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 [9]. A knowledge of the material in [39] 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 .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 .2.1 and .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 .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 $L^{(i+1)} = [L^{(i)}, L^{(i)}]$.
- $\mathrm{Inn}(L)$ 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 $\mathrm{Inn}(L)$ as set-theoretically identical with $L/Z(L)$.
- $\mathrm{Der}(L)$ is the Lie ring of all derivations of L. We treat $\mathrm{Inn}(L)$ naturally as a Lie subring of $\mathrm{Der}(L)$. In fact, $\mathrm{Inn}(L)$ is an ideal in $\mathrm{Der}(L)$.
- $\mathrm{Aut}(L)$ 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 [30].[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 .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 [42]. 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: