THESIS

ASYMPTOTIC ENUMERATION OF MATRIX GROUPS

Submitted by

Brady A. Tyburski

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Master of Science

Colorado State University

Fort Collins, Colorado

Summer 2018

Master's Committee:

Advisor: James B. Wilson

Henry Adams
Rachel Pries
Jesse W. Wilson

ABSTRACT

ASYMPTOTIC ENUMERATION OF MATRIX GROUPS

We prove that the general linear group $\mathrm{GL}_d(p^e)$ has between $p^{d^4e/64-O(d^2)}$ and $p^{d^4e^2\cdot\log_2 p}$ distinct isomorphism types of subgroups. The upper bound is obtained by elementary counting methods, where as the lower bound is found by counting the number of isomorphism types of subgroups of the generalized Heisenberg group. To count these subgroups, we use nuclei of a bilinear map alongside versor products - a division analog of the tensor product.

DEDICATION

To Jennifer Lawson for introducing me to algebra.

TABLE OF CONTENTS

ABSTRACT ii
DEDICATION iii

Chapter 1 Introduction 1
1.1 General Counting Results 1
1.2 Survey of Main Results 4

Chapter 2 Preliminaries 7
2.1 Matrix Notation 7
2.2 The Commutator and Center of a Group 8
2.3 Bimaps and Isotopism 8
2.4 Nuclei of Bimaps 10
2.5 Brahana Correspondence 10

Chapter 3 The Lifting Theorem 12
3.1 The Commutator Bimap 12
3.2 Nuclei of the Commutator Bimap 16
3.3 Versor Products and Universal Mapping Properties 22
3.4 Subgroups of G Modulo J Embed into Small Versors 25
3.5 The Lifting Theorem 29
3.6 $(\uparrow\downarrow\downarrow)$-isotopism 31
3.7 Proof of the Lifting Theorem 34

Chapter 4 Toward an Asymptotic Lower Bound 36
4.1 A Lower Bound for $\#S_i$ 37
4.2 An Upper Bound for $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$ 39
4.3 Optimization 43

Chapter 5 A Closing Remark 46

References 47

Chapter 1

Introduction

This is a paper dedicated to exploring the diversity inherent in even well-studied groups, such as the general linear group, $\mathrm{GL}_d(p^e)$: the group of invertible $d \times d$ matrices over a field of size p^e. We prove:

Theorem 1.1 *The number $f(d, e, p)$ of distinct isomorphism types of subgroups of $\mathrm{GL}_d(p^e)$ satisfies*

$$p^{d^4e/64 - O(d^2)} \leqslant f(d, e, p) \leqslant p^{d^4e^2 \cdot \log_2 p}.$$

As we demonstrate in corollary 1.4 below, the upper bound is easily obtained using elementary enumeration methods. The interesting result is the lower bound.

1.1 General Counting Results

Before commencing this investigation, we first ask a related question: how many groups of order n are there? To answer this question, we define the function $f(n)$ to be the number of isomorphism classes of groups of order n. We can establish a crude upper bound for $f(n)$ by counting the number of possible multiplication tables for groups with n elements (i.e. $n \times n$ grids with entries from a set of size n). This gives us that

$$f(n) \leqslant n^{n^2}.$$

One cannot guarantee that distinct ways of populating an n by n grid with elements of G produce non-isomorphic groups, so n^{n^2} is in general much greater than $f(n)$. For instance, if $n = p$ is prime, then $f(p) = 1 \ll p^{p^2}$. To tighten this upper bound, we first determine a bound on the number of generators for a group of order n.

We say $\{g_1, g_2, \ldots, g_s\}$ is a *minimal generating set* for a group G if $G = \langle g_1, g_2, \ldots, g_s \rangle$ and none of these g_i can be omitted, so for all i, $G \neq \langle g_1, g_2, \ldots, g_{i-1}, g_{i+1}, \ldots, g_s \rangle$.

Proposition 1.2 *If $\{g_1, \ldots, g_s\}$ is a minimal generating set for a finite group G, then $s \leqslant \log_2 |G|$.*

Proof. Define $G_i := \langle g_1, \ldots, g_i \rangle$. Because $\{g_1, \ldots, g_s\}$ is a minimal generating set for G, for each i, $G_i < G_{i+1}$, and so $1 = G_0 < G_1 < \cdots < G_{s-1} < G_s = G$ is a chain of subgroups of G. By Lagrange's Theorem, $|G_i| = m|G_{i-1}|$ with $m \in \mathbb{Z}^+$, and $G_{i-1} \neq G_i$, so $m \neq 1$. This allows us to conclude that for all i, $|G_i : G_{i-1}| \geqslant 2$. Therefore,

$$|G| = \prod_{i=1}^{s} |G_i : G_{i-1}| \geqslant 2^s,$$

and we see that $s \leqslant \log_2 |G|$. □

Corollary 1.3 *The number of subgroups of a finite group G with order n is no more than $n^{\log_2 n}$.*

Proof. A minimal generating set of G has $\log_2 n$ elements, so for every subgroup $H \leqslant G$, $H = \langle g_1, \ldots, g_k \rangle$, where $k \leqslant \log_2 n$ by proposition 1.2. Therefore, to obtain an upper bound on the number of subgroups, we can count the number of sequences in G with length $\log_2 n$. There are at most $n^{\log_2 n}$ such sequences. □

Corollary 1.4 *The number of isomorphism types of subgroups of $\mathrm{GL}_d(K)$ is no greater than $p^{d^4 e^2}$.*

Proof. By counting the number of $d \times d$ matrices over $K = \mathbb{F}_q$ (where $q = p^e$), we see that $|\mathrm{GL}_d(K)| \leqslant q^{d^2}$. Now, using the formula from corollary 1.3, the number of subgroups of $\mathrm{GL}_d(K)$ and therefore the number of isomorphism types of subgroups of $\mathrm{GL}_d(K)$ is no more than

$$q^{d^2 \cdot \log_2 q^{d^2}} = q^{d^4 \cdot \log_2 q} = p^{d^4 e \cdot \log_2 p^e} = p^{d^4 e^2 \cdot \log_2 p}$$

□

In a finite group, each element can be written as a product of generators, so all products in G can be expressed as the product of a generator and a group element. For a group of order n, the

size of a minimal generating set is no bigger than $\log_2 n$ by proposition 1.2, so by counting the ways of populating a $\log_2 n$ by n multiplication table with elements of G we find that

$$f(n) \leqslant n^{n \log_2 n}.$$

In the 1960s, this upper bound was refined for p-groups by Sims [1, Chapter 5]. A few years earlier, Higman had established a lower bound for p-groups [1, Chapter 4]. Collectively, they demonstrated that

$$p^{2/27n^3 - \Omega(n^2)} \leqslant f(p^n) \leqslant p^{2/27n^3 + O(n^{8/3})}.$$

In 1991, Pyber sharpened the upper bound for all finite groups [1, Chapter 16] by showing that

$$f(n) \leqslant n^{2/27\mu(n)^2 + O(\mu(n)^{5/3})},\ \mu(n) = \max_e \{p^e | n : p \text{ prime}\}.$$

A seemingly mundane example that nonetheless exhibits surprising diversity in its quotient structure is the family of *generalized Heisenberg groups*. Let $K = \mathbb{F}_q$ be a finite field of order $q = p^e$ and b be a positive integer. A group of the form

$$G_b = \left\{ \begin{bmatrix} 1 & u & w \\ 0 & I_b & v^t \\ 0 & 0 & 1 \end{bmatrix} : u, v^t \in K^b, w \in K \right\}$$

is a generalized Heisenberg group. If $b = 1$, G_b is the familiar *Heisenberg group* over K.

Generalized Heisenberg groups consist of upper triangular matrices, which appear to be relatively straightforward objects. Despite this, if $p > 2$ and $n \geqslant 12$, Lewis and Wilson [3] showed there is a generalized Heisenberg group of order $p^{5n/4 + O(1)}$ with $p^{n^2/24 + O(n)}$ isomorphism classes of quotients of G_b with order p^n, an enormous number of non-isomorphic quotients relative to the order of G_b. These quotients are unable to be distinguished by the usual isomorphism invariants and therefore must display remarkable diversity.

We expand the notion of a generalized Heisenberg group to include all groups of the form

$$G_{abc} = \left\{ \begin{bmatrix} I_a & U & W \\ 0 & I_b & V \\ 0 & 0 & I_c \end{bmatrix} : U \in \mathbb{M}_{a\times b}(K), V \in \mathbb{M}_{b\times c}(K), W \in \mathbb{M}_{a\times c}(K) \right\},$$

where a, b, c are positive integers and $K = \mathbb{F}_q$ for a prime power $q = p^e$. Without loss of generality, we assume $a \leqslant c$. Now define

$$J_{abc} = \left\{ \begin{bmatrix} I_a & U & W \\ 0 & I_b & 0 \\ 0 & 0 & I_c \end{bmatrix} : U \in \mathbb{M}_{a\times b}(K), W \in \mathbb{M}_{a\times c}(K) \right\} \leqslant G.$$

In this paper, we wish to determine a lower bound for the number of isomorphism classes of subgroups of G_{abc} that contain J_{abc} in terms of a, b, c, p, and e.

For $d = a + b + c$, the generalized Heisenberg group G_{abc} is a subgroup of $\mathrm{GL}_d(p^e)$. Therefore, a lower bound on the number of isomorphism classes of subgroups of G_{abc} also determines a lower bound on the number of isomorphism classes of subgroups of $\mathrm{GL}_d(p^e)$. It may be surprising to realize that much of the variability of isomorphism type of subgroups of $\mathrm{GL}_d(p^e)$ results from subgroups of the generalized Heisenberg groups alone.

1.2 Survey of Main Results

From now on, when the choice of a, b, and c is clear or irrelevant, we will refer to G_{abc} and J_{abc} by just G and J. If we let $j \in \mathbb{N}$ and set $\mathcal{S}_{p^j} = \{H \leqslant G : |H| = p^j \text{ and } H \geqslant J\}$, then the number of isomorphism classes of subgroups of G containing J is given by

$$\sum_{j=0}^{\log_p |G|} |\mathcal{S}_{p^j}/_{\cong}|.$$

Let $\mathcal{S}_{p^j} = \mathcal{S}_i$ for notational convenience. We will show that $\#S_i$ is exponential in b and c and thus the above sum is dominated by a highest exponent. In order to determine a lower bound for the number of isomorphism classes of these subgroups, we will therefore determine the maximum of this dominant summand in terms of b and c.

We say that a subgroup $X \leqslant G_{abc}$ such that $J_{abc} \leqslant X \leqslant G_{abc}$ is *native* to G_{abc} if whenever there is another generalized Heisenberg group $G_{a'b'c'}$ such that $J_{a'b'c'} \hookrightarrow X \hookrightarrow G_{a'b'c'}$, then $b \leqslant b'$. Additionally, we define the central automorphisms of G to be the subset of the automorphisms of G given by

$$\mathcal{C}_{\mathrm{Aut}(G)} = \{\varphi \in \mathrm{Aut}(G) : \varphi\big|_{G/G'} = 1, \varphi\big|_{G'} = 1\}$$

where $G' = [G, G]$ is the commutator subgroup. The normal subgroup of a generalized Heisenberg group given by setting the U and V blocks both equal to 0 matrices is denoted as

$$\mathcal{W} \coloneqq \left\{ \begin{bmatrix} I_a & 0 & W \\ 0 & I_b & 0 \\ 0 & 0 & I_c \end{bmatrix} : W \in \mathbb{M}_{a\times c}(K) \right\}.$$

The first major thoerem we prove is the following lifting theorem:

Theorem 1.5 (The Lifting Theorem) *Assume $X, Y \in \mathcal{S}_i$ are native to G and $X' = Y' = \mathcal{W}$. If $\varphi : X \to Y$ is an isomorphism such that $J\varphi = J$, then there exists a $\hat{\varphi} \in \mathrm{Aut}(G)$ such that $\hat{\varphi}\big|_X = \varphi$. This lift of φ is unique up to a central automorphism.*

To prove this theorem, we utilize the theory of bilinear maps applied to the commutator bilinear map of G. Using a notion of equivalence for bilinear maps combined with the universal properties of the division analog of the tensor product (the versor product), we are able to lift an equivalence of bilinear maps to an automorphism of the commutator bilinear map. In the case that the involved subgroups are native to G_{abc}, the resulting equivalence is unique (up to a central automorphism).

Using this lifting theorem, we will find ourselves in a position to determine a lower bound on the number of isomorphism classes of subgroups of G containing J. Define $\mathrm{Aut}_J(G) = \{\varphi \in$

$\mathrm{Aut}(G) : J\varphi = J\}$. By counting the orbits of the $\mathcal{S}_i$ under the action of $\mathrm{Aut}_J(G)$ modulo $\mathcal{C}_{\mathrm{Aut}(G)}$, we are able to count $|\mathcal{S}_i/_{\cong}|$. Using the pigeonhole principle, we find that a lower bound for the number of these orbits is

$$\frac{\#\mathcal{S}_i}{\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)}).}$$

Next, we determine a lower bound on $\mathcal{S}_i$ and an upper bound for $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$ in order to deduce the desired lower bound.

Quotients of elements of $\mathcal{S}_i$ (modulo J) are shown to be in bijection with the subspaces of $\mathbb{M}_{b\times c}(K)$, a vector space. Therefore, finding a lower bound for $\mathcal{S}_i$ reduces to counting vector subspaces. An upper bound for $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$ is found by utilizing a correspondence between automorphisms of G such that $J\varphi = J$ and automorphisms of the commutator bilinear map. Next, it is shown that these automorphisms act on the nuclei of the commutator map, which, combined with the Skolem-Noether theorem leads to an upper bound for $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$.

