GROUP DECOMPOSITIONS, JORDAN ALGEBRAS, AND ALGORITHMS FOR P-GROUPS

by

JAMES B. WILSON

A DISSERTATION

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

June 2008

University of Oregon Graduate School

Confirmation of Approval and Acceptance of Dissertation prepared by:

James Wilson

Title:

"Group Decompositions, Jordan Algebras, and Algorithms for p-groups"

This dissertation has been accepted and approved in partial fulfillment of the requirements for the degree in the Department of Mathematics by:

William Kantor, Chairperson, Mathematics
Peter Gilkey, Member, Mathematics
Charles Wright, Member, Mathematics
Jonathan Brundan, Member, Mathematics
Eugene Luks, Outside Member, Computer & Information Science

and Richard Linton, Vice President for Research and Graduate Studies/Dean of the Graduate School for the University of Oregon.

June 14, 2008

Original approval signatures are on file with the Graduate School and the University of Oregon Libraries.

An Abstract of the Dissertation of

James B. Wilson for the degree of Doctor of Philosophy

in the Department of Mathematics to be taken June 2008

Title: GROUP DECOMPOSITIONS, JORDAN ALGEBRAS, AND ALGORITHMS FOR P-GROUPS

Approved: _____

Dr. William M. Kantor

Finite p-groups are studied using bilinear methods which lead to using nonassociative rings. There are three main results, two which apply only to p-groups and the third which applies to all groups.

First, for finite p-groups P of class 2 and exponent p the following are invariants of fully refined central decompositions of P: the number of members in the decomposition, the multiset of orders of the members, and the multiset of orders of their centers. Unlike for direct product decompositions, $\mathrm{Aut}\, P$ is not always transitive on the set of fully refined central decompositions, and the number of orbits can in fact be any positive integer. The proofs use the standard semi-simple and radical structure of Jordan algebras. These algebras also produce useful criteria for a p-group to be centrally indecomposable.

In the second result, an algorithm is given to find a fully refined central decomposition of a finite p-group of class 2. The number of algebraic operations used by the algorithm is bounded by a polynomial in the log of the size of the group. The algorithm uses a Las Vegas probabilistic algorithm to compute the structure of a finite ring and the Las Vegas MeatAxe is also used. However, when p is small, the probabilistic methods can be replaced by deterministic polynomial-time algorithms.

The final result is a polynomial time algorithm which, given a group of permutations, matrices, or a polycyclic presentation; returns a Remak decomposition of the group: a fully refined direct decomposition. The method uses group varieties to reduce to the case of p-groups of class 2. Bilinear and ring theory methods are employed there to complete the process.

CURRICULUM VITAE

NAME OF AUTHOR: James B. Wilson

PLACE OF BIRTH: Brisbane, Queensland, Australia

DATE OF BIRTH: July 8, 1980

GRADUATE AND UNDERGRADUATE SCHOOLS ATTENDED:

University of Oregon, Eugene, Oregon
Portland State University, Portland, Oregon

DEGREES AWARDED:

Doctor of Philosophy, University of Oregon, 2008
Master of Science, University of Oregon, 2004
Bachelor of Science, Portland State University, 2002

AREAS OF SPECIAL INTEREST:

Groups, Nonassociative Algebras, Bilinear Maps, Algorithms for Groups and Algebras

PROFESSIONAL EXPERIENCE:

Graduate Teaching Fellow, University of Oregon, 2002-2008

PUBLICATIONS:

J. B. Wilson, Decomposing p-groups via Jordan algebras (submitted), `http://arxiv.org/abs/0711.0201`.

J. B. Wilson, Finding central decompositions of p-groups (submitted), `http://arxiv.org/abs/0801.3434`.

ACKNOWLEDGMENTS

I am very grateful to my advisor W. M. Kantor for the liberty and encouragement to work on these problems, the extensive patience to listen to their early (often mistaken) proofs, and the copious notes on previous drafts. In particular, thank you for suggesting the Jordan product for $\mathrm{Sym}(b)$.

I am also grateful to E. M. Luks and C. R. B. Wright for their extraordinary attention to the ideas contained here. Thanks to all the members of my committee for improving the exposition of this dissertation through your questions and comments.

Thanks also to E. I. Zel'manov and H. P. Petersson for advice on Jordan algebras; and to L. Ronyai for discussing the current state of algorithms for associative algebras.

This research was supported in part by NSF Grant DMS 0242983.

In pursuing this degree God has blessed me with the support of a wonderful wife Karie, and strong friendships with Mark Walsh, Dawn Archey, Laura Hammond, and many others. I thank God and them for their support. I also salute my parents Richard and Laura Wilson, my uncle William Crawford Jr., and my family. They know their rôles in this – as do I.

DEDICATION

To my wife Karie.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

I present three theorems in three chapters. The central theme of each is the use of bilinear maps and algebras to answer questions about p-groups. This would be unremarkable if stated for bilinear forms and, simple groups or simple algebras. For instance, the work of E. Artin, C. Chevalley, T. A. Springer, and J. Tits uses nondegenerate bilinear forms to explain many of the structures of classical and non-classical groups. On the algebra side the same was done by I. N. Herstein, I. L. Kantor, M. Koecher, and N. Jacobson to understand the structure of simple Lie and Jordan algebras. In this work I apply precisely the opposite philosophy.

Unlike bilinear forms, bilinear maps have a rich and complicated structure owing partly to the enormous number of non-isometric bilinear maps of any fixed dimensions. There is no hope to classify or broadly study individual isometry types of bilinear maps. My approach uses groups and algebras to study bilinearity, in contrast to the goals of earlier works. Starting with a bilinear map, associate to it a natural associative $*$-algebra, a Jordan algebra, and a Lie algebra. Also define the group of isometries and conformal maps, just as is done with bilinear forms. Only now the perspective is to use the structure theorems of these algebras and groups to inform us about the structure of bilinear maps. With these tools I will show that bilinear maps have an unexplored "radical and semisimple structure" – where radical here is not the usual radical of a bilinear map. By recognizing this structure and its translation to p-groups it is possible to discover new theorems and algorithms for these groups and other groups.

The use of bilinear maps to studying p-groups I believe began with Baer [6], and my use is similar. These methods have lost favor due to the stronger connections between p-groups and nilpotent Lie algebras. However, sometimes it is best to trade a hard problem for p-groups for an easier problem for bilinear maps, rather than an equivalently hard problem for nilpotent Lie algebras. Indeed, the results in this dissertation can be applied also to nilpotent Lie algebras.

CHAPTER II

DECOMPOSING p-GROUPS VIA JORDAN ALGEBRAS

II.1 Introduction

For finite p-groups P of class 2 and exponent p the following are invariants of fully refined central decompositions of P: the number of members in the decomposition, the multiset of orders of the members, and the multiset of orders of their centers. Unlike for direct product decompositions, $\mathrm{Aut}\, P$ is not always transitive on the set of fully refined central decompositions, and the number of orbits can in fact be any positive integer. The proofs use the standard semi-simple and radical structure of Jordan algebras. These algebras also produce useful criteria for a p-group to be centrally indecomposable.

A *central decomposition* of a group G is a set $\mathcal{H}$ of subgroups in which distinct members commute, and G is generated by $\mathcal{H}$ but by no proper subset. A group is *centrally indecomposable* if its only central decomposition consists of the group itself. A central decomposition is *fully refined* if it consists of centrally indecomposable subgroups.

