we obtain:

$t_2(xy, -(yx)) = \frac{1}{2}[x + y, [x, y]] \qquad (**)$

We now simplify $t_3(xy, -(yx))$:

$t_3(xy, -(yx)) = \frac{1}{12}[xy, [xy, -(yx)]] - \frac{1}{12}[-(yx), [xy, -(yx)]]$

The product $[xy, -(yx)]$ on the inside simplifies to $[x + y, [x, y]]$ based on the above calculations. Thus, we get:

$t_3(xy, -(yx)) = \frac{1}{12}[xy + yx, [x + y, [x, y]]$

We know that $xy + yx = 2t_1(x, y) + 2t_3(x, y)$. Thus:

$t_3(xy, -(yx)) = \frac{1}{12}[2t_1(x, y), [x + y, [x, y]]] + \frac{1}{12}[2t_3(x, y), [x + y, [x, y]]]$

The second term is zero because the degree is six. Simplifying the first term, we get:

$t_3(xy, -(yx)) = \frac{1}{6}[x + y, [x + y, [x, y]]] \qquad (* * *)$

Plugging (**) and (***) into the original formula (*), we obtain:

$[x, y]_{\text{Group}} = [x, y] - \frac{1}{12}[y, [x, [x, y]]] + \frac{1}{2}[x + y, [x, y]] + \frac{1}{6}[x + y, [x + y, [x, y]]]$

Rearranging, we obtain:

$[x, y]_{\text{Group}} = [x, y] + \frac{1}{2}[x + y, [x, y]] + \frac{1}{6}[x + y, [x + y, [x, y]]] - \frac{1}{12}[y, [x, [x, y]]]$

B.1.6 Computing the second inverse Baker-Campbell-Hausdorff formula in the case $c = 2$, and an illustration of why it involves only strictly smaller primes

We will use the case $c = 2$ to illuminate the discussion in Section 7.1.2, specifically the proof of Lemma 7.1.2.

We have:

$M_3(x, y) = [x, y] + \frac{1}{2}[x + y, [x, y]]$

Our goal is to find the expression for $h_{2,3}(x, y)$. In the class two case, the group commutator and Lie bracket coincide, so we know that:

$M_2(x, y) = [x, y], \qquad h_{2,2}(x, y) = [x, y]_{\text{Group}}$

Following the notation of Lemma 7.1.2, we have that:

$(h_{2,2} \circ M_2)(x, y) = [x, y]$

Note that this case is remarkable because the equality holds *exactly*, rather than just modulo $\mathcal{A}^{c+1}$. In particular, this means that the degree $(c+1)$ expression $\chi_{c+1}(x, y)$ defined in Lemma 7.1.2 as the expression such that:

$(h_{2,2} \circ M_2)(x, y) = [x, y]_{\text{Lie}} + \chi_{c+1}(x, y) \pmod{\mathcal{A}^{c+2}}$

turns out to be zero, i.e., $\chi_{c+1}(x, y) = 0$.

We also have that:

$$M_3(x, y) = M_2(x, y) + \xi_{c+1}(x, y)$$

where $\xi_{c+1}(x, y) = \frac{1}{2}[x + y, [x, y]]$. Thus, we obtain that:

$$(h_{2,2} \circ M_3)(x, y) = [x, y]_{\text{Lie}} + \chi_{c+1}(x, y) + \xi_{c+1}(x, y)$$

or more explicity:

$$(h_{2,2} \circ M_3)(x, y) = [x, y]_{\text{Lie}} + \frac{1}{2}[x + y, [x, y]]$$

It therefore follows that:

$$h_{2,3}(x, y) = \frac{[x, y]}{\sqrt{[xy, [x, y]]}}$$

B.2 Some results involving local nilpotency class

B.2.1 3-local class three implies global class three for Lie rings

We prove that nilpotency class three is 3-local.

Lemma B.2.1. Suppose L is a Lie ring with the property that for any subset of L of size at most three, the Lie subring generated by that subset is a subring of nilpotency class at most three. In other words, L has 3-local nilpotency class at most three. Then, L is a nilpotent Lie ring and its nilpotency class is at most three.

Proof. The map $(w, x, y, z) \mapsto [w, [x, [y, z]]]$ is alternating and multi-linear, and hence skew-symmetric, in all pairs of inputs. The "alternating" condition follows from the 3-local class three condition: whenever two inputs are the same, the product is a degree four product in a subring generated by three elements, hence it must equal zero. In particular, this means that the sign of the expression $[w, [x, [y, z]]]$ is reversed under any odd permutation of the inputs and is preserved under any even permutation of the inputs.