Finally, we are able to establish a lower bound for $|\mathcal{S}_i/\cong|$ by dividing the bound for $\#\mathcal{S}_i$ by the bound for $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$ and then using the method of Lagrange multipliers to complete the optimization. Because the generalized Heisenberg group is a subgroup of $\mathrm{GL}_d(p^e)$, the lower bound for the number of isomorphism classes of G also provides a lower bound for the number of isomorphism classes of subgroups of $\mathrm{GL}_d(p^e)$. The lower bound we will arrive at is stated in theorem 1.1.

Chapter 2

Preliminaries

We use K exclusively for the finite field $\mathbb{F}_q$ where $q = p^e$ for a prime p. Throughout this paper, the image of an element x under an operator φ is written as $x\varphi$ or x^φ. We also define $x\varphi^{-1} = \varphi x$. A subgroup H such that $H^\varphi \leqslant H$ is said to be *φ-invariant*.

2.1 Matrix Notation

The additive group of $a \times b$ matrices $\mathrm{Mat}_{a\times b}(K)$ will be written as $\mathbb{M}_{a\times b}$, with the understanding that the matrices are over K. If $a = b$, we write $\mathbb{M}_a$. If $M \in \mathbb{M}_{a\times b}$ is a matrix, we denote its ith row by m_i and its jth column by m^j. In order to describe the commutator bimap in section 3.1, we also use the convention that

$$\underline{\mathrm{m}} = [m_1, \ldots, m_a] \in \mathbb{M}_{1\times ab}$$

is the vector with entries given by the rows of M lined up one after another.

We will frequently utilize block matrices comprised of several identity and zero blocks. Identity blocks of dimension a will be denoted I_a and zero blocks will be denoted similarly by 0_a. Non-square zero blocks will be written as simply 0, but the notation of its neighboring blocks will be sufficient to deduce the size of such a zero block.

Elements of G_{abc} are block matrices of the form

$$\begin{bmatrix} I_a & U & W \\ 0 & I_b & V \\ 0 & 0 & I_c \end{bmatrix},$$

so we will sometimes refer to the superdiagonal block entries as the U-block, V-block, and W-block, respectively. We often refer to the normal subgroups of G_{abc} in which two of the U, V, or W

blocks are set to be 0 matrices. We denote these by

$$\mathcal{U} := \left\{ \begin{bmatrix} I_a & U & 0 \\ 0 & I_b & 0 \\ 0 & 0 & I_c \end{bmatrix} : U \in \mathbb{M}_{a\times b}(K) \right\} \text{ and } \mathcal{W} := \left\{ \begin{bmatrix} I_a & 0 & W \\ 0 & I_b & 0 \\ 0 & 0 & I_c \end{bmatrix} : W \in \mathbb{M}_{a\times c}(K) \right\}.$$

2.2 The Commutator and Center of a Group

Suppose G is a multiplicative group. The *commutator* is a binary operation $[,] : G \times G \to G$ defined by $[M, N] = MNM^{-1}N^{-1}$. We additionally dub the *commutator subgroup* as the subgroup of G generated by its commutators. We will denote this subgroup by $[G, G] = G'$. The center of the group, $Z(G) = \{g : [G, g] = [g, G] = 1\}$, is the subgroup of elements in G which commute with all the elements of G. As the commutator operation is not a homomorphism, it does not have a definable kernel; however, the elements of $Z(G)$ are the ones that do not affect commutation, so we will reduce the commutator operation to $[,] : G/Z(G) \times G/Z(G) \to G'$ (see section 3.1).

2.3 Bimaps and Isotopism

Let K be a field and U, V, W be vector spaces over K. A K-bilinear map, or a K-*bimap*, is a map $\circ : U \times V \rightarrowtail W$ such that for all $u, \hat{u} \in U, v, \hat{v} \in V$, and $k \in K$,

$$(u + k\hat{u}) \circ v = u \circ v + k(\hat{u} \circ v),$$

and

$$u \circ (v + k\hat{v}) = u \circ v + k(u \circ \hat{v}).$$

The radicals of $\circ$ are defined to be $U^{\perp} = \{v \in V : U \circ v = 0\}, V^{\top} = \{u \in U : u \circ V = 0\}$, and $W^{+} = W/(U \circ V)$. When $U^{\perp} = 0$, we say $\circ$ is *right non-degenerate*, when $V^{\top} = 0$ we say $\circ$ is *left non-degenerate*, and when all three radicals are trivial, we say $\circ$ is *fully non-degenerate*. Non-degeneracy allows for a certain kind of cancellation property.

Lemma 2.1 (Cancellation property for non-degenerate bimaps) *Let* $\circ : U \times V \rightarrowtail W$ *be a bimap,* $u, u' \in U$, *and* $v, v' \in V$. *If* $\circ$ *is a right non-degenerate bimap such that for all* $u \in U, u \circ v = u \circ v'$, *then* $v = v'$. *Similarly, if* $\circ$ *is left non-degenerate such that for all* $v \in V, u \circ v = u' \circ v$, *then* $u = u'$.

Proof. Let $\circ$ be right non-degenerate with the property that for all $u \in U, u \circ v = u \circ v'$. By subtracting and then using the distributivity of $\circ$, we see that for all $u \in U$, $u \circ (v - v') = 0$. Therefore, $v - v' \in U^{\perp} = 0$ because $\circ$ is right non-degenerate, so $v = v'$. The left non-degenerate case is handled analogously. □

Next, we define a type of algebraic equivalence between bimaps. Let $\circ : U \times V \rightarrowtail W$ and $\bullet : U' \times V' \rightarrowtail W'$ be K-bimaps. A *homotopism* from $\circ$ to $\bullet$ is a triple $h = (h_U, h_V, h_W) \in \mathrm{Hom}_K(U, U') \times \mathrm{Hom}_K(V, V') \times \mathrm{Hom}_K(W, W')$ such that for all $u \in U, v \in V$,

$$u^h \bullet v^h = (u \circ v)^h.$$

This equality is expressed in the following so-called *bimap diagram.*

$$\begin{array}{ccc} U \times V & \overset{\circ}{\rightarrowtail} & W \\ {\scriptstyle h_U}\downarrow & \downarrow{\scriptstyle h_V} & \downarrow{\scriptstyle h_W} \\ U' \times V' & \overset{\bullet}{\rightarrowtail} & W' \end{array}$$

Figure 2.1: A bimap diagram illustrating the defining property of a homotopism of bimaps.

For brevity, the subscripts will sometimes be omitted on the components of a homotopism. The component of the homotopism being used is made clear by the context: $u^h = u^{h_U}, w^h = w^{h_W}$, and so on. *Isotopism* is defined similarly when the components of h are all isomorphisms. An *endotopism* is a homotopism from a bimap to itself and an *autotopism* is an isotopism from a bimap to itself. The set of homotopisms and isotopisms from $\circ$ to $\bullet$ will be denoted by $\mathrm{Hom}(\circ, \bullet)$ and $\mathrm{Iso}(\circ, \bullet)$. Similarly, the set of autotopisms of $\circ$ will be written as $\mathrm{Aut}(\circ)$.

2.4 Nuclei of Bimaps

Let $\circ : U \times V \rightarrowtail W$ be a K-bimap. Set $\mathcal{L} \subseteq \mathrm{End}(U)^{op} \times \mathrm{End}(W)^{op}, \mathcal{M} \subseteq \mathrm{End}(U) \times \mathrm{End}(V)^{op}$, and $\mathcal{R} \subseteq \mathrm{End}(V) \times \mathrm{End}(W)$. We say that $\circ$ is left $\mathcal{L}$-linear, middle $\mathcal{M}$-linear, and right $\mathcal{R}$-linear if each of the following respective properties holds:

$$\forall \lambda \in \mathcal{L}, \qquad (\lambda u) \circ v = \lambda(u \circ v),$$

$$\forall \mu \in \mathcal{M}, \qquad (u\mu) \circ v = u \circ (\mu v),$$

$$\forall \rho \in \mathcal{R}, \qquad u \circ (v\rho) = (u \circ v)\rho.$$

Additionally, if $\circ$ satisfies all of the above properties, we call it an *$\mathcal{LMR}$-bimap*. We can now define the rings under which $\circ$ is left, middle, and right linear. These are called the left, middle, and right *nuclei*, respectively, and are defined as

$$\mathcal{L}_\circ = \{\lambda \in \mathrm{End}(U)^{op} \times \mathrm{End}(W)^{op} : (\forall u \in U)(\forall v \in V),\ (\lambda u) \circ v = \lambda(u \circ v)\},$$

$$\mathcal{M}_\circ = \{\mu \in \mathrm{End}(U) \times \mathrm{End}(V)^{op} : (\forall u \in U)(\forall v \in V),\ (u\mu) \circ v = u \circ (\mu v)\},$$

$$\mathcal{R}_\circ = \{\rho \in \mathrm{End}(U) \times \mathrm{End}(W) : (\forall u \in U)(\forall v \in V),\ u \circ (v\rho) = (u \circ v)\rho\}.$$

Notice that the middle nucleus is the same as the familiar adjoint ring for a bilinear form. As such, the left and right nuclei can be viewed as the counterparts of the adjoint ring. These rings can be thought of as the 'largest' sets of left, middle, and right scalars for $\circ$. We will formalize this intuition in section 3.3 (see theorem 3.10).

2.5 Brahana Correspondence

Bimaps form a category with homotopisms as morphisms [5]. In fact, there is a functor from the category of bimaps to the category of groups, the idea for which dates back to Brahana [2] but was later formalized in [3]. Under this correspondence, the bimap $\circ : U \times V \rightarrowtail W$ is assigned to

the group on $U \times V \times W$ with product defined for all $(u, v, s), (x, y, t) \in U \times V \times W$ by

$$(u, v, s)(x, y, t) = (u + x, v + y, s + t + u \circ y)$$

and vice-versa. Groups of this form are called *Brahana groups*. In particular, G_{abc} is isomorphic to a Brahana group, where $U = \mathbb{M}_{a\times c}, V = \mathbb{M}_{b\times c}, W = \mathbb{M}_{a\times c}$, and $\circ$ is given by usual matrix multiplication. This is evidenced when multiplying two elements of G :

$$\begin{bmatrix} I_a & U & W \\ 0 & I_b & V \\ 0 & 0 & I_c \end{bmatrix} \begin{bmatrix} I_a & \hat{U} & \hat{W} \\ 0 & I_b & \hat{V} \\ 0 & 0 & I_c \end{bmatrix} = \begin{bmatrix} I_a & U + \hat{U} & W + \hat{W} + U\hat{V} \\ 0 & I_b & V + \hat{V} \\ 0 & 0 & I_c \end{bmatrix}.$$

Notice that isotopic bimaps correspond to isomorphic Brahana groups. The converse also holds [3, Proposition 6.5]. This provides a useful correspondence between isomorphism and isotopism that will play a large part in proving the desired lifting result (see section 3.7 and the proof of theorem 1.5).

Chapter 3

The Lifting Theorem

In this chapter, our aim is to prove theorem 1.5. To accomplish this, we first calculate the commutator bimap (section 1) and its nuclei (section 2). Following this, we define versors as universal objects closely related to bimaps (section 3) and then show that subgroups of G containing J embed into a versor product (section 4). In the second half of the chapter (sections 5-7), we use the findings from the first half of the chapter to prove theorem 1.5.

3.1 The Commutator Bimap

Rather than investigate the subgroups of G directly, we will use the bimap given by the commutator in G. Consider first the example when $a = c = 1$ and $b \geqslant 1$, so $\mathbb{M}_{a\times b} = \mathbb{M}_{1\times b}, \mathbb{M}_{b\times c} = \mathbb{M}_{b\times 1}$, and $\mathbb{M}_{a\times c} = \mathbb{M}_{1\times 1} \cong K$. Letting $u, \hat{u} \in \mathbb{M}_{1\times b}, v, \hat{v} \in \mathbb{M}_{b\times 1}$, and $w, \hat{w} \in K$, we see that the commutator of two elements is

$$\left[\begin{bmatrix} 1 & u & w \\ 0 & I_b & v \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \hat{u} & \hat{w} \\ 0 & I_b & \hat{v} \\ 0 & 0 & 1 \end{bmatrix}\right] = \begin{bmatrix} 1 & 0 & u\hat{v} - \hat{u}v \\ 0 & I_b & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The commutator is in bijection with its W block entries and can therefore be viewed as an element of $\mathbb{M}_{1\times 1} \cong K$. The resulting element of K depends solely on the entries of the U and V blocks from the matrices we were applying the commutator bimap to. The U and V blocks are elements of $\mathbb{M}_{1\times b}$ and $\mathbb{M}_{b\times 1}$, respectively, so the commutator bimap is given by

$$[,] : (\mathbb{M}_{1\times b} \oplus \mathbb{M}_{b\times 1}) \times (\mathbb{M}_{1\times b} \oplus \mathbb{M}_{b\times 1}) \rightarrowtail \mathbb{M}_{1\times 1} \cong K$$

where

$$\Big[u \oplus v, \hat{u} \oplus \hat{v}\Big] \longmapsto \big[u\ v^t\big] \begin{bmatrix} 0_b & I_b \\ -I_b & 0_b \end{bmatrix} \big[\hat{u}\ \hat{v}^t\big]^t.$$

Notice that this bimap has the form $[,] : G/G' \times G/G' \rightarrowtail G'$ because $G' = \mathcal{W}$. The general case for a and c is handled similarly, as the following proposition details.