We prove:

Theorem II.1.1. *For p-groups P of class 2 and exponent p,*

(i) the following are invariants of fully refined central decompositions of P: the number of members, the multiset of orders of the members, and the multiset of orders of the centers of the members; and

(ii) the number of $\mathrm{Aut}\, P$*-orbits acting on the set of fully refined central decompositions can be any positive integer.*

Central decompositions arise from, and give rise to, central products (cf. Section II.2.1), and hence Theorem II.1.1.(i) is a theorem of Krull-Remak-Schmidt type (cf. [49, (3.3.8)]). That

theorem states that the multiset of isomorphism types of fully refined direct decompositions (Remak-decompositions) is uniquely determined by the group, and the automorphism group is transitive on the set of Remak-decompositions. Theorem II.1.1.(*ii*) points out how unrelated the proof of Theorem II.1.1.(*i*) is to that of the classical Krull-Remak-Schmidt theorem. Moreover, inductive proofs do not work for central decompositions. For example, a quotient by a member in a central decomposition generally removes the subtle intersections of other factors and so is of little use. Similarly, automorphisms of a member in a central decomposition usually do not extend to automorphisms of the entire group.

We conjecture that under the hypotheses of Theorem II.1.1, even the multiset of isomorphism types of a fully refined central decomposition of P is uniquely determined by P. For details see Section II.8.1.

While the literature on direct decompositions is vast, little appears to have been done for central decompositions. For p-groups, results similar to Theorem II.1.1 have concentrated on central decompositions with centrally indecomposable subgroups of rank 2 and 3, with various constraints on their centers [1, 2, 55, 56]. Using entirely different techniques, our setting applies to groups of arbitrary rank at the cost of assuming exponent p.

The methods used in this paper involve bilinear maps and non-associative algebras, but not the nilpotent Lie algebras usually associated with p-groups. We introduce a $*$-algebra and a Jordan algebra in order to study central decompositions. The approach leads to a great many other results for p-groups and introduces a surprising interplay between p-groups, symmetric bilinear forms, and various algebras. Most of these ideas will be developed in subsequent works. As the algebras we use are easily computed, in [60] we provide algorithms for finding fully refined central decompositions and related decompositions – even for p-groups of general class and exponent (including 2-groups). In [63] we prove there are $p^{2n^3/27+Cn^2}$ centrally indecomposable groups of order p^n, which is of the same form as the Higman-Sims bound on the total number of groups of order p^n [18, 53]. In [63] we also prove that a *randomly presented* group of order p^n is centrally indecomposable, and we characterize various *minimal* centrally indecomposable p-groups by means of locally finite p-groups, including those p-groups with $P' \cong \mathbb{Z}_p^2$. Finally, in [62] we address central decompositions of 2-groups, p-groups of arbitrary exponent, and p-groups of arbitrary class, by means of an equivalence on p-groups related to the isoclinism of P. Hall [16].

II.1.1 Outline of the Proof

Section II.2 contains background and notation for central decompositions of groups and orthogonal decompositions of bilinear maps.

Section II.3 translates p-groups P of class 2 and exponent p into alternating bilinear maps on P/P' induced by commutation. This approach is well-known and appears as early as Baer's work [6] and refined in [28] and [58]; however, such techniques have been upstaged by appealing to various associated Lie algebras of Kaloujnine, Lazard, Mal'cev and others [32]. By contrast, the bilinear approach translates unwieldy central decompositions into natural-looking orthogonal decompositions, and automorphisms into pseudo-isometries (Theorem II.3.6).

In Section II.4 we introduce two algebraic invariants of bilinear maps: the associative $*$-algebra of adjoint operators, and the Jordan algebra of self-adjoint operators. The first of these encodes isometries, while the second encodes orthogonal decompositions via sets of pairwise orthogonal idempotents (Theorem II.4.29). We use these algebras to give criteria for indecomposable bilinear maps and centrally indecomposable p-groups (Corollary II.4.35 and Theorem II.4.36). We also prove the first part of Theorem II.1.1.(i).

In Section II.5 we prove that a certain subgroup of isometries acts on suitable sets of idempotents of our Jordan algebra with the same orbits as the full isometry group. Using the radical theory of Jordan algebras and the classification of finite dimensional simple Jordan algebras we identify the orbits of the isometry group acting on the set of fully refined orthogonal decompositions (and therefore the orbits of $C_{\mathrm{Aut}\,P}(P')$ on the set of fully refined central decompositions of P) (Corollary II.5.16).

