POLYNOMIAL-TIME COMPUTATION IN MATRIX GROUPS

by

TAKUNARI MIYAZAKI

A DISSERTATION

Presented to the Department of Computer
and Information Science
and the Graduate School of the University of Oregon
in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy

December 1999

"Polynomial-Time Computation in Matrix Groups," a dissertation prepared by Takunari Miyazaki in partial fulfillment of the requirements for the Doctor of Philosophy degree in the Department of Computer and Information Science. This dissertation has been approved and accepted by:

Eugene M Luks

Dr. Eugene M. Luks, Chair of the Examining Committee

11/30/99

Date

Commitee in charge:

Dr. Eugene M. Luks, Chair
Dr. Andrzej Proskurowski
Dr. Christopher B. Wilson
Dr. Charles R. B. Wright

Accepted by:

Marian Friestad

Dean of the Graduate School

An Abstract of the Dissertation of

Takunari Miyazaki for the degree of Doctor of Philosophy
in the Department of Computer and Information Science
to be taken December 1999

Title: POLYNOMIAL-TIME COMPUTATION IN MATRIX GROUPS

Approved: Eugene M Luks
Dr. Eugene M. Luks

This dissertation investigates deterministic polynomial-time computation in matrix groups over finite fields. Of particular interest are matrix-group problems that resemble testing graph isomorphism. The main results are instances where the problems admit polynomial-time solutions and methods that enable such efficiency.

A permutation-group problem that generalizes graph-isomorphism testing is the problem of finding stabilizers of sets. For an integer constant $d > 0$, let Γ_d denote the class of finite groups all of whose nonabelian composition factors lie in S_d. A result of Luks asserts that in Γ_d one can find set-stabilizers in polynomial time. The set-stabilizer problem has important generalizations in matrix groups. Let G be a matrix group on a vector space V over a finite field. The vector-stabilizer problem asks: given $v \in V$, find the subgroup of G stabilizing v. The subspace-stabilizer problem asks: given $W \subset V$, find the subgroup of G stabilizing W.

A critical foundation for group computation is the ability_to perform testing membership of an element in a group. In matrix groups, a polynomial-time method seems unlikely since membership-testing already subsumes the discrete-log problem. Nevertheless, assuming a polynomial bound on the primes in $|G|$ other than the field characteristic, Luks has found polynomial-time solutions for testing membership and also for finding stabilizers of vectors and subspaces in solvable groups.

The main theme of this dissertation is the generalization of the solvable-matrix-group algorithms to algorithms for matrix groups in Γ_d.

Assuming the same bound on these primes, we establish polynomial-time membership-testing in a broader class than Γ_d: matrix groups all of whose nonabelian composition factors have polynomially bounded orders.

Now assume a polynomial bound on the primes in $|G|$ and the field characteristic. Based on the membership-testing algorithm, we then develop a divide-and-conquer paradigm for finding stabilizers of vectors and subspaces in polynomial time for $G \in \Gamma_d$. This result exploits Babai, Cameron, and Pálfy's theorem on the polynomial orders of primitive groups in Γ_d and Rónyai's algorithm for finding irreducible subspaces.

CURRICULUM VITA

NAME OF THE AUTHOR: Takunari Miyazaki

PLACE OF BIRTH: Tôkyô, Japan

DATE OF BIRTH: May 29, 1969

GRADUATE AND UNDERGRADUATE SCHOOLS ATTENDED:

University of Oregon
The University of Kansas

DEGREES AWARDED:

Doctor of Philosophy in Computer and Information Science,
University of Oregon, 1999
Master of Science in Computer and Information Science,
University of Oregon, 1994
Bachelor of Science in Mathematics (Distinction),
The University of Kansas, 1992

AREAS OF SPECIAL INTEREST:

Algebraic Algorithms
Computational Complexity

PROFESSIONAL EXPERIENCE:

Research Assistant, Department of Computer and Information Science,
University of Oregon, Eugene, 1999–

Teaching Assistant, Department of Computer and Information Science,
University of Oregon, Eugene, 1993–1999

AWARDS AND HONORS:

Black–Babcock Fellow, Department of Mathematics,
The University of Kansas, 1991–1992
Mitchell Fellow, Department of Mathematics,
The University of Kansas, 1990–1991

ACKNOWLEDGEMENTS

It is a great pleasure to express my sincere gratitude to my adviser Professor Eugene Luks for invaluable guidance, insight, ideas, patience, and encouragement throughout my years at the University. He is indeed my mentor in all areas of my academic life.

I would also like to thank other members of the committee, Professors Andrzej Proskurowski, Christopher Wilson, and Charles Wright. Special thanks are due to Professor Wright for his helpful comments on the organization and exposition. I am also grateful to Professor William Kantor for his advice and encouragement during the important phase of the dissertation research.

Thanks to Ferenc Rákóczi and Amitabha Roy for their common interests in many areas, suggestions, and encouragement.

The faculty, staff, and students of the Department have made my years at the University very comfortable and enjoyable. I would like to especially thank Graduate Secretaries Betty Lockwood and Jan Saunders for their help. Special thanks also go to Professor Michal Young for generously offering his workstation to me during the last phase of the dissertation work.

Most of all, I am deeply thankful to my parents and sister for their constant love, faith, patience, and support in all areas of my life.

Finally, I would like to acknowledge the financial support by a grant from the National Science Foundation, CCR-9820945, to Professor Luks.

DEDICATION

To my parents

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

§1. Computational Group Theory

In the intersection of abstract algebra and computer science, computational group theory is a research area concerning methods of computation, both theoretical and practical, in groups. Over the last several decades, this subject has experienced a period of vigorous development (cf. [49]).

Two computer algebra systems are particularly known for their rich libraries in groups: GAP [24] (an open system developed by J. Neubüser's school in Aachen, currently updated in St Andrews) and Magma [21] (the product of J. J. Cannon's school in Sydney, regarded as the successor to the system Cayley [20]). Systems such as these have indeed served as important tools for profound discoveries in group theory, combinatorics, as well as other parts of mathematics and science (cf. [49, pp. 674–675]).

In many computational situations, groups are specified as concrete objects with respect to the two classical representation methods, namely, by permutations and matrices. Therefore, numerous algorithms have been designed and implemented based on not only abstract group theory but also the unique structural properties of these representations.

Since the seminal work of Sims [51], [52], many significant results on efficient algorithms for permutation groups have appeared from both sides of theorists and practitioners, making the area of permutation-group computation the most matured sub-discipline (cf. [49, pp. 675–676]). Particularly remarkable is the development of a large library of polynomial-time algorithms, inaugurated in 1980 by the work of Furst, Hopcroft, and Luks [23] on a polynomial-time version of Sims's algorithm (see [5], [33], [34], and [40] for survey of results; [50] for detailed descriptions). There are two apparent reasons for such success: A small generating set of permutations can designate a very large group. Permutation groups offer the ubiquity of group actions on a prescribed set, given implicitly as part of the input.

Matrices are considered to be more natural and desirable objects for group representation. Matrix groups offer very compact representations but also pose serious computational difficulties. One of the basic problems in this category is <u>membership-testing</u>: determine whether or not a given element belongs to a group specified by generators. L. Babai has observed that, based on Mihaĭlova's result [42], the membership-testing problem is <u>undecidable</u> already for groups of invertible integer matrices of dimension four (cf. [3]). For matrix groups over finite fields, the problem is clearly decidable. However, even for 1 × 1 matrices over finite fields, the problem subsumes a version of the well-known <u>discrete-log</u> problem, whose theoretical complexity status is a long-standing open question in complexity theory (see, e.g., [13, pp. 162–165]). Applying techniques developed for permutation groups directly to matrix groups often causes exponential blowups of the input size. Indeed, rewriting matrix groups naïvely as permutation groups on the underlying vector space already requires such a blowup.

Nevertheless, by separating some of these difficult obstacles, the intense quest for efficient matrix-group algorithms has offered some promising results and continues to be very active (cf. [7], [12], [14], [15], [16], and [39]). In fact, the subject of matrix-group computation, both theoretical and practical, is currently considered to be the most actively studied area in the computational group theory community (cf. [49, pp. 677–678]). Unlike in permutation groups, where deterministic algorithms have performed well, randomization appears to be an indispensable tool for many existing matrix-group algorithms.

§2. Computational Complexity in Matrix Groups

As in many subjects of the theory of computing, in computational group theory, polynomial time has been recognized as a robust theoretical criterion of tractability in classifying problems. Indeed, in permutation-group computation, polynomial time has not only offered an elegant theory with considerable generality and power within the area but also established an interface to computational complexity theory [40]. The same spirit has been carried into matrix-group computation.

The work of Babai and Szemerédi [12] first addressed the issue of computational complexity in matrix groups. Their work answers purely complexity-theoretic questions and provides certain promising directions to algorithm designers. In particular, their results assert that, in matrix groups over finite fields, the problems of testing membership and deciding solvability belong to the class **NP**.

The work of Luks [39] first introduced polynomial-time algorithms for matrix groups. Luks showed that the problem of deciding solvability of matrix groups over finite fields has a polynomial-time solution. Methods that must involve membership-testing are unlikely to have polynomial-time efficiency. Nonetheless, with a simple limitation on the input, Luks managed to solve a number of problems, including membership-testing, for solvable matrix groups over finite fields in polynomial time.

In his ground-breaking work [39], in order to separate bottlenecks involving the discrete-log problem, Luks introduced a timing parameter $\mu(G)$ for a matrix group G: the largest prime dividing $|G|$ other than the characteristic of the ground field. With $\mu(G)$ in timing, Luks's main results are a large library of deterministic algorithms for solvable matrix groups over finite fields. In particular, for a given solvable matrix group G, Luks's algorithm solves the three basic problems of finding $|G|$, membership-testing, and finding a presentation for G, in time polynomial in the input length and $\mu(G)$.

With randomization and another timing parameter, Beals and Babai extended from solvable groups to all groups [16]. The Beals–Babai algorithm solves the aforementioned three basic problems for a matrix group G over a finite field in Las Vegas time that is polynomial in the input length, $\mu(G)$, and another parameter $\nu(G)$: the smallest positive integer m such that every nonabelian composition factor of G has a permutation representation of degree at most m. Subsequently, randomized membership-testing has been shown to admit various classes of matrix groups (cf. [14] and [15]).

§3. Relationship with Graph-Isomorphism Testing

A significant link between computational group theory and computational complexity theory is the graph-isomorphism problem (GRAPH-ISO). The problem is of fundamental importance in the theory of computing because of its as yet unresolved status in the polynomial-time hierarchy, and it plays a very interesting rôle in the **P** =?**NP** question [27] (see Chapter IV for technical implications; see also [35]). The following three group-theoretic problems are known to be polynomial-time equivalent to GRAPH-ISO (cf. [6] and [41]). Given a graph X, compute the orbits of $\mathrm{Aut}(X)$;

generators for Aut(X); and the order of Aut(X).

Luks has further observed a class of permutation-group problems that are at least as hard and play similar rôles in the polynomial-time hierarchy as GRAPH-ISO (named the Luks equivalence class by Babai in [6]): finding coset intersections, set-stabilizers, and centralizers of elements and subgroups [38] (cf. [11]).

Based on the fundamental work of Furst, Hopcroft, and Luks [23], using an elegant divide-and-conquer paradigm, sub-cases of the Luks equivalence class problems have been shown to be solvable in polynomial time [38].

For an integer $d > 0$, let Γ_d denote the class of finite groups all of whose nonabelian composition factors are isomorphic to subgroups of the symmetric group of permutations S_d. Evidently, Γ_d includes all solvable groups. From another point of view, for a graph X of valence at most $d + 1$ and an edge e of X, the subgroup of Aut(X) that fixes e belongs to Γ_d [38, Proposition 3.4] (cf. [10]).

Fix an integer constant $d > 0$. Luks's work [38], later strengthened by the work of Babai, Cameron, and Pálfy [8], proves that the set-stabilizer problem is solvable in polynomial time for permutation groups in Γ_d. It is then a corollary that one can test, in polynomial time, isomorphism of graphs of bounded valence.

Based on the aforementioned work on membership-testing in solvable matrix groups, Luks went on to investigate the polynomial-time computability of matrix-group problems resembling the set-stabilizer problem [39]. In particular, for a given solvable matrix group G, Luks developed a divide-and-conquer method, analogous to his earlier work on permutation groups [38], to solve the problems of finding stabilizers of vectors and subspaces and finding centralizers and intersections of subgroups in time polynomial in the input length and $\mu(G)$.

§4. Summary of the Results

This dissertation investigates deterministic polynomial-time computation in matrix groups over finite fields. Of particular interest are matrix-group problems that generalize the set-stabilizer problem: the problems of finding stabilizers of vectors and subspaces. The main results are instances where these problems admit polynomial-time solutions and methods that enable such efficiency.

Motivated by Luks's results in permutation groups [38], we consider instances in the class Γ_d, the best we can hope as a reasonable target, with an assumption on the sizes of certain primes. The main theme of this dissertation is the generalization of Luks's solvable matrix group algorithms to algorithms for matrix groups in Γ_d.

In the first part of the dissertation, we develop basic algorithms for membership-testing. In fact, with $\mu(G)$ in timing, we are able to establish polynomial-time membership-testing in a broader class of matrix groups than those in Γ_d. In Chapter III, we prove that, given a matrix group G such that $\mu(G)$ and the maximum order of a nonabelian composition factor of G are polynomially bounded in the input length, the problems of testing membership, finding $|G|$, and finding a presentation of G can be solved in polynomial time.

As in Luks's method, our approach to membership-testing involves top-down decomposition of a given group G; in particular, we construct a series of G-normal subgroups $G = N_1 > N_2 > \cdots > N_r = 1$ specified by presentations of G/N_i. This paradigm reduces membership-testing to the problem of finding a representation of each N_i with kernel N_{i+1}. Our results exploit polynomial-time permutation-group machinery for such representations.

As corollaries, we also prove that, for these matrix groups admitting polynomial-time membership-testing, one can find composition series and the kernels of certain homomorphisms in polynomial time.

In the second part of the dissertation, we consider the problems of finding stabilizers of vectors and subspaces. In Chapter IV, we develop a divide-and-conquer paradigm for a matrix group $G \in \Gamma_d$, where the primes dividing $|G|$ and the characteristic of the ground field are polynomially bounded, to solve the vector-stabilizer and subspace-stabilizer problems in polynomial time.

As in Luks's classical method [38], the main component of our approach involves two levels of divide and conquer. First, for a given group G, we seek a G-invariant subspace W or an imprimitivity system $\mathcal{V}$ for G in the underlying vector space V. If such a subspace W is found, we consider the induced actions of G on W and V/W. On the other hand, if an imprimitivity system $\mathcal{V}$ is found, we consider the natural permutation representation of G on $\mathcal{V}$. Using a standard algorithm for finding block systems in permutation groups, we then construct a primitive permutation representation of G on blocks of $\mathcal{V}$. When such decomposition bottoms out, we appeal to the celebrated result of Babai, Cameron, and Pálfy: the orders of primitive permutation groups in Γ_d are polynomially bounded.

It should be emphasized that, unlike in the solvable-group case [39], for divide-and-conquer involving nonabelian quotients, we rely on Rónyai's algorithm [47] to find irreducible subspaces. The main complexity-theoretic bottleneck in finding irreducible subspaces is polynomial factorization. Presently, deterministic polynomial-time methods are only available in finite fields with polynomially bounded characteristics. Therefore, in our results, we assume that the field characteristic is polynomially bounded.

On the other hand, Las Vegas polynomial-time factorization methods are available in finite fields of any characteristics [17]. Indeed, as with factoring polynomials, we may remove the condition on the field characteristic if we interpret our results as Las Vegas instead of deterministic.

CHAPTER II

PRELIMINARIES

In this chapter, we review basic terminologies of group theory, finite fields, permutation representations, linear representations, and polynomial-time computability. Our general references are [28], [29], and [36]. We will also use deeper group-theoretic results from [1], [32], and [55]. For permutation groups, we refer to [22] and [57]. For matrix groups, we refer to [54]. A standard reference on polynomial-time computability is [25].

§1. Generalities

Let G be a group. We write $H \leq G$ and $N \trianglelefteq G$ to indicate, respectively, H is a subgroup of G, and N is a normal subgroup of G; to emphasize strict inclusion, we write $H < G$ and $N \triangleleft G$, respectively. A normal series for G is a series $1 = H_\ell \trianglelefteq \cdots \trianglelefteq H_1 = G$. A subgroup H of G is subnormal in G, denoted by $H \trianglelefteq\trianglelefteq G$, if there exists a series $H = H_i \trianglelefteq \cdots \trianglelefteq H_1 = G$; if $H < G$, then we write $H \triangleleft\triangleleft G$. A G-normal series for G is a series $1 = N_\ell \leq \cdots \leq N_1 = G$ such that each $N_i \trianglelefteq G$. For a subset $S \subseteq G$, let $\langle S \rangle = \langle s \mid s \in S \rangle$ denote the subgroup of G generated by S. For $x, y \in G$, the conjugate of x by y is $x^y = y^{-1}xy$; for a subset $X \subseteq G$, write $X^y = \{x^y \mid x \in X\}$. The normal closure of X in G, denoted by $\langle X^G \rangle$, is the subgroup generated by the sets X^g for all $g \in G$ (that is, the smallest normal subgroup of G containing X); we call X normal generators for $\langle X^G \rangle$ in G. Let $H \leq G$. The normalizer of X in H is the subgroup $N_H(X) = \{h \in H \mid X^h = X\}$. The centralizer of X in H is the subgroup $C_H(X) = \{h \in H \mid x^h = x \text{ for all } x \in X\}$. If $X = \{x\}$, then we write $C_H(x) = C_H(X)$. The center of G is the subgroup $Z(G) = C_G(G)$.

For $x, y \in G$, the commutator of x and y is $[x, y] = x^{-1}y^{-1}xy$. For subsets $X, Y \subseteq G$, write $[X, Y] = \langle [x, y] \mid x \in X \text{ and } y \in Y \rangle$. The derived group of G is the subgroup $G' = G^{(1)} = [G, G]$. For integers $i > 1$, recursively write $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$. We say G is solvable if $G^{(n)} = 1$ for some integer $n > 0$. Now, write $L_1(G) = G$, and proceeding recursively, write $L_i(G) = [L_{i-1}(G), G]$ for integers $i > 1$. We say G is nilpotent if $L_n(G) = 1$ for some integer $n > 0$. The class of a nilpotent group G is the integer m such that $L_m(G) > L_{m+1}(G) = 1$.

Let G be a finite group. Let p be a prime. We say G is a p-group if $|G|$ is a power of p. We say G is an elementary abelian p-group if every nonidentity element of G has order p.

A composition series for G is a normal series $1 = K_\ell \lhd \cdots \lhd K_1 = G$ maximal subject to $K_i \lhd K_{i-1}$. The composition factors of G are $K_1/K_2, \ldots, K_{\ell-1}/K_\ell$, uniquely determined by G up to isomorphism and the order in which they appear. A chief series for G is a G-normal series $1 = C_\ell < \cdots < C_1 = G$ maximal subject to $C_i \lhd G$. The chief factors of G are $C_1/C_2, \ldots, C_{\ell-1}/C_\ell$, also uniquely determined by G up to isomorphism and the order in which they appear.

We say G is quasisimple if $G = G'$, and if $G/Z(G)$ is nonabelian simple. We say G is semisimple if $G = G'$, and if $G/Z(G)$ is isomorphic to a direct product of nonabelian simple groups.

Let k be a finite field. The image of the integers $\mathbf{Z}$ in k is an integral domain and thus isomorphic to $\mathbf{Z}/p\mathbf{Z} = \mathrm{GF}(p)$ for some prime p. We call p the characteristic of k, denoted by $\operatorname{char} k$, and $\mathrm{GF}(p)$ the prime field of k.

Typically, k is encoded by an irreducible polynomial f of degree $d = |k : \mathrm{GF}(p)|$ over $\mathrm{GF}(p)$. Under an isomorphism $k \cong \mathrm{GF}(p)[X]/(f)$, each element of k is then a d-tuple of elements of $\mathrm{GF}(p)$ (i.e., a polynomial of degree at most $d-1$ over $\mathrm{GF}(p)$), and addition and multiplication in k are defined by those in $\mathrm{GF}(p)[X]/(f)$.

§2. Permutation Representations

Let $\mathrm{Sym}(\Omega)$ denote the symmetric group of permutations on an m-element set Ω. A permutation group is a subgroup of $\mathrm{Sym}(\Omega)$. A group G acts on Ω if there is a homomorphism $\pi : G \to \mathrm{Sym}(\Omega)$. We call π a permutation representation of G. If π is an injection, then π is faithful. We call m the degree of π; if $G \leq \mathrm{Sym}(\Omega)$, then we call m the degree of G.

Let G act on Ω. We denote the images of a point $\alpha \in \Omega$ and a subset $\Delta \subseteq \Omega$ under $g \in G$ by α^g and Δ^g, respectively. The relation $\sim$ on Ω defined by $\alpha \sim \beta$ if $\alpha^g = \beta$ for some $g \in G$ is an equivalence relation, and we call the equivalence classes orbits. We say G acts transitively on Ω if Ω itself forms a single orbit. For a point $\alpha \in \Omega$, the point-stabilizer of α is the subgroup $G_\alpha = \{g \in G \mid \alpha^g = \alpha\}$. For a subset $\Delta \subseteq \Omega$, the set-stabilizer of Δ is the subgroup $\mathrm{Stab}_G(\Delta) = \{g \in G \mid \Delta^g = \Delta\}$. If Ω possesses a group structure preserved by G, then we often write $C_G(\alpha)$ and $N_G(\Delta)$ for G_α and $\mathrm{Stab}_G(\Delta)$, respectively.

Let G act transitively on Ω. A subset $\Delta \subseteq \Omega$ is a block if, for each $g \in G$, either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$. The set of images of a block, called a system of blocks, forms a G-invariant partition of Ω. A system of blocks is trivial if it is the partition into singletons or the partition with Ω itself. If a transitive group G has no nontrivial system of blocks, then G is primitive.

Let H be a group and K be a permutation group on a set Γ. Consider the cartesian product $\prod_\Gamma H$ consisting of $|\Gamma|$ copies of H and identify each element $f \in \prod_\Gamma H$ as a function from Γ into H. The wreath product H wr K is the split extension of a base group $\prod_\Gamma H$ by K, where the action of K on $\prod_\Gamma H$ is defined by permuting $|\Gamma|$ copies of H as the elements of Γ (i.e., for $\gamma \in \Gamma$ and $k \in K$, we define $f^k(\gamma) = f(\gamma^{k^{-1}})$).

§3. Linear Representations

Let k be a field and V an n-dimensional vector space over k. Let $\mathrm{End}_k(V) = \mathrm{Hom}_k(V, V)$ denote the algebra of all the linear transformations of V into itself. The units of $\mathrm{End}_k(V)$ form the general linear group $\mathrm{GL}(V) = \mathrm{GL}(V, k)$. If $S \subseteq \mathrm{End}_k(V)$, then $\mathrm{Span}(S)$ is the subalgebra of $\mathrm{End}_k(V)$ spanned by S. If $G \leq \mathrm{GL}(V)$, then $k[G] = \mathrm{Span}(G)$ is the linear span of G (or enveloping algebra of G).

An isomorphism between $\mathrm{End}_k(V)$ and the algebra $M(n, k)$ of all the $n \times n$ matrices over k defines an isomorphism between $\mathrm{GL}(V)$ and the group $\mathrm{GL}(n, k)$ of all the $n \times n$ invertible matrices over k. Under such an isomorphism, we regard each element of $\mathrm{End}_k(V)$ as a matrix. A matrix group is a subgroup of $\mathrm{GL}(n, k)$, and we regard a subgroup of $\mathrm{GL}(V)$ as a matrix group. If k is a finite field of order q, we often write $M(n, q) = M(n, k)$ and $\mathrm{GL}(n, q) = \mathrm{GL}(n, k)$.