Proposition 3.1 *If $U, \hat{U} \in \mathbb{M}_{a\times b}, V, \hat{V} \in \mathbb{M}_{b\times c}$, then the commutator bimap of G_{abc} is given by*

$$[,] : (\mathbb{M}_{a\times b} \oplus \mathbb{M}_{b\times c}) \times (\mathbb{M}_{a\times b} \oplus \mathbb{M}_{b\times c}) \rightarrowtail \mathbb{M}_{a\times b}$$

where

$$\Big[U \oplus V, \hat{U} \oplus \hat{V}\Big]_{ij} \longmapsto \big[\underline{u}\ \underline{v}^t\big] \begin{bmatrix} 0_a & E_{ij} \\ -E_{ij}^t & 0_c \end{bmatrix} \big[\underline{\hat{u}}\ \underline{\hat{v}^t}\big]^t$$

and $E_{ij} \in \mathbb{M}_{a\times c}(\mathbb{M}_b)$.

Before proving this proposition in full generality, we consider two instructive examples. First, consider the case in which $a > 1$ and $c = 1$. Letting $U, \hat{U} \in \mathbb{M}_{a\times b}, v, \hat{v} \in \mathbb{M}_{b\times 1}$, and $w, \hat{w} \in \mathbb{M}_{a\times 1}$, the commutator of two elements is given by

$$\left[\begin{bmatrix} I_a & U & w \\ 0 & I_b & v \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} I_a & \hat{U} & \hat{w} \\ 0 & I_b & \hat{v} \\ 0 & 0 & 1 \end{bmatrix}\right] = \begin{bmatrix} I_a & 0 & \cdots u_i\hat{v} - \hat{u}_i v \cdots \\ 0 & I_b & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

As with the case where $a = c = 1$, for each i we can write $u_i\hat{v} - \hat{u}_i v = \big[u_i\ v^t\big] \begin{bmatrix} 0_b & I_b \\ -I_b & 0_b \end{bmatrix} \big[\hat{u}_i\ \hat{v}^t\big]^t$. Therefore, the commutator bimap is given by

$$[,] : (\mathbb{M}_{a\times b} \oplus \mathbb{M}_{b\times 1}) \times (\mathbb{M}_{a\times b} \oplus \mathbb{M}_{b\times 1}) \rightarrowtail \mathbb{M}_{a\times 1}$$

where

$$\Big[U \oplus v, \hat{U} \oplus \hat{v}\Big]_i \longmapsto \big[\underline{u}\ v^t\big]\hat{T}_{i1}\big[\underline{\hat{u}}\ \hat{v}^t\big]^t$$

and

$$\hat{T}_{i1} = \left[\begin{array}{ccccc|c} & & & & & 0_b \\ & & & & & \vdots \\ & & 0_{ab} & & & I_b \\ & & & & & \vdots \\ & & & & & 0_b \\ \hline 0_b & \cdots & -I_b & \cdots & 0_b & 0_b \end{array}\right] = \begin{bmatrix} 0_a & e_i \\ -e_i^t & 0_1 \end{bmatrix} \otimes I_b$$

are square $(ab + b) \times (ab + b)$ matrices. To emphasize the similarity of this matrix to the one in the case where $a = c = 1$, we can identify $\mathbb{M}_{ab\times bc}$ with $\mathbb{M}_{a\times b} \otimes \mathbb{M}_b \cong \mathbb{M}_{a\times b}(\mathbb{M}_b)$. This gives the correspondence

$$\hat{T}_{i1} = \begin{bmatrix} 0_a & e_i \\ -e_i^t & 0_1 \end{bmatrix} \otimes I_b \cong \begin{bmatrix} 0_a & E_i \\ -E_i^t & 0_1 \end{bmatrix} = T_{i1}$$

where $E_i \in \mathbb{M}_{a\times 1}(\mathbb{M}_b)$. Substituting T_{i1} in place of $\hat{T}_{i1}$ in the above definition of the commutator bimap, we get a result consistent with proposition 3.1 when $j = 1$.

Next, consider the example for which $a = 1$ and $c > 1$. Let $u, \hat{u} \in \mathbb{M}_{1\times b}, V, \hat{V} \in \mathbb{M}_{b\times c}$, and $w, \hat{w} \in \mathbb{M}_{1\times c}$. Then the commutator is

$$\left[\begin{bmatrix} 1 & u & w \\ 0 & I_b & V \\ 0 & 0 & I_c \end{bmatrix}, \begin{bmatrix} 1 & \hat{u} & \hat{w} \\ 0 & I_b & \hat{V} \\ 0 & 0 & I_c \end{bmatrix}\right] = \begin{bmatrix} 1 & 0 & \cdots u\hat{v}_j - \hat{u}v_j \cdots \\ 0 & I_b & 0 \\ 0 & 0 & I_c \end{bmatrix}.$$

Similarly to the previous examples, the commutator bimap is given by

$$[,] : (\mathbb{M}_{1\times b} \oplus \mathbb{M}_{b\times c}) \oplus (\mathbb{M}_{1\times b} \times \mathbb{M}_{b\times c}) \rightarrowtail \mathbb{M}_{1\times c}$$

where

$$\Big[u \oplus V, \hat{u} \oplus \hat{V}\Big]_j \longmapsto \big[u\ \underline{v}^t\big]\hat{T}_{1j}\big[\hat{u}\ \underline{\hat{v}}^t\big]^t.$$

and

$$\hat{T}_{1j} = \left[\begin{array}{c|ccccc} 0_b & 0_b & \dots & I_b & \dots & 0_b \\ \hline 0_b & & & & & \\ \vdots & & & & & \\ -I_b & & & 0_{bc} & & \\ \vdots & & & & & \\ 0_b & & & & & \end{array}\right] = I_b \otimes \begin{bmatrix} 0_1 & e_i^t \\ -e_i & 0_c \end{bmatrix}$$

are square $(b + bc) \times (b + bc)$ matrices. Using the same kind of correspondence as before, we identify $\hat{T}_{1j}$ with

$$T_{1j} = \begin{bmatrix} 0_1 & E_j \\ -E_j^t & 0_c \end{bmatrix}$$

where $E_j \in \mathbb{M}_{1\times c}(\mathbb{M}_b)$. Again, this example is consistent with the conclusion of proposition 3.1 when $i = 1$. In fact, the proof of this proposition follows almost immediately by combining the methodology of the previous two examples.

Proof. Let $U, \hat{U} \in \mathbb{M}_{a\times b}, V, \hat{V} \in \mathbb{M}_{b\times c}$, and $W, \hat{W} \in \mathbb{M}_{a\times c}$. We then have the commutator bimap

$$[,] : (\mathbb{M}_{a\times b} \oplus \mathbb{M}_{b\times c}) \times (\mathbb{M}_{a\times b} \oplus \mathbb{M}_{b\times c}) \rightarrowtail \mathbb{M}_{a\times c}$$

where

$$\Big[U \oplus V, \hat{U} \oplus \hat{V}\Big]_{ij} \longmapsto \big[\underline{u}\ \underline{v}^t\big]T_{ij}\big[\underline{\hat{u}}\ \underline{\hat{v}}^t\big]^t.$$

and

$$T_{ij} = \begin{bmatrix} 0_a & E_{ij} \\ -E_{ij}^t & 0_c \end{bmatrix}$$

with $E_{ij} \in \mathbb{M}_{a\times c}(\mathbb{M}_b)$. □

Treating the T_{ij} as slices of a tensor, we have the following corollary.

Corollary 3.2 *The commutator bimap of G_{abc} is given by an $(ab+bc)\times(ab+bc)\times(ac)$ tensor over K.*

3.2 Nuclei of the Commutator Bimap

Next, we calculate the nuclei of the commutator bimap - the rings of scalars over which the commutator bimap is left, middle, and right linear, respectively (see section 2.4). For ease of notation, denote the commutator bimap as specified in proposition 3.1 by $*$.

Proposition 3.3 *The middle nucleus $\mathcal{M}_*$ of the commutator bimap of G_{abc} is*

$$\left\{ \left(\begin{bmatrix} A & B \\ C & D \end{bmatrix}, \begin{bmatrix} D^t & -B^t \\ -C^t & A^t \end{bmatrix} \right) : A,B,C,D \in \mathbb{M}_b \right\} \text{ if } a=c=1;$$

$$\left\{ \left(\begin{bmatrix} A\otimes I_a & 0 \\ u & B \end{bmatrix}, \begin{bmatrix} B^t\otimes I_a & 0 \\ -u^\dagger & A^t \end{bmatrix} \right) : A,B \in \mathbb{M}_b, u \in \mathbb{M}_{1\times a}(\mathbb{M}_b) \right\} \text{ if } a>1, c=1;$$

$$\left\{ \left(\begin{bmatrix} A & u \\ 0 & B\otimes I_c \end{bmatrix}, \begin{bmatrix} B^t & -u^\dagger \\ 0 & A^t\otimes I_c \end{bmatrix} \right) : A,B \in \mathbb{M}_b, u \in \mathbb{M}_{1\times c}(\mathbb{M}_b) \right\} \text{ if } a=1, c>1;$$

or

$$\left\{ \left(\begin{bmatrix} A\otimes I_a & 0 \\ 0 & B\otimes I_c \end{bmatrix}, \begin{bmatrix} B^t\otimes I_a & 0 \\ 0 & A^t\otimes I_c \end{bmatrix} \right) : A,B \in \mathbb{M}_b \right\} \text{ if } a,c>1,$$

where $u_i^\dagger = u_i^t$.

Proof. If $a, c = 1$, then $(u \oplus v) * (\hat{u} \oplus \hat{v}) = \begin{bmatrix} u\, v^t \end{bmatrix} \begin{bmatrix} 0_b & I_b \\ -I_b & 0_b \end{bmatrix} \begin{bmatrix} \hat{u}\, \hat{v}^t \end{bmatrix}$ by proposition 3.1. Therefore, $(F, G) \in \mathcal{M}_*$ precisely when

$$\begin{bmatrix} F_{11} & F_{12} \\ F_{21} & F_{22} \end{bmatrix} \begin{bmatrix} 0 & I_b \\ -I_b & 0 \end{bmatrix} = \begin{bmatrix} 0 & I_b \\ -I_b & 0 \end{bmatrix} \begin{bmatrix} G_{11}^t & G_{21}^t \\ G_{12}^t & G_{22}^t \end{bmatrix}$$

where $F_{ij}, G_{ij} \in \mathbb{M}_b$. Equality occurs if, and only if, the following equations hold:

$$-F_{12} = G_{12}^t, F_{11} = G_{22}^t, F_{22} = G_{11}^t, -F_{21} = G_{21}^t.$$

Therefore, the middle nucleus when $a = c = 1$ is

$$\mathcal{M}_* = \left\{ \left(\begin{bmatrix} A & B \\ C & D \end{bmatrix}, \begin{bmatrix} D^t & -B^t \\ -C^t & A^t \end{bmatrix} \right) : A, B, C, D \in \mathbb{M}_b \right\}.$$

Next, if $a > 1$ and $c = 1$, then $*$ is given by a tensor with slices $T_i = \begin{bmatrix} 0_a & -E_i \\ E_i^t & 0_1 \end{bmatrix}, E_i \in \mathbb{M}_{a \times 1}(\mathbb{M}_b)$. Thus, $(F, G) \in \mathcal{M}_*$ if, and only if, for all $i \in \{1, ..., a\}, FT_i = T_i G^t$. Since $F, G \in \mathbb{M}_{ab+b}$, we can partition F and G^t using $(b \times b)$-blocks. For the sake of calculation, these matrices can now be viewed as square $(a + 1) \times (a + 1)$ matrices over $\mathbb{M}_b$. Now, for all $i \in \{1, ..., a\}$ we have that

$$\left[\begin{array}{c|c|c|c} & -F_{1,a+1} & & F_{1,i} \\ & \vdots & & \vdots \\ \hline & -F_{i,a+1} & & F_{i,i} \\ \hline & & & \\ & \vdots & & \vdots \\ & & & \\ \hline & -F_{a+1,a+1} & & F_{a+1,i} \end{array}\right] = \left[\begin{array}{c|c|c|c} & & & \\ \hline G^t_{a+1,1} \quad \cdots & G^t_{a+1,i} & \cdots & G^t_{a+1,a+1} \\ \hline & & & \\ & & & \\ & & & \\ \hline -G^t_{i,1} \quad \cdots & -G^t_{i,i} & \cdots & -G^t_{i,a+1} \end{array}\right]$$

where $F_{ij}, G_{ij} \in \mathbb{M}_b$, and blank areas denote zero blocks. This allows us to deduce that for all $i \in \{1, ..., a\}$,

$$G^t_{a+1,k} = \begin{cases} -F_{i,a+1} & k = i \\ F_{i,i} & k = a+1 \\ 0 & \text{otherwise,} \end{cases} \quad G^t_{i,k} = \begin{cases} F_{a+1,a+1} & k = i \\ -F_{a+1,i} & k = a+1 \\ 0 & \text{otherwise,} \end{cases} \quad F_{k,i} = 0 \text{ if } k \neq i, a+1.$$

As these equations must hold for each $i \in \{1, \ldots, a\}$, we conclude that

$$F_{1,1} = \cdots = F_{a,a}, \quad G^t_{1,1} = \cdots = G^t_{a,a} = F_{a+1,a+1}, \text{ and } F_{k,a+1} = G^t_{a+1,k} = 0, k \neq a+1.$$

From these relations, we conclude that the middle nucleus is $\mathcal{M}_* = \{(M, N^t) : F_{ij} \in \mathbb{M}_b\}$ where

$$M = \left[\begin{array}{ccc|c} F_{11} & & & 0 \\ & \ddots & & \vdots \\ & & F_{11} & 0 \\ \hline F_{a+1,1} & \cdots & F_{a+1,a} & F_{a+1,a+1} \end{array}\right] \text{ and } N = \left[\begin{array}{ccc|c} F_{a+1,a+1} & & & 0 \\ & \ddots & & \vdots \\ & & F_{a+1,a+1} & 0 \\ \hline -F_{a+1,1} & \cdots & -F_{a+1,a} & F_{11} \end{array}\right].$$