In Section II.6, semi-refined central decompositions are introduced. These are derived from properties of symmetric bilinear forms and then interpreted in the setting of p-groups, leading to the proof of Theorem II.1.1.(i).

Section II.7 proves Theorem II.1.1.(ii). We also build families of centrally indecomposable groups of the types in Theorem II.4.36. These examples are only a sample of the known constructions of this sort and the proofs provided are self-contained versions of broader results in [63].

Section II.8 has concluding remarks.

II.2 Background

Unless stated otherwise, all groups, algebras, and vector spaces will be finite and p will be an odd prime. We begin with brief introductions to central products and central decompositions of groups, followed by orthogonal decompositions of bilinear maps.

II.2.1 Central Decompositions and Products

Let $\mathcal{H}$ be a central decomposition of a group G (cf. Section II.1). The condition $[H, K] = 1$ for distinct $H, K \in \mathcal{H}$ shows that $H \cap \langle \mathcal{H} - \{H\} \rangle \leq Z(G)$ for all $H \in \mathcal{H}$. Whence, the members of $\mathcal{H}$ are normal subgroups of G.

Central decompositions can be realized by means of central products. Fix a set $\mathcal{H}$ of groups and a subgroup N of $\widetilde{\mathcal{H}} := \prod_{H \in \mathcal{H}} H$ such that $N \cap H = 1$ for all $H \in \mathcal{H}$. The *central product* of $\mathcal{H}$ with respect to N is $\widetilde{\mathcal{H}}/N$. If $\mathcal{H}$ is a central decomposition of a group G, then define $\pi : \widetilde{\mathcal{H}} \to G$ by $(x_H)_{H \in \mathcal{H}} \mapsto \prod_{H \in \mathcal{H}} x_H$. Then $G \cong \widetilde{\mathcal{H}}/\ker \pi$. These two treatments are equivalent [5, (11.1)].

In an arbitrary central decomposition $\mathcal{H}$ of a group G, in general $H \cap K$ and $H \cap J$ are distinct, for distinct elements $H, K, J \in \mathcal{H}$.

Definition II.2.1. *Given a subgroup $M \leq G$ and a central decomposition $\mathcal{H}$ of G, we call $\mathcal{H}$ an* M-central decomposition *if $M = H \cap K$ for all distinct $H, K \in \mathcal{H}$. The associated central product is an* M-central product.

Every central decomposition induces a $Z(G)$-central decomposition

$$\mathcal{H}Z(G) := \{HZ(G) : H \in \mathcal{H}\}.$$

Some authors write $H_1 * \cdots * H_s$ or $H_1 \circ \cdots \circ H_s$ for a $Z(G)$-central product. These notations still depend on the given $N \leq H_1 \times \cdots \times H_s$. We require a precise meaning in the following specific case:

$$\overbrace{H \circ \cdots \circ H}^{n} = \overbrace{H \times \cdots \times H}^{n}/N \tag{II.1}$$

where $N := \langle (1, \ldots, \overset{i}{x}, 1, \ldots, \overset{j}{x^{-1}}, 1, \ldots) | 1 \leq i < j \leq n, x \in Z(H) \rangle$.

II.2.2 Central Decompositions of p-groups of Class 2 and Exponent p

Using standard group theory, we show that central decompositions of a finite p-group P of class 2 and exponent p reduce to central decompositions of a subgroup Q where $P' = Q' = Z(Q)$ and $P = QZ(P)$. Furthermore, we show that for our purposes we may consider only $Z(Q)$-central decompositions (cf. Corollary II.2.9).