A group G acts on V if there is a homomorphism $\phi : G \to \mathrm{GL}(V)$. We call ϕ a linear representation of G over k (or kG-representation) and V a representation module for ϕ (or kG-module). If ϕ is an injection, then ϕ is faithful. We call n the degree of ϕ over k; if $G \leq \mathrm{GL}(V)$, then we call n the degree of G over k.

Let G act on V. Since $\mathrm{GL}(V) \leq \mathrm{Sym}(V)$, the notations of permutation groups apply to G. A subspace W of V is a G-subspace (or invariant under G) if $W^g \subseteq W$ for all $g \in G$. If the only G-subspaces are 0 and V, then G is irreducible; otherwise,

G is reducible. We say G is completely reducible if there are minimal G-subspaces $W_1, \ldots, W_r$, $r \geq 1$, forming a direct sum $V = W_1 \oplus \cdots \oplus W_r$; in particular, an irreducible group is completely reducible. For a minimal G-subspace $W \subseteq V$, the homogeneous G-subspace of V determined by W is the sum of all the minimal G-subspaces that are G-isomorphic to W.

An irreducible group G is imprimitive if there are subspaces $V_1, \ldots, V_m$, $m \geq 2$, forming a direct sum $V = V_1 \oplus \cdots \oplus V_m$ such that, for each $g \in G$, the map $V_i \mapsto V_i^g$ is a permutation of the set $\mathcal{V} = \{V_1, \ldots, V_m\}$. We call $\mathcal{V}$ a system of imprimitivity for G; if no such system exists, G is primitive. We call $\mathcal{V}$ a minimal system of imprimitivity for G if the G-action on $\mathcal{V}$ is a primitive permutation representation of degree m.

An element x of $\mathrm{End}_k(V)$ is unipotent if x has its n eigenvalues all equal to 1 (i.e., $(x-1)^n = 0$). A subgroup G of $\mathrm{GL}(V)$ is unipotent if all the elements of G are unipotent; if $\mathrm{char}\, k = p$, then G is unipotent if and only if G is a p-group.

We define that an abelian subgroup A of $\mathrm{GL}(V)$ is uniform if, for every integer $m \geq 1$, the subgroup A^m of A has no nonzero fixed vectors in V (i.e, $C_V(A^m) = 0$) unless $A^m = 1$.

§4. Polynomial-Time Computability

A problem, with an input encoded by a string of length ℓ, has a polynomial-time solution if it is solvable by an algorithm that runs in $O(\ell^c)$ steps for a fixed constant $c \geq 1$. A problem P_1 is polynomial-time reducible to a problem P_2, denoted by $P_1 \leq^p P_2$, if the existence of a polynomial-time solution to P_2 implies the existence of such a solution to P_1. Problems P_1 and P_2 are polynomial-time equivalent, denoted by $P_1 \equiv^p P_2$, if P_1 and P_2 are polynomial-time reducible to each other.

The length of a subgroup series is often essential to polynomial running time of algorithms. By Lagrange's theorem, a strictly increasing series of subgroups in S_m has length at most $\log m! = O(m \log m)$. In fact, according to Babai's bound [4], such a series has length at most $2m - 1$. In $\mathrm{GL}(n, q)$, Lagrange's theorem yields that the length of a subgroup series is at most $n \log q$. For more accurate estimates on the length of a subgroup series, we refer to [19], [48], [53], and [56].

To formalize complexity analysis, we define three parameters on groups. For a finite group G, define $\kappa(G)$ to be the maximum order of a nonabelian composition factor of G and $\gamma(G)$ to be the maximum order of a nonabelian chief factor of G. For $G \leq \mathrm{GL}(n, k)$, define $\mu(G)$ to be the largest prime dividing $|G|$ other than $\mathrm{char}\, k$.

CHAPTER III

MANAGEMENT OF MATRIX GROUPS

In this chapter, we investigate the polynomial-time computability of membership-testing. First, we formalize the problem of membership-testing with a general paradigm of manageability. After summarizing basic polynomial-time tools and preliminary facts on normal structure, we establish the manageability of matrix groups having polynomial bounds on the orders of nonabelian chief factors. We then generalize our method for matrix groups having polynomial bounds on the orders of nonabelian composition factors.

§1. Statement of the Results

In computational group theory, one of the most basic problems is membership-testing. In matrix groups over a finite field k, it is formally defined as

Membership-test.

Instance: $G \leq \mathrm{GL}(n,k)$ and $x \in \mathrm{GL}(n,k)$.

Question: $x \in G$?

In this chapter, we directly generalize Luks's membership-test algorithm from solvable groups to all groups using another natural timing parameter $\kappa(G)$: the maximum order of a nonabelian composition factor of G. In addition to the basic tools of [39], we also adapt a variant of [16, Lemma 5.1] in our deterministic setting.

Let k be a finite field of order q. For an input/output $G \leq \mathrm{GL}(n,k)$, we assume that G is specified by a generating set of matrices S. We also assume some reasonable encoding of the field k so that a polynomial in the input length throughout means a polynomial in n, $\log q$, and $|S|$, unless it is specified otherwise.

The following is the main result of this chapter.

Theorem 3.1.1. Let k be a finite field. Given a matrix group $G \leq \mathrm{GL}(n, k)$, one can solve the following list of problems in time polynomial in these three parameters: the input length, the largest prime dividing $|G|$ other than $\operatorname{char} k$, and the maximum order of a nonabelian composition factor of G.

(i) Find $|G|$.

(ii) Given $x \in \mathrm{GL}(n, k)$, test whether or not $x \in G$.

(iii) Find a generator-relator presentation of G.

We list four applications in the following corollary.

Corollary 3.1.2. The list of problems in Theorem 3.1.1 continues as follows.

(iv) Find a composition series of G.

(v) Find a G-normal series

$$G = G_1 > G_2 > \cdots > G_r = 1$$

such that each G_i/G_{i+1} is a nonabelian chief factor of G or an elementary abelian group.

(vi) Find the kernel of a given homomorphism $G \to M$, where M is a finite group equipped with a polynomial-time algorithm for testing membership and finding presentations.

(vii) Given a normal subgroup N of G, find $C_G(N)$.

To prove Theorem 3.1.1 and Corollary 3.1.2, we also make the following additional assumption.

Let $p = \operatorname{char} k$. Observe that, with some reasonable encoding of the field k (e.g., an irreducible polynomial f over the prime field $\mathrm{GF}(p)$ such that $k \cong \mathrm{GF}(p)[X]/(f)$), it is elementary to convert our setting to matrix groups over $\mathrm{GF}(p)$ by blowing up by a factor of $\deg f$. Thus, we assume that $k \cong \mathrm{GF}(p)$.

§2. Membership-Testing with Manageable Groups

In this section, we describe the overall structure of a generic membership-test procedure we will adapt. The method we describe here was originally formalized for solvable matrix groups in [39, §§4.1–4.2].

We begin with a brief outline. Given $G \le \mathrm{GL}(n, k)$, the method constructs, in a top-down fashion, a G-normal series

$$G = N_1 > N_2 > \cdots > N_r = 1$$

specified by generator-relator presentations of G/N_i and G-homomorphisms $\pi_i : N_i \to M_i$, where $N_{i+1} = \operatorname{Ker} \pi_i$, and M_i are finite groups equipped with certain basic polynomial-time machinery. With such a series, membership-testing can be performed by a sifting process: map a candidate x for membership in N_i by π_i to M_i;

find an $a \in N_i$ such that $\pi_i(a) = \pi_i(x)$; then test membership of xa^{-1} in N_{i+1} (cf. [23]).

In order to formalize our method, we must first define algorithmic notions of presentations (cf. [39, §4.2]).

Let $\mathcal{F}(X)$ denote the free group on a set X. Then, for a group G and a function $\phi : X \to G$, there is a natural extension of ϕ to a homomorphism $\hat{\phi} : \mathcal{F}(X) \to G$.

Let G be a group and N a normal subgroup of G. A constructive presentation of G mod N is $\Pi = (X, \phi, \psi, \mathcal{R})$ in which X is a set, $\phi : X \to G$ is a function, $\psi : G \to \mathcal{F}(X)$ is a homomorphism, and $\mathcal{R}$ is a subset of $\mathcal{F}(X)$, satisfying the following properties.

(1) $g\hat{\phi}(\psi(g))^{-1} \in N$ for each $g \in G$.

(2) $\hat{\phi}^{-1}(N) = \langle \mathcal{R}^{\mathcal{F}(X)} \rangle$.

For computational purposes, we assume that $\Pi = (X, \phi, \psi, \mathcal{R})$ is specified by $\phi(X)$, $\mathcal{R}$, and a procedure for determining $\psi(g)$ for any $g \in G$.

For $g \in G$, write $\text{sift}_\Pi(g) = g\hat{\phi}(\psi(g))^{-1}$. The following result is observed in [39, Lemmas 4.1, 4.2].

Lemma 3.2.1. Let G be a group and N a normal subgroup of G. If $\Pi = (X, \phi, \psi, \mathcal{R})$ is a constructive presentation of G mod N, then the following hold.

(i) $\langle X | \mathcal{R} \rangle$ is a generator-relator presentation of G/N, with mutually-inverse isomorphisms $G/N \leftrightarrows \mathcal{F}(X)/\langle \mathcal{R}^{\mathcal{F}(X)} \rangle$ naturally induced by $\hat{\phi}$ and ψ.

(ii) If $G = \langle S \rangle$, then $N = \langle (\hat{\phi}(\mathcal{R}) \cup \text{sift}_\Pi(S))^G \rangle$; in particular, if $G = \langle \phi(X) \rangle$, then $N = \langle \hat{\phi}(\mathcal{R})^G \rangle$. □

Observe that, by (ii) above, given generators for G and a constructive presentation of G mod N for $N \trianglelefteq G$, one can construct a subset, called normal generators, $R \subseteq N$ such that $\langle R^G \rangle = N$ (that is, N is the normal closure of R in G).

The following result, observed in [39, Lemma 4.3], provides a recipe for gluing presentations together.

Lemma 3.2.2. Let G be a group and N and K normal subgroups of G such that $K \leq N$. If $\Pi_1 = (X_1, \phi_1, \psi_1, \mathcal{R}_1)$ and $\Pi_2 = (X_2, \phi_2, \psi_2, \mathcal{R}_2)$ are constructive presentations of G mod N and N mod K, respectively, then $\Pi = (X, \phi, \psi, \mathcal{R})$ defined by

(i) $X = X_1 \dot{\cup} X_2$,

(ii) $\phi(x) = \begin{cases} \phi_1(x) \text{ for } x \in X_1, \\ \phi_2(x) \text{ for } x \in X_2, \end{cases}$

(iii) $\psi(g) = \psi_2(\mathrm{sift}_{\Pi_1}(g))\psi_1(g)$ for $g \in G$, and

(iv) $\mathcal{R} = \mathcal{R}_2 \cup \mathcal{S}_1 \cup \mathcal{S}_2$, where $\mathcal{S}_1 = \{r\psi_2(\hat{\phi}_1(r))^{-1} \,|\, r \in \mathcal{R}_1\}$ and $\mathcal{S}_2 = \{({x_2}^{x_1})^{-1}\psi_2(\phi_2(x_2)^{\phi_1(x_1)}) \,|\, x_1 \in X_1 \text{ and } x_2 \in X_2\}$,

is a constructive presentation of G mod K. □

In what follows, we define our notion of manageability involving finite groups equipped with certain basic polynomial-time machinery.

A finite group M specified by some input string is manageable if there is a polynomial-time algorithm for testing membership of a given element and finding a constructive presentation for all the subgroups of M.

Theorem 3.2.3. The following finite groups are manageable.

(i) Permutation groups $G \leq \mathrm{Sym}(\Omega)$ (Sims [51]; Furst–Hopcroft–Luks [23]).

(ii) Solvable matrix groups $G \leq \mathrm{GL}(n, k)$ such that $\mu(G)$, the largest prime dividing $|G|$ other than $\mathrm{char}\, k$, is bounded by a fixed polynomial in the input length of G (Luks [39]). □

Let G be a finite group and N a normal subgroup N of G. A manageable representation for N is a homomorphism $\pi : N \to M$ for some manageable group M, where $\pi(N) \neq 1$, such that π is equipped with an action of G on $\pi(N)$ satisfying $\pi(x)^g = \pi(x^g)$ for $x \in N$ and $g \in G$. Very often, π is defined as the restriction of a homomorphism $G \to M$ on N. For computational purposes, we assume that π is a procedure for determining $\pi(x)$ for any $x \in N$.

A manageable series of a finite group G is a G-normal series

$$G = N_1 > N_2 > \cdots > N_r = 1$$

specified by constructive presentations of G mod N_i and manageable representations $\pi_i : N_i \to M_i$ for manageable groups M_i such that $N_{i+1} = \mathrm{Ker}\, \pi_i$.

The following problem is our main interest.

Manageable representation.

Input: $G \leq \mathrm{GL}(n, k)$ and a constructive presentation of G mod N for $N \trianglelefteq G$.

Find: a manageable representation $\pi : N \to M$ for a manageable group M.

Suppose, for the moment, that a procedure to solve the manageable representation problem is available. Given $G \leq \mathrm{GL}(n, k)$, we construct a manageable series of G, in a top-down fashion, as follows.

Let $N_1 = G$, and start with the trivial constructive presentation of G mod N_1. As a generic step, suppose that a constructive presentation of G mod N_i for $N_i \trianglelefteq G$ is given. Then we may assume that we have normal generators R_i for N_i. Here, find a manageable representation $\pi_i : N_i \to M_i$ for some manageable group M_i. Then, as π_i is a G-homomorphism, obtain, in M_i, generators for and a constructive presentation of $\pi_i(N_i) = \langle \pi_i(R_i)^G \rangle$. All of this can be pulled back to $N_i/\operatorname{Ker}\pi_i$. Now, define $N_{i+1} = \operatorname{Ker}\pi_i$, and use the constructive presentations of G mod N_i and N_i mod N_{i+1} to form a constructive presentation of G mod N_{i+1}. Repeat the procedure until we reach $N_i = 1$.

When $N_r = 1$ is reached, a manageable series of G is complete. Membership-testing can be then performed by the sifting procedure through this series as described before.

That is, to prove that a matrix group G is manageable, it suffices to design a polynomial-time algorithm to solve the manageable representation problem for all the subgroups of G. We entirely devote the rest of the chapter to the manageable representation problem.

§3. Basic Polynomial-Time Tools

We review basic polynomial-time tools developed earlier in [39]. We also develop a variant of the distilling lemma [16, Lemma 5.1].

We begin with the following elementary observation.

Lemma 3.3.1. Let $G \leq \mathrm{GL}(n,k)$ and a subset $\{g_1, \ldots, g_m\}$ of G be a basis of the linear span $k[G]$. If $x \in \mathrm{GL}(n,k)$, then $k[G]^x = k[G^x]$, and $\{{g_1}^x, \ldots, {g_m}^x\}$ forms a basis of $k[G^x]$. □

The following result is observed in [39, Theorem 4.5].

Theorem 3.3.2. Given $G \leq \mathrm{GL}(n,k)$ and $R \subset \mathrm{GL}(n,k)$, where $N := \langle R^G \rangle$, in polynomial time one can find a basis B of the linear span $k[N]$ such that $B \subseteq N$. □

In general, observe that an element $a \in \mathrm{GL}(n,k)$ centralizes $G \leq \mathrm{GL}(n,k)$ if and only if a commutes with a basis of $k[G]$. In particular, Theorem 3.3.2 yields the following corollary.

Corollary 3.3.3. Given $G \leq \mathrm{GL}(n,k)$ and $R \subset \mathrm{GL}(n,k)$, where $N := \langle R^G \rangle$, in polynomial time one can either prove that N is abelian, or find $a, b \in N$ such that $[a,b] \neq 1$. □

Luks also found a way to strengthen Theorem 3.3.2 and Corollary 3.3.3 by applying the following elementary observation.

For an n-dimensional vector space V over k and a set of vectors $X \subseteq V$, let $\mathrm{Span}(X)$ denote the subspace of V spanned by X. For $G \leq \mathrm{GL}(V)$, let X^G and $X^{k[G]}$ denote the images of X under G and $k[G]$, respectively. Then we have $\mathrm{Span}(X^G) = \mathrm{Span}(X^{k[G]})$.

Proposition 3.3.4 (Luks). Given $G \leq \mathrm{GL}(n,k)$, and $R, Q \subset \mathrm{GL}(n,k)$, where $N := \langle R^G \rangle$ and $L := \langle Q^N \rangle$, in polynomial time one can

(i) find a basis B of the linear span $k[L]$ such that $B \subseteq L$, and

(ii) prove that L is abelian, or find $a, b \in L$ such that $[a,b] \neq 1$.

Proof. Let $\bar{\ } : \mathrm{GL}(n,k) \to \mathrm{GL}(M(n,k))$ be the conjugation action of $\mathrm{GL}(n,k)$ on $M(n,k)$. Regarding Q as a set of vectors of the vector space $M(n,k)$, we have

$k[L] = \mathrm{Span}(Q^{\overline{N}}) = \mathrm{Span}(Q^{k[\overline{N}]})$. Since $\overline{N} = \langle \overline{R}^{\overline{G}} \rangle$, a basis of $k[\overline{N}]$ as elements of $\overline{N}$ is available by Theorem 3.3.2.

Note that, with respect to normal generators, the depth of L from G is two, and the algorithm squares an upper bound of a dimension twice: Let $m = n^2 = \dim_k M(n,k)$. Since $\overline{N} \leq \mathrm{GL}(M(n,k)) \cong \mathrm{GL}(m,k)$, the linear span $k[\overline{N}]$ is a k-vector space of dimension at most m^2, that is, at most n^4. □

The task of testing nilpotence and solvability is somewhat more involved. For details, we refer to [39, §5].

Theorem 3.3.5. Given $G \leq \mathrm{GL}(n,k)$, in polynomial time one can test whether or not G is solvable, and if so, whether or not G is nilpotent. □

Next, we state reduction theorems developed for solvable matrix groups by Luks in [39]. For $G \leq \mathrm{GL}(n,k)$, recall that $\mu(G)$ denotes the largest prime dividing $|G|$ other than $\mathrm{char}\, k$. Let $V(n,k)$ denote the underlying n-dimensional vector space over k.

The following result is observed in [39, §4.3].

Theorem 3.3.6. Given $G \leq \mathrm{GL}(n,k)$, a constructive presentation of G mod N for $N \trianglelefteq G$, and a proper G-subspace W of $V(n,k)$, in polynomial time one can either find

(i) a manageable representation $\pi : N \to M$ for a manageable group M, or

(ii) a homomorphism $\phi : G \to \mathrm{GL}(m,k)$ such that $m < n$ and $\phi(N) \neq 1$. □

The following result, implicit in [39, §4.7], is built on the manageability of abelian matrix groups.

Theorem 3.3.7. Given $G \leq \mathrm{GL}(n,k)$, a constructive presentation of G mod N for $N \trianglelefteq G$, and an abelian group $A < \mathrm{GL}(n,k)$ such that $A^G = A$ and $1 < C_N(A) < N$, one can either find

(i) a proper G-subspace of $V(n,k)$ or

(ii) a homomorphism $\phi : G \to \mathrm{GL}(m,k)$, where $m \leq n$ and $|\phi(N)| \leq |N|/2$,

in time polynomial in the input length and $\mu(G)$. □

The following result, implicit in [39, §4.7], is built on the manageability of nilpotent matrix groups.

Theorem 3.3.8. Given $G \leq \mathrm{GL}(n,k)$, a constructive presentation of G mod N for $N \trianglelefteq G$, and a class-2 nilpotent group $B < \mathrm{GL}(n,k)$ such that $B^G = B$ and $1 < C_N(B) < N$, one can find

(i) a proper G-subspace of $V(n,k)$,

(ii) an abelian group $A \leq B$ such that $A^G = A$ and $1 < C_N(A) < N$, or

(iii) a manageable representation $\pi : N \to \mathrm{Sym}(\Omega)$, where $|\Omega| \leq n^2$,

in time polynomial in the input length and $\mu(G)$. □

In what follows, we summarize tools for locating a nonidentity element in a proper normal subgroup.

The following result has appeared in another version involving randomization (cf. [7], [14], and [16]). Our version is built on Proposition 3.3.4 using the argument of [16, Lemma 5.1].

Proposition 3.3.9. Given the following inputs:

(i) $G \leq \mathrm{GL}(n,k)$, $R, Q \subset G$, where $N := \langle R^G \rangle$ and $L := \langle Q^N \rangle$ such that $L \leq N$, and L is nonabelian, and

(ii) nonidentity elements $a, b \in L$ such that a or b belongs to a proper N-normal subgroup of L,

in polynomial time one can find a nonidentity element c in a proper N-normal subgroup of L.

Proof. If $[a,b] \neq 1$, then $[a,b]$ suffices for c as

$$c = [a,b] = a^{-1}b^{-1}ab = (b^{-1})^a b = a^{-1}a^b \in \langle a^N \rangle \cap \langle b^N \rangle.$$

Suppose $[a,b] = 1$. By Proposition 3.3.4, one can test whether or not a centralizes $\langle b^N \rangle$, and find $d \in \langle b^N \rangle$ such that $[a,d] \neq 1$ in case a does not centralize $\langle b^N \rangle$.

If such d is found, then $[a,d]$ suffices for c since $[a,d] \in \langle a^N \rangle \cap \langle b^N \rangle$.

Suppose a centralizes $\langle b^N \rangle$. Again, by Proposition 3.3.4, test whether or not a centralizes $L = \langle Q^N \rangle$. If $a \in Z(L)$, then return $c = a$ since $Z(L)$ is a proper N-normal subgroup of L. If $a \notin Z(L)$, then $\langle b^N \rangle < L$; thus, return $c = b$. □

Note that, if two arbitrary nonidentity elements of L are given to the algorithm described in the above proof, a nonidentity element in L is always returned. Therefore, Proposition 3.3.9 generalizes as

Corollary 3.3.10. Given the following inputs:

(i) $G \leq \mathrm{GL}(n,k)$, $R, Q \subset G$, where $N := \langle R^G \rangle$ and $L := \langle Q^N \rangle$ such that $L \leq N$, and L is nonabelian, and

(ii) a set of nonidentity elements $X \subseteq L$ such that at least one element of X belongs to a proper N-normal subgroup of L,

one can find a nonidentity element in a proper N-normal subgroup of L in time polynomial in the input length and $|X|$. □

Also, we have the following useful result.

Corollary 3.3.11. Given $G \leq \mathrm{GL}(n,k)$ and $R \subset G$, where $N := \langle R^G \rangle$ is nonabelian containing a proper G-normal subgroup $K > 1$, one can find a nonidentity element in a proper G-normal subgroup of N in time polynomial in the input length and some known upper bound γ on the index $|N : K|$.

Proof. Let $\gamma \geq |N : K|$. Form a set of $\gamma + 1$ distinct elements X of N. Then two of these elements, say a and b, must belong to the same one coset of K in N so that $a^{-1}b \in K$. That is, at least one of the $\gamma(\gamma+1)$ products of the form $x^{-1}y$, where $x, y \in X$, belongs to K. □

In Corollary 3.3.11, we assume that an upper bound on $|N : K|$ is known. Not only it is critical in meeting its guaranteed timing, but also the termination of the algorithm depends on this bound.

§4. Normal Structure

We now review basic facts about normal closures and normal series. We begin with the following elementary result (see, e.g., [22, Lemma 4.4C]).

Lemma 3.4.1. Let G be a finite group and L a subnormal subgroup of G. Then every composition factor of $\langle L^G \rangle$ is isomorphic to some composition factor of L. □

In particular, if $P \trianglelefteq\trianglelefteq G$, and P is a p-group, then $\langle P^G \rangle$ is also a p-group. If $L \trianglelefteq\trianglelefteq G$, and L is solvable, then $\langle L^G \rangle$ is also solvable. For nonabelian simple groups, the above lemma can be strengthened in the following familiar result. We include a proof based on H. Wielandt's argument (see, e.g., [46, 13.3.1]).