Alternatively, by fixing $A = F_{11}, B = F_{a+1,a+1}$, and $u_i = F_{a+1,i}$, we see that

$$\mathcal{M}_* = \left\{ \left(\begin{bmatrix} A \otimes I_a & 0 \\ u & B \end{bmatrix}, \begin{bmatrix} B^t \otimes I_a & 0 \\ -u^\dagger & A^t \end{bmatrix} \right) : A, B \in \mathbb{M}_b, u \in \mathbb{M}_{1\times a}(\mathbb{M}_b) \right\}.$$

The case where $a > 1, c = 1$ is handled in much the same way. The resulting middle nucleus is

$$\mathcal{M}_* = \left\{ \left(\begin{bmatrix} A & u \\ 0 & B \otimes I_c \end{bmatrix}, \begin{bmatrix} B^t & -u^\dagger \\ 0 & A^t \otimes I_c \end{bmatrix} \right) : A, B \in \mathbb{M}_b, u \in \mathbb{M}_{1\times c}(\mathbb{M}_b) \right\}.$$

Finally, if $a, c > 1$, the commutator bimap corresponds to a tensor with slices $T_{ij} = \begin{bmatrix} 0_a & -E_{ij} \\ {E_{ij}}^t & 0_c \end{bmatrix} \in \mathbb{M}_{a+c}(\mathbb{M}_b)$ where $E_{ij} \in \mathbb{M}_{a\times c}(\mathbb{M}_b)$. Therefore, $(F, G) \in \mathcal{M}_*$ precisely if for all $i \in \{1, ..., a\}$ and $j \in \{1, ..., c\}$, the equality $FT_{ij} = T_{ij}G^t$ holds. Write F, G, respectively, as block matrices $\begin{bmatrix} F_{11} & F_{12} \\ F_{21} & F_{22} \end{bmatrix}, \begin{bmatrix} G_{11}^t & G_{21}^t \\ G_{12}^t & G_{22}^t \end{bmatrix} \in \mathbb{M}_{a+c}(\mathbb{M}_b)$ where $F_{11}, G_{11}^t \in \mathbb{M}_a(\mathbb{M}_b), F_{22}, G_{22}^t \in \mathbb{M}_c(\mathbb{M}_b), F_{12}, G_{21}^t \in \mathbb{M}_{a\times c}(\mathbb{M}_b)$, and $F_{21}, G_{12}^t \in \mathbb{M}_{c\times a}(\mathbb{M}_b)$. Now, $FT_{ij} = T_{ij}G^t$ is equivalent to

$$\begin{bmatrix} F_{11} & F_{12} \\ F_{21} & F_{22} \end{bmatrix} \begin{bmatrix} 0_a & -E_{ij} \\ {E_{ij}}^t & 0_c \end{bmatrix} = \begin{bmatrix} 0_a & -E_{ij} \\ {E_{ij}}^t & 0_c \end{bmatrix} \begin{bmatrix} G_{11}^t & G_{21}^t \\ G_{12}^t & G_{22}^t \end{bmatrix}.$$

After multiplying, we get that for each E_{ij}, the system of equations

$$\begin{cases} F_{11}E_{ij} = E_{ij}G_{22}^t \\ F_{22}E_{ij}^t = E_{ij}^t G_{11}^t \\ -F_{12}E_{ij}^t = E_{ij}G_{12}^t \\ -F_{21}E_{ij} = E_{ij}^t G_{21}^t \end{cases}$$

must be satisfied. The last two equations in the system allow us to deduce that F_{12}, F_{21}, G_{21}^t, and G_{12}^t are all zero matrices by the following lemma.

Lemma 3.4 (The adjoint ring of (L, L^t) is trivial) *Let $E_{ij} \in \mathbb{M}_{m\times n}$. If A, B are matrices such that for all $(i, j) \in \{1, \ldots, m\} \times \{1, \ldots n\}$,*

$$AE_{ij} = E_{ij}^t B$$

holds, then A and B are both zero matrices. This statement also applies when E_{ij} and E_{ij}^t are switched.

Proof. If $AE_{ij} = E_{ij}^t B$, then for all i, j

$$\left[\begin{array}{c|c|c} & \overset{j}{} & \\ 0 & a^i & 0 \\ & & \end{array}\right] = i \left[\begin{array}{c} 0 \\ \hline b_j \\ \hline 0 \end{array}\right].$$

For a fixed i, then, the entries of a^i are given by

$$A_{ki} = \begin{cases} b_{ij} & k = j \\ 0 & k \neq j \ . \end{cases}$$

Since this applies for all j, we conclude that for all i, $a^i = 0$ and therefore $A = 0$. Now $E_{ij}^t B = 0$, so $B = 0$ as well. In the case that E_{ij} and E_{ij}^t are switched, the proof proceeds in a similar manner or by noting that $\mathrm{Adj}(E_{ij}, E_{ij}^t) = \mathrm{Adj}(E_{ij}^t, E_{ij}) = 0$. □

Next we are left to consider the implications of the first two equations of the system. For notational simplicity, define $W = F_{11}, X = F_{22}, Y = G_{11}^t$, and $Z = G_{22}^t$. After multiplying, we get that for all i and for all j,

$$\left[\begin{array}{c|c|c} & \overset{j}{} & \\ 0 & w^i & 0 \\ & & \end{array}\right] = i \left[\begin{array}{c} 0 \\ \hline z_j \\ \hline 0 \end{array}\right] \text{ and } \left[\begin{array}{c|c|c} & \overset{i}{} & \\ 0 & x^j & 0 \\ & & \end{array}\right] = j \left[\begin{array}{c} 0 \\ \hline y_i \\ \hline 0 \end{array}\right].$$

Hence, $(F, G) \in \mathcal{M}_*$ if, and only if, for all i and for all $j, W_{ii} = Z_{jj}, X_{jj} = Y_{ii}$, and all other off-diagonal entries of X, Y, W, Z are 0. These deductions lead to the conclusion that the middle nucleus of the commutator when $a, c > 1$ is

$$\mathcal{M}_* = \left\{ \left(\begin{bmatrix} A \otimes I_a & 0 \\ 0 & B \otimes I_c \end{bmatrix}, \begin{bmatrix} B^t \otimes I_a & 0 \\ 0 & A^t \otimes I_c \end{bmatrix} \right) : A, B \in \mathbb{M}_b \right\}.$$

□

The left and right nuclei of the commutator bimap can be calculated similarly, as the following proposition details.

Proposition 3.5 *The commutator bimap of G_{abc} has left and right nuclei of $\{(kI_{ab+bc}, kI_{ac}) : k \in K\} \cong K$.*

The action of these nuclei on the commutator bimap amounts to nothing more than the action of scalar multiplication on the appropriate components, which is an action that any K-bimap admits by definition. For this reason, this is the smallest that $\mathcal{L}_*$ and $\mathcal{R}_*$ could possibly be for a K-bimap. This result does not come as a surprise because if there were additional actions that preserved the result of the commutator, these actions would need to act on the left (respectively, the right) of $\mathbb{M}_{a\times b} \oplus \mathbb{M}_{b\times c}$ and $\mathbb{M}_{a\times c}$ simultaneously. There are few non-trivial ring homomorphisms that act simultaneously on both an $(ab + bc)$-dimensional and an ac-dimensional vector space. Even so, a calculation shows these actions are not elements of the left or right nucleus.

The calculations to prove these results are similar to those for $\mathcal{M}_*$ but with appropriate modifications. For example, if $a = c = 1$, then the matrix corresponding to the commutation bimap is $\begin{bmatrix} 0_b & I_b \\ -I_b & 0_b \end{bmatrix}$. The left nucleus calculations concern actions on the U and W components of the bimap, so by slicing this matrix 'perpendicular to the V direction,' we obtain the slices of the tensor needed to calculate $\mathcal{L}_*$. In this case, slices are elements of $\mathbb{M}_{(ab+bc)\times c} = \mathbb{M}_{2b\times 1}$, which are vectors in K^{2b}. Specifically, the slices are

$$T_1 = -e_{b+1}, T_2 = -e_{b+2}, \ldots T_b = -e_{2b}, T_{b+1} = e_1, T_{b+2} = e_2, \ldots, T_{2b} = e_b.$$

Therefore $\lambda = (F^t, k) \in \mathbb{M}_{2b} \times K$ is an element of $\mathcal{L}_*$ precisely if for all i, $Fe_i = e_i k$. This is the case if, and only if, for all i, $f^i = ke_i$, leading to the conclusion that when $a = c = 1, \mathcal{L}_* = \{(kI_{2b}, k) : k \in K\}$. Calculations for the other $\mathcal{L}_*$ cases and $\mathcal{R}_*$ proceed in an analogous fashion.

Before we apply these $\mathcal{LMR}$ results, we investigate a universal construction that is formed using the components of $\mathcal{LMR}$-bimaps.

3.3 Versor Products and Universal Mapping Properties

Given a middle $\mathcal{M}$-linear bimap $\bullet : U \times V \rightarrowtail W$, there is a universal bimap through which $\bullet$ factors: the *tensor product* $\otimes : U \times V \rightarrowtail U \otimes_{\mathcal{M}} V$. Typically, the universal property of the tensor product is represented with the commutative diagram shown below.

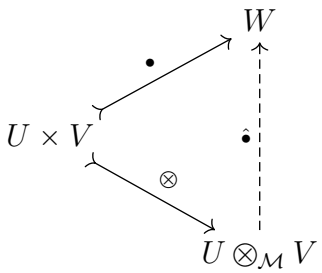

Figure 3.1: The standard commutative diagram used to illustrate the universal property of the tensor product.

However, to emphasize that this universality is intertwined with a homotopism from $\otimes$ to $\bullet$, we prefer to draw the equivalent bimap diagram shown on the next page. Take note of the fact that the tensor product $U \otimes_{\mathcal{M}} V$ is associated with a bimap $\otimes$ along with a universal property.

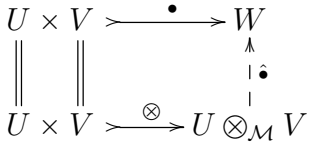

Figure 3.2: A bimap diagram from $\otimes$ to $\bullet$ illustrating the universal property of the tensor product.

As described in [6], the tensor product can be thought of as a *universal multiplication* of U and V. In a similar fashion, we can define a *universal left division* of U into W. Suppose $\circ : U \times V \rightarrowtail W$ is left $\mathcal{L}$-linear. Define a *left versor product* of U and W over $\mathcal{L}$ to be a K-vector space $U_{\mathcal{L}} \diagdown W$ which has an associated left $\mathcal{L}$-linear bimap $\diagdown : U \times U_{\mathcal{L}} \diagdown W \rightarrowtail W$ with the universal property that for any left $\mathcal{L}$-linear bimap $\bullet : U \times V \rightarrowtail W$, there exists a unique homomorphism $\vec{\bullet} : V \to U_{\mathcal{L}} \diagdown W$ such that $u \diagdown (v\vec{\bullet}) = u \bullet v$. Similarly, if $\circ$ is right $\mathcal{R}$-linear, we define a *right versor product* of V and W over $\mathcal{R}$ to be $W \oslash_{\mathcal{R}} V$ with the associated right $\mathcal{R}$-linear bimap $\oslash : W \oslash_{\mathcal{R}} V \times V \rightarrowtail W$ with the universal property that for any right $\mathcal{R}$-linear bimap $\bullet : U \times V \rightarrowtail W$, there exists a unique homomorphism $\overleftarrow{\bullet} : U \to U \oslash_{\mathcal{R}} W$ such that $(u\overleftarrow{\bullet}) \oslash v = u \bullet v$. As with the tensor product, the universal properties of the left and right versor products are best represented with bimap diagrams, as shown below.

(a) (b)

Figure 3.3: Bimap diagrams illustrating the universal property of the left versor product (a) and the right versor product (b).

For brevity, we also denote the homotopisms indicated in the above diagrams by $\vec{\bullet}$ and $\overleftarrow{\bullet}$, respectively. Before continuing, we illustrate the existence and uniqueness of versor products in the next two propositions.

Proposition 3.6 *Versors are unique up to isomorphism.*

Proof. This proof follows the typical uniqueness argument for a universal object. Suppose that $U_{\mathcal{L}} \oslash W$ and $(U_{\mathcal{L}} \oslash W)'$ are both left versors of U and W over $\mathcal{L}$. Because the associated bimaps $\oslash$ and $\oslash'$, respectively, are left $\mathcal{L}$-linear, there are unique homomorphisms $\vec{\oslash} : U \oslash W \to (U \oslash W)'$ and $\vec{\oslash} : (U \oslash W)' \to U \oslash W$. Composing these maps, we have that $\vec{\oslash}\vec{\oslash}' : U \oslash W \to U \oslash W$. Another endomorphism of $U \oslash W$ is the identity map. By the universality of the versor, $\vec{\oslash}\vec{\oslash}' = 1$, so $\vec{\oslash}^{-1} = \vec{\oslash}'$, and so $U_{\mathcal{L}} \oslash W \cong (U_{\mathcal{L}} \oslash W)'$ via $\vec{\oslash}$. A similar proof also works for right versors. □

Proposition 3.7 (Versors exist) $\mathrm{Hom}_{\mathcal{L}}(U, W)$ *with the associated bimap* $\oslash : U \times \mathrm{Hom}_{\mathcal{L}}(U, W) \rightarrowtail W$ *defined by* $u \oslash \varphi \mapsto u\varphi$ *gives a left versor. A right versor can be defined similarly using* $\mathrm{Hom}_{\mathcal{R}}(V, W)$.