Definition II.2.2. *An automorphism $\varphi \in \operatorname{Aut} P$ is* upper central *if $Z(P)x\varphi = Z(P)x$, for all $x \in P$, and* lower central *if $P'x\varphi = P'x$, for all $x \in P$. The group of upper central automorphisms we denote by $\operatorname{Aut}_\zeta P$ and the lower central automorphisms by $\operatorname{Aut}_\gamma P$.*

As P has class 2, $\operatorname{Aut}_\gamma P \leq \operatorname{Aut}_\zeta P$. Furthermore, every $\alpha \in \operatorname{Aut}_\gamma P$ is also the identity on P'.

Lemma II.2.3. *(i) There are subgroups Q and A of P such that $Z(Q) = Q' = P'$, $A \leq Z(P)$ and $P = Q \times A$.*

(ii) Given subgroups Q and R of P such that $Z(Q) = Q' = P' = R' = Z(R)$ and $P = QZ(P) = RZ(P)$, if A is a complement to Q as in (i) then it is also a complement to R so that $P = Q \times A = R \times A$. Furthermore, there is an upper central automorphism of P sending Q to R and identity on $Z(P)$.

Proof. (i). Since P/P' is elementary abelian, there is $P' \leq Q \leq P$ such that $Q \cap Z(P) = P'$ and $P = QZ(P)$. Furthermore, $P' = [QZ(P), QZ(P)] = Q'$ and $[P, Z(Q)] = [QZ(P), Z(Q)] = 1$, so $Q' \leq Z(Q) \leq Q \cap Z(P) = Q'$.

Also, $Z(P)$ is elementary abelian, so there is a complement A to P' in $Z(P)$. Whence, $P = QZ(P) = QA$ and $Q \cap A \leq Q \cap Z(P) \cap A = P' \cap A = 1$. As A is central in P, $P = Q \times A$.

(ii). Fix two subgroups Q and R as described in the hypothesis. So there is a complement A to Q as in (i). Since $Q \cap Z(P) = P' = R \cap Z(P)$ it follows that $P = Q \times A = R \times A$. Let $\pi : P \to P$ be the projection of P to R with kernel A. Restricting π to Q gives a homomorphism $\alpha : Q \to R$. Furthermore, $P = QA$ so α is surjective, and $Q \cap A = 1$ so α is injective. Hence α is an isomorphism. Indeed, $Q' = P' = R'$ and π is the identity on R, so α is the identity on $Q' = R'$. Then $\beta = \alpha \times 1_A : Q \times A \to R \times A$ is a upper central automorphism of P sending Q to R. □

Definition II.2.4. *If $\mathcal{H}$ is a central decomposition of P, then define $Z(\mathcal{H}) = \{H \in \mathcal{H} : H \leq Z(P)\}$.*

Lemma II.2.5. *Let $\mathcal{H}$ be a fully refined central decomposition of P. If $Q = \langle \mathcal{H} - Z(\mathcal{H}) \rangle$ and $A = \langle Z(\mathcal{H}) \rangle$, then $P = Q \times A$, $Q' = Z(Q)$ and $Q'A = Z(P)$.*

Proof. Certainly $A \leq Z(P)$ and $P = QA$. Also $P' = Q'$ and $Z(P) = Z(Q)A$. As $\mathcal{H}$ is fully refined, every $H \in \mathcal{H} - \mathcal{A}$ is centrally indecomposable and so also directly indecomposable. By Lemma II.2.3 it follows that $H' = Z(H)$, for all $H \in \mathcal{H} - Z(\mathcal{H})$. As a result, $Q' = Z(Q)$. Thus $P = Q \times A$. □

Definition II.2.6. *Two central decompositions $\mathcal{H}$ and $\mathcal{K}$ of a group G are* exchangeable *if, for each $\mathcal{J} \subseteq \mathcal{H}$, there is an $\alpha \in \operatorname{Aut} G$ such that $\mathcal{J}\alpha \subseteq \mathcal{K}$ and $(\mathcal{H} - \mathcal{J})\alpha = \mathcal{H} - \mathcal{J}$.*

For instance, if $G = H_1 \circ \cdots \circ H_s = K_1 \circ \cdots \circ K_t$ are exchangeable decompositions, then $s = t$ and, for each $1 \leq i \leq s$,

$$G = H_1 \circ \cdots \circ H_i \circ K_{i+1} \circ \cdots \circ K_t.$$

Replacing $\circ$ with $\times$ we recognize this as the usual exchange property for direct decompositions. The Krull-Remak-Schmidt theorem states that all fully refined direct decompositions (Remak-decompositions) are exchangeable [49, (3.3.8)]. In light of Theorem II.1.1.(*ii*), a general p-group of class 2 and exponent p will have fully refined central decompositions which are not exchangeable.