Lemma 3.4.2. Suppose a finite group G has a subnormal subgroup T such that T is nonabelian simple. Then $\langle T^G \rangle$ is a direct product of G-conjugates of T, where G acts transitively on the set of these conjugates.

Proof. Since T is simple, and $T \trianglelefteq\trianglelefteq G$, for each $g \in G$, either $T \cap T^g = T$ or 1. Then it suffices to show $[T, T^g] = 1$ for each $g \in G$ such that $T \cap T^g = 1$.

Let $g \in G$ such that $T \cap T^g = 1$ and $X = \langle T, T^g \rangle$. Then $T \lhd\lhd X$ as well as $T^g \lhd\lhd X$. Let $s(X : T)$ denote the minimal length of a subnormal series of T in X. We proceed our proof by induction on $s(X : T)$.

Suppose $s(X : T) = 1$; that is, $T \lhd X$. Here, we have $[T, T^g] \trianglelefteq T$. Suppose $[T, T^g] \neq 1$. Since T is simple, $T = [T, T^g]$, where $[T, T^g] \trianglelefteq \langle (T^g)^T \rangle \leq \langle (T^g)^X \rangle$. That is, $T \leq \langle (T^g)^X \rangle$ as well as $T^g \leq \langle (T^g)^X \rangle$. Since X is the smallest group containing T and T^g, we have $\langle (T^g)^X \rangle = X$. However, we know $T^g \lhd\lhd X$, where $T^g \neq X$, a contradiction.

Suppose $s(X : T) > 1$; that is, T is not normal in X. Since $T \lhd\lhd X$, we have $\langle T^X \rangle \lhd X$ and thus $s(\langle T^X \rangle : T) < s(X : T)$. Since T is not normal in X, there is $a \in T^g$ such that $T \neq T^a$. That is, $T \cap T^a = 1$. Let $Y = \langle T, T^a \rangle$, then $Y \leq \langle T^X \rangle$ and thus $s(Y : T) \leq s(\langle T^X \rangle : T) < s(X : T)$. By induction, we have $[T, T^a] = 1$. Observe that, for all $x, y \in T$, we have

$$1 = [x, y^a] = [x, y[y,a]] = [x, [y,a]][x, y]^{[y,a]} = ([y,a]^{-1})^x [x, y][y, a]$$

so that $[x, y] \in [T, T^g]$ and thus $T' \leq [T, T^g]$. Since T is nonabelian simple, $T' = T$. From $T \leq [T, T^g]$, it follows that $T \leq \langle (T^g)^X \rangle$ as well as $T^g \leq \langle (T^g)^X \rangle$ just as before, yielding $\langle (T^g)^X \rangle = X$, a contradiction. □

The following result is then immediate (see, e.g., [46, 13.3.4]).

Lemma 3.4.3. Let G be a finite group and N a normal subgroup of G. Suppose N has a normal subgroup T such that T is nonabelian simple. Then N is a nonabelian minimal normal subgroup of G if and only if $N = \langle T^G \rangle$. □

The above lemma then yields

Proposition 3.4.4. Let G be a finite group and N a normal subgroup of G. If L is a nonabelian minimal normal subgroup of N, then $\langle L^G \rangle$ is a nonabelian minimal normal subgroup of G.

Proof. Suppose $L = T_1 \cdots T_r$, where the T_i are isomorphic nonabelian simple groups. Since $T_1 \trianglelefteq\trianglelefteq G$, we know $\langle {T_1}^G \rangle$ is isomorphic to a direct product of G-conjugates of T_1. Now, $\langle {T_1}^N \rangle = L$ so that $L \leq \langle {T_1}^G \rangle$ and thus $\langle L^G \rangle \leq \langle {T_1}^G \rangle$. Clearly, $\langle {T_1}^G \rangle \leq \langle L^G \rangle$ since $T_1 \leq L$. Thus, $\langle {T_1}^G \rangle = \langle L^G \rangle$. □

In what follows, we derive a few elementary facts about chief and composition factors based on the Jordan–Hölder theorem. We first begin with chief factors.

Proposition 3.4.5. Suppose a finite group G has a chief factor N/K. If L_1 is a normal subgroup of N such that $L_1 \not\leq K$, then there is a proper N-normal subgroup L_2 of L_1 such that L_1/L_2 is simple.

Proof. Since $L_1K/K \trianglelefteq N/K$, we know L_1K/K is isomorphic to a direct product of isomorphic simple groups. There is $L_2 < L_1$ such that

$$L_1K/K \cong L_1/(L_1 \cap K) \rhd L_2/(L_1 \cap K) = L_2/(L_2 \cap K) \cong L_2K/K,$$

where $(L_1/(L_1 \cap K))/(L_2/(L_1 \cap K)) \cong L_1/L_2$ is simple, and $L_2K/K \lhd N/K$.

It remains to show that $L_2 \lhd N$.

Let $X = \langle {L_2}^N \rangle$. Clearly, $L_2K \leq XK$. Now, $X \leq \langle (L_2K)^N \rangle$ and $K \leq \langle (L_2K)^N \rangle$ so that $XK \leq \langle (L_2K)^N \rangle$. Since $L_2K/K \lhd N/K$, we have $\langle (L_2K)^N \rangle = L_2K$ and thus $XK \leq L_2K$. Consequently, $XK = L_2K$.

Now, $X < L_1$ since $XK/K = L_2K/K \lhd L_1K/K$. Since $L_2 \leq X < L_1$, we have $X/L_2 \lhd L_1/L_2$. Then $X = L_2$ by the simplicity of L_1/L_2. □

A naïve counting argument yields

Proposition 3.4.6. Suppose a finite group G has a nonabelian chief factor N/K. Let $L_1, \ldots, L_r$ be nonabelian normal subgroups of N such that $[L_i, L_j] = 1$ for all pairs $L_i \neq L_j$. If each $L_i \not\leq K$, then $r \leq \log |N/K|$.

Proof. Choose a pair L_i, L_j. Suppose $L_i \neq L_j$. Since $[L_i, L_j] = 1$, we have $[L_iK/K, L_jK/K] = K/K$. Now, N/K is a direct product of isomorphic nonabelian simple groups so that $(L_iK/K) \cap (L_jK/K) = K/K$.

Conversely, if $L_i = L_j$, we have $L_iK/K = L_jK/K$.

That is, for all pairs L_i, L_j, we have $L_i = L_j$ if and only if $L_iK/K = L_jK/K$.

Since N/K is a direct product of isomorphic nonabelian simple groups, N/K has at most $\log |N/K|$ distinct nontrivial normal subgroups that centralize each other. Consequently, $r \leq \log |N/K|$. □

We now derive an elementary lemma that states that the maximum order of the nonabelian composition (or chief) factors of a finite group G is preserved in the subgroups and homomorphic images of G.

For a finite group G, recall that $\kappa(G)$ denotes the maximum order of a nonabelian composition factor of G, and $\gamma(G)$ denotes the maximum order of a nonabelian chief factor of G.

Clearly, $\kappa(G) \leq \gamma(G)$. The following result is a direct consequence of the Jordan–Hölder theorem (cf. [38, Lemma 3.3]).

Proposition 3.4.7. Let G be a finite group.

(i) If H is a subgroup of G, then $\kappa(H) \leq \kappa(G)$ and $\gamma(H) \leq \gamma(G)$.

(ii) If $\overline{G}$ is a homomorphic image of G, then $\kappa(\overline{G}) \leq \kappa(G)$ and $\gamma(\overline{G}) \leq \gamma(G)$.

Proof. Suppose that G has a composition series $G = G_1 \rhd \cdots \rhd G_\ell = 1$.

Let $H_i = G_i \cap H$ for $i = 1, \ldots, \ell$. Then H has a normal series $H = H_1 \trianglerighteq \cdots \trianglerighteq H_\ell = 1$, where each factor H_i/H_{i+1} is isomorphic to a subgroup of G_i/G_{i+1}. Thus, $\kappa(H) \leq \kappa(G)$.

Now, under the homomorphism $^{-} : G \rightarrow \overline{G}$, form a normal series $\overline{G} = \overline{G_1} \trianglerighteq \cdots \trianglerighteq \overline{G_\ell} = 1$, where each factor $\overline{G_i}/\overline{G_{i+1}}$ is a homomorphic image of G_i/G_{i+1}. Thus, $\kappa(\overline{G}) \leq \kappa(G)$.

The same argument yields that $\gamma(H) \leq \gamma(G)$ and $\gamma(\overline{G}) \leq \gamma(G)$. □

§5. Small Chief Factors

In this section, we prove that matrix groups $G \leq \mathrm{GL}(n, k)$ such that $\mu(G)$ and $\gamma(G)$ are bounded by a fixed polynomial in the input length are manageable. We begin with the following result, immediate from Corollaries 3.3.10 and 3.3.11.

Proposition 3.5.1. Given $G \leq \mathrm{GL}(n,k)$ and $R \subset G$, where $N := \langle R^G \rangle$ is nonabelian, one can either

(i) prove that N is a minimal normal subgroup of G, or

(ii) find a nonidentity element in a proper G-normal subgroup of N,

in time polynomial in the input length and $\gamma(G)$.

Proof. Write $\gamma = \gamma(G)$.

Suppose $|N| \leq \gamma$. Then list all the elements of N, and find a nonidentity element c such that, in case N has a proper G-normal subgroup, c lies in such a subgroup. If $\langle c^G \rangle = N$, then we have (i), otherwise (ii).

Suppose $|N| > \gamma$. First, form a set X of $\gamma + 1$ distinct elements of N and then the set Y of $\gamma(\gamma+1)$ products of the form $x^{-1}y$, where $x, y \in X$. Now, find $a, b \in N$ such that $[a,b] \neq 1$, and add $[a,b]$ to Y.

Here, we observe that Y contains at least one nonidentity element in a proper G-normal subgroup of N as follows: Suppose there is a G-chief factor N/K. If N/K is nonabelian, then at least one of the $\gamma(\gamma+1)$ products belongs to K. If N/K is abelian, then $[a,b]$ belongs to K. □

We are now ready to prove

Proposition 3.5.2. Matrix groups $G \leq \mathrm{GL}(n,k)$ such that $\mu(G)$ and $\gamma(G)$ are bounded by a fixed polynomial in the input length are manageable.

Proof. Our goal is to find a manageable representation for a given normal subgroup $N = \langle R^G \rangle$ of G, specified by normal generators R. Recall that, since solvable groups are manageable, if N happens to be indeed solvable, one can complete the normal closure to find generators for N and verify its solvability (cf. Theorems 3.2.3 (ii) and 3.3.5). Therefore, we may assume that N is nonsolvable.

The following is a polynomial-time algorithm to find a manageable representation for $N = \langle R^G \rangle$, given by R, when N is nonsolvable.

Let $\bar{}: G \to \mathrm{GL}(k[N])$ denote the conjugation action of G on $k[N]$.

```
procedure SMALL_CHIEF
Input: $G \leq \mathrm{GL}(n, k)$ and $R \subset G$, where $N := \langle R^G \rangle$ is nonsolvable.
Output: a manageable representation $\pi : N \to \mathrm{Sym}(\Omega)$, where $|\Omega|$ is
    polynomially bounded, or a nilpotent group of class at most two $B < N$
    such that $B^G = B$ and $1 < C_N(B) < N$.

begin
    let $Q := R$ and $X$ denote $\langle Q^G \rangle$;
    while $\overline{X}$ is nonabelian containing a proper $\overline{G}$-normal subgroup do
        begin
            find $1 \neq \bar{a} \in \overline{X}$ such that $\langle \bar{a}^{\overline{G}} \rangle < \overline{X}$;
            let $a$ be a preimage of $\bar{a}$ in $G$ so that $\langle a^G \rangle < X$;
            let $Q := \{a\}$ and $X$ denote $\langle Q^G \rangle$;
        end;
    if $\overline{X}$ is abelian then return $B := X$;
    else return $\pi : G \to \mathrm{Aut}(\overline{X})$;
end.
```

At any point, $\overline{X} \neq 1$ so that X acts nontrivially on $k[N]$ by conjugation; that is, $C_N(X) < N$.

Suppose $\overline{X}$ is found to be abelian. Then $[\overline{X}, \overline{X}] = 1$ and thus $[X, X] \leq Z(N)$. Therefore, X is nilpotent of class at most two. Here, observe that $C_N(X) \neq 1$ as follows: if X is abelian, then $1 < X \leq C_N(X)$; if X is nonabelian, then $1 < [X, X] \leq C_N(X)$ since $[X, X] \leq Z(X)$.

If $\overline{X}$ is found to be nonabelian and a minimal normal subgroup of $\overline{G}$, then return π as defined by the conjugation action of $\overline{G}$ on $\overline{X}$. Here, $\pi(N) \neq 1$ since $\overline{X}$ is nonabelian. □

§6. Small Composition Factors

From now on, we relax the condition on the chief factors. That is, we assume that we are dealing with $G \leq \mathrm{GL}(n,k)$ such that $\mu(G)$ and $\kappa(G)$ are polynomially bounded. As in the previous section, our goal is to show the manageability of G, and we will maintain the overall structure of the algorithm roughly the same. In this section, we focus on the main difficulty of finding a nonidentity element of a proper G-normal subgroup of a normal subgroup $N = \langle R^G \rangle$, given by normal generators R, in case N is not minimal normal in G.

First, note that, if N is a minimal normal subgroup of G, then $\gamma(N) \leq \kappa(G)$. When $\gamma(N) \leq \kappa(G)$, Proposition 3.5.2 asserts that all the subgroups of N are manageable; in particular, membership-testing allows us to complete the normal closure and find generators for N. The following procedure tests whether or not a nonabelian normal subgroup $N = \langle R^G \rangle$, given by R, is a minimal normal subgroup of G.

```
procedure TEST_MIN_NORM
Input: $G \leq \mathrm{GL}(n,k)$ and $R \subset G$, where $N := \langle R^G \rangle$ is nonabelian.
Output: a nonabelian simple group $T \trianglelefteq N$ if $N$ is a minimal normal subgroup
    of $G$; otherwise, false.

begin
    assuming $\gamma(N) \leq \kappa(G)$, attempt to find generators $Q$ for $N$ and a non-
        abelian simple group $T \trianglelefteq N$ based on Proposition 3.5.2;
    if the above attempt fails to find $Q$ or $T$ within the assumed polynomial-
        time then return false;
    if the above attempt succeeds, and $\langle T^G \rangle = N$, then return $T$;
    else return false;
end.
```

The algorithm returns the correct answer since N is a minimal normal subgroup of G if and only if $\langle T^G \rangle = N$ (cf. Lemma 3.4.3).

If N is not a minimal normal subgroup of G, then there are normal subgroups K_i, $i \in I$, of G such that N/K_i are G-chief factors. Our main objective now is to locate a nonidentity element in one of these normal subgroups K_i. To find such an element, we will exploit the following important structural properties of chief factors.

Consider one of these chief factors, say N/K. If N/K happens to be abelian, then a nonidentity commutator of elements of N lies in K.

Suppose that N/K happens to nonabelian. Then $N/K = T_1/K \times \cdots \times T_\ell/K$, where the T_i/K are isomorphic to a nonabelian simple group T/K. Furthermore, the T_i/K are the only minimal normal subgroups of N/K, and consequently, G acts transitively on the set $\{T_1/K, \ldots, T_\ell/K\}$ (cf. Lemma 3.4.2). Now, suppose that X/K, where $X \neq K$, is a proper normal subgroup of N/K. Then, without loss of generality, $X/K = T_1/K \times \cdots \times T_j/K$ for some $j < \ell$. By the transitivity of G, there is $g \in G$ such that $X/K \cap X^g/K$ has a fewer than j copies of T/K, or X/K commutes with X^g/K for all $g \in G$ such that $X/K \neq X^g/K$.

The following subroutine, based on the above observation, descends inside a chief factor N/K or constructs the conjugation action of G on a set of the linear spans of normal subgroups of N that commute one another.

```
**procedure** PERM_REP
Input: $G \leq \mathrm{GL}(n,k)$, $R \subset G$, and $x \in G$, where $N := \langle R^G \rangle$ is nonabelian, and
    $L := \langle x^N \rangle$ is nonabelian properly contained in $N$.
Output: one of the following:
    (A) $1 \neq y \in L^g$ for some $g \in G$ such that $\langle y^N \rangle < L^g$;
    (B) $1 \neq c \in N$ such that $\langle c^G \rangle < N$;
    (C) the set $\mathcal{E}$ of $G$-conjugates of $k[L]$, where each $E \in \mathcal{E}$ centralizes all
        $F \in \mathcal{E}$, $F \neq E$, and $|\mathcal{E}| < n^2 \log p$.
```

```
begin
    let $\mathcal{E} := \{k[L]\}$;
    for each $E \in \mathcal{E}$ and each $s \in S$ do
        begin
            if $E^s \notin \mathcal{E}$ and $E^s$ does not commute with some $F \in \mathcal{E}$ then
                begin
                    find $[a,b] \neq 1$, where $a$ and $b$ are basis elements of
                      $E^s$ and $F$, respectively;
                    return $y := [a,b]$ for (A);
                end;
            else if $E^s \notin \mathcal{E}$ then
                add $E^s$ to $\mathcal{E}$;
            if $|\mathcal{E}| \geq n^2 \log p$ then
                begin
                    collect the following in a set $X$: $[a,b] \neq 1$, where
                      $a, b \in L$, and a basis of each $E \in \mathcal{E}$;
                    from $X$, find $c \in N$ such that $\langle c^G \rangle < N$;
                    return $c$ for (B);
                end;
        end;
end.
```

In what follows, we verify the correctness of the procedure PERM_REP.

Suppose that there are $E \in \mathcal{E}$ and $s \in S$ such that $E^s \notin \mathcal{E}$, and E^s does not commute with some $F \in \mathcal{E}$. Here, $E^s = k[L^{g_1}]$ and $F = k[L^{g_2}]$ for some $g_1, g_2 \in G$. Then there are $a \in L^{g_1}$ and $b \in L^{g_2}$ such that $[a,b] \neq 1$. Clearly, $[a,b] \in L^{g_1} \cap L^{g_2}$, where $L^{g_1} \neq L^{g_2}$, so that $L^{g_1} \cap L^{g_2} < L^{g_1}$. Hence, we establish Output (A).

Suppose that, during the for loop, $|\mathcal{E}|$ reaches or exceeds $n^2 \log p$. Then N/K is abelian, or there is $E \in \mathcal{E}$, where $E = k[L^g]$ for some $g \in G$, such that $L^g \leq K$ (cf. Proposition 3.4.6). Let X be a set of elements of N consisting of a commutator $[a,b] \neq 1$, where $a, b \in L$, and a basis of each $E \in \mathcal{E}$. Then at least one element of X must belong to K; hence, we establish Output (B).

If PERM_REP fails to return Outputs (A) and (B), then its outcome is Output

(C). Therefore, PERM_REP returns the correct outputs in all three cases.

To descend further in N/K when PERM_REP outputs (C), we will make use of a point-stabilizer of G under the permutation representation found in (C). We will rely on the following well-known lemma to find such a point-stabilizer (see, e.g., [22, Theorem 3.6A]).

Lemma 3.6.1 (Schreier). Let G be a group and H a subgroup of G. If S is a generating set for G, and R is a complete set of right coset representatives of H in G, then the set $T = \{r_1 s {r_2}^{-1} \,|\, r_1, r_2 \in R, s \in S, \text{ and } r_1 s {r_2}^{-1} \in H\}$ generates H. The set T is called Schreier generators for H. □

With the procedure PERM_REP and Lemma 3.6.1, we are now ready to prove the following.

Proposition 3.6.2. Given $G \leq \mathrm{GL}(n, k)$ and $R \subset G$, where $N := \langle R^G \rangle$ is nonabelian, one can either

(i) prove that N is a minimal normal subgroup of G, or

(ii) find a nonidentity element in a proper G-normal subgroup of N,

in time polynomial in the input length and $\kappa(G)$.

Proof. Let ℓ denote the maximum length of a composition series of a subgroup of $\mathrm{GL}(n, k)$. Here, recall that ℓ is polynomially bounded (cf. Chapter II, §4). As usual, we use S to denote the given generating set for $G \leq \mathrm{GL}(n, k)$. We first outline our main algorithm and then formalize it in the procedure PROPER_NORM.

Step 1. First, recall again that solvability of N can be tested (cf. the proof of Theorem 3.5.2). If N is solvable, then it suffices to return a nontrivial commutator of two elements of N since all the G-chief factors of N are abelian.

Step 2. Suppose that N is nonsolvable, containing a proper G-normal subgroup, and there is a G-chief factor N/K. In Step 2, we construct a sequence of N-normal subgroups

$$N = L_1, L_2, \ldots, L_r,$$

where $r \leq \ell$, each $L_{i+1} < {L_i}^{g_i}$ for some $g_i \in G$, and each $L = L_i$ is represented by an element x such that $L = \langle x^N \rangle$. Step 2 is a loop, consisting of four sub-steps (a)–(d), that iterates at most ℓ^2 times and forces L to step down the above sequence at most ℓ times.

Step 2 (a). If L is found to be abelian or a minimal normal subgroup of N, the loop halts and returns $\langle L^G \rangle$ (cf. Proposition 3.4.4).

Step 2 (b). Suppose that L is nonabelian. Step 2 (b) calls the procedure PERM_REP as a subroutine. If PERM_REP returns an element y for Output (A), then we let $x := y$ and descend the sequence with a new $L := \langle x^N \rangle$. If PERM_REP returns an element c for Output (B), then we halt the loop and return $c \in N$ such that $\langle c^G \rangle < N$.

Steps 2 (c), (d). Now, suppose that PERM_REP returns Output (C). Let $E = k[L]$. Here, G acts on the set $\mathcal{E}$ of polynomially-bounded size. Thus, we may assume that we have Schreier generators U for the point-stabilizer G_E. Since N normalizes L, we know N stabilizes $E = k[L]$ so that $N \leq G_E$. Thus, $L = \langle x^N \rangle \leq \langle x^{G_E} \rangle$.

Steps 2 (c) and (d) consider the following two cases, respectively.

(1) There is $1 \neq g \in G_E$ such that $L \neq L^g$.

(2) G_E normalizes L.

When Case (1) holds, Step 2 (c) works as follows. As $G_E = \langle U \rangle$, there is $u \in U$ such that $L \neq L^u$. Recall that $k[L^u] = k[L]$ is noncommutative (otherwise, L would be abelian). Hence, there are basis elements a of $k[L]$ and b of $k[L^u]$, where $a \in L$ and $b \in L^u$, such that $[a, b] \neq 1$. Since $[a, b] \in L \cap L^u < L$, we step down the tower.

When Case (2) holds, Step 2 (d) works as follows. We consider the case when $L \not\leq K$. Here, we have $L^{G_E} = L$ so that $L = \langle x^N \rangle \leq \langle x^{G_E} \rangle \leq \langle L^{G_E} \rangle = L$ and thus $L = \langle x^N \rangle = \langle x^{G_E} \rangle$. Therefore, distinct elements of L can be now listed so that we can find $a \in L$ such that $\langle a^N \rangle < L$ (cf. Corollary 3.3.10, Proposition 3.4.5).

Every time L steps down the tower, we first assume Case (1) and repeat Step 2 (c) for ℓ times. After these ℓ iterations, if L is not found to be a minimal normal subgroup of N, then Case (2) must hold. If $L \not\leq K$, then Step 2 (d) finds a proper N-normal subgroup of L, and we step down the tower.

Finally, when the loop reaches $L = L_\ell$, then we conclude that either L is a minimal normal subgroup of N, or $L \leq K$.