Proof. $\mathrm{Hom}_{\mathcal{L}}(U, W)$ is a K-vector space and because the elements of $\mathrm{Hom}_{\mathcal{L}}(U, W)$ are $\mathcal{L}$-linear homomorphisms, $\oslash$ is also $\mathcal{L}$-linear. Let $\circ : U \times V \rightarrowtail W$ be a left $\mathcal{L}$-linear bimap. Define $\vec{\circ} : V \to \mathrm{Hom}_{\mathcal{L}}(U, W)$ by $v \mapsto (u \mapsto u \circ v)$. By hypothesis, $\circ$ is a left $\mathcal{L}$-linear bimap, so $u \mapsto u \circ v$ is left $\mathcal{L}$-linear map and thus an element of $\mathrm{Hom}_{\mathcal{L}}(U, W)$. It follows immediately from the definitions of $\oslash$ and $\vec{\circ}$ that $u \oslash (v\vec{\circ}) = u \circ v$. If there exists $\vec{\circ}'$ with the property that $u \oslash (v\vec{\circ}') = u \circ v$, then for all $u \in U$, $u \oslash (v\vec{\oslash}) = u \oslash (v\vec{\oslash}')$. By definition of $\oslash$, this occurs precisely when the homomorphisms, $v\vec{\oslash}$ and $v\vec{\oslash}'$, are equal, so $\vec{\oslash}$ is unique. An analogous argument proves the proposition for right versors. □

Remark 3.8 *The familiar* $\otimes$-Hom *adjunction,* $\mathrm{Hom}(A \otimes B, C) \cong \mathrm{Hom}(A, \mathrm{Hom}(B, C))$, *is now expressible as* $(A \otimes B) \oslash C \cong A \oslash (B \oslash C)$ *which is reminiscent of how* $\frac{c}{ab} = \frac{\frac{c}{b}}{a}$ *with numbers. This both justifies the* $\oslash$ *notation and solidifies the sense in which the left versor product can be viewed as a universal division.*

Corollary 3.9 (Right non-degeneracy of $\oslash$) *The left versor bimap $\oslash$ is right non-degenerate and the right versor bimap $\oslash$ is left non-degenerate.*

Proof. Consider the bimap $\oslash : U \times \mathrm{Hom}_{\mathcal{L}}(U, W) \rightarrowtail W$. Because $U \oslash W \cong \mathrm{Hom}_{\mathcal{L}}(U, W)$, and $\oslash$ is isotopic to any other left versor bimap, it suffices to show that this bimap is right non-degenerate. If $\varphi \in \mathrm{Hom}_{\mathcal{L}}(U, W)$ such that for all $u \in U, u \oslash \varphi = u\varphi = 0$, then $\varphi = 0$ because the 0 map is unique. Therefore, $\oslash$ is right non-degenerate. The right versor bimap $\oslash$ is shown to be left non-degenerate in a similar way. □

In light of these results, when utilizing the left versor product, we will use the $\mathrm{Hom}_{\mathcal{L}}(U, W)$ interpretation with the understanding that this is one of possibly many isomorphic representations.

Given an $\mathcal{LMR}$- bimap $\circ : U \times V \rightarrowtail W$, we can form the left versor, tensor, and right versor over $\mathcal{L}, \mathcal{M}$, and $\mathcal{R}$, respectively. At this point, a natural question arises: what is the 'largest' ring over which the versor or tensor can be formed? The answer to this query follows almost immediately by appealing to the fundamental connection we have established between bimaps, nuclei, versors, and tensors.

Theorem 3.10 (Universality of Scalar Rings) [6, Theorem 3.4] *If $\circ : U \times V \rightarrowtail W$ is an $\mathcal{LMR}$-bimap, then the image of the representation $\mathcal{L} \to \mathrm{End}(U) \times \mathrm{End}(W)$ lies in $\mathcal{L}_\circ$ and $\vec{\circ} : V \to U_{\mathcal{L}} \oslash W$ factors through $U_{\mathcal{L}_\circ} \oslash W$. Similarly, $\mathcal{M} \to \mathcal{M}_\circ$ and $\mathcal{R} \to \mathcal{R}_\circ$, and $\hat{\circ}$ and $\vec{\circ}$ factor through $U \otimes_{\mathcal{M}_\circ} V$ and $W \oslash_{\mathcal{R}_\circ} V$, respectively (See figure 3.4).*

3.4 Subgroups of G Modulo J Embed into Small Versors

In this section, we use a decomposition of the commutator bimap and its left nucleus to demonstrate that when S is a subgroup of G containing J, S/J embeds into $\mathbb{M}_{a\times b}\mathcal{L}_*\oslash\mathbb{M}_{b\times c} \cong \mathrm{Hom}_{\mathcal{L}_*}(\mathbb{M}_{a\times b}, \mathbb{M}_{a\times c}) \cong \mathbb{M}_{b\times c}$. This will then allow us to conclude that $*\big|_{\mathbb{M}_{a\times b}\times X/J}$ embeds naturally into ${}_{\mathcal{L}_*}\oslash$, which is a lemma that plays a part in the lifting proof. To begin, we investigate the structure of S/J for a subgroup $S \leqslant G$ containing J.

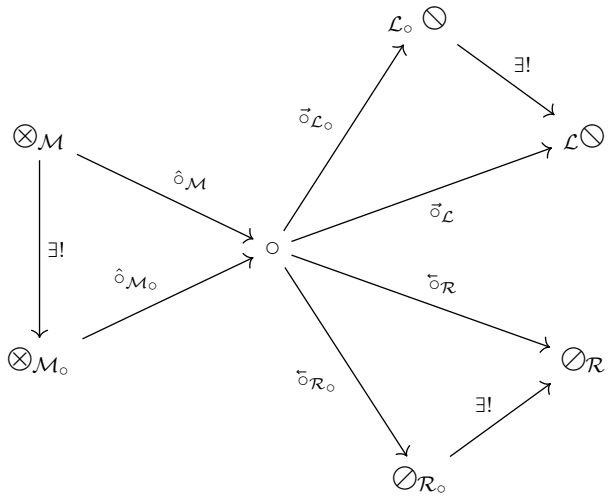

Figure 3.4: Commutative diagram of bimaps depicting the universality of scalars.

Lemma 3.11 *If S is a subgroup of G containing J then S/J is isomorphic to a subgroup of $\mathbb{M}_{b\times c}$.*

Proof. Define a map $\pi : \langle G_{abc}, \cdot\rangle \to \langle \mathbb{M}_{b\times c}, +\rangle$ by

$$\begin{bmatrix} I_a & U & W \\ 0 & I_b & V \\ 0 & 0 & I_c \end{bmatrix} \longmapsto V.$$

This is a group homomorphism because multiplying two elements in G corresponds to adding two matrices in $\mathbb{M}_{b\times c}$:

$$\begin{bmatrix} I_a & U & W \\ 0 & I_b & V \\ 0 & 0 & I_c \end{bmatrix} \begin{bmatrix} I_a & U' & W' \\ 0 & I_b & V' \\ 0 & 0 & I_c \end{bmatrix} = \begin{bmatrix} I_a & * & * \\ 0 & I_b & V+V' \\ 0 & 0 & I_c \end{bmatrix}.$$

As $\ker(\pi) = J$, and π is surjective, $G/J \cong \mathbb{M}_{b\times c}$. Take a subgroup $S \leqslant G$ that contains J. As $J \leqslant S$, $\pi(S) = S/J$ is a subgroup of $G/J \cong \mathbb{M}_{b\times c}$ by Noether's Isomorphism Theorem, hence quotients of subgroups containing J are isomorphic to subgroups of $\mathbb{M}_{b\times c}$. □

We now return to the commutation bimap of G,

$$[,] : (\mathbb{M}_{a\times b} \oplus \mathbb{M}_{b\times c}) \times (\mathbb{M}_{a\times b} \oplus \mathbb{M}_{b\times c}) \to \mathbb{M}_{a\times c}$$

given by $(U, V) \times (U', V') \mapsto UV' + U'V$. We need only consider *half* of this bimap as $[,]$ admits a maximal totally isotropic decomposition. Such a decomposition exists because there is an idempotent $e \in \mathbb{M}_{a\times b} \oplus \mathbb{M}_{b\times c}$ of maximal rank such that $(e, e^*) = (e, 1-e) \in \mathcal{M}_{[,]}$ (see section 3.2 for the structure of this ring). The following result indicates how such a decomposition would be formed from an idempotent middle nucleus pair.

Proposition 3.12 *Let* $\circ : U \times V \rightarrowtail W$ *be a bimap. If* $\mu = (F, G) \in \mathcal{M}_\circ$, *then* $\mathrm{Ker}(F) \circ \mathrm{Im}(G) = 0$ *and* $\mathrm{Im}(F) \circ \mathrm{Ker}(G) = 0$.

In the case of the commutator bimap, an idempotent is

$$e = \begin{bmatrix} I_{a\times b} & 0 \\ 0 & 0 \end{bmatrix},$$

where

$$I - e = \begin{bmatrix} 0 & 0 \\ 0 & I_{b\times c} \end{bmatrix}.$$

This idempotent is unique in the case that $a, c > 1$ and unique up to conjugation if $a = 1$ or $c = 1$ so this is the minimal decomposition of $[,]$. It is shown in [4] that such idempotents characterize the Brahana correspondence. In our context, this means the decomposition of $[,]$ is equivalent to the bimap given by usual matrix multiplication:

$$* : \mathbb{M}_{a\times b} \times \mathbb{M}_{b\times c} \to \mathbb{M}_{a\times c}$$

where $U * V' = UV'$. This aligns with our prior observation in section 2.5 that G is a Brahana group with respect to the bimap given by usual matrix multiplication.

To ensure this is the unique minimal decomposition of $[,]$, we assume $a, c > 1$ from now on.

Lemma 3.13 ($*$ is the left versor bimap over $\mathcal{L}_*$) $\mathcal{L}_* = \{(\lambda, \lambda) : \lambda \in \mathbb{M}_a\} = \mathbb{M}_a$ *and similarly* $\mathcal{M}_* = \mathbb{M}_b$ *and* $\mathcal{R}_* = \mathbb{M}_c$. *Additionally,* $\mathbb{M}_{a\times b}\mathcal{L}_* \oslash \mathbb{M}_{a\times c} \cong \mathbb{M}_{b\times c}$, *and* $* = {}_{\mathcal{L}_*}\oslash$.

Proof. By the associativity of matrix multiplication, $\mathbb{M}_a \hookrightarrow L_*$, $\mathbb{M}_b \hookrightarrow M_*$, and $\mathbb{M}_c \hookrightarrow R_*$. Now,

$$\begin{aligned} * \in \mathrm{Hom}_{\mathcal{L}_*\otimes\mathcal{R}_*}(\mathbb{M}_{a\times b} \otimes_{\mathcal{M}_*} \mathbb{M}_{b\times c}, \mathbb{M}_{a\times c}) &\cong \mathrm{Hom}_{\mathbb{M}_a\otimes\mathbb{M}_c}(\mathbb{M}_{a\times b} \otimes_{\mathbb{M}_b} \mathbb{M}_{b\times c}, \mathbb{M}_{a\times c}) \\ &\cong \mathrm{Hom}_{\mathbb{M}_a\otimes\mathbb{M}_c}(K^a \otimes_K K^c, \mathbb{M}_{a\times c}) \\ &\cong \mathrm{Hom}_{\mathbb{M}_c}(K^c, K^c) \\ &\cong K, \end{aligned}$$

so $*$ is in a one-dimensional space and is uniquely given by those $\mathcal{L}_* = \mathbb{M}_a, \mathcal{M}_* = \mathbb{M}_b, \mathcal{R}_* = \mathbb{M}_c$. In particular,

$$\begin{aligned} \mathbb{M}_{a\times b}\mathcal{L}_* \oslash \mathbb{M}_{b\times c} &\cong \mathrm{Hom}_{\mathbb{M}_a}(\mathbb{M}_{a\times b}, \mathbb{M}_{a\times c}) \\ &\cong \mathrm{Hom}_K(K^b, K^c) \\ &\cong \mathbb{M}_{b\times c} \end{aligned}$$

Consequently, $* = {}_{\mathcal{L}_*}\oslash$. □

For a subgroup $S \leqslant G$ containing J, define $*_S$ as the bimap

$$*_S : \mathbb{M}_{a\times b} \times S/J \rightarrowtail \mathbb{M}_{a\times c}$$

so that $*_S \coloneqq *\big|_{\mathbb{M}_{a\times b}\times S/J}$ is the restriction of $*$ in the V component to the subgroup S/J, which is isomorphic to a subgroup of $\mathbb{M}_{b\times c}$ by lemma 3.11.

Proposition 3.14 *If S is a subgroup of G containing J, then $*_S$ is homotopic to $* = {}_{\mathcal{L}_*}\oslash$ via a natural embedding.*

Proof. As $*_S$ is a restriction of $*$, $\mathcal{L}_{*_S} \leqslant \mathcal{L}_*$, and $*_S$ is left $\mathcal{L}_*$-linear. Therefore, there exists a unique homomorphism $\vec{*_S} : S/J \to \mathbb{M}_{b\times c} \cong \mathbb{M}_{a\times b\mathcal{L}_*} \oslash \mathbb{M}_{b\times c}$ such that

$$M \oslash (N\vec{*_S}) = M *_S N$$

by the universal property of the left versor. Because $M *_S N = M * N$, the definition of $\vec{*_S}$ guaranteees that $(1, \vec{*_S}, 1)$ gives a homotopism from $*_S$ to $*$. In particular, $\vec{*_S}$ is an injection due to the fact that S/J is isomorphic to a subgroup of $\mathbb{M}_{b\times c}$, so this homotopism is an embedding of $*_S$ into $*$. □

3.5 The Lifting Theorem

In this section, we lay out the hypotheses of theorem 1.5 and build the groundwork for the proof of this theorem. The theorem states that under certain assumptions, isomorphisms of subgroups of G lift to automorphisms of G that are unique up to a *central automorphism*. As the commutator bimap of G has the form $[,] : G/G' \times G/G' \rightarrowtail G'$, the central automorphisms are in the kernel of the commutator bimap.