Subgroups in $Z(\mathcal{H})$ can only be exchanged with subgroups in $Z(\mathcal{K})$, and similarly for the complements of these sets.

Lemma II.2.7. *If $\mathcal{H}$ and $\mathcal{K}$ are two fully refined central decompositions of P such that $\mathcal{H} - Z(\mathcal{H}) = \mathcal{K} - Z(\mathcal{K})$, then $\mathcal{H}$ and $\mathcal{K}$ are exchangeable.*

Proof. Set $Q = \langle \mathcal{H} - Z(\mathcal{H}) \rangle$, $A = \langle Z(\mathcal{H}) \rangle$, $R = \langle \mathcal{K} - Z(\mathcal{K}) \rangle$ and $B = \langle Z(\mathcal{K}) \rangle$. By Lemma II.2.3.(*i*) it follows that $P = Q \times A = R \times B$ and by Lemma II.2.3.(*ii*), $P = Q \times B$ as well. The projection endomorphism π from P to B with kernel Q makes $\alpha = 1_Q \times \pi$ an automorphism sending A to B and identity on Q. Since A and B are abelian, any fully refined central decomposition is a direct decomposition so $(Z(\mathcal{H}))\alpha$ is exchangeable with $Z(\mathcal{K})$ by automorphisms of B. As $\operatorname{Aut} B$ extends to $\operatorname{Aut} P$ inducing the identity on Q, it follows that $\mathcal{H}$ and $\mathcal{K}$ are exchangeable. □

Theorem II.2.8. *If $\mathcal{H}$ and $\mathcal{K}$ are two fully refined central decompositions of P such that $\mathcal{H}Z(P) = \mathcal{K}Z(P)$, then $\mathcal{H}$ and $\mathcal{K}$ are exchangeable.*

Proof. It suffices to prove that a single subgroup of $\mathcal{H}$ can be exchanged with one in $\mathcal{K}$. Let $M = Z(P)$ and fix $H \in \mathcal{H} - Z(\mathcal{H})$. As $\mathcal{H}M = \mathcal{K}M$ there is a $K \in \mathcal{K}$ such that $HM = KM$. Since H is not contained in $Z(P)$ neither is K. If $J \in \mathcal{K}$ such that $HM = JM$ then $J \leq \langle K, M \rangle$, and so $\mathcal{K} - \{J\}$ generates P. As $\mathcal{K}$ is fully refined this cannot occur. So K is uniquely determined by H.

By Lemma II.2.3.(i) and the assumption that $\mathcal{H}$ and $\mathcal{K}$ are fully refined, it follows that $H' = Z(H)$ and $K' = Z(K)$. As $Z(HM) = M = Z(KM)$ it follows that $HZ(HM) = HM = KM = KZ(KM)$. So by Lemma II.2.3.($ii$) there is an automorphism α of $HM = KM$ which is the identity on M and maps H to K. Extend α to P by defining α as the identity on all $J \in \mathcal{H} - \{H\}$. This extension exchanges H and K. □

Corollary II.2.9. *Let P be a p-group of class 2 and exponent p.*

(i) $\mathrm{Aut}_\zeta P$ *is transitive on Remak-decompositions.*

(ii) Given two fully refined central decompositions $\mathcal{H}$ and $\mathcal{K}$ of P, there is a $\varphi \in \mathrm{Aut}_\zeta P$ such that $\mathcal{H}\varphi = \mathcal{K}$ if, and only if, $\mathcal{H}Z(P) = \mathcal{K}Z(P)$.