The following procedure PROPER_NORM formalizes our method.

```
procedure PROPER_NORM
Input: $G \leq \mathrm{GL}(n, k)$ and $R \subset G$, where $N := \langle R^G \rangle$ is nonabelian.
Output: a nonidentity element in a proper $G$-normal subgroup of $N$, or "$N$ is a
    minimal normal subgroup of $G$".

begin
Step 1. (* Halt if $N$ is solvable or a minimal normal subgroup of $G$. *)
    if $N$ is solvable then
        find $a, b \in N$ such that $[a, b] \neq 1$ and return $d := [a, b]$;
    if TEST_MIN_NORM($G, R$) then
        return "$N$ is a minimal normal subgroup of $G$";
Step 2. (* Form a sequence $N = L_1, \ldots, L_r$, where $r \leq \ell$. *)
    find $a \in N$ such that $\langle a^N \rangle < N$;
    let $x := a$ and $L$ denote $\langle x^N \rangle$;
    let $i := 1$ and $j := 1$;
    while $i \leq \ell$ do
        begin
            let $found := false$;
        (a). if $L$ is abelian then return $d := x$;
            if TEST_MIN_NORM$(G, \{x\})$ then return $d := x$;
        (b). PERM_REP$(G, R, x)$;
            if PERM_REP returns $y$ for (A) then
                let $found := true$, $x := y$, and $L$ denote $\langle x^N \rangle$;
            else if PERM_REP returns $c$ for (B) then return $d := c$;
            else
                begin
                    let $E$ denote $k[L]$;
                    under the $G$-action on $\mathcal{E}$ by conjugation, obtain
                      Schreier generators $U$ for the point-stabilizer $G_E$;
        (c). (* When $L^{G_E} \neq L$, we find $1 \neq c \in [L, L^u] < L$ for some $u \in U$. *)
                    if $j \leq \ell$ then
                        begin
                            let $Y := \emptyset$;
                            for each $u \in U$ do
                                add $[a, b] \neq 1$, where $a \in L$ and
                                  $b \in L^u$, to $Y$;
                            from $Y$, find $c \in L$ such that $\langle c^N \rangle \leq L$
                              (and $\langle c^N \rangle < L$ when $L^{G_E} \neq L$);
                            let $x := c$ and $L$ denote $\langle x^N \rangle$;
                            let $j := j + 1$;
                        end;
        (d). (* When $j = \ell$, we have $L^{G_E} = L$ and thus $\langle x^N \rangle = \langle x^{G_E} \rangle$. *)
                    else
                        begin
                            as $L^{G_E} = L$, find $a \in L$ such that
                              $\langle a^N \rangle \leq L$ (and $\langle a^N \rangle < L$ if $L \not\leq K$);
                            let $x := a$ and $L$ denote $\langle x^N \rangle$;
                            let $found := true$;
                        end;
                end;
            if $found$ then let $i := i + 1$ and $j := 1$;
        end;
    return $d := x$;
end.                                                                     □
```

We are finally ready to prove Theorem 3.1.1. As we have already discussed in

§2, in order to prove Theorem 3.1.1, it suffices to establish manageability.

Proposition 3.6.3. Matrix groups $G \leq \mathrm{GL}(n,k)$ such that $\mu(G)$ and $\kappa(G)$ are bounded by a fixed polynomial in the input length are manageable.

Proof. Recall again that, given a normal subgroup $N = \langle R^G \rangle$ of G, specified by normal generators R, one can test solvability of N (cf. the proof of Theorem 3.5.2). Therefore, we may assume that N is nonsolvable.

The following is a polynomial-time algorithm to find a manageable representation for $N = \langle R^G \rangle$, given by R, when N is nonsolvable.

Let $\bar{} : G \to \mathrm{GL}(k[N])$ denote the conjugation action of G on $k[N]$.

```
procedure SMALL_COMP
Input: $G \leq \mathrm{GL}(n,k)$ and $R \subset G$, where $N := \langle R^G \rangle$ is nonsolvable.
Output: a manageable representation $\pi : N \to \mathrm{Sym}(\Omega)$, where $|\Omega|$ is
    polynomially bounded, or a nilpotent group of class at most two $B < N$
    such that $B^G = B$ and $1 < C_N(B) < N$.

begin
    let $Q := R$ and $X$ denote $\langle Q^G \rangle$;
    while $\overline{X}$ is nonabelian containing a proper $\overline{G}$-normal subgroup do
        begin
            let $\bar{a}$ := PROPER_NORM($\overline{G}, \overline{Q}$) (i.e, find $1 \neq \bar{a} \in \overline{X}$
              such that $\langle \bar{a}^{\overline{G}} \rangle < \overline{X}$);
            let $a$ be a preimage of $\bar{a}$ in $G$ so that $\langle a^G \rangle < X$;
            let $Q := \{a\}$ and $X$ denote $\langle Q^G \rangle$;
        end;
    if $\overline{X}$ is abelian then return $B := X$;
    else
        begin
            let $\overline{T}$ := TEST_MIN_NORM($\overline{G}, \overline{Q}$);
            collect the $\overline{G}$-conjugates of each $\bar{t} \in \overline{T}$ in a set $\mathcal{T}$;
            return $\pi : G \to \mathrm{Sym}(\mathcal{T})$;
        end;
end.
```

The argument in the proof of Proposition 3.5.2 shows that B is nilpotent of class at most two such that $B^G = B$ and $1 < C_N(B) < N$. □

§7. Finding Composition Series and Kernels

In this section, we prove Corollary 3.1.2. We continue to assume the basic hypothesis of the preceding section. Assume also that, for $G \leq \mathrm{GL}(n,k)$ and a normal subgroup N of G, an element Ng of the quotient group G/N is a pair comprised of generators for N and a right coset representative g.

We first describe an algorithm to find composition series for a manageable $G \leq \mathrm{GL}(n,k)$. The following result is based on Proposition 3.3.9 and essentially solves our problem.

Lemma 3.7.1. Given the following inputs:

(i) $G \leq \mathrm{GL}(n,k)$, a normal subgroup N of G such that G/N is nonabelian, and

(ii) $a, b \in G$, where $a, b \notin N$, such that Na or Nb belongs to a proper normal subgroup of G/N,

one can find $c \in G$, where $c \notin N$, such that Nc belongs to a proper normal subgroup of G/N in time polynomial in the input length, $\mu(G)$, and $\kappa(G)$.

Proof. If $[Na, Nb] \neq N$, then $[a,b]$ suffices for c as

$$Nc = [Na, Nb] \in \langle (Na)^{G/N} \rangle \cap \langle (Nb)^{G/N} \rangle.$$

Suppose $[Na, Nb] = N$. Test whether or not Na centralizes $\langle (Nb)^{G/N} \rangle =$

$(N\langle b^G\rangle)/N$, and find $d \in N\langle b^G\rangle$ such that $[Na, Nd] \neq N$ in case Na does not centralize $\langle (Nb)^{G/N}\rangle$.

If such d is found, then $[a, d]$ suffices for c since $[Na, Nd] \in \langle (Na)^{G/N}\rangle \cap \langle (Nb)^{G/N}\rangle$.

Suppose Na centralizes $\langle (Nb)^{G/N}\rangle$. Test whether or not $Na \in Z(G/N)$. If $Na \in Z(G/N)$, then return $c = a$ since $Z(G/N)$ is a proper normal subgroup of G/N. If $Na \notin Z(G/N)$, then $\langle (Nb)^{G/N}\rangle < G/N$; thus, return $c = b$. □

The following result, based on Proposition 3.5.1, refines a subnormal series, and therefore, proves Corollary 3.1.2 (iv).

Proposition 3.7.2. Given $G \leq \mathrm{GL}(n, k)$ and a normal subgroup N of G, one can either

(i) prove that G/N is simple, or

(ii) find a normal subgroup K of G such that $N \lhd K \lhd G$,

in time polynomial in the input length, $\mu(G)$, and $\kappa(G)$.

Proof. Suppose G/N is abelian. Choose $g \in G$ such that $g \notin N$. The hypothesis on $\mu(G)$ enables us to determine the order of the element $Ng \in G/N$. By forming suitable prime powers e, find an element $(Ng)^e$ of a prime order.

Suppose G/N is nonabelian. Based on Lemma 3.7.1, use the method of Proposition 3.5.1 on the factor group G/N. That is, if G/N is not simple, list at least $\kappa(G)$ distinct right coset representatives of N in G, and find an element $g \in G$, where $g \notin N$, such that Ng belongs to a proper normal subgroup of G/N. □

Next, we prove Corollary 3.1.2 (v). In what follows, p is an arbitrary prime, unrelated to char k. First, we observe the following.

Lemma 3.7.3. Suppose a finite group G has an abelian normal p-subgroup A. If a is an element of A of order p, then $\langle a^G \rangle$ is an elementary abelian p-group.

Proof. Denote $\Omega_1(A)$ the subgroup of A generated by all the elements of A of order p. Note that $\Omega_1(A)$ is characteristic in A; therefore, $\Omega_1(A)$ is normal in G.

Since A is abelian, every element of $\Omega_1(A)$ has order at most p. That is, $\Omega_1(A)$ is elementary abelian. Since $a \in \Omega_1(A)$, we have $\langle a^G \rangle \leq \Omega_1(A)$. Therefore, $\langle a^G \rangle$ is elementary abelian. □

The following result proves Corollary 3.1.2 (v) (see [34, §4] for a related result in permutation groups).

Proposition 3.7.4. Given $G \leq \mathrm{GL}(n, k)$ and normal subgroups N and K of G such that $K < N$, one can

(i) prove that N/K is a nonabelian chief factor of G,

(ii) prove that N/K is elementary abelian, or

(iii) find a normal subgroup L of G such that $K < L < N$,

in time polynomial in the input length, $\mu(G)$, and $\kappa(G)$.

Proof. First, we find a composition series for N/K. Then we have a simple group $T/K \trianglelefteq\trianglelefteq N/K$. Form $\langle (T/K)^{G/K} \rangle = \langle T^G \rangle / K$ and write $M = \langle T^G \rangle$.

If T/K is nonabelian, then M/K is a nonabelian minimal normal subgroup of G/K. If $M/K = N/K$, then we establish (i). Otherwise, we have $M/K < N/K$ and return M as L for (iii).

Suppose that T/K is a cyclic group of order p. Then M/K is a p-group. In the derived series of M/K, find the nontrivial abelian subgroup A/K. Find an element $Ka \in A/K$ of order p. Form $\langle (Ka)^{G/K} \rangle = (K\langle a \rangle^G)/K$ and write $L = K\langle a \rangle^G$. Then L/K is elementary abelian. If $L/K = N/K$, then we establish (ii). Otherwise, we have $L/K < N/K$ and return L for (iii). □

As in the solvable case [39, §4.6], one can also find the kernel of a homomorphism into a manageable group in the desired timing. For $G \leq \mathrm{GL}(n, k)$, generated by S, suppose that we are given a homomorphism $\phi : G \to M$ specified by $\phi(S)$ for some manageable group M. Then obtain a constructive presentation of $\phi(G)$ and thus $G \bmod \operatorname{Ker} \phi$. Form normal generators for $\operatorname{Ker} \phi$, and finally complete the normal closure to find generators for $\operatorname{Ker} \phi$. Therefore, Corollary 3.1.2 (vi) holds.

Now, observe that, for $G \leq \mathrm{GL}(n, k)$ and a normal subgroup N of G, the centralizer $C_G(N)$ is the kernel of the conjugacy action of G on the linear span $k[N]$. Thus, one can find the centralizer of a normal subgroup, and in particular, the center $Z(G)$, in the desired timing.

CHAPTER IV

DIVIDE AND CONQUER IN MATRIX GROUPS

In this chapter, we investigate the polynomial-time computability of the problems of finding stabilizers of vectors and subspaces. The main result is a theorem (stated as Theorem 4.1.4) that provides a divide-and-conquer paradigm with respect to cosets and invariant subspaces in Γ_d.

We first describe algorithms for the vector-stabilizer and subspace-stabilizer problems in Γ_d based on the result of Theorem 4.1.4. The rest of the chapter is devoted to the proof of Theorem 4.1.4.

§1. Statement of the Results

A familiar permutation group problem known for generalizing the graph-isomorphism problem (GRAPH-ISO) is the set-stabilizer problem (SET-STAB): given a permutation group $G \le \mathrm{Sym}(\Omega)$ and a subset $\Delta \subset \Omega$, find the subgroup $\{g \in G \mid \Delta^g = \Delta\}$.

Let k be a finite field and V an n-dimensional vector space over k. In this chapter, we consider matrix group problems resembling SET-STAB.

Vector-stabilizer (VEC-STAB).

Input: a matrix group $G \le \mathrm{GL}(V)$ and a vector $v \in V$.

Find: $C_G(v) = \{g \in G \mid v^g = v\}$.

Subspace-stabilizer (SUBSP-STAB).

Input: a matrix group $G \leq \mathrm{GL}(V)$ and a subspace $W \subset V$.

Find: $N_G(W) = \{g \in G \mid W^g = W\}$.

Recall that $\leq^p$ denotes "is polynomial-time reducible to" as discussed in Chapter II. The following relationship is known [40, §10].

$$\text{GRAPH-ISO} \leq^p \text{SET-STAB} \leq^p \text{VEC-STAB} \leq^p \text{SUBSP-STAB}.$$

It is generally considered that GRAPH-ISO and even SET-STAB are not particularly hard in practice. Nevertheless, none of these problems have proven to be solvable in polynomial time. On the other hand, as with GRAPH-ISO [27], certain evidence suggests that the equivalent decision version of SET-STAB is unlikely to be **NP**-complete: if it were **NP**-complete, the polynomial-time hierarchy would collapse to $\Sigma_2^p = \Pi_2^p$ [11].

Polynomial-time solutions have been found for certain restricted classes of inputs. In particular, the following class of groups has played an important rôle in the theory of polynomial-time computability in permutation groups.

Definition. For an integer $d > 0$, let Γ_d denote the class of finite groups all of whose nonabelian composition factors are isomorphic to subgroups of S_d.

The following theorem is the celebrated result of [8].

Theorem 4.1.1 (Babai–Cameron–Pálfy). For an integer $d > 0$, there is a function $c(d)$ satisfying the following: if G is a primitive permutation group of degree m such that $G \in \Gamma_d$, then $|G| \leq m^{c(d)}$. □

The function $c(d)$ was further studied in [9] and [44] (cf. [37]). See also [26] for related work in Γ_d.

Fix an constant $d > 0$. Luks has shown earlier in [38] that one can solve SET-STAB in Γ_d in polynomial time. In fact, it was in Luks's complexity analysis [38] when Γ_d originally arose and motivated deeper investigations resulting in Theorem 4.1.1. Luks went on to show that one can solve VEC-STAB and SUBSP-STAB in solvable matrix groups $G \leq \mathrm{GL}(V)$ in time polynomial in the input length and the largest prime dividing $|G|$ other than $\mathrm{char}\, k$.

The following is our main result.

Theorem 4.1.2. Fix an integer constant $d > 0$. Given $G \leq \mathrm{GL}(V)$ such that $G \in \Gamma_d$, one can solve the following problems in time polynomial in these three parameters: the input length, the largest prime dividing $|G|$, and $\mathrm{char}\, k$.

(i) Given $v \in V$, find $C_G(v)$ (VEC-STAB).

(ii) Given $W \subseteq V$, find $N_G(W)$ (SUBSP-STAB).

We list two applications of Theorem 4.1.2 in the following corollary.

Corollary 4.1.3. The list of problems in Theorem 4.1.2 continues as follows.

(i) Given $x \in \mathrm{GL}(V)$, find $C_G(x)$; further, given $X \leq \mathrm{GL}(V)$, find $C_G(X)$.

(ii) Given $H \leq \mathrm{GL}(V)$ such that $H \in \Gamma_d$, find $G \cap H$.

Critical to Theorem 4.1.2 is the following divide-and-conquer paradigm that is built on [39, Theorem 6.1] for Γ_d.

Theorem 4.1.4. Fix an integer constant $d > 0$. Given $G \leq \mathrm{GL}(V)$ such that $G \in \Gamma_d$, one can perform one of the following in time polynomial in these three parameters: the input length, the largest prime dividing $|G|$, and $\operatorname{char} k$.

(i) Prove that G is nonabelian simple.

(ii) Find an abelian subgroup A of G such that $|G : A| \leq 24n$.

(iii) Find a proper G-subspace $W \subset V$.

(iv) Find a subgroup H of G and a set of H-subspaces $\{V_1, \ldots, V_m\}$, $m \geq 2$, such that

(a) $V = V_1 \oplus \cdots \oplus V_m$,

(b) $\dim_k V_i = n/m$ for $i = 1, \ldots, m$, and

(c) $|G : H| = O(m^{c_1})$ for a constant $c_1 > 0$.

To prove Theorem 4.1.4 in the sections to follow, we begin with preliminary results concerning basic representation theory, abelian groups and class-2 nilpotent groups, semisimple groups, and matrix groups in Γ_d. We then develop divide-and-conquer tools involving abelian quotients. Most of these algorithms are adapted from the solvable-group machinery of [39]. With the same spirit, we develop another tool involving nonabelian quotients. In the last section, we put all of these pieces together to complete the proof of Theorem 4.1.4.

§2. Vector-Stabilizers and Subspace-Stabilizers

In this section, we prove Theorem 4.1.2 and Corollary 4.1.3 based on Theorem 4.1.4. We will prove Theorem 4.1.4 in the sections to follow. The method of our proof in this section is almost identical to Luks's in [39, §§6.2–6.4]. We present the complete proof, including the part that was omitted in [39], since it is crucial to our main result.

Throughout this section, let k be a finite field and V an n-dimensional vector space over k. Fix an integer constant $d > 0$. For a given input $G \leq \mathrm{GL}(V)$, assume that $G \in \Gamma_d$, and $\mu(G)$ and $\mathrm{char}\, k$ are polynomially bounded in the input length.

In general, the divide-and-conquer paradigm of Theorem 4.1.4 applies to problems that have the following characteristics.

(1) One can solve the problem in polynomial time for abelian groups.

(2) Given a proper G-subspace $W \subset V$, one can solve the problem in a polynomial number of steps together with recursive calls to induced problems on W and V/W.

Note that, for nonabelian simple groups, we may apply brute-force methods.

In what follows, we consider two applications of this paradigm: VEC-STAB and SUBSP-STAB.

First, we solve VEC-STAB. To accommodate recursion involving cosets, we consider the following generalization.

For $G \leq \mathrm{GL}(V)$, a function $f : G \to V$ is a crossed homomorphism (or derivation) if $f(xy) = f(x)^y + f(y)$ for all $x, y \in G$.

Crossed-homomorphism fiber.

Input: $G \leq \mathrm{GL}(V)$, a crossed homomorphism $f : G \to V$, and $v \in V$.

Find: $\{x \in G \mid f(x) = v\}$.

Observe that the solution to $f(x) = v$ is either $\emptyset$ or a right coset of the subgroup $\{x \in G \mid f(x) = 0\}$.

Let $v \in V$ and $f(x) = v^x - v$. Then $C_G(v)$ is the solution to $f(x) = 0$. More generally, for another given $w \in V$, the solution to $f(x) = w - v$ solves the following problem.

Vector-transporter.

Input: $G \leq \mathrm{GL}(V)$ and $v, w \in V$.

Find: $\mathrm{Trans}_G(v, w) = \{g \in G \mid v^g = w\}$.

Proof of Theorem 4.1.2 (i). We describe an algorithm to solve the crossed-homomorphism fiber problem. If G is nonabelian simple, then it is trivial. Therefore, we consider the remaining two cases.

Case 1. Suppose that G is abelian, where $G = \langle S \rangle$.

First, form a G-subspace $U = \mathrm{Span}(f(G)) = \mathrm{Span}(f(S))^G$. Here, let $f(g_1), \ldots, f(g_m)$, where each $g_i \in G$, denote a basis of U.

If $v \notin U$, then return $\emptyset$.

Suppose that $v \in U$. Observe that, since G is abelian, if there is $g \in G$ such that $f(g) = v$, then $f(x)^g = f(x) + v^x - v$ for all $x \in G$. Let $\widehat{\ } : G \to \mathrm{GL}(U)$ be the restriction of G on U. Here, form a linear transformation t of U defined by $f(g_i)^t = f(g_i) + v^{g_i} - v$ for the basis $f(g_1), \ldots, f(g_m)$. If $t \in \widehat{G}$, then a constructive membership test finds an element $\hat{a} \in \widehat{G}$ such that $f(x)^{\hat{a}} = f(x) + v^x - v$ for all $x \in G$. If $C = C_G(U)$, the kernel of $\widehat{\ } : G \to \mathrm{GL}(U)$, and a is a preimage of $\hat{a}$, then $Ca = \{g \in G \mid f(x)^g = f(x) + v^x - v \text{ for all } x \in G\}$.

Now, observe that for $y \in C$, we have $f(ya) = v$ if and only if $f(y) = v - f(a)$. Here, $f(y_1 y_2) = f(y_1) + f(y_2)$ for all $y_1, y_2 \in C$; thus, $f|_C : C \to U$ is a homomorphism.

The equation $f(y) = v - f(a)$ can be solved via membership-testing, and $\{y \in C \mid f(y) = 0\}$ is the kernel of $f|_C$.

Case 2. Suppose that we have a proper G-subspace $W \subset V$.

Let $\bar{\ } : V \to V/W$ be the homomorphism defined by $v \mapsto W + v$ for $v \in V$ and $\bar{\ } : G \to \mathrm{GL}(\overline{V})$ the linear representation defined by $\bar{v}^{\bar{g}} \mapsto \overline{v^g}$ for $v \in V$ and $g \in G$. Let $\bar{f} : \overline{G} \to \overline{V}$ be the crossed homomorphism defined by $\bar{f}(\bar{x}) = \overline{f(x)}$ for $x \in G$.

Solving for $\{\bar{x} \in \overline{G} \mid \bar{f}(\bar{x}) = \bar{v}\}$, we obtain a coset $\overline{H_0}\bar{a}$, where $\overline{H_0} = \{\bar{x} \in \overline{G} \mid \bar{f}(\bar{x}) = \bar{0}\}$ and $\bar{a} \in \overline{G}$ such that $\bar{f}(\bar{a}) = \bar{v}$. Let H_0 denote a preimage of $\overline{H_0}$. Find the kernel N of the action $\bar{\ } : G \to \mathrm{GL}(\overline{V})$. If $H = \langle H_0, N \rangle$, and a is a preimage of $\bar{a}$, then $Ha = \{x \in G \mid \bar{f}(\bar{x}) = \bar{v}\}$.

Observe that, in general, $f(xy) = v$ if and only if $f(x) = (v - f(y))^{y^{-1}}$ for $x, y \in G$ and $v \in V$.

Since $\bar{f}(\bar{y}) = \bar{0}$ for all $y \in H$, it follows that $f(H) \subseteq W$. Let $\hat{\ } : G \to \mathrm{GL}(W)$ be the restriction of G on W and $\hat{f} : \widehat{H} \to W$ the crossed homomorphism defined by $\hat{f}(\hat{y}) = \widehat{f(y)}$ for $y \in H$.

Now, solving for $\{\hat{y} \in \widehat{H} \mid \hat{f}(\hat{y}) = (v - f(a))^{a^{-1}}\}$, we first obtain a coset $\widehat{K_0}\hat{b}$, where $\widehat{K_0} = \{\hat{y} \in \widehat{H} \mid \hat{f}(\hat{y}) = \hat{0}\}$ and $\hat{b} \in \widehat{H}$ such that $\hat{f}(\hat{b}) = (v - f(a))^{a^{-1}}$, and then a coset $Kb = \{y \in H \mid f(y) = (v - f(a))^{a^{-1}}\}$.

The solution to $f(x) = v$ is Kba. □

For SUBSP-STAB, we consider the following generalization.

Subspace-transporter.

Input: $G \leq \mathrm{GL}(V)$ and subspaces $W_1, W_2 \subset V$.

Find: $\mathrm{Trans}_G(W_1, W_2) = \{g \in G \mid {W_1}^g = W_2\}$.

Here, observe that $\mathrm{Trans}_G(W_1, W_2)$ is either empty or a right coset of $N_G(W_1)$. The following proof involves reductions to the vector transporter problem.

Proof of Theorem 4.1.2 (ii). We describe an algorithm to solve the subspace transporter problem. As before, we consider two cases.

Case 1. Suppose that G is abelian.

Observe that, since G is abelian, for any $x \in G$, we have $\mathrm{Trans}_G(W_1, W_2) = \mathrm{Trans}_G({W_1}^x, {W_2}^x)$.