The lifting theorem only concerns isomorphisms of subgroups *native* to G. Recall that a subgroup $X \leqslant G_{abc}$ such that $J_{abc} \leqslant X \leqslant G_{abc}$ is native to G_{abc} if whenever there is another generalized Heisenberg group $G_{a'b'c'}$ such that $J_{a'b'c'} \hookrightarrow X \hookrightarrow G_{a'b'c'}$, then $b \leqslant b'$. The Brahana correspondence between bimaps and generalized Heisenberg groups along with theorem 3.10 explain that X is native to G precisely when $\mathcal{L}_{*_X} = \mathcal{L}_*$. In fact, X is native to G_{abc}, if, and only if, the smallest versor product into which X/J embeds is $\mathbb{M}_{a\times b\mathcal{L}_*} \oslash \mathbb{M}_{a\times c} \cong \mathbb{M}_{b\times c}$. As we discuss in the closing remarks to this paper, non-native subgroups are asymptotically uncommon as a, b, c increase, so this result applies to most subgroups of the desired form.

Remark 3.15 *The assumption that $X' = Y' = \mathcal{W}$ is equivalent to the assumption that the commutator bimap $[,] : G/G' \times G/G' \rightarrowtail G'$ restricted to $X \times X$ and $Y \times Y$ is fully non-degenerate.*

Isomorphisms satisfying the assumptions of the lifting theorem give rise to isotopisms from $*_X$ to $*_Y$. To show this, we need a lemma.

Lemma 3.16 (Structure of Isomorphisms under which J is Invariant) *If $X, Y \in \mathcal{S}_i$ such that $X' = Y' = \mathcal{W}$ and $\varphi : X \to Y$ is a isomorphism under which J is invariant, then $\mathcal{U}^\varphi = \mathcal{U}$ and $\mathcal{W}^\varphi = \mathcal{W}$.*

Proof. As φ is a homomorphism, we have that $X'\varphi \leqslant Y'$, and equality follows because φ is an isomorphism. This gives us that $\mathcal{W}^\varphi = \mathcal{W}$, which in turn causes $\mathcal{U}^\varphi = \mathcal{U}$ as $J^\varphi = J$. □

Proposition 3.17 *Given $X, Y \in \mathcal{S}_i$ such that $X' = Y' = \mathcal{W}$ and an isomorphism $\varphi : X \to Y$ under which J is invariant, there is an isotopism from*

$$*_X : \mathbb{M}_{a\times b} \times X/J \to \mathbb{M}_{a\times c}$$

to

$$*_Y : \mathbb{M}_{a\times b} \times Y/J \to \mathbb{M}_{a\times c}.$$

Proof. By the lemma, α acts independently on $\mathcal{U}$, X/J, and $\mathcal{W}$. Therefore, there exist α, β, and γ so that φ can be written as the triple $(\alpha, \beta, \gamma) \in \mathrm{Aut}(\mathbb{M}_{a\times b}) \times \mathrm{Iso}(X/J, Y/J) \times \mathrm{Aut}(\mathbb{M}_{a\times b})$. As $\varphi\big|_{\mathbb{M}_{a\times b}} = \alpha, \varphi\big|_{X/J} = \beta$, and $\varphi\big|_{\mathbb{M}_{a\times c}} = \gamma$, we also have that for all $A \in \mathbb{M}_{a\times c}$ and for all $B \in X/J$,

$$A^\alpha * B^\beta = A^\varphi * B^\varphi = (A * B)^\varphi = (A * B)^\gamma,$$

so (α, β, γ) is an isotopism from $*_X$ to $*_Y$. □

Using this proposition, we can translate isomorphisms, $\varphi : X \to Y$, to isotopisms of $*_X$ and $*_Y$. Additionally, proposition 3.14 informs us that $*_X \cong *_Y$ both embed into $*$. Recall that $G \cong \mathrm{Grp}(*)$, so autotopisms of $*$ correspond to automorphisms of G. The bimaps $*_X$ and $*_Y$ are restrictions of $*$,

so if we can lift isotopisms between these restricted bimaps to autotopisms of $*$ itself, then Brahana correspondence would grant us automorphisms of G that are lifts of φ. For this reason, we set out to show that elements of $\mathrm{Iso}(*_X, *_Y)$ lift to elements of $\mathrm{Aut}(*_X, *_Y)$. To accomplish this, we use the bijection between isotopisms and what we call '$(\uparrow\downarrow\downarrow)$-isotopisms.'

3.6 $(\uparrow\downarrow\downarrow)$-isotopism

Given two bimaps $\circ : X_2 \times X_1 \rightarrowtail X_0$ and $\bullet : Y_2 \times Y_1 \rightarrowtail Y_0$, define a $(\uparrow\downarrow\downarrow)$-*homotopism* as a triple $(f_2, f_1, f_0) \in \mathrm{Hom}(Y_2, X_2) \times \mathrm{Hom}(X_1, Y_1) \times \mathrm{Hom}(X_0, Y_0)$ such that for all $x_1 \in X_2, x_2 \in X_2$,

$$x_2 \bullet {x_1}^g = ({x_2}^{f_2} \circ x_1)^{f_0}.$$

In other words, a $(\uparrow\downarrow\downarrow)$-homotopism is a triple of homomorphisms that satisfy the bimap diagram below.

$$\begin{array}{ccc} X_2 \times X_1 & \xrightarrow{\circ} & X_0 \\ {\scriptstyle f_2}\uparrow & \downarrow{\scriptstyle f_1} & \downarrow{\scriptstyle f_0} \\ Y_2 \times Y_1 & \xrightarrow{\bullet} & Y_0 \end{array}$$

Figure 3.5: A bimap diagram illustrating the defining property of a $(\uparrow\downarrow\downarrow)$-homotopism of bimaps.

We define $(\uparrow\downarrow\downarrow)$-*isotopism* similarly. The set of $(\uparrow\downarrow\downarrow)$-homotopisms and $(\uparrow\downarrow\downarrow)$-isotopisms from $\circ$ to $\bullet$ are denoted by $\Psi\,\mathrm{Hom}(\circ, \bullet)$ and $\Psi\,\mathrm{Iso}(\circ, \bullet)$, respectively. Intuitively, it seems as though $(\uparrow\downarrow\downarrow)$-isotopisms can be formed by flipping the appropriate arrow in an isotopism. This is, indeed, the case.

Proposition 3.18 (Bijection between isotopism and $(\uparrow\downarrow\downarrow)$-isotopism) *If* $\circ : X_2 \times X_2 \rightarrowtail X_0$ *and* $\bullet : Y_2 \times Y_1 \rightarrowtail Y_0$ *are both* K*-bimaps, then* $f = (f_2, f_1, f_0) \in \mathrm{Iso}(\circ, \bullet)$ *if, and only if,* $g = ({f_2}^{-1}, f_1, f_0) \in \Psi\,\mathrm{Iso}(\circ, \bullet)$.

Proof. On the one hand, f is an isotopism from $\circ$ to $\bullet$, if for all $x_2 \in X_2$ and $x_1 \in X_1$,

$$x_2{}^{f_2} \bullet x_1{}^{f_1} = (x_2 \circ x_1)^{f_0}.$$

On the other hand, g is a $(\uparrow\downarrow\downarrow)$-isotopism from $\circ$ to $\bullet$, if for all $x_1 \in X_1$ and $y_2 \in Y_2$,

$$y_2 \bullet x_1{}^{f_1} = (y_2{}^{f_2{}^{-1}} \circ x_1)^{f_0}.$$

If f is an isotopism, f_2 is an isomorphism, so $f_2{}^{-1}$ is also an isomorphism, making g into a candidate for a $(\uparrow\downarrow\downarrow)$-isotopism. In fact, by setting $y_2 = x_2^{f_2}$ we see that $g \in \Psi\,\mathrm{Iso}(\circ, \bullet)$. If g is a $(\uparrow\downarrow\downarrow)$-isotopism, we can make the same argument to show $f \in \mathrm{Iso}(\circ, \bullet)$. □

Corollary 3.19 *Under the same hypotheses as proposition 3.18, if* $f_2 \in \mathrm{Iso}(X_2, Y_2)$*, then* $f = (f_2, f_1, f_0) \in \mathrm{Hom}(\circ, \bullet)$ *if, and only if,* $g = (f_2{}^{-1}, f_1, f_0) \in \Psi\,\mathrm{Hom}(\circ, \bullet)$.

Remark 3.20 *In general, the category of homotopisms is not equivalent to the category of* $(\uparrow\downarrow\downarrow)$*-homotopisms, yet they have the same equivalence classes of isomorphism types (J. B. Wilson 2018, personal communication).*

As promised, these correspondences can be used to make progress toward finding the desired automorphism.

Proposition 3.21 *Consider the* K*-bimap* $\circ : U \times V \rightarrowtail W$ *and the corresponding left versor bimap* ${}_{\mathcal{L}\circ}\oslash : U \times U \oslash W \rightarrowtail W$*. Given* $(f_2, f_0) \in \mathrm{Aut}(U) \times \mathrm{End}(W)$*, there exists a unique homotopism* $(f_2, f_1, f_0) \in \mathrm{Hom}(\circ, \oslash)$*. In particular,* $f_1 = \vec{\circ} := f_2 \oslash f_0$.

Proof. Define $g : V \to U \oslash W$ such that for all $u \in U$,

$$u \oslash v^g = (u^{f_2{}^{-1}} \circ v)^{f_0}.$$

Note that g is well-defined: if $v = \hat{v}$, then for all $u \in U$, $u \oslash v^g = u \oslash \hat{v}^g$ so $v^g = \hat{v}^g$ because $\oslash$ is right non-dengenerate and the $u's$ 'cancel' by lemma 2.1. Also, g is a K-linear map because $\circ$ is

K-bilinear and f_0 is K-linear. If $v, \hat{v} \in V$ and $k \in K$ then for all $u \in U$,

$$\begin{aligned} u \oslash (v + \hat{v})^g &= [u^{{f_2}^{-1}} \circ (v + \hat{v})]^{f_0} \\ &= [(u^{{f_2}^{-1}} \circ v) + (u^{{f_2}^{-1}} \circ \hat{v})]^{f_0} \\ &= (u^{{f_2}^{-1}} \circ v)^{f_0} + (u^{{f_2}^{-1}} \circ \hat{v})^{f_0} \\ &= u \oslash v^g + u \oslash \hat{v}^g, \end{aligned}$$

and

$$\begin{aligned} u \oslash (kv)^g &= [u^{{f_2}^{-1}} \circ (kv)]^{f_0} \\ &= [k(u^{{f_2}^{-1}} \circ v)]^{f_0} \\ &= k[u^{{f_2}^{-1}} \circ v]^{f_0} \\ &= k[u \oslash v^g]. \end{aligned}$$

The definition of g ensures that (f_2^{-1}, g, f_0) is a $(\uparrow\downarrow\downarrow)$-homotopism from $\circ$ to $\oslash$, which corresponds to $(f_2, g, f_0) \in \mathrm{Hom}(\circ, \oslash)$ by the previous corollary. In fact, by the universal property of the left versor product, $g = \vec{\circ}$ is unique, so this is the unique homotopism from $\circ$ to $\oslash$ formed using both f_2 and f_0. To emphasize that g depends on f_2, f_0, and is unique to the left versor product over $\mathcal{L}_\circ$ we define $g := f_2 \oslash f_0$. □

Corollary 3.22 *If X and Y are native to G, then an isotopism (α, β, γ) from $*_X$ to $*_Y$ lifts to a unique autotopism $(\alpha, \alpha \oslash \gamma, \gamma)$ of $*$.*

Proof. In $*_X$ and $*_Y$, the U and W components are the same, so $(\alpha, \gamma) \in \mathrm{Aut}(U) \times \mathrm{Aut}(W)$. These are also the U and W components of $*$, which is the left versor bimap corresponding to $*_X$ and $*_Y$ because X, Y are native to G, which implies $\mathcal{L}_{*_X} = \mathcal{L}_*$. The left versor bimap corresponding to $* = \oslash$ is itself, so by the previous proposition, $(\alpha, \alpha \oslash \gamma, \gamma)$ is the unique endotopism of $*$. In fact, $\alpha \oslash \gamma = \vec{\oslash}$ is the identity map, so $(\alpha, \alpha \oslash \gamma, \gamma)$ is an autotopism of $*$ as claimed. □

3.7 Proof of the Lifting Theorem

With these results in tow, we are finally in a position to prove the titular lifting theorem.

Proof of Theorem 1.5. We begin with an isomorphism $\varphi : X \to Y$ such that J is φ-invariant, which we will lift to an automorphism of G.

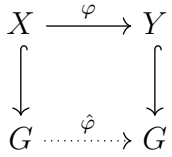

Figure 3.6: A commutative diagram depicting the desired outcome of the proof.

By hypothesis, $X' = Y' = \mathcal{W}$, so the bimap functoriality outlined in proposition 3.17 allows us to conclude that $*_X \cong *_Y$ via $\varphi = (\alpha, \beta, \gamma)$. Additionally, proposition 3.14 tells us that $*_X$ and $*_Y$ each embed uniquely into $*$. Finally, by corollary 3.22, the isotopism (α, β, γ) lifts uniquely to an autotopism of $*$, $\Phi = (\alpha, \alpha \oslash \gamma, \gamma)$. All of this is shown in the diagram below.