Proof. (i). This is the Krull-Remak-Schmidt theorem.

(ii). Suppose that $\mathcal{H}\varphi = \mathcal{K}$ for some $\varphi \in \mathrm{Aut}_\zeta P$. Given $H \in \mathcal{H}$ set $K := H\varphi$. Then $HZ(P)/Z(P) = (HZ(P)/Z(P))\varphi = KZ(P)/Z(P)$ so $HZ(P) = KZ(P)$. Thus $\mathcal{H}Z(P) = \mathcal{K}Z(P)$.

For the reverse direction, let $\mathcal{H}Z(P) = \mathcal{K}Z(P)$. Then by Theorem II.2.8 there is a $\varphi \in \mathrm{Aut}_\zeta P$ sending $\mathcal{H}$ to $\mathcal{K}$. □

II.2.3 Bilinear and Hermitian maps, Isometries, and Pseudo-Isometries

In this section we introduce terminology and elementary properties for bilinear maps which we will use frequently. Throughout, let V and W be vector spaces over a field k.

A map $b : V \times V \to W$ is *k-bilinear* if it satisfies

$$b(su + u', tv + v') = stb(u, v) + tb(u', v) + sb(u, v') + b(u', v')$$

for all $u, u', v, v' \in V$ and $s, t \in k$. Given $X, Y \subseteq V$ define

$$b(X, Y) := \langle b(u, v) : u \in X, v \in Y \rangle.$$

For convenience we assume all our bilinear maps have $W = b(V, V)$. Whenever $X \leq V$ we can restrict b to

$$b_X : X \times X \to b(X, X). \tag{II.2}$$

The *radical* of b is

$$\operatorname{rad} b := \{u \in V : b(u, V) = 0 = b(V, u)\}.$$

If $\operatorname{rad} b = 0$ then b is *non-degenerate*. A k-bilinear map $b : V \times V \to W$ is called *θ-Hermitian* if $\theta \in \mathrm{GL}(W)$ and

$$b(u, v) = b(v, u)\theta, \qquad \forall u, v \in V. \tag{II.3}$$

As $W = b(V, V)$, θ is an *involution* (which in this paper will mean $\theta^2 = 1$ and allow $\theta = 1$). Furthermore, θ is uniquely determined by b (assuming $W \neq 0$) and so it is sufficient to say b is Hermitian.

If $\theta = 1_W$ we say that b is *symmetric* and if $\theta = -1_W$ we call b *skew-symmetric*. As we work in odd characteristic it follows that every skew-symmetric bilinear map is equivalently *alternating* in the sense that $b(v, v) = 0$ for all $v \in V$.

Given two k-bilinear maps $b : V \times V \to W$ and $b' : V' \times V' \to W'$ a *morphism* from b to b' is a pair (α, β) of linear maps $\alpha : V \to V'$ and $\beta : W \to W'$ such that

$$b'(u\alpha, v\alpha) = b(u, v)\beta, \qquad \forall u, v \in V. \tag{II.4}$$

When α is surjective it follows that $W' = b'(V\alpha, V\alpha)$; so, β is uniquely determined by α. In this case we often write $\hat{\alpha}$ for β. If α and $\hat{\alpha}$ are isomorphisms then we say b and b' are *pseudo-isometric*. The term *isometric* is reserved for the special circumstance where $W = W'$ and $\hat{\alpha} = 1_W$.