Form $U = \mathrm{Span}({W_1}^G)$. Also, find $g_1, \ldots, g_m \in G$ such that $U = {W_1}^{g_1} + \cdots + {W_1}^{g_m}$, where each ${W_1}^{g_i} \not\subseteq {W_1}^{g_1} + \cdots + {W_1}^{g_{i-1}}$. Clearly, U is G-invariant; therefore, we may assume that $U = V$. Here, observe that, if $\dim_k W_1 = 1$, then ${W_1}^{g_1} + \cdots + {W_1}^{g_m}$ is necessarily a direct sum.

First, suppose that ${W_1}^{g_1} + \cdots + {W_1}^{g_m}$ is not a direct sum; that is, there is ${W_1}^{g_i}$ such that $0 \neq {W_1}^{g_i} \cap ({W_1}^{g_1} + \cdots + {W_1}^{g_{i-1}}) \subset {W_1}^{g_i}$. Without loss of generality, assume that $g_i = 1$. Let $X = W_1 \cap ({W_1}^{g_1} + \cdots + {W_1}^{g_{i-1}})$ and $Y = W_2 \cap ({W_2}^{g_1} + \cdots + {W_2}^{g_{i-1}})$. Then $N_G(W_1) \leq N_G(X)$ and $\mathrm{Trans}_G(W_1, W_2) \subseteq \mathrm{Trans}_G(X, Y)$. Suppose that X is G-invariant. If there is $g \in G$ such that ${W_1}^g = W_2$, then $X = Y$. Therefore, we recursively find $\mathrm{Trans}_G(W_1/X, W_2/X)$ under the action $G \to \mathrm{GL}(V/X)$. Suppose otherwise; that is, $N_G(X) < G$. First, we recursively solve for $\mathrm{Trans}_G(X, Y)$. If the solution is empty, then $\mathrm{Trans}_G(W_1, W_2) = \emptyset$; otherwise, we have $H = N_G(X)$ and $a \in G$ such that $Ha = \mathrm{Trans}_G(X, Y)$. Here, X is clearly H-invariant, and $X = Y^{a^{-1}} \subset {W_2}^{a^{-1}}$. Since $\mathrm{Trans}_G(W_1, W_2) \subseteq Ha$, it suffices to find $\mathrm{Trans}_H(W_1/X, {W_2}^{a^{-1}}/X)$ under the action $H \to \mathrm{GL}(V/X)$.

Now, suppose that $V = {W_1}^{g_1} \oplus \cdots \oplus {W_1}^{g_m}$. If there is $g \in G$ such that ${W_1}^g = W_2$, then we also have $V = {W_2}^{g_1} \oplus \cdots \oplus {W_2}^{g_m}$. For $i = 1, \ldots, m$, find $e_i \in \mathrm{End}_k(V)$ such that e_i is the projection from V onto ${W_1}^{g_i}$ and $f_i \in \mathrm{End}_k(V)$ such that f_i is the projection from V onto ${W_2}^{g_i}$. Choose $t \in G$. Observe that ${W_1}^t = W_2$ if and only if ${e_i}^t = f_i$ for $i = 1, \ldots, m$. To see this, let $v \in V$ such that $v = w_1 + \cdots + w_m$, where each $w_i \in {W_1}^{g_i}$. If ${W_1}^t = W_2$, then, for each e_i, we have $v^{e_i t} = {w_i}^t = v^{tf_i}$. Conversely, if ${e_i}^t = f_i$ for $i = 1, \ldots, m$, then, for each $w_i \in {W_1}^{g_i}$, we have ${w_i}^t = {w_i}^{e_i t} = {w_i}^{tf_i} \in {W_2}^{g_i}$. That is, under the G-action on $\mathrm{End}_k(V)$ by conjugation, it suffices to find the vector transporters $t \in G$ such that ${e_i}^t = f_i$ for $i = 1, \ldots, m$.

Case 2. Suppose that we have a proper G-subspace $W \subset V$.

First, note that $\mathrm{Trans}_G(W_1, W_2) \subseteq \mathrm{Trans}_G(W_1 \cap W, W_2 \cap W)$. Recursively, solve for $\mathrm{Trans}_G(W_1 \cap W, W_2 \cap W)$ under the the restriction $G \to \mathrm{GL}(W)$. If the solution is empty, then $\mathrm{Trans}_G(W_1, W_2) = \emptyset$; otherwise, we have $H = N_G(W_1 \cap W)$ and $a \in G$ such that $Ha = \mathrm{Trans}_G(W_1 \cap W, W_2 \cap W)$. Then it suffices to find $\mathrm{Trans}_H(W_1, {W_2}^{a^{-1}})$.

Now, solve recursively for $\mathrm{Trans}_H((W + W_1)/W, (W + {W_2}^{a^{-1}})/W)$ under the action $H \to \mathrm{GL}(V/W)$. If the solution is empty, then $\mathrm{Trans}_H(W_1, {W_2}^{a^{-1}}) = \emptyset$; otherwise, we have $K = N_H((W + W_1)/W)$ and $b \in H$ such that $Kb = \mathrm{Trans}_H((W + W_1)/W, (W + {W_2}^{a^{-1}})/W)$. Then all we need is the solution for $\mathrm{Trans}_K(W_1, {W_2}^{a^{-1}b^{-1}})$.

Write $W_0 = {W_2}^{a^{-1}b^{-1}}$. Suppose that there is $g \in K$ such that ${W_1}^g = W_0$. Form $X = W + W_1 = W + W_0$ and $Y = W_1 \cap W = W_0 \cap W$. Here, we have $X/Y = W/Y \oplus W_1/Y = W/Y + W_0/Y$. Find $e_1 \in \mathrm{End}_k(X/Y)$ such that e_1 is the projection from X/Y onto W_1/Y and $e_0 \in \mathrm{End}_k(X/Y)$ such that e_0 is the projection from X/Y onto W_0/Y. Let $\bar{\ }: K \to \mathrm{GL}(X/Y)$ denote the induced action of K on X/Y. Choose $t \in K$. Then observe that ${W_1}^t = W_0$ if and only if ${e_1}^{\bar{t}} = e_0$. To see this, suppose first that $\bar{t}^{-1} e_1 \bar{t} = e_0$. Then $(W_1/Y)^{\bar{t}} = (X/Y)^{e_1 \bar{t}} = (X/Y)^{\bar{t} e_0} = (X/Y)^{e_0} = W_0/Y$. Conversely, fix $Y + x = (Y + w_1) + (Y + w_0)$, where $w_1 \in W_1$ and $w_0 \in W_0$, and suppose that ${W_1}^t = W_0$. Then $(Y+x)^{\bar{t}^{-1}e_1\bar{t}} = (Y+x^{t^{-1}})^{e_1\bar{t}} = ((Y+{w_1}^{t^{-1}})+(Y+{w_0}^{t^{-1}}))^{e_1\bar{t}} = (Y+{w_0}^{t^{-1}})^{\bar{t}} = Y + w_0 = (Y+x)^{e_0}$.

Therefore, under the K-action on $\mathrm{End}_k(X/Y)$ by conjugation, it suffices to find the vector transporter $\mathrm{Trans}_K(e_1, e_0)$. □

Corollary 4.1.3 is immediate from elementary observations.

Proof of Corollary 4.1.3. Given $x \in \mathrm{GL}(V)$, the centralizer $C_G(x)$ is the vector-stabilizer of $x \in \mathrm{End}_k(V)$ under the action of G on $\mathrm{End}_k(V)$ by conjugation.

Given $H \leq \mathrm{GL}(V)$, under the natural action of $G \times H$ on $V \oplus V$, the centralizer of the linear transformation $(v, w) \mapsto (w, v)$ for all $v, w \in V$ is the subgroup $\{(x, x) \mid x \in G \cap H\}$. □

§3. Complete Reducibility and Tensor Products

Throughout this section, let k be a finite field and V an n-dimensional vector space over k. We note, however, that Theorem 4.3.1 and Lemma 4.3.2 in fact hold on any ground field.

We begin with a classical theorem of A. H. Clifford (see, e.g., [54, Theorems 16.1, 16.2]).

Theorem 4.3.1 (Clifford). Let G be an irreducible subgroup of $\mathrm{GL}(V)$ and N a normal subgroup of G.

(i) If W is a minimal N-subspace of V, there are $1 = g_1, \ldots, g_r \in G$, where $r \mid n$, such that V decomposes as a direct sum

$$V = W^{g_1} \oplus \cdots \oplus W^{g_r}.$$

In particular, N is completely reducible, and the irreducible components $N|W^{g_i}$ are isomorphic linear groups of degree n/r.

(ii) If $U_1, \ldots, U_h$ are the distinct homogeneous N-subspaces of V determined by the minimal N-subspaces $W^{g_1}, \ldots, W^{g_r}$ of (i), then V decomposes as a direct sum

$$V = U_1 \oplus \cdots \oplus U_h,$$

where each U_j is the direct sum of all the N-isomorphic W^{g_i}. If $h \geq 2$, then $\{U_1, \ldots, U_h\}$ forms a system of imprimitivity for G. □

In (i) above, suppose that a map $\phi_i : W \to W^{g_i}$ is an N-isomorphism; that is, the irreducible components $N|W$ and $N|W^{g_i}$ are equivalent: if $w \in W$, then $\phi_i(w^x) = \phi_i(w)^x$ for all $x \in N$. If all the W^{g_i} are pairwise N-isomorphic (in particular, when G is primitive), then all the irreducible components $N|W^{g_i}$ are pairwise equivalent, and N acts faithfully on each W^{g_i}. The next observation follows immediately from Theorem 4.3.1 (cf. [54, Lemma 16.4]).

Lemma 4.3.2. Let $G = NM$ be an irreducible subgroup of $\mathrm{GL}(V)$, where N and M are normal subgroups of G centralizing each other. Let W be a minimal N-subspace of V. If $1 = g_1, \ldots, g_r \in M$ such that $V = W^{g_1} \oplus \cdots \oplus W^{g_r}$, then the W^{g_i} are pairwise N-isomorphic. □

Let G be an irreducible subgroup of $\mathrm{GL}(V)$ and $K = \mathrm{End}_{kG}(V)$. By Schur's lemma, K is a finite extension of k. Then the action of K on V makes V into a K-space as we define the multiplication of $a \in K$ on $v \in V$ as $av = v^a$. Furthermore, the K-space structure extends the k-space structure and is preserved by G. That is, for

$g \in G$, $a \in K$, and $v \in V$, we have $a(v^g) = v^{ga} = v^{ag} = (av)^g$ so that $G \subseteq \mathrm{End}_K(V)$ and thus $G \leq \mathrm{GL}(V, K)$.

The following result is implicit in [1, 27.14]. We present a constructive proof since it will be used in Proposition 4.8.2.

Theorem 4.3.3. Let $G = NM$ be an irreducible subgroup of $\mathrm{GL}(V)$, where N and M are normal subgroups of G centralizing each other. Let W_1 be a minimal N-subspace of V and $U = \mathrm{Hom}_{kN}(W_1, V)$. Then there is a finite extension K of k, where $K \cong \mathrm{End}_{kN}(W_1)$, such that the following hold.

(i) V is a KG-module, W_1 is a KN-module, and U is a KM-module, with an isomorphism $V \cong W_1 \otimes_K U$ as K-spaces.

(ii) If $G = N \times M$, then $\pi : N \times M \to \mathrm{GL}(V, K)$ defined by $\pi(x, y) : v \mapsto v^{xy}$ for $v \in V$ is a faithful K-representation equivalent to the tensor product of faithful K-representations of N on W_1 and M on U.

Proof. By Clifford's theorem, $V = W_1 \oplus \cdots \oplus W_r$, $r \mid n$, where each $W_i = {W_1}^{g_i}$ for some $g_i \in M$, and the irreducible components $N|W_i$ are equivalent. That is, the W_i are kN-isomorphic so that N acts on each W_i faithfully. There are kN-isomorphisms $b_i : W_1 \to W_i$ such that $b_i = g_i|W_1$. Composing each b_i with the inclusion $W_i \subseteq V$, we may regard $b_i \in U$. Choose $b_1 = g_1 = 1$, and denote $B = \{b_1, \ldots, b_r\}$.

Schur's lemma yields that $K_1 = \mathrm{End}_{kN}(W_1)$ is a finite extension of k. Let each $K_i = {g_i}^{-1} K_1 g_i$. Form a field $K \subseteq \mathrm{End}_{kN}(V)$ consisting all the elements of the form, with respect to $V = W_1 \oplus \cdots \oplus W_r$,

$$a = \begin{pmatrix} a_1 & & & 0 \\ & {g_2}^{-1}a_1g_2 & & \\ & & \ddots & \\ 0 & & & {g_r}^{-1}a_1g_r \end{pmatrix}$$

for $a_1 \in K_1$. Here, $a|W_i = {g_i}^{-1}a_1g_i$. Then we have a scalar multiplication of K on each W_i, extending that of k, defined by $aw_i = {w_i}^a = {w_i}^{{g_i}^{-1}a_1g_i}$ for $w_i \in W_i$, making each W_i into a K-space. Observe that, for $w_1 \in W_1$, we have

$$(aw_1)^{b_i} = {w_1}^{ab_i} = {w_1}^{a_1g_i} = {w_1}^{g_i({g_i}^{-1}a_1g_i)} = {w_1}^{g_ia} = {w_1}^{b_ia} = a(w_1^{b_i}).$$

That is, each b_i is also a KN-isomorphism; hence, $b_i \in \mathrm{Hom}_{KN}(W_1, W_i)$. There is also a K-space structure on V, extending that on k, defined by $av = v^a$ for $v \in V$, where

$$a({v_1}^{b_1} + \cdots + {v_r}^{b_r}) = a({v_1}^{b_1}) + \cdots + a({v_r}^{b_r})$$

for $v_1, \ldots, v_r \in W_1$.

Elementary facts yield that $U = \mathrm{Hom}_{kN}(W_1, V) = \mathrm{Hom}_{kN}(W_1, \bigoplus_{i=1}^r W_i) = \bigoplus_{i=1}^r \mathrm{Hom}_{kN}(W_1, W_i) \cong \bigoplus_{i=1}^r \mathrm{End}_{kN}(W_i) \cong K^r$ regarded as a k-space. Since W_1 is also a K_1-space, the scalar maps $K_1 \subseteq \mathrm{End}_{K_1N}(W_1)$, where $\mathrm{End}_{K_1N}(W_1)$ is a k-subspace of $\mathrm{End}_{kN}(W_1) = K_1$, so that $\mathrm{End}_{K_1N}(W_1) = K_1$. Therefore, we have $\mathrm{Hom}_{KN}(W_1, V) \cong \bigoplus_{i=1}^r \mathrm{End}_{KN}(W_i) \cong \bigoplus_{i=1}^r \mathrm{End}_{K_iN}(W_i) \cong K^r$ as a K-space. As $\mathrm{Hom}_{KN}(W_1, V)$ is a k-subspace of U, it follows that $U = \mathrm{Hom}_{KN}(W_1, V)$ so that U is also a K-space. In this K-space U, note that $a \in K$ defines the scalar map $W_1 \to V$ by $w_1 \mapsto aw_1 = {w_1}^{a_1}$ for $w_1 \in W_1$. That is, the scalar multiplication of K on U is regarded as $au = a_1u \in \mathrm{Hom}_{kN}(W_1, V)$ for $u \in U$.

Observe that the K-space $U = \mathrm{Hom}_{KN}(W_1, W_1)\oplus\cdots\oplus\mathrm{Hom}_{KN}(W_1, W_r)$, where each $\mathrm{Hom}_{KN}(W_1, W_i)$ is a K-space spanned by b_i. That is, B is a K-basis for U.

Let $\phi : N \to \mathrm{GL}(W_1, K)$ be a K-representation defined by $\phi(x) : w_1 \mapsto {w_1}^x$ for $w_1 \in W_1$. Clearly, ϕ is irreducible. Recall that, since $G = NM$, where N and M centralize each other, N acts faithfully on each minimal N-subspace (cf. Lemma 4.3.2). Thus, ϕ is faithful.

Let $\psi : M \to \mathrm{GL}(U, K)$ be a K-representation defined by $\psi(y) : u \mapsto uy$ for $u \in U$. Indeed, ψ is well-defined since the composition $uy \in \mathrm{Hom}_{kN}(W_1, V)$ $= U = \mathrm{Hom}_{KN}(W_1, V)$ as $(au)^{\psi(y)} = (au)y = a_1uy = a(uy) = a(u^{\psi(y)})$. To confirm ψ is faithful, choose $y \in M$, and suppose $b_iy = b_i$ for all $b_i \in B$. Let $w_i \in W_i$. Then there is $w_1 \in W_1$ such that $w_i = {w_1}^{b_i}$. That is, $w_i = {w_1}^{b_i} = {w_1}^{b_iy} = {w_i}^y$. Therefore, y fixes every vector in W_i and thus every $v \in V$.

Observe that, for $u \in U$ and $w_1 \in W_1$, we have ${w_1}^{au} = {w_1}^{ua}$ since we already proved that $(aw_1)^{b_i} = a(w_1)^{b_i}$ for each $b_i \in B$. Then, for $y \in M$ and $v = {v_1}^{b_1} + \cdots + {v_r}^{b_r} \in V$, where each $v_i \in W_1$, we have

$$\begin{aligned}
(av)^y &= (a({v_1}^{b_1}) + \cdots + a({v_r}^{b_r}))^y \\
&= ((av_1)^{b_1} + \cdots + (av_r)^{b_r})^y \\
&= {v_1}^{a(b_1y)} + \cdots + {v_r}^{a(b_ry)} \\
&= {v_1}^{(b_1y)a} + \cdots + {v_r}^{(b_ry)a} \\
&= a({v_1}^{b_1y} + \cdots + {v_r}^{b_ry}) \\
&= a(v^y).
\end{aligned}$$

That is, M preserves the K-structure on V.

A routine check yields that $(av)^g = a(v^g)$ for $v \in V$ and $g \in G$; therefore, G preserves the K-space structure of V.

Let $\{v_1, \ldots, v_s\}$ be a K-basis for W_1. Then

$$\{{v_1}^{b_1}, \ldots, {v_s}^{b_1}, \ldots, {v_1}^{b_r}, \ldots, {v_s}^{b_r}\}$$

is a K-basis for V. Here, the map ${v_j}^{b_i} \mapsto v_j \otimes b_i$ induces a K-isomorphism $\theta : V \to W_1 \otimes_K U$. Therefore, (i) holds.

Now, suppose $G = N \times M$. Consider the K-representation $\pi : N \times M \to \mathrm{GL}(V, K)$ defined by $\pi(x, y) : v \mapsto v^{xy}$ for $v \in V$. Clearly, π is faithful since $v^{\pi(x,y)} = v^{xy} = v$ for all $v \in V$ if and only if $x = y = 1$.

A routine check yields that, for $x \in N$ and $y \in M$, we have $\theta({v_j}^{\phi(x) b_i \psi(y)}) = \theta({v_j}^{x b_i y}) = {v_j}^{\phi(x)} \otimes {b_i}^{\psi(y)}$.

Finally, let $\tau : N \times M \to \mathrm{GL}(W_1 \otimes_K U)$ be the tensor product representation of ϕ and ψ defined by $\tau(x, y) : v_j \otimes b_i \mapsto {v_j}^{\phi(x)} \otimes {b_i}^{\psi(y)}$. To confirm π and τ are equivalent, we shall show that θ is a KG-isomorphism; that is, it suffices to show that $\theta(v^{\pi(x,y)}) = \theta(v)^{\tau(x,y)}$ for all $v \in V$. Indeed,

$$\theta(({v_j}^{b_i})^{\pi(x,y)}) = \theta({v_j}^{x b_i y}) = {v_j}^{\phi(x)} \otimes {b_i}^{\psi(y)} = \theta({v_j}^{b_i})^{\tau(x,y)},$$

so the proof of (ii) is complete. □

In the next proposition, we summarize some of the useful facts arising from the above proof of Theorem 4.3.3.

Proposition 4.3.4. Let $G = NM$ be a subgroup of $\mathrm{GL}(V)$, where N and M are normal subgroups of G centralizing each other. If N is noncyclic, then the following hold.

(i) M is reducible.

(ii) Suppose that G is irreducible. If W_1 is a minimal N-subspace of V, then there is a proper M-subspace $V_1 \subset V$ such that

$$\dim_k V_1 = \frac{nd_1}{\dim_k W_1} < n,$$

where d_1 is the degree of the finite extension $\mathrm{End}_{kN}(W_1)$ over k.

Proof. We will prove (i) first. Suppose conversely that M is irreducible. By Schur's lemma, we know $\mathrm{End}_{kM}(V)$ is a finite field containing N, a contradiction.

Next, we will prove (ii). Suppose that G is irreducible. Let W_1 be a minimal N-subspace of V and $U = \mathrm{Hom}_{kN}(W_1, V)$. By Theorem 4.3.3, there is a finite extension K of k, where $K \cong \mathrm{End}_{kN}(W_1)$, such that V is a KG-module, W_1 is a KN-module, and U is a KM-module, with an isomorphism $V \cong W_1 \otimes_K U$ as K-spaces.

Let $0 \neq v_1 \in W_1$ and $\{b_1, \ldots, b_r\}$ a K-basis of U. Then the K-subspace V_1 of V spanned by $\{{v_1}^{b_1}, \ldots {v_1}^{b_r}\}$ is isomorphic to U and invariant under M.

Since $V \cong W_1 \otimes_K U$, where $\dim_K U = \dim_K V_1$, it follows that $\dim_K V = \dim_K W_1 \dim_K U = \dim_K W_1 \dim_K V_1$. Let $d_1 = |K : k|$. Then it immediately follows that $nd_1 = \dim_k W_1 \dim_k V_1$.

It remains to show that $\dim_k V_1 < n$. Suppose conversely that $\dim_k V_1 = n$. Since $\dim_k U = \dim_k V_1 = n = \dim_k V$, it follows that $\dim_K U = \dim_K V$. We also know that $\dim_K V = \dim_K W_1 \dim_K U$; therefore, $\dim_K W_1 = 1$. Here, recall that a

K-representation $\phi : N \to \mathrm{GL}(W_1, K)$ defined by $\phi(x) : w_1 \mapsto {w_1}^x$ for $w_1 \in W_1$ is faithful (cf. Lemma 4.3.2). Since N is noncyclic, we have a contradiction. □

§4. Abelian Groups and Class-2 Nilpotent Groups

We review several important facts used earlier for solvable-group algorithms in [39]. Since most of these facts were not formalized in [39], we present them with their complete proofs.

Throughout this section, let k be a finite field and V an n-dimensional vector space over k. In this section, p is an arbitrary prime, unrelated to char k, unless it is specified otherwise.

For an abelian group A and an integer $m \geq 1$, write $A^m = \{a^m \mid a \in A\}$. Recall that an abelian subgroup $A \leq \mathrm{GL}(V)$ is uniform if, for every integer $m \geq 1$, the subgroup A^m of A has no nonzero fixed vectors in V (i.e, $C_V(A^m) = 0$) unless $A^m = 1$.

Proposition 4.4.1. If A is a uniform abelian subgroup of $\mathrm{GL}(V)$, then char k does not divide $|A|$.

Proof. Suppose char $k = p \neq 0$, and p divides the order of A, say $|A| = pr$ for some integer $r \geq 1$. Then the subgroup A^r is a nontrivial p-group and thus unipotent. That is, A^r fixes a nonzero vector in V, a contradiction. □

Recall that, if K is a field, the diagonal group $D(n, K)$ is the subgroup of $\mathrm{GL}(n, K)$ consisting all the elements of the form

$$\begin{pmatrix} \omega_1 & & 0 \\ & \ddots & \\ 0 & & \omega_n \end{pmatrix} \in \mathrm{GL}(n, K),$$

where $\omega_i \in K$.

For an extension K of k, write $V^K = K \otimes_k V$. Under the natural embedding $\mathrm{GL}(V, k) \to \mathrm{GL}(V^K, K)$, we may identify any $G \leq \mathrm{GL}(V, k)$ as a subgroup of $\mathrm{GL}(V^K, K)$ (see, e.g., [1, §25]).