We will show that for all w, x, y, $z \in L$, the Lie bracket $[w, [x, [y, z]]]$ equals 0. The elements w, x, y, and z are fixed but arbitrary for the duration of this proof.

In particular, we obtain that $[w, [x, [y, z]]] = [w, [y, [z, x]]] = [w, [z, [x, y]]]$ for all $w, x, y, z \in L$. Combining with the Jacobi identity, we obtain that for all $w, x, y, z \in L$, we have that:

$$3[w, [x, [y, z]]] = 0 \qquad (\dagger)$$

We also obtain that

$$[w, [x, [y, z]]] = [[y, z], [w, x]] \qquad (*)$$

The proof is as follows: Use the Jacobi identity to get $[w, [x, [y, z]]] + [x, [[y, z], w]] +$

$[[y, z], [w, x]] = 0$. Now, the middle term $[x, [[y, z], w]]$ is the negative of $[x, [w, [y, z]]]$, which by the alternating condition we know to be the negative of $[w, [x, [y, z]]]$. So, the middle term equals $[w, [x, [y, z]]]$. Thus, the Jacobi identity expression gives $2[w, [x, [y, z]]] + [[y, z], [w, x]] = 0$. Combine with (†) to obtain that $[w, [x, [y, z]]] = [[y, z], [w, x]]$.

Similarly, we obtain that:

$$[y, [z, [w, x]]] = [[w, x], [y, z]] \qquad (**)$$

Combine (*), (**), and the fact that $[w, [x, [y, z]]] = [y, [z, [w, x]]]$ because of the alternating nature of the map, and obtain that:

$$[[y, z], [w, x]] = [[w, x], [y, z]] \qquad (***)$$

On the other hand, we have, by the alternating nature of the Lie bracket, that:

$$[[y, z], [w, x]] = -[[w, x], [y, z]] \qquad (****)$$

Combining (***) and (****), we obtain that:

$$2[[y, z], [w, x]] = 0$$

Combining with (*), we obtain that:

$$2[w, [x, [y, z]]] = 0$$

Combining with (†), we obtain that:

$$[w, [x, [y, z]]] = 0$$

as desired. $\square$

B.3 Proofs related to isoclinism

We begin with the proof of Theorem 2.1.4. The theorem is restated below.

> Suppose G_1 and G_2 are isoclinic groups. Suppose c is a positive integer. Let m_1 be the number of conjugacy classes in G_1 of size c (so that the *total* number of elements in such conjugacy classes is m_1c). Let m_2 be the number of conjugacy classes in G_2 of size c (so that the *total* number of elements in such conjugacy classes is m_2c). Then, m_1 is nonzero if and only if m_2 is nonzero, and if so, $m_1/m_2 = |G_1|/|G_2|$.
>
> In particular, if G_1 and G_2 additionally have the same order, then they have precisely the same multiset of conjugacy class sizes.

Proof. Let W be the group identified with $\mathrm{Inn}(G_1) \cong \mathrm{Inn}(G_2)$, and T be the group identified with $G_1' \cong G_2'$. Denote by $\alpha_1 : G_1 \to W$ and $\alpha_2 : G_2 \to W$ the respective quotient maps. Denote by $\omega : W \times W \to T$ the group commutator map. Note that the map ω is the same for both groups – that's precisely the point of their being isoclinic.

For $w \in W$, the centralizer in G_1 of any element in $\alpha_1^{-1}(w)$ is precisely $\alpha_1^{-1}(\mathcal{C}(w))$ where

$$\mathcal{C}(w) = \{u \in W \mid \omega(u, w) \text{ is the identity element of } T\}$$

Thus, the size of the conjugacy class in G_1 of any element in $\alpha_1^{-1}(w)$ is the index of the subgroup $\mathcal{C}(w)$ in W.

From this, it follows that the set of elements of G_1 with conjugacy class size c is $\alpha_1^{-1}(S)$ where S is the set of $w \in W$ for which the index of the subgroup $\mathcal{C}(w) = \{u \in W \mid \omega(u, w) \text{ is the identity element of } T\}$ in W is c.