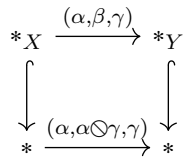

Figure 3.7: A commutative diagram of bimaps showing how $\varphi = (\alpha, \beta, \gamma)$ is lifted to $\Phi = (\alpha, \alpha \oslash \gamma, \gamma)$.

Next, we invoke the Brahana correspondance (see section 2.5) and apply the functor that maps bimaps to groups to the previous diagram. The result is a diagram of (Brahana) groups, as shown on the next page.

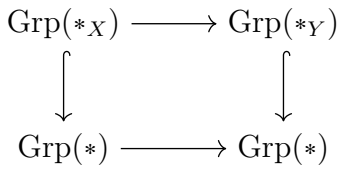

Figure 3.8: The resulting commutative diagram of groups when Brahana correspondence is applied to the previous diagram in figure 3.7.

Because G is isomorphic to a Brahana group with corresponding bimap $*$, there is an isomorphism $\mu : G \to \mathrm{Grp}(*)$. Similarly, $X \cong \mathrm{Grp}(*_X)$ and $Y \cong \mathrm{Grp}(*_Y)$. These isomorphisms allow us to merge the diagrams in figures 3.6 and 3.8 into a new diagram.

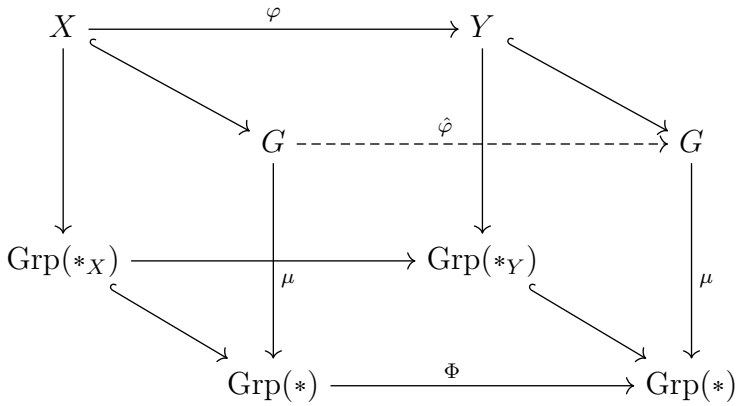

Figure 3.9: The commutative diagram obtained by combining the diagrams in figures 3.6 (top of cube) and 3.8 (bottom of cube).

Finally, we have an automorphism of G, $\hat{\varphi} = \mu^{-1}\Phi\mu$, which is a lift of φ as we can deduce from the injections in the diagram. This automorphism is unique up to a central automorphism [4, Proposition 3.8iii]. □

Chapter 4

Toward an Asymptotic Lower Bound

We now use the prior lifting result alongside versors and the nuclei of $*$ in order to establish a lower bound on the number of isomorphism classes of subgroups of $\mathrm{GL}_d(p^e)$. The lifting theorem from the previous chapter states that if $X, Y \in \mathcal{S}_i$, are native to G, then any isomorphism $\varphi : X \to Y$ under which J is invariant lifts to a unique automorphism of G up to a central automorphism. As we argue in the closing remarks to this paper, non-native subgroups are asymptotically rare. For this reason, we now ignore the hypothesis that subgroups are native because including all subgroups will not substantially affect our asymptotic counting.

Let $\mathrm{Aut}_J(G) = \{\varphi \in \mathrm{Aut}(G) : J\varphi = J\}$. By the lifting theorem, we have the following corollary that allows us to count isomorphism classes of the elements of $\mathcal{S}_i$.

Corollary 4.1 $|\mathcal{S}_i/_{\cong}| = \#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)}$-*orbits of* $\mathcal{S}_i)$.

Now, determining the number of isomorphism classes of $\mathcal{S}_i$ is equivalent to counting the number of orbits of $\mathcal{S}_i$ under the action of $\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)}$. The pigeonhole principle leads us to a lower bound for the number of these orbits.

Corollary 4.2 $\dfrac{\#\mathcal{S}_i}{\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})} \leqslant \#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)}$-*orbits of* $\mathcal{S}_i)$.

Proof. The minimum number of orbits occurs when the orbits are as big as possible. The largest an orbit can be is $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$, and in the case that all orbits are this size, the pigeonhole principle informs us that the largest orbit must have size

$$\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)}) = \left\lceil \frac{\#\mathcal{S}_i}{\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})\text{-orbits}} \right\rceil .$$

Therefore, the number of $(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$-orbits of $\mathcal{S}_i$ is no less than

$$\left\lceil \frac{\#\mathcal{S}_i}{\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})} \right\rceil \geqslant \frac{\#\mathcal{S}_i}{\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})}.$$

□

This inequality informs us that a lower bound on the number of isomorphism classes of $\mathcal{S}_i$ can be obtained by dividing a lower bound on $\#\mathcal{S}_i$ by an upper bound on $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$. The next two sections are devoted to bounding these quantities.

4.1 A Lower Bound for $\#S_i$

Using the bijection between the elements of $\mathcal{S}_i$ and subgroups of $\mathbb{M}_{b\times c}$ (see lemma 3.11), counting $\#\mathcal{S}_i$ reduces to counting subspaces of a vector space over $K = \mathbb{Z}_q$. As such, a lower bound for $\#\mathcal{S}_i$ can be determined using the following result.

Proposition 4.3 (Counting Vector Subspaces) *Let V be a d-dimensional vector space over $\mathbb{F}_q$, q a prime power. A lower bound for the number of vector subspaces $W \leqslant V$ with dimension $k \leqslant d$ is $q^{k(d-k)}$.*

Proof. We must pick K linearly independent basis elements from V, which contains q^d elements. Our first basis element can be any element, aside from 0, so we have $q^d - 1$ choices. When choosing the ith basis element ($1 < i \leqslant k$), we need to choose an element that is linearly independent of $\langle b_1, ..., b_{i-1}\rangle$, which has cardinality q^{i-1} (count the number of $(i-1)$-tuples of coefficients of the elements of the span). Therefore, there are $q^d - q^{i-1}$ choices for the ith basis element. Combining this information together, we conclude that there are $\prod_{i=0}^{k-1} q^d - q^i$ bases for k-dimensional subspaces of V. However, each distinct k-dimensional subspace has $\prod_{i=0}^{k} q^k - q^i$ bases by the previous logic. This informs us that the number of vector subspaces $W \leqslant V$ with dimension $k \leqslant d$ is

$$\frac{\prod_{i=0}^{k-1} q^d - q^i}{\prod_{i=0}^{k} q^k - q^i}.$$

For all i, note that $\dfrac{q^d - q^i}{q^k - q^i} \geqslant \dfrac{q^d}{q^k} = q^{d-k}$. The above product has k terms, so a lower bound on the number of k-dimensional vector spaces is $(q^{d-k})^k = q^{k(d-k)}$. □

Proposition 4.4 *For $i \neq 0$, set $k = \dfrac{b^2c^2}{i}$ and define*

$$f(b,c) = \begin{cases} \left(\dfrac{1}{k} - \dfrac{1}{k^2}\right) b^2c^2, & i \neq 0 \\ 0, & i = 0. \end{cases}$$

A lower bound for $\#\mathcal{S}_i$ is $q^{f(b,c)}$.

Proof. By lemma 3.11, subgroups of G containing J are in bijection with subgroups of $\mathbb{M}_{b\times c}$. In particular, a subgroup of G/J with order i corresponds to a subgroup of G that contains J of order $i|J|$. From this, we note that

$$\#\mathcal{S}_i = \#\left(\text{Subgroups of } \mathbb{M}_{b\times c} \text{ of order } \frac{i}{|J|}\right).$$

As $\mathbb{M}_{b\times c}$ is a bc-dimensional vector space over $K = \mathbb{F}_q$, proposition 4.3 informs us that

$$\#\left(\text{Subgroups of } \mathbb{M}_{b\times c} \text{ of order } \frac{i}{|J|}\right) = q^{f(b,c)}$$

where

$$f(b,c) = \frac{i}{|J|}\left(bc - \frac{i}{|J|}\right) = \frac{i}{bc}\left(bc - \frac{i}{bc}\right).$$

The order of a subgroup of $\mathbb{M}_{b\times c}$ is in between 0 and bc, so $0 \leqslant \dfrac{i}{bc} \leqslant bc$. If $i = 0$, then $f(b,c) = 0$. Otherwise, $\dfrac{i}{bc} \neq 0$, and we can write $\dfrac{i}{bc} = \dfrac{1}{k}bc$ where $k = \dfrac{b^2c^2}{i}$. In this case,

$$f(b,c) = \frac{1}{k}bc\left(bc - \frac{1}{k}bc\right) = \left(\frac{1}{k} - \frac{1}{k^2}\right)b^2c^2,$$

as claimed. □

4.2 An Upper Bound for $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$

A naïve upper bound for $\#\,\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)}$ is easy to obtain. For $\varphi \in (\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$, $J\varphi = J$ so we conclude that φ induces an automorphism of $G/J \cong \mathbb{M}_{b\times c}$. There are $q^{(bc)^2}$ such automorphisms. Using this as an upper bound for $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$, and the lower bound for $\#\mathcal{S}_i$ from proposition 4.4, we calculate a lower bound for $|\mathcal{S}_i/_{\cong}|$ of

$$\frac{\#\mathcal{S}_i}{\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})} = \frac{q^{f(b,c)}}{q^{b^2c^2}} = q^{\hat{f}(b,c)}$$

where $\hat{f}(b,c) = \left(\dfrac{1}{k} - \dfrac{1}{k^2}\right)b^2c^2 - b^2c^2 < 0$. This gives us a trivial lower bound so, a naïve upper bound for $\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)}$ is not enough to establish the desired lower bound for $|\mathcal{S}_i/_{\cong}|$. From this calculation, we see that the upper bound we find for $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$ must have an exponent of degree less than 4 to be useful. To find such an upper bound, we first establish a correspondence between $\mathrm{Aut}_J(G)$ and the autotopisms of $*$, which allows us to count autotopisms instead of automorphisms.

Lemma 4.5 *If* $(f, g, h) \in \mathrm{End}(\mathbb{M}_{a\times b}) \times \mathrm{End}(\mathbb{M}_{b\times c}) \times \mathrm{End}(\mathbb{M}_{a\times c})$ *and* $\psi : G \to G$ *is defined by*

$$\begin{bmatrix} I_a & U & W \\ 0 & I_b & V \\ 0 & 0 & I_c \end{bmatrix} \longmapsto \begin{bmatrix} I_a & U^f & W^h \\ 0 & I_b & V^g \\ 0 & 0 & I_c \end{bmatrix},$$

then ψ *is a group automorphism of* G *precisely when* (f, g, h) *is an autotopism of* $*$.

Proof. Let $M = \begin{bmatrix} I_a & U & W \\ 0 & I_b & V \\ 0 & 0 & I_c \end{bmatrix}, N = \begin{bmatrix} I_a & \hat{U} & \hat{W} \\ 0 & I_b & \hat{V} \\ 0 & 0 & I_c \end{bmatrix} \in G$. Then $M^\psi N^\psi = (MN)^\psi$ is the same as

$$\begin{bmatrix} I_a & U^f & W^h \\ 0 & I_b & V^g \\ 0 & 0 & I_c \end{bmatrix} \begin{bmatrix} I_a & \hat{U}^f & \hat{W}^h \\ 0 & I_b & \hat{V}^g \\ 0 & 0 & I_c \end{bmatrix} = \begin{bmatrix} I_a & (U+\hat{U})^f & (W+\hat{W}+U\hat{V})^h \\ 0 & I_b & (V+\hat{V})^g \\ 0 & 0 & I_c \end{bmatrix}$$

or

$$\begin{bmatrix} I_a & U^f + \hat{U}^f & W^h + \hat{W}^h + U^f\hat{V}^g \\ 0 & I_b & V^g + \hat{V}^g \\ 0 & 0 & I_c \end{bmatrix} = \begin{bmatrix} I_a & (U+\hat{U})^f & W^h + \hat{W}^h + (UV)^h \\ 0 & I_b & (V+\hat{V})^g \\ 0 & 0 & I_c \end{bmatrix}.$$

The equations $U^f + \hat{U}^f = (U+\hat{U})^f$, $V^g + \hat{V}^g = (V+\hat{V})^g$, and $W^h + \hat{W}^h = (W+\hat{W})^h$ are satisfied because f, g, and h are homomorphisms. Therefore, ψ is a group homomorphism if, and only if, for all $U \in \mathbb{M}_{a\times b}$ and $V \in \mathbb{M}_{b\times c}$ $U^f V^g = (UV)^h$, but this is exactly what it means for (f, g, h) to be an autotopism of $*$. □

We next demonstrate that these autotopisms act as ring automorphisms on the nuclei of $*$ and then appeal to the Skolem-Noether Theorem to determine the structure of these ring automorphisms. Recall from lemma 3.13 that the nuclei of $*$ are $\mathbb{M}_a, \mathbb{M}_b$, and $\mathbb{M}_c$, respectively, so by

demonstrating that the autotopisms of $*$ act on these relatively large rings, we are able to effectively determine a sharper upper bound on $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$ that was previously impossible using the naïve counting methods outlined at the beginning of the section.