Proposition 4.4.2. Let A be a uniform abelian subgroup of $\mathrm{GL}(V, k)$. Then the following hold.

(i) A is completely reducible.

(ii) There are an extension K of k and $t \in \mathrm{GL}(V^K, K)$ such that A^t is isomorphic to a subgroup of $D(n, K)$.

Proof. The assertion (i) is an immediate consequence of a classical theorem of H. Maschke (see, e.g., [1, 12.9]).

Recall that, for $G \leq \mathrm{GL}(n, k)$, the elements of G are diagonalizable over some extension fields of k if and only if $\operatorname{char} k$ does not divide the order of G (see, e.g., [54, Lemma 17.4]). In fact, if G is abelian, and if $\operatorname{char} k$ does not divide the order of G, there are an extension K of k and $t \in \mathrm{GL}(n, K)$ such that $G^t \leq D(n, K)$ (see, e.g., [54, Lemma 17.1]). □

The following observation is elementary.

Lemma 4.4.3. Let A be a uniform abelian subgroup of $\mathrm{GL}(V)$. Let W be an A-subspace of V such that the restriction $A|W$ is cyclic. If an element $a_0 \in A$ fixes a nonzero vector $w_0 \in W$, then a_0 fixes all $w \in W$.

Proof. Suppose $A|W$ is a cyclic group of order ν. Then we have one element $a \in A$ such that, for each $x \in A$, there is an integer $\alpha, 0 \leq \alpha < \nu$, satisfying $w^x = w^{a^\alpha}$ on all $w \in W$.

Suppose $w^{a_0} = w^{a^{\alpha_0}}$ on all $w \in W$ for some $\alpha_0, 0 \leq \alpha_0 < \nu$. Then ${w_0}^{a_0} = {w_0}^{a^{\alpha_0}} = w_0$. For each $x \in A$, we have ${w_0}^{x^{\alpha_0}} = {w_0}^{(a^\alpha)^{\alpha_0}} = {w_0}^{(a^{\alpha_0})^\alpha} = w_0$, where $0 \leq \alpha < \nu$. That is, the subgroup A^{α_0} fixes a nonzero vector. By the uniformity of A, it follows that $A^{\alpha_0} = 1$. In particular, $w^{a_0} = w^{a^{\alpha_0}} = w$ on all $w \in W$. □

The following result is implicit in [39, Lemma 4.6]. Our proof appeals to the above lemma.

Lemma 4.4.4. Let A be a uniform abelian subgroup of $\mathrm{GL}(V)$. If $V_1, \ldots, V_m$ are the distinct maximal A-subspaces of V such that the restrictions $A|V_i$ are cyclic, then V decomposes as a direct sum $V = V_1 \oplus \cdots \oplus V_m$.

Proof. If A is cyclic, then the assertion is trivial. Thus, suppose that A is noncyclic; that is, $m \geq 2$. Since A is completely reducible, there are minimal A-subspaces $W_1, \ldots, W_r$ forming a direct sum $V = W_1 \oplus \cdots \oplus W_r$. Here, since A is irreducible on each W_i, it follows that each $A|W_i$ is cyclic. Therefore, it suffices to show that $V_1 + \cdots + V_m$ is a direct sum.

For $i = 1, \ldots, m$, let K_i be the kernel of the restriction $A \to \mathrm{GL}(V_i)$ and $U_i = C_V(K_i)$. Here, each U_i is A-invariant; that is, we have the restriction $\phi_i : A \to \mathrm{GL}(U_i)$.

Since each $K_i \leq \operatorname{Ker}\phi_i \leq A$, and A/K_i is cyclic, it follows that each $A/\operatorname{Ker}\phi_i$ is also cyclic. Clearly, each $V_i \subseteq U_i$; therefore, $V_i = U_i$ by the maximality of V_i.

Suppose that $V_1 + \cdots + V_m$ is not a direct sum. Then there is $v \in V$ such that $v = v_1 + \cdots + v_m = w_1 + \cdots + w_m$, where the pairs $v_i, w_i \in V_i$, and at least two of these pairs satisfy $v_i \neq w_i$. That is, there is a sum $u = u_1 + \cdots + u_m = 0$, where each $u_i \in V_i$, and at least two of the summands are nonzeros. Assume further that the number of nonzero summands in u is minimum amongst all such sums. Without loss of generality, assume that u_1 and u_2 are nonzeros.

Here, we claim that there is $a \in K_1$ such that ${u_2}^a \neq u_2$. To see this, suppose otherwise. Then, from Lemma 4.4.3, it follows that K_1 fixes all the vectors in V_2. That is, $V_2 \subseteq C_V(K_1) = V_1$, a contradiction.

By the above claim, the number of nonzero summands in the sum $u - u^a$ is less than those in u, contradicting our choice of u. Thus, $V_1 + \cdots + V_m = V_1 \oplus \cdots \oplus V_m$. □

We quote the following result from [39, Lemma 4.7].

Lemma 4.4.5. If N is a class-2 nilpotent subgroup of $\mathrm{GL}(V)$ such that $Z(N)$ is cyclic and uniform, then $|N : Z(N)| \leq n^2$. □

The following result was used in proving [39, Theorem 6.1]. We include a proof since it did not appear in [39].

Lemma 4.4.6. Let $G \leq \mathrm{GL}(V)$ and A a normal subgroup of G. If A is cyclic and uniform, then $|G : C_G(A)| \leq n$.

Proof. Let $\bar{k}$ denote the algebraic closure of k and $U = V^{\bar{k}}$. Consider G as a subgroup of $\mathrm{GL}(U, \bar{k})$.

Suppose $A = \langle a \rangle$. Clearly, a is diagonalizable so that the roots of the minimal polynomial of a are all distinct. Let $\lambda_1, \ldots, \lambda_m$ be the distinct eigenvalues of a and each U_{λ_i} denote the eigenspace for λ_i. That is, each $U_{\lambda_i} = \{u \in U \mid u^a = \lambda_i u\}$. Since the roots of the minimal polynomial of a are all distinct, it follows that $U = U_{\lambda_1} \oplus \cdots \oplus U_{\lambda_m}$.

We shall show that G acts on the set of these subspaces $\{U_{\lambda_1}, \ldots, U_{\lambda_m}\}$.

Let $g \in G$. Clearly, a and a^g share the same minimal polynomial and thus the same eigenvalues. Since A is cyclic and normal in G, there is an integer $\alpha > 0$ such that $a^g = a^\alpha$. Choose U_{λ_i}. Then, for $u \in U_{\lambda_i}$, we have $u^{a^\alpha} = \lambda_i{}^\alpha u$. That is, $\lambda_i{}^\alpha$ is an eigenvalue for a^α and thus $\lambda_i{}^\alpha = \lambda_j$ for some $j, 1 \leq j \leq m$. In fact, G acts on the set $\{\lambda_1, \ldots, \lambda_m\}$ defined by $\lambda_i{}^g = \lambda_i{}^\alpha$ on each λ_i.

It is then easy to verify that the G-action on the set of eigenvalues extends to the set of the eigenspaces. In particular, if $\lambda_i{}^g = \lambda_j$, then $(U_{\lambda_j})^g = U_{\lambda_i}$ as follows. Indeed, suppose $u \in U_{\lambda_i}$, then $u^{a^g} = u^{a^\alpha} = \lambda_i{}^\alpha u = \lambda_j u$. Since $u^{g^{-1}} \in U_{\lambda_j}$, we have $U_{\lambda_i} \subseteq (U_{\lambda_j})^g$. Conversely, suppose $\lambda_j{}^{g^{-1}} = \lambda_i{}^\beta$, where $a^{g^{-1}} = a^\beta$, for some integer $\beta > 0$. Suppose $v \in U_{\lambda_j}$, then $v^{a^\beta} = \lambda_j{}^\beta v = \lambda_j{}^{g^{-1}} v = \lambda_i v$. Since $v^g \in U_{\lambda_i}$, we have $U_{\lambda_j} \subseteq (U_{\lambda_i})^{g^{-1}}$ and thus $(U_{\lambda_j})^g \subseteq U_{\lambda_i}$. Therefore, we have $(U_{\lambda_j})^g = U_{\lambda_i}$.

Let $G_1 = N_G(U_{\lambda_1}) = \{g \in G \mid (U_{\lambda_1})^g = U_{\lambda_1}\}$. Clearly, $|G : G_1| \leq m \leq n$. Then it suffices to show that $G_1 \leq C_G(A)$.

Let $b \in G_1$ and $0 \neq u \in U_{\lambda_1}$. Since the action of a on U_{λ_1} is defined by the scalar multiplication by λ_1, and b stabilizes the subspace U_{λ_1}, we have $u^{[a,b]} = u$. Clearly, $[a, b] \in A$ so that $[a, b] = a^r$ for some integer $r > 0$. Since A is uniform, and a^r fixes a nonzero vector u, it follows that $a^r = 1$. That is, $[a, b] = 1$ and thus $G_1 \leq C_G(A)$. □

Recall that the exponent of a finite group G, denoted by $\exp(G)$, is the least common multiple of the orders of the elements of G. Clearly, if P is a p-group, then $\exp(P)$ is the maximum order of an element of P. It is easy to see that the same assertion also holds for nilpotent groups.

If E is an elementary abelian p-group of order p^ℓ for some $\ell \geq 1$, then $p = \exp(E)$, and ℓ is the rank of E.

The following result is well-known and has appeared in numerous versions (cf. [32, Satz III.13.7], [54, Theorem 19.2]). The method of our proof involves an algorithm that will be used in Proposition 4.7.4.

Proposition 4.4.7. If N is a finite class-2 nilpotent group such that $Z(N)$ is cyclic, then there are $a_1, b_1, \ldots, a_\ell, b_\ell \in N$ such that the following hold.

(i) $[a_i, a_j] = [a_i, b_j] = [b_i, b_j] = 1$ for $i \neq j$, $i = 1, \ldots, \ell$, $j = 1, \ldots, \ell$.

(ii) $[a_i, b_i]$ is an element of order $\nu_i > 1$ for $i = 1, \ldots, \ell$, where $\nu_i \mid \nu_{i-1}$ for $i = 2, \ldots, \ell$.

(iii) $N = Z(N)\langle a_\ell\rangle\langle b_\ell\rangle \cdots \langle a_1\rangle\langle b_1\rangle$, and every $x \in N$ can be written uniquely in the form

$$x = z{a_\ell}^{\alpha_\ell}{b_\ell}^{\beta_\ell} \cdots {a_1}^{\alpha_1}{b_1}^{\beta_1},$$

where $z \in Z(N)$, $0 \leq \alpha_i < \nu_i$, and $0 \leq \beta_i < \nu_i$ for $i = 1, \ldots, \ell$.

(iv) If $N/Z(N)$ is an elementary abelian p-group, then $\nu_1 = \cdots = \nu_\ell = p$, and N' is the subgroup of $Z(N)$ of order p.

Proof. Since N is class-2 nilpotent, we know that $N/Z(N)$ is abelian. Then observe that commutators in N behave like a bilinear form; that is, if $a, b, c \in N$, then $[a, bc] = [a, b][a, c] = [a, c][a, b] = [a, cb]$ and $[ab, c] = [a, c][b, c] = [b, c][a, c] = [ba, c]$.

Write $Z = Z(N)$. For $a \in N$ and $H \leq N$, write $[a, H] = \{[a, x] \mid x \in H\}$. Clearly, $[a, H]$ is a subgroup of Z so that $[a, H]$ is cyclic.

It is easy to see that Za is an element of N/Z of order ν if and only if $[a, N]$ has order ν. Indeed, for any positive integer α, we have $(Za)^\alpha = Z$ if and only if $[a^\alpha, x] = [a, x]^\alpha = 1$ for all $x \in N$.

Let Za_1 be an element of N/Z having the maximum order, say ν_1. Then there is $b_1 \in N$ such that $[a_1, b_1]$ generates $[a_1, N]$. Let N_1 denote the centralizer of the two elements a_1 and b_1 in N.

In what follows, we shall show $N = N_1\langle a_1\rangle\langle b_1\rangle$.

Let $\phi_1 : N \to [a_1, N]$ be a homomorphism defined by $\phi_1(x) = [a_1, x]$ for $x \in N$. Observe that $\operatorname{Ker}\phi_1 = C_N(a_1)$ so that $N/C_N(a_1) \cong [a_1, N]$. Clearly, $b_1 \notin C_N(a_1)$. For any positive integer β, we have $(C_N(a_1)b_1)^\beta = C_N(a_1)$ if and only if $[a_1, {b_1}^\beta] = [a_1, b_1]^\beta = 1$. Hence, $N/C_N(a_1) = \langle C_N(a_1)b_1\rangle$ and thus $N = C_N(a_1)\langle b_1\rangle$.

Clearly, $[b_1, C_N(a_1)] \leq [b_1, N]$, whose order is at most ν_1. Since $[a_1, b_1] = [b_1, a_1]^{-1}$ and $[b_1, a_1] \in [b_1, C_N(a_1)]$, it follows that $[a_1, N] = \langle [a_1, b_1]\rangle = \langle [b_1, a_1]\rangle \leq [b_1, C_N(a_1)] \leq [b_1, N]$ and thus $[a_1, N] = [b_1, C_N(a_1)] = [b_1, N]$. That is, Zb_1 is an element of N/Z having the same order ν_1.

Let $\phi_2 : C_N(a_1) \to [b_1, C_N(a_1)]$ defined by $\phi_2(y) = [b_1, y]$ for $y \in C_N(a_1)$. Clearly, $\operatorname{Ker}\phi_2 = N_1$ and $C_N(a_1)/N_1 \cong [b_1, C_N(a_1)]$. It then follows that $C_N(a_1) = N_1\langle a_1\rangle$, where $|C_N(a_1) : N_1| = \nu_1$; thus, we have $N = N_1\langle a_1\rangle\langle b_1\rangle$, where $|N : N_1| = {\nu_1}^2$.

If $Z < N_1$, then N_1 similarly decomposes as $N_1 = N_2\langle a_2\rangle\langle b_2\rangle$, where Za_2 and Zb_2 are elements of N_1/Z having the same maximum order, say ν_2, and N_2 is the centralizer of a_2 and b_2 in N_1.

We repeat the factorization until $Z = N_i$ for some i; that is, until we reach $N = Z\langle a_i\rangle\langle b_i\rangle\cdots\langle a_1\rangle\langle b_1\rangle$. Since $\nu_i = \exp(N_{i-1}/Z)$ for $i = 2,\ldots,\ell$, it follows that $\nu_i \mid \nu_{i-1}$ for $i = 2,\ldots,\ell$.

Suppose N/Z is an elementary abelian p-group. Clearly, $\nu_1 = \cdots = \nu_\ell = p$. Since each $[a_i, b_i]$ is an element of order p, it follows that each $[a_i, b_i]$ generates the unique subgroup Z_0 of Z of order p. It is then easy to see that, for all $x, y \in N$, we have $[x, y] \in Z_0$. Therefore, $N' = Z_0$. □

§5. Semisimple Groups

In this section, we review properties of a certain central extension of a direct product of nonabelian simple groups.

Let G be a finite group. Recall that we say G is quasisimple if $G = G'$, and if $G/Z(G)$ is nonabelian simple; more generally, we say G is semisimple if $G = G'$, and if $G/Z(G)$ is isomorphic to a direct product of nonabelian simple groups.

The following elementary fact summarizes how semisimple groups arise in our setting (cf. [55, II, 6.6.5]).

Proposition 4.5.1. If G is a finite group such that $G/Z(G) \cong G_1/Z(G) \times \cdots \times G_\ell/Z(G)$, where each $G_i/Z(G)$ is nonabelian simple, then the following hold.

(i) ${G_1}',\ldots,{G_\ell}'$ are quasisimple, and G is a central product of ${G_1}',\ldots,{G_\ell}'$, and $Z(G)$.

(ii) G' is semisimple; in particular, G' is a central product of ${G_1}',\ldots,{G_\ell}'$.

Proof. Since each $G_i/Z(G)$ is nonabelian simple, we know each $Z(G_i) = Z(G)$. Write $Z = Z(G)$, and choose a factor G_i.

Elementary facts yield that $G_i/Z = [G_i/Z, G_i/Z] = ([G_i, G_i]Z)/Z$ so that $G_i = [G_i, G_i]Z$ (see, e.g., [55, II, Theorem 4.1.5]). Since $G_i = G_i'Z$, we know $G_i/G_i^{(2)}$ is abelian so that $G_i' = G_i^{(2)}$. We also know that $G_i'/Z(G_i') \cong G_i/Z$; thus, G_i' is quasisimple.

If $\ell > 1$, choose another factor $G_j \neq G_i$. Clearly, $[G_i, G_j] \leq Z$. From the three subgroup lemma, it follows that

$$1 = [[G_j, G_i], G_i] = [[G_i, G_i], G_j] = [[G_i, G_i]Z, G_j] = [G_i, G_j].$$

Therefore, (i) holds.

Recall that a central product of semisimple groups is semisimple (see, e.g., [55, II, Theorem 6.6.4]). Let $H = G_1' \cdots G_\ell'$. Then H is semisimple. Since $G = HZ$, where $H = H'$, we conclude $G' = H$. Therefore, (ii) holds. □

The following lemma has appeared as [8, Proposition 2.7] (see [38, Lemma 3.8] for a related result in permutation groups). We include a proof since it will be an indispensable tool later.

Lemma 4.5.2. Let G be a finite group such that $G/Z(G)$ is isomorphic to a direct product of ℓ nonabelian simple groups, one of which is $G_1/Z(G)$. If G has a faithful irreducible linear representation of degree n over a finite field, where the restriction to G_1 has a constituent of degree n_1, then $n \geq 2^{\ell-1}n_1$.

Proof. We prove by induction on ℓ.

For $\ell = 1$, the assertion is clearly true.

For $\ell > 1$, write $G/Z = N/Z \times M/Z$, where M/Z is nonabelian simple, and $G_1 \leq N$. By Proposition 4.5.1, we know $[N, M] = 1$.

Let V be an n-dimensional vector space over a finite field, and regard G as an irreducible linear group acting on V. Since $G = NM$ and $[N, M] = 1$, Clifford's theorem and Lemma 4.3.2 yield that V decomposes as a direct sum of minimal N-spaces $V = W_1 \oplus \cdots \oplus W_{n/m}$, where the irreducible action of N on each W_i is faithful and has degree m. Then, by induction, $m \geq 2^{\ell-2}n_1$.

Let $D = \text{End}_N(V)$ and $E = \text{End}_N(W_i)$ for some W_i. By Schur's lemma, E is a finite division algebra and thus a field, and $D \cong M(n/m, E)$, where $E \cong Z(D)$. Let $c \in C_G(N)$. Clearly, for $v \in V$ and $a \in N$, we have $v^{ac} = v^{ca}$; that is, c is an N-homomorphism. Therefore, $C_G(N) \subseteq \text{End}_N(V) \cong M(n/m, E)$ so that $M \leq C_G(N) \leq \text{GL}(n/m, E)$. Since M is noncyclic, it follows that $n/m \geq 2$ and thus $n \geq 2m \geq 2^{\ell-1}n_1$. □

We now review an elementary fact concerning the automorphism groups of semisimple groups.

An automorphism σ of a group G is central if the induced action of σ on $G/Z(G)$ is the identity; that is, $Z(G)g^\sigma = Z(G)g$ for each $g \in G$. Observe that the central automorphisms of G leave every element of G' fixed (see [31] for related work).

The following result is then immediate (see [45, Lemma 2.1] for a related result).

Proposition 4.5.3. If G is a group such that $G = G'$, then $\text{Aut}(G)$ is isomorphic to a subgroup of $\text{Aut}(G/Z(G))$.

Proof. There is a natural homomorphism $\phi : \text{Aut}(G) \to \text{Aut}(G/Z(G))$ defined by $(Z(G)g)^{\phi(\sigma)} = Z(G)g^\sigma$ for $g \in G$ and $\sigma \in \text{Aut}(G)$. Here, $\text{Ker}\,\phi$ consists of the central automorphisms of G. Since the central automorphisms of G leave every element of $G' = G$ fixed, it follows that $\text{Ker}\,\phi = 1$. □

§6. Matrix Groups in the Class Γ_d

Throughout this section, let k be a finite field and V an n-dimensional vector space over k.

We need the following simple estimate derived from the upper bound on the orders of primitive permutation groups by Wielandt [58] and Praeger and Saxl [43] (cf. [8, Lemma 2.2]; see also [22, Theorem 5.8A]).

Lemma 4.6.1. Let G be a permutation group of degree m. If no composition factor of G is isomorphic to an alternating group of degree greater than d, where $d \geq 6$, then $|G| < d^{m-1}$. □

For an integer $d > 0$, recall that Γ_d denotes the class of finite groups all of whose nonabelian composition factors are isomorphic to subgroups of S_d.

The following result plays one of the crucial rôles in performing divide-and-conquer via nonabelian quotients. The method of our proof is closely related to the techniques used in proving [8, Theorem 3.2] and [38, Proposition 3.9].

Proposition 4.6.2. Fix an integer constant $d > 0$, and let G be an irreducible subgroup of $\mathrm{GL}(V)$ such that $G \in \Gamma_d$. Suppose G has a cyclic normal subgroup $A \geq 1$, and G/A has a nonabelian minimal normal subgroup N/A. Let $H = N'$. Then $C_G(H)$ is reducible, and there are positive constants c_1 and c_2 such that at least one of the following holds.

(i) $V = V_1 \oplus \cdots \oplus V_m$ such that $\mathcal{V} = \{V_1, \ldots, V_m\}$ forms a system of imprimitivity for G, where the transitive permutation representation of G on $\mathcal{V}$ is primitive and has the kernel L such that $H \leq L$ and $|G : L| \leq m^{c_1}$.

(ii) $|G : C_G(H)| = O(t^{c_2})$, where t is the dimension of a minimal H-subspace W_1 of V over the finite extension $K_1 = \mathrm{End}_{kH}(W_1)$ of k such that $t \geq 2$ and $t \mid n$.

Proof. We first prove that $A = Z(N)$. Clearly, $A \leq C_N(A) \leq N$. Since N/A is a minimal normal subgroup of G/A, either $A = C_N(A)$ or $C_N(A) = N$. Suppose $A = C_N(A)$. Then $N/A = N/C_N(A)$ is isomorphic to a subgroup of $\mathrm{Aut}(A)$. However, we know that $\mathrm{Aut}(A)$ is abelian, a contradiction. Hence, $C_N(A) = N$. That is, $A \leq Z(N) < N$ and thus $A = Z(N)$.

Since $N/Z(N)$ is a direct product of nonabelian simple groups, we know that $H = N'$ is semisimple by Proposition 4.5.1. In fact, since $N/Z(N) = HZ(N)/Z(N) \cong H/(H \cap Z(N))$, we also know that $Z(H) = H \cap Z(N)$ so that $N/Z(N) \cong H/Z(H)$.

Since H is noncyclic, $C_G(H)$ is reducible by Proposition 4.3.4 (i).

Let W_1 be a minimal H-subspace of V. Then Clifford's theorem yields that $V = W_1 \oplus \cdots \oplus W_r$, $r \mid n$, where each $W_i = {W_1}^{g_i}$ for some $g_i \in G$. Let $U_1, \ldots, U_h$ be the distinct homogeneous H-subspaces of V determined by $W_1, \ldots W_r$.

Suppose $h \geq 2$. The set $\mathcal{U} = \{U_1, \ldots, U_h\}$ forms a system of imprimitivity. Under the transitive permutation representation of G on $\mathcal{U}$, let $\mathcal{V} = \{V_1, \ldots, V_m\}$ be a minimal system of imprimitivity for G, where the V_j are direct sums of the U_i, so that G acts primitively on $\mathcal{V}$. Let L be the kernel of the G-action on $\mathcal{V}$, then G/L is a primitive permutation group of degree m. By Theorem 4.1.1, there is a constant $c_1 > 0$ such that $|G : L| \leq m^{c_1}$. Thus, (i) holds.