Thus, we get the equality of the following two expressions for the number of elements of G_1 in conjugacy classes of size c:

$$m_1c = |S||Z(G_1)|$$

Analogously, we have:

$$m_2 c = |S||Z(G_2)|$$

The crucial thing to note is that the subset S of W is the same in both cases.

Taking the quotient, we get that m_1 is nonzero if and only if m_2 is nonzero, and if so:

$$\frac{m_1}{m_2} = \frac{|Z(G_1)|}{|Z(G_2)|}$$

Since $[G_1 : Z(G_1)] = |W| = [G_2 : Z(G_2)]$, we have $|Z(G_1)|/|Z(G_2)| = |G_1|/|G_2|$, so we obtain:

$$\frac{m_1}{m_2} = \frac{|G_1|}{|G_2|}$$

$\square$

We now turn to the proof of the result on irreducible representations. We need some preliminary definitions.

Definition (Projective general linear group)**.** Suppose K is a field and d is a positive integer. The *projective general linear group* of degree d over K, denoted $PGL_d(K)$, is defined as the quotient group of the general linear group $GL_d(K)$ by the subgroup of scalar matrices in $GL_d(K)$. The subgroup of scalar matrices in $GL_d(K)$ is precisely the center of $GL_d(K)$. Hence, $PGL_d(K)$ is isomorphic to the inner automorphism group of $GL_d(K)$.

Definition (Projective representation)**.** Suppose G is a group and K is a field. A *projective representation* of G over K of degree d is a homomorphism from G to the projective general linear group $PGL_d(K)$ for some positive integer d. The value d here is termed the *degree of the projective representation.*

A projective representation $\rho : G \to PGL_d(K)$ is said to have a linear lift $\theta : G \to GL_d(K)$ if $\pi \circ \theta = \rho$, where $\pi : GL_d(K) \to PGL_d(K)$ is the natural quotient map. The term "linear lift" here refers to the fact that θ is a *linear* representation that serves as a "lift" of ρ.

A projective representation may or may not admit a linear lift. The next lemma describes the nature of the set of linear lifts assuming that a linear lift exists.

Lemma B.3.1. Suppose G is a finite group and $\rho : G \to PGL_d(\mathbb{C})$ is a projective representation. Suppose $\theta : G \to GL_d(\mathbb{C})$ a linear representation of G that is a lift of ρ. In other words, if $\pi : GL_d(\mathbb{C}) \to PGL_d(\mathbb{C})$ is the natural quotient map, then we want that $\rho = \pi \circ \theta$. We know that the set of one-dimensional representations of G (identified as the Pontryagin dual of G/G') acts naturally on the set of irreducible representations of G. The claim is that the stabilizer of θ is precisely the set of one-dimensional representations of G whose kernel contains the subgroup generated by G' and all the elements g of G on which the trace of $\theta(g)$ takes a nonzero value.

Proof. One direction (one-dimensional representation whose kernel contains G' and the elements with nonzero trace values for θ must be in the stabilizer of θ): If a one-dimensional representation β has a kernel containing all the points where θ has a nonzero-valued character, then that means that for any $g \in G$, either $\theta(g)$ has trace zero or $\beta(g)$ is the identity. Thus, in all cases, we have that $\beta(g)\theta(g)$ and $\theta(g)$ have the same trace. Thus, $\beta\theta$ and θ have the same character, hence, by basic character theory, are equivalent as representations.

Reverse direction (one-dimensional representation that stabilizes θ must have kernel containing G' and the elements with nonzero trace values): Let β be a one-dimensional representation of G that stabilizes θ. Note that the kernel of any one-dimensional representation already contains G', so G' is contained in the kernel of β. Thus, we only need to show it contains all the elements at which the trace of θ is nonzero. Suppose $g \in G$ is an element at which $\theta(g)$ has nonzero trace, and β is a one-dimensional representation in the stabilizer of θ. Then $\beta\theta$ and θ are equivalent representations, hence they have the same character. Thus, $\beta(g)\theta(g)$ and $\theta(g)$ have the same trace. By assumption, $\theta(g)$ has nonzero trace, so this forces the complex number $\beta(g)$ to equal 1, so g is in the kernel of β, as desired. □

We can now turn to the proof of Theorem 2.1.5, the main theorem about irreducible representations.