Lemma 4.6 (Autotopisms of a bimap act on the nuclei) *Let* $\circ : U \times V \rightarrowtail W$ *be a bimap given by* $(u, v) \mapsto u \circ v$. *Then* $\mathrm{Aut}(\circ)$ *acts on* $\mathcal{L}_\circ, \mathcal{M}_\circ$, *and* $\mathcal{R}_\circ$ *as ring automorphisms.*

Proof. Let $\phi \in \mathrm{Aut}(\circ)$ and $\lambda \in \mathcal{L}_\circ$. Define the action of ϕ on λ as $\lambda^\phi = (\,\phi|_U^{-1}\ \lambda|_U\ \phi|_U\,,\ \phi|_W^{-1}\ \lambda|_W\ \phi|_W)$. Because λ^ϕ is defined by conjugating λ by an automorphism, $\lambda^\phi \in \mathrm{End}(U) \times \mathrm{End}(W)$, so we only need to prove that $\lambda^\phi \in \mathcal{L}_\circ$. To accomplish this, we show that for all $u \in U, v \in V$,

$$(\phi|_U^{-1}\ \lambda|_U\ \phi|_U)(u) \circ v = (\phi|_W^{-1}\ \lambda|_W\ \phi|_W)(u \circ v)$$

Starting from the right hand side,

$$\begin{aligned}
(\phi|_W^{-1}\ \lambda|_W\ \phi|_W)(u \circ v) &= (\phi|_W^{-1}\ \lambda|_W\,(\phi|_U\,(u) \circ \phi|_V\,(v)) \\
&= \phi|_W^{-1}\,(\lambda|_U\ \phi|_U\,(u) \circ \phi|_V\,(v)) \\
&= \phi|_U^{-1}\ \lambda|_U\ \phi|_U\,(u) \circ \phi|_V^{-1}\ \phi|_V\,(v) \\
&= \phi|_U^{-1}\ \lambda|_U\ \phi|_U\,(u) \circ v
\end{aligned}$$

so $\lambda^\phi \in \mathcal{L}_\circ$ and $\mathrm{Aut}(\circ)$ acts on $\mathcal{L}_\circ$. The proof that $\mathrm{Aut}(\circ)$ acts on the other two nuclei as ring automorphisms is accomplished similarly. □

In particular, $\mathcal{L}_* = \mathbb{M}_a, \mathcal{M}_* = \mathbb{M}_b$, and $\mathcal{R}_* = \mathbb{M}_c$ so the autotopisms of $*$ therefore act on simple rings as ring automorphisms. In fact, for each $n \in \mathbb{N}$, $\mathbb{M}_n$ for $n \in \mathbb{N}$ is a *central-simple algebra*, meaning $\mathbb{M}_n$ is a simple, finite-dimensional algebra over its center, $Z(\mathbb{M}_n) \cong K$.

Corollary 4.7 [6, Corollary 1.5] *There is a homomorphism* $\mathrm{Aut}(*) \to (\mathrm{Aut}(\mathcal{L}_*) \times \mathrm{Aut}(\mathcal{M}_*) \times \mathrm{Aut}(\mathcal{R}_*)) \rtimes \mathrm{Gal}(K)$ *with kernel* 1.

The nuclei are central-simple algebras over K, so the Skolem-Noether theorem alongside the previous corollary allows us to pinpoint the ring automorphisms and then determine an upper bound on $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$.

Theorem 4.8 (The Skolem-Noether Theorem) *Let K be a field and let $f, g : A \to B$ be K-linear homomorphisms from the K-algebra A to the K-algebra B. If A is simple, and B is central-simple over K, then there exists an invertible element $b \in B$ such that for all $a \in A$ $f(a) = b \cdot g(a) \cdot b^{-1}$.*

Corollary 4.9 *There is a monomorphism* $\mathrm{Aut}(*) \to (\mathrm{GL}_a(K) \times \mathrm{GL}_b(K) \times \mathrm{GL}_c(K)) \rtimes \mathrm{Gal}(K)$.

Proof. The elements $(\phi_1, \phi_2, \phi_3) \in (\mathrm{Aut}(\mathcal{L}_*) \times \mathrm{Aut}(\mathcal{M}_*) \times \mathrm{Aut}(\mathcal{R}_*)) \rtimes \mathrm{Gal}(K)$ are K-linear and ring automorphisms by proof of the previous corollary, so they are also K-algebra homomorphisms. The Skolem-Noether Theorem now applies and leads us to conclude that the ring automorphisms are given by conjugating automorphisms of the form $\phi_i\sigma_i^{-1}$ by the invertible $n \times n$ matrices where $n = a, b,$ or c. The claim follows. □

Using the fact that $\mathrm{Aut}(*)$ acts on $\mathrm{Aut}(\mathbb{M}_{a\times b\mathcal{L}_*} \oslash \mathbb{M}_{a\times c})$, we can prove:

Theorem 4.10 *There is a homomorphism* $\mathrm{Aut}_J(*) \hookrightarrow (\mathrm{GL}_b(K) \times \mathrm{GL}_c(K)) \rtimes \mathrm{Gal}(K)$.

Proof. The autotopisms of $*$ act on $\mathrm{Aut}(\mathbb{M}_{b\times c}) \cong \mathrm{Aut}(\mathbb{M}_{a\times b\mathcal{L}_*} \oslash \mathbb{M}_{a\times c})$ by lemmas 3.13 and 4.6. As $\mathbb{M}_{a\times b\mathcal{L}_*} \oslash \mathbb{M}_{a\times c}$, is a versor product over $\mathcal{L}_*$, $\mathcal{L}_*$, must be fixed under the action of an autotopism of $*$. Now, corollary 4.9 combined with this finding completes the proof. □

Corollary 4.11 *An upper bound for* $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$ *is* $e \cdot q^{b^2+c^2}$.

Proof. Using the theorems of this section, we have that $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)}) = \#\,\mathrm{Aut}(*) \leqslant |\,\mathrm{GL}_b(K) \times \mathrm{GL}_c(K) \rtimes \mathrm{Gal}(K)| = |\,\mathrm{GL}_b(K)| \cdot |\,\mathrm{GL}_c(K)| \cdot |\,\mathrm{Gal}(K)|$. By counting all $b \times b$ and $c \times c$ matrices, respectively, over K, we see that $|\,\mathrm{GL}_b(K)| \leqslant q^{b^2}$ and $|\,\mathrm{GL}_c(K)| \leqslant q^{c^2}$. Next, $\mathrm{Gal}(K) = \mathrm{Gal}(\mathbb{F}_{p^e}/\mathbb{F}_p)$ is a cyclic subgroup of order e generated by the Frobenius automorphism, which has order e. Therefore, $|\,\mathrm{Gal}(K)| = e$. Putting these results together, we find that an upper bound for $\#\,\mathrm{Aut}(G)$ is $e \cdot q^{b^2+c^2}$. □

4.3 Optimization

Due to the fact that the upper bound for $\#(\mathrm{Aut}_J(G)/\mathcal{C}_{\mathrm{Aut}(G)})$ from the previous section has an exponent of degree 2, this can be used to obtain a non-trivial lower bound for $|\mathcal{S}_i/_{\cong}|$, which we now determine.

Proposition 4.12 *The number of isomorphism classes of subgroups of G containing J with order $i = \dfrac{b^2c^2}{k}$ is at least $p^{g(b,c,e,k)}$ where*

$$g(b,c,e,k) = \left(\frac{1}{k} - \frac{1}{k^2}\right) b^2c^2e - (b^2+c^2)e - \log_p e.$$

Proof. Using proposition 4.4 and corollary 4.11 the number of isomorphism classes of subgroups of G containing J is at least

$$\frac{q^{f(b,c)}}{eq^{b^2+c^2}}, \text{ where } f(b,c) = \left(\frac{1}{k} - \frac{1}{k^2}\right) b^2c^2.$$

Re-writing these powers with a base of p, this becomes

$$\frac{p^{f(b,c)e}}{p^{b^2e+c^2e+\log_p e}} = p^{f(b,c)e-(b^2+c^2)e-\log_p e},$$

which is the stated bound. □

This gives $\#(\mathcal{S}_{p^j})$, so in order to find a lower bound for $\displaystyle\sum_{j=0}^{\log_p |G|} |\mathcal{S}_{p^j}/_{\cong}|$, we determine a lower bound for the size of the dominant summand by maximizing

$$g(b,c,e,k) = \left(\frac{1}{k} - \frac{1}{k^2}\right) b^2c^2e - (b^2+c^2)e - \log_p e$$

over b, c, and k. We maximize $\left(\dfrac{1}{k} - \dfrac{1}{k^2}\right) b^2c^2e$, because asymptotically this term dominates g.

Before doing so, we will normalize the variables. To this end, define $s = b + c$ and let $x = \dfrac{b}{s}$, $y = \dfrac{c}{s}$ and set

$$G(k, x, y) = \frac{\left(\dfrac{1}{k} - \dfrac{1}{k^2}\right) b^2 c^2 e}{s^2} = e\left(\frac{1}{k} - \frac{1}{k^2}\right) x^2 y^2.$$

As the original variables have been normalized, $x + y = 1$, so we maximize $F(x, y)$ subject to the constraint $c(x, y) = x + y = 1$. To accomplish this, we turn to the method of Lagrange multipliers and search for a point that satisfies

$$\nabla G = \lambda \nabla c.$$

This is equivalent to solving the following system of equations:

$$\begin{cases} 2e\left(\dfrac{1}{k} - \dfrac{1}{k^2}\right) xy^2 = \lambda \\ 2e\left(\dfrac{1}{k} - \dfrac{1}{k^2}\right) x^2 y = \lambda \\ e\left(\dfrac{2}{k^3} - \dfrac{1}{k^2}\right) x^2 y^2 = 0 \\ x + y = 1 \end{cases} \quad \equiv \quad \begin{cases} xy^2 = x^2 y \\ e\left(\dfrac{2}{k^3} - \dfrac{1}{k^2}\right) x^2 y^2 = 0 \\ x + y = 1. \end{cases}$$

After doing some arithmetic and noting that $x, y \neq 0$, we determine that $x = y$ and $k = 2$ solve the system and therefore maximize G.

We would like to state the a lower bound of the number of isomorphism classes of subgroups of G containing J in terms of the dimension of elements of $\mathrm{GL}_d(p^e) \geqslant G_{abc}$, so we let $d = a + b + c$, where $a > 1$ is a constant. We find that by setting $s = d - a$, the maximum occurs when $b = c =$

$\frac{s}{2} = \frac{d}{2} - \frac{a}{2}$. Both b and c are squared in the function being maximized, so we want b, c as large as possible to obtain a maximum. To this end, set $a = 2$. Now, a lower bound on the number of isomorphism classes of subgroups of $\mathrm{GL}_d(p^e)$ is

$$p^{b^2c^2e/4-(b^2+c^2)e^2-\log_p e} = p^{d^4e/64-O(d^2)}.$$

This is precisely the lower bound of Theorem 1.1 that we set out to prove.

Chapter 5

A Closing Remark

As a closing remark, we explain why non-native subgroups of G containing J are asymptotically uncommon. Fix $*$ to be the decomposition of the commutator bimap given in section 3.4 (the bimap for regular matrix multiplication). If X is a native subgroup of G, such that $*_X$ embeds into ${}_{\mathcal{L}}\oslash$, then $\mathcal{L} \leqslant \mathcal{L}_*$. However, in the case that X is non-native to G, $*_X$ may embed into ${}_{\mathcal{L}_{*'}}\oslash$ where $\mathcal{L}_* \nleqslant \mathcal{L}_{*'}$. Now, $\mathcal{L}_{*'}$ has $\mathcal{L}_*$ as a subalgebra so $\mathcal{L}_{*'}$ is an $\mathbb{M}_a$-bimodule (Recall that $\mathcal{L}_* = \mathbb{M}_a$ by proposition 3.13). Heuristically, $X/J \hookrightarrow \mathbb{M}_{a\times b\mathcal{L}} \oslash \mathbb{M}_{a\times c}$ is unlikely to satisfy more linear equations than minimally required by $\mathcal{L}_*$. Therefore, the most common eventuality is that $\mathcal{L}_{*'} = \mathcal{L}_*$ and X is native to G. Thus, including the non-native subgroups would not have influenced the asymptotic lower bound on the number of isomorphism classes of subgroups. A formal proof is as follows.

Due to the simplicity of $\mathbb{M}_a$, we conclude that $\mathcal{L}_{*'} = \bigoplus_{i=1}^{r} \mathbb{M}_a$ and hence $\dim(\mathcal{L}_{*'}) = a^2 r$. On top of this, $\mathcal{L}_* \hookrightarrow \mathbb{M}_{ab}$ via $A \mapsto A \otimes I_b$, so $\mathcal{L}_{*'}$ must be $\mathbb{M}_a$-bisubmodule of $\mathbb{M}_{ab}$. There are 2^b such submodules, which is far fewer than $|\mathbb{M}_{ab}| = q^{(ab)^2}$, and as such non-native subgroups are asymptotically scarce.

References

[1] Simon R. Blackburn, Peter M. Neumann, and Geetha Venkataraman, *Enumeration of finite groups*, Cambridge Tracts in Mathematics, vol. 173, Cambridge University Press, Cambridge, 2007. MR2382539

[2] H. R. Brahana, *Metabelian groups and trilinear forms*, Duke Math. J. **1** (1935), no. 2, 185–197. MR1545875

[3] Mark L. Lewis and James B. Wilson, *Isomorphism in expanding families of indistinguishable groups*, Groups Complex. Cryptol. **4** (2012), no. 1, 73–110. MR2921156

[4] James B. Wilson, *Decomposing p-groups via Jordan algebras*, J. Algebra **322** (2009), no. 8, 2642–2679. MR2559855

[5] ———, *Division, adjoints, and dualities of bilinear maps*, Comm. Algebra **41** (2013), no. 11, 3989–4008. MR3169502

[6] ———, *On automorphisms of groups, rings, and algebras*, Comm. Algebra **45** (2017), no. 4, 1452–1478. MR3576669