Suppose $h = 1$. First, observe that the irreducible components $H|W_i$ are equivalent so that H acts faithfully on each W_i. Schur's lemma yields that $K_1 = \mathrm{End}_{kH}(W_1)$ is a finite extension of k. Then a K_1-representation $\phi : H \rightarrow \mathrm{GL}(W_1, K_1)$ defined by $\phi(x) : w_1 \mapsto {w_1}^x$ for $w_1 \in W_1$ is irreducible and faithful. Let $t = |W_1 : K_1|$; that is, t

is the degree of the faithful irreducible representation ϕ.

Now, write $Z = Z(H)$ and $H/Z \cong H_1/Z \times \cdots \times H_\ell/Z$, where each H_i/Z is isomorphic to a nonabelian simple group T.

Since H is noncyclic, we know $t \geq 2$. Let t_1 be the degree of the restriction of ϕ on H_1. Then it follows from Lemma 4.5.2 that $t \geq 2^{\ell-1}t_1$ and thus $\ell \leq \log(t/t_1)+1 \leq \log t + 1$.

Let G act on H by conjugation. Then $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. Since H is semisimple, $\mathrm{Aut}(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H/Z)$ by Proposition 4.5.3. Therefore, $G/C_G(H)$ is faithfully represented in $\mathrm{Aut}(H/Z)$.

Recall that, since T is nonabelian simple, $\mathrm{Aut}(T^\ell) \cong \mathrm{Aut}(T)$ wr S_ℓ (see, e.g., [22, Exercise 4.3.9]). Evidently, $|T| \leq d!$ and thus $|\mathrm{Aut}(T)| < (d!)^{\log(d!)}$ (in fact, the confirmation of the Schreier conjecture by the Classification of Finite Simple Groups asserts that the outer automorphism group $\mathrm{Out}(T) = \mathrm{Aut}(T)/T$ is solvable, where $|\mathrm{Out}(T)| \leq |T|$, so that $|\mathrm{Aut}(T)| \leq |T|^2$ (see, e.g., [18], [44])). Using $c_3 = (d!)^{\log(d!)}$ for an upper bound on $|\mathrm{Aut}(T)|$, we have $|\mathrm{Aut}(T) \text{ wr } S_\ell| < {c_3}^\ell \ell!$.

Each element of $\mathrm{Aut}(H/Z)$ induces a permutation on $\{H_1/Z, \ldots, H_\ell/Z\}$. Now, write $G_0 \cong G/C_G(H)$ so that $G_0 \leq \mathrm{Aut}(H/Z)$, and let L_0 be the normal subgroup of G_0 leaving each H_i/Z invariant. Then L_0 is a subgroup of $\mathrm{Aut}(H_1/Z) \times \cdots \times \mathrm{Aut}(H_\ell/Z) \cong \mathrm{Aut}(T)^\ell$, and G_0/L_0 is a subgroup of S_ℓ.

Let $c_4 = \max\{d, 6\}$. Since no composition factor of G_0/L_0 is isomorphic to an alternating group of degree greater than c_4, it follows from Lemma 4.6.1 that $|G_0/L_0| < {c_4}^{\ell-1}$ so that $|G/C_G(H)| = |L_0||G_0/L_0| < {c_3}^\ell {c_4}^{\ell-1}$. Write $c_5 = c_3c_4$, then

$$|G/C_G(H)| < {c_5}^\ell \leq {c_5}^{\log t+1} = c_5 t^{\log c_5}.$$

Thus, (ii) holds. □

§7. Divide and Conquer: via Abelian Quotients

We first develop divide-and-conquer tools for abelian quotients. Most of the algorithms in this section were developed earlier for solvable groups in [39]. Since these results were not formalized in [39], we present them with their complete proofs for the class Γ_d.

Throughout this section, let k be a finite field and V an n-dimensional vector space over k. As before, p is an arbitrary prime, unrelated to $\operatorname{char} k$, unless it is specified otherwise. Fix an integer constant $d > 0$. For a given input $G \leq \mathrm{GL}(V)$, assume that $G \in \Gamma_d$, and $\mu(G)$ is polynomially bounded in the input length.

Proposition 4.7.1. Given $G \leq \mathrm{GL}(V)$ and a non-uniform abelian normal subgroup A of G, in polynomial time one can find a proper G-subspace $W \subset V$.

Proof. Since A is not uniform, there is an integer $r \geq 1$ such that $A^r \neq 1$, where A^r fixes a nonzero vector in V. Clearly, A^r is normal in G. Then $C_V(A^r)$ is a proper G-subspace of V. □

We quote the following result from [39, Lemma 4.6] (cf. Lemma 4.4.4).

Lemma 4.7.2. Given a uniform abelian subgroup A of $\mathrm{GL}(V)$, in polynomial time one can find the set of the maximal A-subspaces $\{V_1, \dots, V_m\}$ of V such that the restrictions $A|V_i$ are cyclic. These subspaces form a direct sum $V = V_1 \oplus \cdots \oplus V_m$. □

The following result is a consequence of Theorem 4.1.1.

Proposition 4.7.3. Given $G \leq \mathrm{GL}(V)$ and a uniform abelian normal subgroup A of G such that A is noncyclic, in polynomial time one can find

(i) a proper G-subspace $W \subset V$ or

(ii) a decomposition $V = V_1 \oplus \cdots \oplus V_m$, forming a minimal system of imprimitivity $\mathcal{V} = \{V_1, \ldots, V_m\}$ for G, and the kernel L of the permutation representation of G on $\mathcal{V}$ such that $|G : L| \leq m^{c_1}$ for a constant $c_1 > 0$.

Proof. Since A is uniform, we can find the maximal A-subspaces $U_1, \ldots, U_s$, $s \geq 2$, of V such that the restrictions $A|U_i$ are cyclic. Then $V = U_1 \oplus \cdots \oplus U_s$. If $g \in G$, it is easy to see that each $U_i{}^g$ is also a maximal A-subspace of V such that $A|U_i{}^g$ is cyclic. That is, for each $g \in G$, the map $U_i \mapsto U_i{}^g$ is a permutation of the set $\mathcal{U} = \{U_1, \ldots, U_s\}$.

If the G-action on $\mathcal{U}$ is intransitive, then a nontrivial orbit of $\mathcal{U}$ yields a proper G-subspace of V.

Suppose the G-action on $\mathcal{U}$ is transitive. A standard procedure to find a minimal block system in permutation groups yields a minimal system of imprimitivity $\mathcal{V} = \{V_1, \ldots, V_m\}$ for G, where the V_j are direct sums of U_i, so that G acts primitively on $\mathcal{V}$ (see, e.g., [2]). Find the kernel L of the G-action on $\mathcal{V}$, then G/L is a primitive permutation group of degree m. By Theorem 4.1.1, there is a constant $c_1 > 0$ such that $|G : L| \leq m^{c_1}$. □

The proof of [39, Theorem 6.1] also appeals to the following result. We include a proof since it did not appear in [39].

Proposition 4.7.4. Given $G \leq \mathrm{GL}(V)$ and a class-2 nilpotent normal subgroup N of G such that $Z(N)$ is cyclic and uniform, where $N/Z(N)$ is an elementary abelian

p-group centralized by G of rank 2ℓ for $\ell \geq 1$, in polynomial time one can perform one of the following.

(i) Find a decomposition $V = V_1 \oplus \cdots \oplus V_m$ such that $\{V_1, \ldots, V_m\}$ forms a minimal system of imprimitivity for G, where

(a) $m = p^\ell$ if $p \neq 2$,

(b) $m = 2^{\lfloor \ell/2 \rfloor}$ if $p = 2$ and $\ell \geq 2$, or

(c) $m = 2$ if $p = 2$ and $\ell = 1$.

(ii) In the event (i)(c) fails when $p = 2$ and $\ell = 1$, find a quaternion group Q of order 8 such that $N' < Q \leq N$.

Proof. Write $Z = Z(N)$. By Proposition 4.4.7, we can find $a_1, b_1, \ldots, a_\ell, b_\ell \in N$ such that $N = Z\langle a_\ell \rangle \langle b_\ell \rangle \cdots \langle a_1 \rangle \langle b_1 \rangle$, where $[a_i, a_j] = [a_i, b_j] = [b_i, b_j] = 1$ for all pairs $i \neq j$, and every $[a_i, b_i]$ is an element of N' of order p. Note that $Za_1, Zb_1, \ldots, Za_\ell, Zb_\ell$ form a basis of N/Z.

As we find each pair a_i and b_i, we also enforce the following two additional conditions.

(1) $|{b_i}^p|$ divides $|{a_i}^p|$ for $i = 1, \ldots, \ell$.

(2) $[a_1, b_1] = \cdots = [a_\ell, b_\ell] = z_0$ for some $z_0 \in Z$.

If a pair a_i and b_i fail to meet (1) and (2), we modify the pair so that they will meet these conditions as follows.

We fix an element $1 \neq z_0 \in N'$ throughout. Write $a = a_i$ and $b = b_i$ to simplify the notation. We may assume that $|a^p|_p \geq |b^p|_p$. Find $\delta = (|a^p|, |b^p|)$ and positive integers δ_1 and δ_2 such that $|a^p| = \delta\delta_1$ and $|b^p| = \delta\delta_2$. Since p does not divide δ_2, it follows that $[a, b^{\delta_2}] = [a, b]^{\delta_2} \neq 1$. Replace b with b^{δ_2} so that $|b^p|$ divides δ. Now, if $[a, b] \neq z_0$, then we find a positive integer β such that $[a, b]^\beta = [a, b^\beta] = z_0$. Clearly, $|b^{p\beta}|$ divides $|b^p|$ so that $|b^{p\beta}|$ divides δ. Replace b with b^β, then $|b^p|$ divides δ so that $|b^p|$ divides $|a^p|$.

Case 1. Suppose that $p \neq 2$.

In what follows, we construct an elementary abelian p-group E of rank $\ell + 1$ such that $E < N$ and $E \lhd G$. To do this, we will find ℓ distinct elements $e_1, \ldots, e_\ell \notin Z$ of order p as follows.

Choose i, and write $a = a_i$ and $b = b_i$. Since $a^p, b^p \in Z$, where Z is cyclic, and $|b^p|$ divides $|a^p|$, it follows that $\langle b^p \rangle \leq \langle a^p \rangle$. Then we can find an integer $\varepsilon \geq 0$ such that $a^{p\varepsilon} b^p = 1$. Observe that, in general, if $x, y \in N$, then

$$(x^\alpha y^\beta)^\gamma = x^{\alpha\gamma} y^{\beta\gamma} [x, y]^{\alpha\beta\binom{\gamma}{2}}$$

for all integers α, β, and γ (see, e.g., [32, Hilfssatz III.1.3]). Since $p > 2$, and $[a, b]$ has order p, it follows that $(a^\varepsilon b)^p = a^{p\varepsilon} b^p = 1$. Clearly, $b \notin Z$. Now, if $a^\varepsilon b \in Z$, then $Zb \in \langle Za \rangle$, a contradiction. Therefore, $a^\varepsilon b \notin Z$. So we let $e_i = a^\varepsilon b$.

Let $E = \langle e_1, \ldots, e_\ell, z_0 \rangle$. Then E is an elementary abelian p-group of rank $\ell + 1$ contained in N.

It remains to show that E is normal in G. Let $g \in G$ and $1 \neq x \in E$. Since G centralizes N/Z, it follows that $x^g = zx$ for some $z \in Z$. Suppose $z \neq 1$. Since x is an element of order p, the order of x^g is clearly p. Then z has order p. Since Z is cyclic, $\langle z_0 \rangle$ is the unique subgroup N' of Z of order p so that $\langle z \rangle = N'$. That is, $z \in N' \leq E$ and thus $zx \in E$.

Since Z contains p-elements, the order of Z is pr for some positive integer r. Since Z is cyclic, Z^r is a cyclic group of order p so that $N' = Z^r$. Since Z is uniform, and $Z^r \neq 1$, it is straight from the definition that N' fixes no nonzero vectors in V.

For $m = 1, 2, \ldots,$ observe that $(N')^m = 1$ if p divides m and $(N')^m = N'$ otherwise. Choose $m \geq 1$. Since $(N')^m \leq E^m$, it follows that, if p does not divide m, then E^m fixes no nonzero vectors in V. If p divides m, then it is clear that $E^m = 1$. Therefore, E is uniform.

Find the maximal E-subspaces $V_1, \ldots, V_m$ of V such that the restrictions $E|V_j$ are cyclic. Then $V = V_1 \oplus \cdots \oplus V_m$. For each $g \in G$, the map $V_j \mapsto V_j{}^g$ is a permutation of the set $\mathcal{V} = \{V_1, \ldots, V_m\}$.

Now, N' acts nontrivially on each V_j. Choose V_j. Then there is an element $e_0 \in E$ of order p such that, for each $x \in E$, there is an integer λ, $0 \leq \lambda < p$, satisfying $v^x = v^{e_0{}^{\lambda}}$ on all $v \in V_j$. In particular, there is an integer λ_0, $0 < \lambda_0 < p$, such that $v^{z_0} = v^{e_0{}^{\lambda_0}}$ on all $v \in V_j$. Since z_0 is also an element of order p, we may assume that $z_0 = e_0$. Then there are integers $\lambda_1, \ldots, \lambda_\ell$, where $0 \leq \lambda_i < p$ for each λ_i, such that $v^{e_i} = v^{z_0{}^{\lambda_i}}$ on all $v \in V_j$. With these integers $\lambda_1, \ldots, \lambda_\ell$, we label $V_{(\lambda_1, \ldots, \lambda_\ell)} = V_j$.

In fact, these integers $\lambda_1, \ldots, \lambda_\ell$ uniquely label each V_j. To see this, suppose that there are subspaces $V_{(\lambda_1, \ldots, \lambda_\ell)}$ and $V_{(\lambda_1{}', \ldots, \lambda_\ell{}')}$, where $0 \leq \lambda_i < p$ and $0 \leq \lambda_i{}' < p$ for $i = 1 \ldots, \ell$. Without loss of generality, suppose that $\lambda_1 > \lambda_1{}'$. We claim that $V_{(\lambda_1, \ldots, \lambda_\ell)} \cap V_{(\lambda_1{}', \ldots, \lambda_\ell{}')} = 0$. To confirm our claim, suppose otherwise; that is, there is $0 \neq v_0 \in V_{(\lambda_1, \ldots, \lambda_\ell)} \cap V_{(\lambda_1{}', \ldots, \lambda_\ell{}')}$. Then $v_0{}^{e_1} = v_0{}^{z_0{}^{\lambda_1}} = v_0{}^{z_0{}^{\lambda_1{}'}}$. Let $\zeta = \lambda_1 - \lambda_1{}'$. Then $v_0{}^{z_0{}^{\zeta}} = v_0$, where $0 < \zeta < p$. That is, $\langle z_0{}^{\zeta} \rangle = N'$ fixes v_0, a contradiction. Therefore, $m \leq p^\ell$.

Now, N acts transitively on $\mathcal{V}$. To see this, let $v \in V_{(\lambda_1,\ldots,\lambda_\ell)}$ and choose $e_i = {a_i}^{\varepsilon_i} b_i$. Since $v^{e_i} = v^{{z_0}^{\lambda_i}}$, it follows that

$$v^{a_i e_i} = v^{{a_i}^{\varepsilon_i+1} b_i} = v^{{a_i}^{\varepsilon_i} b_i a_i z_0} = v^{e_i a_i z_0} = v^{a_i {z_0}^{\lambda_i+1}}.$$

That is, $(V_{(\lambda_1,\ldots,\lambda_\ell)})^{a_i} = V_{(\lambda_1,\ldots,\lambda_i+1 \pmod p),\ldots,\lambda_\ell)}$. Therefore, $m = p^\ell$.

In fact, N acts primitively on $\mathcal{V}$. Indeed, a_1 preserves a partition of the subspaces $V_{(*,\ldots,*,0)} \mid \cdots \mid V_{(*,\ldots,*,p-1)}$, whereas a_2 preserves another partition $V_{(*,\ldots,*,0,*)} \mid \cdots \mid V_{(*,\ldots,*,p-1,*)}$; therefore, the only nontrivial partition preserved by N is V itself. Since $N \leq G$, the G-action on $\mathcal{V}$ is also primitive.

Case 2. Suppose that $p = 2$ and $\ell \geq 2$.

We will construct an elementary abelian 2-group E of rank $\lfloor \ell/2 \rfloor + 1$ such that $E < N$ and $E \lhd G$. As in Case 1, we will find $\lfloor \ell/2 \rfloor$ distinct elements $e_1, \ldots, e_{\lfloor \ell/2 \rfloor} \notin Z$ of order 2 as follows.

As before, choose i, and write $a = a_i$ and $b = b_i$. We can find an integer $\varepsilon \geq 0$ such that $a^{2\varepsilon} b^2 = 1$. Then a routine check yields that $(a^\varepsilon b)^4 = 1$ so that $a^\varepsilon b$ has order 2 or 4. Let $d_i = a^\varepsilon b$.

Since z_0 is the unique element of Z of order 2, it follows that ${d_i}^2 = 1$ or z_0; thus, $(d_i d_j)^2 = {d_i}^2 {d_j}^2 = 1$ for $i \neq j$, $i = 1, \ldots, \ell$, $j = 1 \ldots, \ell$. Now, let $e_1 = d_1 d_2, e_2 = d_3 d_4, \ldots$, and $e_{\lfloor \ell/2 \rfloor} = d_{\ell-2} d_{\ell-1}$ if ℓ is odd, or $e_{\lfloor \ell/2 \rfloor} = d_{\ell-1} d_\ell$ if ℓ is even.

Let $E = \langle e_1, \ldots, e_{\lfloor \ell/2 \rfloor}, z_0 \rangle$. Then E is an elementary abelian 2-group as desired. By the same argument used in Case 1, E is normal in G. Furthermore, the maximal subspaces $V_1, \ldots, V_m$ such that the restrictions $E|V_i$ are cyclic yield a minimal system of imprimitivity $\{V_1, \ldots, V_m\}$ for G, where $m = 2^{\lfloor \ell/2 \rfloor}$.

Case 3. Suppose that $p = 2$ and $\ell = 1$.

Write $a = a_1$ and $b = b_1$. As before, we can find an integer $\varepsilon \geq 0$ such that $a^{2\varepsilon}b^2 = 1$. Let $d = a^{\varepsilon}b$. Then $|d|$ is 2 or 4. Also, note that $[a, d] = z_0$. In what follows, we construct an elementary abelian 2-group E of rank 2 such that $E < N$ and $E \lhd G$ or find a quaternion group Q of order 8 such that $N' < Q \leq N$.

Suppose that $|d| = 2$. Then let $e = d$ and $E = \langle e, z_0 \rangle$.

Suppose that $|d| = 4$. Since $[a, b] = z_0$, it follows that $[a, b]^{|a|} = 1$ so that $|a|$ is even. Find an odd integer η such that $|a| = |a|_2\eta$.

If $|a|_2 = 2$, then let $e = a^{\eta}$ and $E = \langle e, z_0 \rangle$.

Suppose that $|a|_2 \geq 8$. That is, $|a|_2 = 2^r$ for some $r \geq 3$. Let $z_1 = a^{2^{r-2}\eta}$. Then z_1 is an element of Z of order 4, where ${z_1}^2 = z_0$. Clearly, $(z_1 d)^2 = {z_1}^2 d^2 = {z_0}^2 = 1$. Since $z_1 \in Z$ while $d \notin Z$, it follows that $z_1 d \notin Z$. Thus, let $e = z_1 d$ and $E = \langle e, z_0 \rangle$.

Except for the case $|d| = 4$ and $|a|_2 = 4$, we have an elementary abelian 2-group E as desired. The maximal subspaces V_1 and V_2 such that the restrictions $E|V_i$ are cyclic form a minimal system of imprimitivity $\{V_1, V_2\}$ for G.

Finally, suppose that $|d| = 4$ and $|a|_2 = 4$. Let $x = a^{\eta}$ and $y = d$. Clearly, x and y both have order 4, and $[x, y] = z_0$. Then a routine check yields that $\langle x, y \rangle$ is a quaternion group of order 8. □

The following result is a slight generalization of [39, Theorem 6.1]. We include a complete proof since it did not appear in [39].

Proposition 4.7.5. Given $G \leq \mathrm{GL}(V)$ and normal subgroups N and A of G such that A is cyclic and uniform, N centralizes A, and N/A is elementary abelian, in polynomial time one can perform one of the following.

(i) Prove that $|G : A| \leq 24n$.

(ii) Find an abelian normal subgroup B of G such that $A < B$.

(iii) Find a normal subgroup M of G, where $A < M$, such that M/A is a nonabelian minimal normal subgroup of G/A.

(iv) Find a normal subgroup H of G and a decomposition $V = V_1 \oplus \cdots \oplus V_m$, forming a minimal system of imprimitivity $\mathcal{V} = \{V_1, \ldots, V_m\}$ for H such that $|G : H| \leq m^{c_1}$ for a constant $c_1 > 0$, and find the kernel L of the permutation representation of H on $\mathcal{V}$ such that $|H : L| \leq m^{c_2}$ for a constant $c_2 > 0$.

Proof. We describe a polynomial-time algorithm in three steps. Throughout, we write $Z = Z(N)$.

Step 1. Suppose that N/A is an elementary abelian p-group.

If N is abelian, return N as B for (ii). Suppose otherwise; that is, N is class-2 nilpotent. If $A < Z$, then return Z as B for (ii). Otherwise, $A = Z$.

By Lemma 4.4.5, we know that $|N : Z| \leq n^2$. Here, the conjugation action of G on N/Z induces a linear representation ϕ over a finite field of order p. In fact, since $|N/Z| \leq n^2$, we may assume that ϕ is irreducible. Suppose that the rank of N/Z is 2ℓ for $\ell \geq 1$. Find $H = \operatorname{Ker} \phi$. From the work of Babai–Cameron–Pálfy [8, Corollary 3.3], there is a constant $c_3 > 0$ such that $|G : H| \leq p^{c_3(2\ell)}$.

Now, we appeal to Proposition 4.7.4 and obtain one of the following.

(1) A decomposition $V = V_1 \oplus \cdots \oplus V_m$ such that $\mathcal{V} = \{V_1, \ldots, V_m\}$ forms a minimal system of imprimitivity for H, where $m = p^\ell$ if $p \neq 2$, $m = 2^{\lfloor \ell/2 \rfloor}$ if $p = 2$ and $\ell \geq 2$, or $m = 2$ if $p = 2$ and $\ell = 1$.

(2) A quaternion group Q of order 8 such that $N' < Q \leq N$.

Step 2. Suppose that we obtain (1).

By Proposition 4.7.4, there is a constant $c_1 > 0$ such that $|G : H| \leq m^{c_1}$; furthermore, the permutation representation of H on $\mathcal{V}$ is primitive. Find its kernel L. Then, by Theorem 4.1.1, there is a constant $c_2 > 0$ such that $|H : L| \leq m^{c_2}$. Therefore, we have (iv).

Step 3. Suppose that we obtain (2). Let $Q_1 = Q$.

Before we proceed, we need to prove that $Q \trianglelefteq G$ and $|G : C_G(N)| \leq 24n$.

First, we prove that Q is normal in G. Recall that $N' = \langle z_0 \rangle$, where z_0 is the unique element of order 2 in Z and centralized by G. Also, recall that $Q = \langle x, y \rangle$, where x and y are elements of Q of order 4 such that $[x, y] = z_0$ and $x^2 = y^2 = z_0$. That is, $N = Z\langle x \rangle \langle y \rangle$. Let $g \in G$. Since $x^g \in N$, we have $x^g = zx^\alpha y^\beta$ for some $z \in Z$, $\alpha = 0$ or 1, and $\beta = 0$ or 1. Since $x \notin Z$, we cannot have $\alpha = 0$ and $\beta = 0$. In the three other cases, we have $(x^g)^2 = {z_0}^g = z_0$ and thus $z = z_0$ or 1. Therefore, $x^g \in Q$. By the same argument, $y^g \in Q$ and thus $Q \trianglelefteq G$.