> Suppose G_1 and G_2 are isoclinic finite groups. Suppose d is a positive integer. Let m_1 denote the number of equivalence classes of irreducible representations of G_1 over $\mathbb{C}$ that have degree d. Let m_2 denote the number of equivalence classes of irreducible representations of G_2 over $\mathbb{C}$ that have degree d. Then, m_1 is nonzero if and only if m_2 is nonzero, and if so, $m_1/m_2 = |G_1|/|G_2|$.
>
> In particular, if G_1 and G_2 additionally have the same order, then they have precisely the same multiset of degrees of irreducible representations.

Proof. Let W be the group identified with $\mathrm{Inn}(G_1) \cong \mathrm{Inn}(G_2)$, and T be the group identified with $G_1' \cong G_2'$. Denote by $\alpha_1 : G_1 \to W$ and $\alpha_2 : G_2 \to W$ the respective quotient maps. $\omega : W \times W \to T$ the group commutator map, which is the same for both groups.

We have short exact sequences:

$$1 \to Z(G_1) \to G_1 \to W \to 1$$

and

$$1 \to Z(G_2) \to G_2 \to W \to 1$$

We will show the following:

1. For any irreducible projective representation $\rho : W \to PGL_d(\mathbb{C})$, there exists a linear representation of G_1 that descends to ρ if and only if there exists a linear representation of G_2 that descends to ρ.

2. Further, if so, the ratio of the number of linear representations of G_1 that descend to ρ equals the number of linear representations of G_2 that descend to ρ is $|G_1|/|G_2|$.

Note that once we have (1) and (2), the result will follow: first, simply list all the projective representations of W of degree d that lift to linear representations in the groups G_1 and/or G_2. For each, the number of lifts in the two groups is in the proportion $|G_1| : |G_2|$, so the overall proportion is also $|G_1| : |G_2|$.

Proof of (1): This follows from Isaacs, Theorem 11.13, and the observation that the condition Isaacs specifies for the representation to lift is satisfied for G_1 if and only if it is satisfied for G_2.

Proof of (2): If a projective representation lifts to G_1, then the set of lifts has a transitive action on it of the set of one-dimensional linear representations of G_1, which is the Pontryagin dual of G_1/G_1'. By the fundamental theorem of group actions, the size of the set of lifts equals the index of the stabilizer in this Pontryagin dual of any lift. So the question is: what is the necessary and sufficient condition for a one-dimensional representation χ of G_1/G_1' to fix a linear lift of ρ to G_1?

The notion of whether the trace is zero is a well-defined notion for ρ, even though the outputs are in $PGL_d(\mathbb{C})$ rather than being matrices themselves. Let $\mathcal{N}(\rho)$ be the subgroup of W generated by W' and all those elements of W for which the trace of the image under ρ is nonzero. By the preceding lemma (Lemma B.3.1), the stabilizer of any lift of ρ is precisely the set of one-dimensional representations of G_1 whose kernel contains $\alpha_1^{-1}(\mathcal{N}(\rho))$. Another way of putting it is that it is the Pontryagin dual of $G_1/\alpha_1^{-1}(\mathcal{N}(\rho))$, viewed as a subgroup of the Pontryagin dual of G_1/G_1'.

The number of linear lifts is therefore:

$$\frac{|G_1/G_1'|}{|G_1/\alpha_1^{-1}(\mathcal{N}(\rho))|}$$

By the third isomorphism theorem of basic group theory, this is the same as:

$$|\alpha_1^{-1}(\mathcal{N}(\rho))/G_1'|$$

This simplifies to:

$$\frac{|\mathcal{N}(\rho)||Z(G_1)|}{|G_1'|}$$

Similarly, the number of lifts of ρ to G_2 is:

$$\frac{|\mathcal{N}(\rho)||Z(G_2)|}{|G_2'|}$$

Note the crucial fact that $\mathcal{N}(\rho)$ is the same in both cases.

Taking the quotient, we get $|Z(G_1)|/|Z(G_2)|$, which is the same as $|G_1/G_2|$ because the groups have isomorphic inner automorphism groups. This completes the proof of (2), and hence of the original statement. $\square$

REFERENCES

[1] Jonathan L. Alperin and George Glauberman. *Limits of Abelian Subgroups of Finite p-Groups. Journal of Algebra*, Vol. 203 (1998), Page 533–566.

[2] Michael Aschbacher. *The Status of the Classification of the Finite Simple Groups. Notices of the American Mathematical Society*, Vol. 51, No. 7 (2004), Page 736–740. Available online at http://www.ams.org/notices/200407/fea-aschbacher.pdf

[3] Reinhold Baer. *Groups with Abelian Central Quotient Group. Transactions of the American Mathematical Society*, Vol. 44, No. 3 (November 1938), Page 357–386. Available online at http://www.jstor.org/stable/1989886

[4] A. Bak, G. Donadze and N. Inassaridze. *Homology of multiplicative Lie rings. Journal of Pure and Applied Algebra*, Vol. 208 (2007), Page 761–777.

[5] Gilbert Baumslag. *Some aspects of groups with unique roots. Acta mathematica*, Vol. 104 (1960), Page 217–303.

[6] F. R. Beyl. *Isoclinisms of group extensions and the Schur multiplicator. Groups St. Andrews 1981. London Mathematical Society Lecture Note Series*, Vol. 71, Page 169–185.

[7] Mitya Boyarchenko and Maria Sabitova. *The orbit method for profinite groups and a p-adic analogue of Brown's theorem. Israel Journal of Math*, Vol. 165 (2008), Page 67–91. Available on the ArXiV at http://arxiv.org/abs/math/0608126

[8] Ronald Brown and Jean-Louis Loday. *Van Kampen theorems for diagrams of spaces. Topology*, Vol. 26, No. 3 (1987), Page 311–335.

[9] Serena Cicalo, Willem A. de Graaf and M. R. Vaughan-Lee. *An effective version of the Lazard correspondence. Journal of Algebra*, Vol. 352 (2012), Page 430–450. Available online at http://dx.doi.org/10.1016/j.jalgebra.2011.11.031

[10] David S. Dummit and Richard M. Foote. *Abstract Algebra. John Wiley & Sons* (2003). ISBN 0471433349

[11] Timothy E. Easterfield. *The orders of products and commutators in prime-power groups. Cambridge Philosophical Society*, Vol. 36 (1940), Page 14–26.

[12] Beno Eckmann, Peter J. Hilton, and Urs Stammbach. *On the homology theory of central group extensions: I - The commutator map and stem extensions. Commentarii Mathematici Helvetici*, Vol. 47, No. 1 (1972), Page 102–122.

[13] Bettina Eick, Max Horn, and Seiran Zandi. *Schur multipliers and the Lazard correspondence. Archiv der Mathematik*, Vol. 99 (2012), Page 217–226. Available online at http://dx.doi.org/10.1007/s00013-012-0426-7

[14] Bettina Eick and E. A. O'Brien. *Enumerating p-groups. Journal of the Australian Mathematical Society*, Vol. 67 (1999), Page 191–205.

[15] Graham Ellis. *The non-abelian tensor product of finite groups is finite. Journal of Algebra*, Vol. 111 (1987), Page 203–205. Available online at http://dx.doi.org/10.1016/0021-8693(87)90249-3

[16] Graham Ellis. *A non-abelian tensor product of Lie algebras. Glasgow Journal of Math*, Vol. 33 (1991), Page 101–120.

[17] Graham Ellis. *On five well-known commutator identities. Journal of the Australian Mathematical Society*, Vol. 54 (1993), Page 1–19.

[18] Tuval Foguel and Abraham A. Ungar. *Involutory Decomposition of Groups Into Twisted Subgroups and Subgroups*. Available online at http://paws.wcu.edu/tsfoguel/inv.pdf

[19] George Glauberman. *A partial extension of Lazard's correspondence for finite p-groups.Groups, Geometry, and Dynamics*, Vol. 1, Issue 4 (2007). Available online at http://dx.doi.org/10.4171/GGD/21

[20] George Glauberman, *Abelian subgroups of small index in finite p-groups. Journal of Group Theory*, Vol. 8 (2005), Page 539–560. Available online at http://dx.doi.org/10.1515/jgth.2005.8.5.539

[21] Jon Gonzalez-Sanchez. *Kirillov's orbit method for p-groups and pro-p-groups. Commutative Algebra*, Vol. 37, No. 12 (2009), Page 4476–4488.

[22] Marshall Hall and James Kuhn Senior. *The groups of order* 2^n $(n \leq 6)$.