Since $|\mathrm{Aut}(Q)| = 24$, it follows that $|G : C_G(Q)| \leq 24$. Then it is easy to see that $|G : C_G(N)| \leq 24n$ as follows. Since $N = ZQ$, we have $C_G(N) = C_G(Z) \cap C_G(Q)$ and thus

$$C_G(Q)/C_G(N) \cong (C_G(Z)C_G(Q))/C_G(Z) \leq G/C_G(Z).$$

Since Z is cyclic and uniform, by Proposition 4.4.6, we have $|G : C_G(Z)| \leq n$. Therefore, $|G : C_G(N)| = |G : C_G(Q)||C_G(Q) : C_G(N)| \leq 24n$.

Find $C_G(N)$. If $A = C_G(N)$, then we have (i).

Suppose that $A < C_G(N)$. Find a normal subgroup M of G, where $A < M \leq C_G(N)$, such that M/A is an elementary abelian group or a nonabelian minimal normal subgroup of G/A.

If M/A is nonabelian, then return M for (iii).

Suppose that M/A is elementary abelian. Clearly, M centralizes A. Regarding M as N, we perform Step 1. If we obtain (1), then we have (iv).

Suppose that we obtain (2), say, Q_2 such that $M' < Q_2 \leq M$.

Observe that $Z = Z(N) = Z(M) = A$, where N and M centralize each other. That is, $N \cap M = Z$ and thus $(N/Z) \cap (M/Z) = Z/Z$. Now, N/Z and M/Z are both elementary abelian 2-groups of rank 2 so that $(NM)/Z$ is an elementary abelian 2-group of rank 4. The conjugation action of G on $(NM)/Z$ induces a linear representation ψ of degree 4 over a finite field of order 2. Find $H = \operatorname{Ker} \psi$. Then $|G : H| \leq |\mathrm{GL}(4,2)| < 2^4$.

Since Q_1 and Q_2 centralize each other, $Q_1 \neq Q_2$. Then we can find $d_1 \in Q_1 \setminus Q_2$ and $d_2 \in Q_2 \setminus Q_1$. Here, d_1 and d_2 both must have order 4. Also, note that $d_1 d_2 \notin Z$ (otherwise, it would mean that $Zd_1 = (Zd_2)^{-1}$, a contradiction). Let $e = d_1 d_2$. Since $e^2 = (d_1 d_2)^2 = {d_1}^2 {d_2}^2 = z_0 z_0 = 1$, we have $|e| = 2$. Let $E = \langle e, z_0 \rangle$. Then E is an elementary abelian 2-group of rank 2 such that $E < NM$ and $E \lhd H$. The maximal subspaces V_1 and V_2 such that the restrictions $E|V_i$ are cyclic form a minimal system of imprimitivity $\mathcal{V} = \{V_1, V_2\}$ for H. If L is the kernel of the H-action on $\mathcal{V}$, then $|H : L| = 2$. Thus, we have (iv). □

§8. Divide and Conquer: via Nonabelian Quotients

We now consider algorithms for divide-and-conquer via nonabelian quotients.

Throughout this section, let k be a finite field and V an n-dimensional vector space over k.

Our algorithm will appeal to the following result [47, §5.2].

Theorem 4.8.1 (Rónyai). Given a set $S \subset \mathrm{End}_k(V)$, one can find a proper subspace $W \subset V$ such that $W^s \subseteq W$ for all $s \in S$, or prove that no such W exists, in time polynomial in the input length and $\mathrm{char}\, k$. □

In particular, given $G \leq \mathrm{GL}(V)$ such that $\mathrm{char}\, k$ is polynomially bounded, one can find a minimal G-subspace $W \subseteq V$ in polynomial time.

Now, suppose that we are given an irreducible subgroup $G \leq \mathrm{GL}(V)$ and a minimal invariant subspace W_1 of V for a normal subgroup H of G. Then, based on Clifford's theorem (Theorem 4.3.1), the following simple procedure finds a direct sum of H-isomorphic minimal H-subspaces or a system of imprimitivity for G (cf. [30, §2.1]).

```
procedure CLIFFORD
Input: an irreducible group $G \leq \mathrm{GL}(V)$ and a minimal $H$-subspace $W_1$ of $V$ for
    a normal subgroup $H$ of $G$.
Output: a direct sum of $H$-isomorphic minimal $H$-subspaces of $V$ or a system of
    imprimitivity for $G$.

begin
    decompose $V = W_1 \oplus \cdots \oplus W_r$, where each $W_i = {W_1}^{g_i}$ for some $g_i \in G$;
    let $\mathcal{U} := \{W_1, \ldots, W_r\}$;
    repeat
        if there are $U \in \mathcal{U}$ and $s \in S$ such that $U^s \notin \mathcal{U}$ then
            begin
                find the minimum collection of subspaces $U_i, \ldots, U_j \in \mathcal{U}$ such
                  that $U^s \subset U_i \oplus \cdots \oplus U_j$;
                replace $U_i, \ldots, U_j \in \mathcal{U}$ with $U_i \oplus \cdots \oplus U_j$;
            end
    until $G$ permutes the members of $\mathcal{U}$;
    if $|\mathcal{U}| = 1$ then return $H$-isomorphic $H$-subspaces $W_1, \ldots, W_r$;
    else return a system of imprimitivity $\mathcal{U}$ for $G$;
end.
```

Fix an integer constant $d > 0$. From now on, for a given input $G \leq \mathrm{GL}(V)$, assume that $G \in \Gamma_d$, and $\mu(G)$ and $\operatorname{char} k$ are polynomially bounded in the input length.

The following result is built on Theorem 4.3.3, Proposition 4.3.4, Theorem 4.8.1, and the procedure CLIFFORD.

Proposition 4.8.2. Given $G \leq \mathrm{GL}(V)$ and normal subgroups N and A of G such that A is cyclic, $1 \leq A < N$, and N/A is a nonabelian minimal normal subgroup of G/A, in polynomial time one can perform one of the following.

(i) Find a proper G-subspace $W \subset V$.

(ii) Find a decomposition $V = V_1 \oplus \cdots \oplus V_m$, forming a minimal system of imprimitivity $\mathcal{V} = \{V_1, \ldots, V_m\}$ for G, and the kernel L of the permutation representation of G on $\mathcal{V}$ such that $|G : L| \leq m^{c_1}$ for a constant $c_1 > 0$.

(iii) Find $H = N'$, $C_G(H)$ such that $|G : C_G(H)| = O(t^{c_2})$, where $t \geq 2$ and $t \mid n$, and c_2 is a constant > 0, and minimal $C_G(H)$-subspaces $M_1, \ldots, M_e$ of V of the same dimension such that $V = M_1 \oplus \cdots \oplus M_e$, where $e \geq t$.

Proof. By Theorem 4.8.1, we may assume that G is irreducible. We describe a polynomial-time algorithm to perform (ii) or (iii). Recall that G is specified by a generating set S.

First, we find $H = N'$ and a minimal H-subspace W_1 of V. Then we call the procedure CLIFFORD to find a direct sum of H-isomorphic minimal H-subspaces or a system of imprimitivity for G (cf. [30, §2.1]).

Suppose the procedure CLIFFORD returns a system of imprimitivity $\mathcal{U} = \{U_1, \ldots, U_h\}$. A standard procedure to find minimal block systems in permutation groups yields a minimal system of imprimitivity $\mathcal{V} = \{V_1, \ldots, V_m\}$ for G, where the V_j are direct sums of U_i, so that G acts primitively on $\mathcal{V}$ (see, e.g., [2]). Thus, (ii) holds.

Suppose the procedure CLIFFORD returns $V = W_1 \oplus \cdots \oplus W_r$, where the W_i are H-isomorphic minimal H-subspaces. Then the action of H on each W_i is irreducible and faithful.

Find $C_G(H)$, and let $D = C_G(H)H$. Find a minimal D-subspace V_0 of V. We may assume V_0 contains W_1. Let $\bar{\ } : D \to \mathrm{GL}(V_0)$ denote the restriction of D on V_0. Then $\overline{D} = \overline{C_G(H)}\,\overline{H}$ is an irreducible subgroup of $\mathrm{GL}(V_0)$.

Theorem 4.3.3 yields that, if $U_0 = \mathrm{Hom}_{kH}(W_1, V_0)$, there is a finite extension K of k, where $K \cong K_1 = \mathrm{End}_{kH}(W_1)$, such that V_0 is a KD-module, W_1 is a KH-module, and U_0 is a $KC_G(H)$-module, with an isomorphism $V_0 \cong W_1 \otimes_K U_0$ as K-spaces.

Now, let $g_1 = 1$, and find $g_2, \ldots, g_s \in C_G(H)$ such that $V_0 = W_1 \oplus {W_1}^{g_2} \oplus \cdots \oplus {W_1}^{g_s}$. Form kH-isomorphisms $b_i : W_1 \to {W_1}^{g_i}$ such that $b_i = g_i|W_1$.

Observe that $K_1 = \mathrm{End}_{kH}(W_1)$ is the centralizer of the linear span of the restriction $H|W_1$ over k in $\mathrm{End}_k(W_1)$. Thus, one can find a k-basis of K_1. Find a k-basis of the field $K \subseteq \mathrm{End}_{kH}(V_0)$, $K \cong K_1$, consisting of all the elements of the form, with respect to $V_0 = W_1 \oplus {W_1}^{g_2} \oplus \cdots \oplus {W_1}^{g_s}$,

$$a = \begin{pmatrix} a_1 & & & 0 \\ & {g_2}^{-1} a_1 g_2 & & \\ & & \ddots & \\ 0 & & & {g_s}^{-1} a_1 g_s \end{pmatrix}$$

for $a_1 \in K_1$.

Next, we will find a proper $C_G(H)$-subspace M_0 of V_0 by following the proof of Proposition 4.3.4 (ii). Now, as we have seen in the proof of Theorem 4.3.3, the set $\{b_1, \ldots, b_s\}$ forms a K-basis of $U_0 = \mathrm{Hom}_{kH}(W_1, V_0)$. Choose $0 \neq v_1 \in W_1$, and form a K-subspace M_0 spanned by $\{{v_1}^{b_1}, \ldots, {v_1}^{b_s}\}$. Here, observe that M_0 is K-isomorphic to U_0 and invariant under $C_G(H)$. Clearly, M_0 is also a k-subspace of V_0. From the k-basis of K and the K basis of M_0, one can find a k-basis of M_0.

Find a minimal $C_G(H)$-subspace M_1 in M_0. By Clifford's theorem, one can find minimal $C_G(H)$-subspaces $M_2, \ldots, M_e$ of the same dimension $\dim_k M_1$ such that $V = M_1 \oplus \cdots \oplus M_e$.

Let $t = \dim_{K_1} W_1$. In Proposition 4.6.2, we have shown that $|G : C_G(H)| = O(t^{c_2})$ for a constant $c_2 > 0$. Therefore, it remains to show that $e \geq t$.

Since $V_0 \cong W_1 \otimes_K U_0$ as K-spaces, we have $\dim_K V_0 = \dim_K W_1 \dim_K U_0$. That is, $\dim_k V_0 = \dim_K W_1 \dim_k U_0$. Here, recall that $t = \dim_{K_1} W_1 = \dim_K W_1$; thus, $\dim_k V_0 = t \dim_k U_0$. By Clifford's theorem, there is an integer $r_0 \geq 1$ such that $\dim_k V = r_0 \dim_k V_0$. Therefore, $n = r_0 t \dim_k U_0$. Since $\dim_k M_1 \leq \dim_k M_0 = \dim_k U_0$, it follows that

$$e = \frac{n}{\dim_k M_1} \geq \frac{n}{\dim_k U_0} = r_0 t.$$

Therefore, $e \geq t$. □

§9. Divide and Conquer: Pasting Together

We are finally ready to complete the proof of Theorem 4.1.4.

Proof of Theorem 4.1.4. We describe a polynomial-time algorithm in three steps.

Step 1. If G is nonabelian simple, then we have (i). If G is abelian, then we immediately establish (ii). Otherwise, find a nonabelian minimal normal subgroup N of G or an abelian normal subgroup A of G. If we have N, then we use Proposition 4.8.2 for (iii) or (iv).

Step 2. Suppose that we have an abelian normal subgroup A of G. If A is non-uniform, then we use Proposition 4.7.1 for (iii). If A is noncyclic and uniform, then we use Proposition 4.7.3 for (iii) or (iv).

Step 3. Suppose that A is cyclic and uniform. Find $C_G(A)$. If $A = C_G(A)$, then Proposition 4.4.6 yields that $|G : A| \leq n$ so that we return A to establish (ii). If $A < C_G(A)$, then find a normal subgroup N of G, where $A < N \leq C_G(A)$, such that N/A is a nonabelian minimal normal subgroup of G/A or an elementary abelian group. If N/A is nonabelian, then we again use Proposition 4.8.2 for (iii) or (iv). If N/A is elementary abelian, then we appeal to Proposition 4.7.5 to establish (ii) or (iv) or obtain one of the following.

(1) An abelian normal subgroup B of G such that $A < B$.

(2) A normal subgroup M of G such that M/A is a nonabelian minimal normal subgroup of G/A.

If we obtain (1), then we regard B as A and recursively perform Step 2 and, if necessary, Step 3. If we obtain (2), then we regard M as N and use Proposition 4.8.2 for (iii) or (iv). □

BIBLIOGRAPHY

[1] M. Aschbacher, *Finite group theory*, Cambridge Stud. Adv. Math., vol. 10, Cambridge Univ. Press, Cambridge, 1986.

[2] M. D. Atkinson, *An algorithm for finding the blocks of a permutation group*, Math. Comp. **29** (1975), 911–913.

[3] L. Babai, *Trading group theory for randomness*, Proceedings of the 17th Annual ACM Symposium on the Theory of Computing, Providence, R.I., May 6–8, 1985, ACM, New York, 1985, pp. 421–429.

[4] ——, *On the length of chains of subgroups in the symmetric group*, Comm. Algebra **14** (1986), 1729–1736

[5] ——, *Computational complexity in finite groups*, Proc. Internat. Congr. Math., Kyôto, 1990, vol. 2, Kyôto, Aug. 21–29, 1990, Springer, Tôkyô, 1991, pp. 1479–1489.

[6] ——, *Automorphism groups, isomorphism, reconstruction*, Handbook of Combinatorics, vol. 2 (L. Lovász, R. L. Graham, and M. Grötschel, eds.), Elsevier, Amsterdam, 1995, pp. 1447–1540.

[7] L. Babai and R. Beals, *A polynomial-time theory of black box groups*. I, Groups St Andrews 1997 in Bath, vol. I, Bath, Jul. 26–Aug. 9, 1997 (C. M. Campbell, E. F. Robertson, N. Ruskuc, and G. C. Smith, eds.), London Math. Soc. Lecture Note Ser., vol. 260, Cambridge Univ. Press, Cambridge, 1999, pp. 30–64.

[8] L. Babai, P. J. Cameron, and P. P. Pálfy, *On the orders of primitive groups with restricted nonabelian composition factors*, J. Algebra **79** (1982), 161–168.

[9] L. Babai, W. M. Kantor, and E. M. Luks, *Computational complexity and the classification of finite simple groups*, Proceedings of the 24th Annual Symposium on Foundation of Computer Science, Tucson, Nov. 7–9, 1983, IEEE Comput. Soc. Press, Washington, D.C., 1983, pp. 162–171.

[10] L. Babai and L. Lovász, *Permutation groups and almost regular graphs*, Studia Sci. Math. Hungar. **8** (1973), 141–150.

[11] L. Babai and S. Moran, *Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes*, J. Comput. System Sci. **36** (1988), 254–276.

[12] L. Babai and E. Szemerédi, *On the complexity of matrix group problems.* I, Proceedings of the 25th Annual Symposium on Foundation of Computer Science, Singer Island, Fla., Oct. 24–26, 1984, IEEE Comput. Soc. Press, Washington, D.C., 1984, pp. 229–240.

[13] E. Bach, *Number theoretic algorithms*, Annual Review of Computer Science, vol. 4, 1989–1990, Annual Review Inc., Palo Alto, Calif., 1990, pp. 119–172.

[14] R. Beals, *Towards polynomial time algorithms for matrix groups*, Groups and Computation. II, Piscataway, N.J., Jun. 7–10, 1995 (L. Finkelstein and W. M. Kantor, eds.), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 28, Amer. Math. Soc., Providence, R.I., 1997, pp. 31–54.

[15] ———, *Algorithms for matrix groups and the Tits alternative*, J. Comput. System Sci. **58** (1999), 260–279.

[16] R. Beals and L. Babai, *Las Vegas algorithms for matrix groups*, Proceedings of the 34th Annual Symposium on Foundation of Computer Science, Palo Alto, Calif., Nov. 3–5, 1993, IEEE Comput. Soc. Press, Los Alamitos, Calif., 1993, pp. 427–436.

[17] E. R. Berlekamp, *Factoring polynomials over large finite fields*, Math. Comp. **24** (1970), 713–735.

[18] P. J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), 1–22.

[19] P. J. Cameron, R. Solomon, and A. Turull, *Chains of subgroups in symmetric groups*, J. Algebra **127** (1989), 340–352.

[20] J. J. Cannon, *An introduction to the group theory language Cayley*, Computational Group Theory, Durham, Jul. 30–Aug. 9, 1982 (M. D. Atkinson, ed.), Academic Press, London, 1984, pp. 145–183.

[21] J. J. Cannon and C. Playoust, *An introduction to algebraic programming in Magma*, School of Mathematics and Statistics, University of Sydney, Sydney, 1996.

[22] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Math., vol. 163, Springer, New York, 1996.

[23] M. Furst, J. E. Hopcroft, and E. M. Luks, *Polynomial-time algorithms for permutation groups*, Proceedings of the 21st Annual Symposium on Foundation of Computer Science, Syracuse, N.Y., Oct. 13–15, 1980, IEEE Comput. Soc. Press, Washington, D.C., 1980, pp. 36–41.

[24] The GAP Group, *GAP–Groups, Algorithms, and Programming*, version 4.1, Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen; School of Mathematical and Computational Sciences, University of St Andrews, St Andrews, 1999.

[25] M. R. Garey and D. S. Johnson, *Computers and intractability*, Freeman, New York, 1979.

[26] D. Gluck, Á. Seress, and A. Shalev, *Bases for primitive permutation groups and a conjecture of Babai*, J. Algebra **199** (1998), 367–378.

[27] O. Goldreich, S. Micali, and A. Wigderson, *Proofs that yield nothing but their validity and a methodology of cryptographic protocol design*, Proceedings of the 27th Annual Symposium on Foundation of Computer Science, Toronto, Oct. 27–29, 1986, IEEE Comput. Soc. Press, Washington, D.C., 1986, pp. 168–195.

[28] M. Hall, Jr., *The theory of groups*, 2nd ed., Chelsea, New York, 1976.

[29] I. N. Herstein, *Topics in algebra*, 2nd. ed., Wiley, New York, 1975.

[30] D. F. Holt, C. R. Leedham-Green, E. A. O'Brien, and S. Rees, *Testing matrix groups for primitivity*, J. Algebra **184** (1996), 795–817.

[31] N. J. S. Hughes, *The structure and order of the group of central automorphisms of a finite group*, Proc. London Math. Soc. (2) **52** (1951), 377–385.

[32] B. Huppert, *Endliche Gruppen.* I, Grundlehren Math. Wiss., Bd. 134, Springer, Berlin, 1967.

[33] W. M. Kantor, *Simple groups in computational group theory*, Proc. Internat. Congr. Math., Berlin, 1998, Berlin, Aug. 18–27, 1998, Doc. Math. J. DMV Extra Volume ICM II (1998), 77–86.

[34] W. M. Kantor and E. M. Luks, *Computing in quotient groups*, Proceedings of the 22nd Annual ACM Symposium on the Theory of Computing, Baltimore, May 14–16, 1990, ACM, New York, 1990, pp. 524–534.

[35] J. Köbler, U. Schöning, and J. Torán, *The graph isomorphism problem: its structural complexity*, Progr. Theoret. Comput. Sci., Birkhäuser, Boston, 1993.

[36] S. Lang, *Algebra*, 3rd. ed., Addison-Wesley, Reading, Mass., 1993.

[37] M. W. Liebeck and L. Pyber, *Upper bounds for the number of conjugacy classes of a finite group*, J. Algebra **198** (1997), 538–562.

[38] E. M. Luks, *Isomorphism of graphs of bounded valence can be tested in polynomial time*, J. Comput. System Sci. **25** (1982), 42–65.

[39] ——, *Computing in solvable matrix groups*, Proceedings of the 33rd Annual Symposium on Foundation of Computer Science, Pittsburgh, Oct. 24–27, 1992, IEEE Comput. Soc. Press, Los Alamitos, Calif., 1992, pp. 111–120.

[40] ——, *Permutation groups and polynomial-time computation*, Groups and Computation, Piscataway, N.J., Oct. 7–10, 1991 (L. Finkelstein and W. M. Kantor, eds.), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. **11**, Amer. Math. Soc., Providence, R.I., 1993, pp. 139–175.

[41] R. Mathon, *A note on the graph isomorphism counting problem*, Infom. Process. Lett. **8** (1979), 131–132.

[42] K. A. Mihaĭlova, *The occurrence problem for a direct product of groups*, Dokl. Acad. Nauk **119** (1958), 1103–1105; Mat. Sb. (N.S.) **70** (112) (1966), 241–251 (Russian).

[43] C. E. Praeger and J. Saxl, *On the orders of primitive permutation groups*, Bull. London Math. Soc. **37** (1980), 303–307.

[44] L. Pyber, *Asymptotic results for permutation groups*, Groups and Computation, Piscataway, N.J., Oct. 7–10, 1991 (L. Finkelstein and W. M. Kantor, eds.), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, Amer. Math. Soc., Providence, R.I., 1993, pp. 197–219.

[45] ——, *Enumerating finite groups of given order*, Ann. of Math. (2) **137** (1993), 203–220.

[46] D. J. S. Robinson, *A course in the theory of groups*, 2nd ed., Graduate Texts in Math., vol. 80, Springer, New York, 1996.

[47] L. Rónyai, *Computing the structure of finite algebras*, J. Symbolic Comput. **9** (1990), 355–373.

[48] G. M. Seitz, R. Solomon, and A. Turull, *Chains of subgroups in groups of Lie type*. II, J. London Math. Soc. (2) **42** (1990), 93–100.

[49] Á. Seress, *An introduction to computational group theory*, Notices Amer. Math. Soc. **44** (1997), 671–679.

[50] ——, *Permutation group algorithms*, Cambridge Univ. Press, Cambridge (to appear).

[51] C. C. Sims, *Computational methods in the study of permutation groups*, Computational Problems in Abstract Algebra, Oxford, Aug. 29–Sep. 2, 1967 (J. Leech, ed.), Pergamon Press, Oxford, 1970, pp. 169–183.

[52] ——, *Computation with permutation groups*, Proceedings of the Second Symposium on Symbolic and Algebraic Manipulation, Los Angeles, Mar. 23–25, 1971 (S. R. Petrick, ed.), ACM, New York, 1971, pp. 23–28.

[53] R. Solomon and A. Turull, *Chains of subgroups in groups of Lie type.* I, III, J. Algebra **132** (1990), 174–184; J. London Math. Soc. (2) **44** (1991), 437–444.

[54] D. A. Suprunenko, *Matrix groups*, "Nauka", Moscow, 1972 (Russian); English transl., Transl. Math. Monographs, vol. 45, Amer. Math. Soc., Providence, R.I., 1976.

[55] M. Suzuki, *Group theory.* I, II, Iwanami Shoten, Tôkyô, 1977, 1978 (Japanese); English transl., Grundlehren Math. Wiss., Bd. 247, 248, Springer, Berlin, 1982, 1986.

[56] A. Turull and A. Zame, *Number of prime divisors and subgroup chains*, Arch. Math. (Basel) **55** (1990), 333–341.

[57] H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.

[58] ——, *Permutation groups through invariant relations and invariant functions*, Lecture notes, The Ohio State University, Columbus, 1969.