[23] Philip Hall. *The classification of prime-power groups. Journal fur die reine und angewandte Mathematik*, Vol. 69 (1937). Available online at http://dx.doi.org/10.1515/crll.1940.182.130

[24] N. S. Hekster. *On the structure of n-isoclinism classes of groups*, Vol. 40 (1986), Page 63–85. Available online at http://dx.doi.org/10.1016/0022-4049(86)90030-7

[25] Peter Hilton, Guido Mislin, and Joe Roitberg. *Localization of Nilpotent Groups and Spaces. North-Holland Mathematics Studies* (55). *American Elsevier* (1975). ISBN 0444107762

[26] I. Martin Isaacs. *Character Theory of Finite Groups. Dover* (2012). ISBN 0486680142

[27] Rodney James, M. F. Newman, and E. A. O'Brien. *The groups of order 128. Journal of Algebra*, Vol. 129, No. 1 (February 1990), Page 136–158. Available online at http://dx.doi.org/10.1016/0021-8693(90)90244-I.

[28] Gregory Karpilovsky. *The Schur Multiplier. Oxford University Press* (1987). ISBN 0198535546

[29] Evgenii I. Khukhro. *p-Automorphisms of Finite p-groups. Cambridge University Press* (1998). ISBN 052159717X

[30] Michel Lazard. *Sur les groupes nilpotents et les anneaux de Lie. Annales scientifiques de l'E.N.S.* Third Series, Vol. 71, No. 2 (1954), Page 101–190.

[31] C. R. Leedham-Green and Susan McKay. *Baer-invariants, isologism, varietal laws and homology. Acta Mathematica*, Vol. 137, Issue 1 (1976), Page 99–150. Available online at http://dx.doi.org/10.1007/BF02392415

[32] Avinoam Mann. *Some questions about p-groups. Journal of the Australian Mathematical Society*, Vol. 67 (1999), Page 356–379.

[33] E. A. O'Brien and C. Voll. *Enumerating classes and characters of p-groups.* Available on the ArXiV at http://arxiv.org/abs/1203.3050

[34] J. Peter May and Kate Ponto. *More Concise Algebraic Topology: Localization, Completion and Model Categories. University of Chicago Press* (2012). ISBN 0226511782

[35] Aidan McDermott. *The non-abelian tensor product of groups: computations and structural results.* Ph. D. thesis at National University of Ireland, Galway, under the supervision of Dr. Graham J. Ellis (February 1998). Available online at http://web.math.unifi.it/users/fumagal/articles/McDermott.pdf

[36] Clair Miller. *The second homology group of a group; relations among commutators. Proceedings of the American Mathematical Society*, Vol. 3 (1952), Page 588–595. Available online at http://www.ams.org/journals/proc/1952-003-04/S0002-9939-1952-0049191-5/S0002-9939-1952-0049191-5.pdf

[37] John Willard Milnor. *Introduction to algebraic K-theory. Annals of Mathematics Studies* (72), *Princeton University Press* (1971). ISBN 0691081018

[38] Kay Moneyhun. *Isoclinisms in Lie Algebras. Algebras Groups Geom.*, Vol. 11 (1994), Page 9–22.

[39] E. A. O'Brien. *The groups of order 256. Journal of Algebra*, Vol. 143 (1991), Page 219–235. Available online at http://dx.doi.org/10.1016/0021-8693(91)90261-6

[40] Foroud Parvaneh, Mohammad Reza R. Moghaddam, A. Khaksar. *Some Properties of n-Isoclinism in Lie Algebras. Italian Journal of Pure and Applied Mathematics*, Vol. 28 (2011), Page 165–176.

[41] Donald H. Pilgrim. *Engel conditions on groups. Proceedings of the Iowa Academy of Sciences*, Vol. 71 (1964), Page 377–383.

[42] B. I. Plotkin. *On some criteria of locally nilpotent groups. Uspekhi Mat. Nauk*, 9:3 (61) (1954), Page 181–186.

[43] Joseph J. Rotman. *An Introduction to the Theory of Groups. Springer Graduate Texts in Mathematics* (1999). ISBN 0387942858

[44] John Stallings. *Homology and central series of groups. Journal of Algebra*, Vol. 2 (1965), Page 170–181.

[45] Michio Suzuki. *Group Theory II. Springer* (1986). ISBN 0387109161

[46] Veeravalli S. Varadarajan. *The Lie group-Lie algebra correspondence*. Lecture notes on Lie theory, Chapter 9.

[47] Charles Weibel. *An Introduction to Homological Algebra. Cambridge University Press* (1995). ISBN 0521559871

[48] Thomas S. Weigel. *Exp and log functors for the categories of powerful p-central groups and Lie algebras*. Habilitationsschrift (Ph.D. thesis) at Freiburg im Breisgau (1994).