The *pseudo-isometry group* is

$$\begin{aligned} \mathrm{Isom}^*(b) :=& \{(\alpha, \hat{\alpha}) \in \mathrm{GL}(V) \times \mathrm{GL}(W) : \\ & b(u\alpha, v\alpha) = b(u, v)\hat{\alpha}, \forall u, v \in V\}, \end{aligned} \tag{II.5}$$

and the *isometry group* is

$$\mathrm{Isom}(b) := \{\alpha \in \mathrm{GL}(V) : b(u\alpha, v\alpha) = b(u, v), \forall u, v \in V\}. \tag{II.6}$$

(The decision to write the isometry group as a subgroup of $\mathrm{GL}(V)$ rather than $\mathrm{GL}(V) \times \mathrm{GL}(W)$ is to match with the classical definition of the isometry group of a bilinear form.) When b is a bilinear k-form (i.e.: $W = k$), the pseudo-isometry group goes by various names, including the group of *similitudes* and the *conformal* group of b. The following is obvious:

Proposition II.2.10. *(i) If $(\varphi, \hat{\varphi})$ is a pseudo-isometry from b to b' then* $\mathrm{Isom}^*(b) \cong \mathrm{Isom}^*(b')$ *via* $(\alpha, \hat{\alpha}) \mapsto (\alpha^{\varphi}, \hat{\alpha}^{\hat{\varphi}})$, *and* $\mathrm{Isom}(b) \cong \mathrm{Isom}(b')$ *via* $\alpha \mapsto \alpha^{\varphi}$.

(ii) If $b : V \times V \to W$ is a bilinear map, then $(\alpha, \hat{\alpha}) \mapsto \hat{\alpha}$ is a homomorphism from $\mathrm{Isom}^*(b)$ *into* $\mathrm{GL}(W)$ *with kernel naturally identified with* $\mathrm{Isom}(b)$.

In light of Proposition II.2.10.(*ii*) we will view $\mathrm{Isom}(b)$ as a subgroup of $\mathrm{Isom}^*(b)$ and $\mathrm{Isom}^*(b)/\mathrm{Isom}(b)$ as a subgroup of $\mathrm{GL}(W)$.

II.2.4 $\perp$-Decompositions

Definition II.2.11. *Let $b : V \times V \to W$ be a k-bilinear map.*

(i) A set $\mathcal{X}$ of subspaces of V is a $\perp$-decomposition *of b if: (a) $b(X, Y) = 0$ for all distinct $X, Y \in \mathcal{X}$ and (b) $V = \langle \mathcal{Y} \rangle$ for $\mathcal{Y} \subseteq \mathcal{X}$ if, and only if, $\mathcal{Y} = \mathcal{X}$.*

(ii) A subspace X of V is a $\perp$-factor if there is a $\perp$-decomposition $\mathcal{X}$ containing X. Furthermore, define

$$X^{\perp} := \langle \mathcal{X} - \{X\} \rangle.$$

(iii) We say b is $\perp$-indecomposable *if is has only the trivial $\perp$-decomposition $\{V\}$.*

(iv) A $\perp$-decomposition $\mathcal{X}$ of b is completely refined *if b_X is $\perp$-indecomposable for each $X \in \mathcal{X}$ (cf.* (II.2)*).*

When b is Hermitian it is also *reflexive* in the sense that $b(u, v) = 0$ if, and only if, $b(v, u) = 0$, for $u, v \in V$. Also, $X^{\perp} = \{x \in V : b(X, x) = 0\}$.

Let $\mathcal{X}$ be a $\perp$-decomposition of b and take $X \in \mathcal{X}$. For each $x \in X \cap \langle \mathcal{X} - \{X\} \rangle$ we know $b(x, \langle \mathcal{X} - \{X\} \rangle) = 0$ and $b(x, X) = 0$; thus, $b(x, V) = 0$. Hence, $X \cap \langle \mathcal{X} - \{X\} \rangle \leq \operatorname{rad} b$. Thus a fully refined $\perp$-decomposition is also a direct decomposition of V (and more generally any $\perp$-decomposition, if the bilinear map is non-degenerate.)

The pseudo-isometry group (II.5) acts on the set of all $\perp$-decompositions, but may not be transitive on the set of all fully refined decompositions. This fact can already be seen for symmetric bilinear forms (see Theorem II.5.5).

II.2.5 Symmetric Bilinear Forms

Various parts of our proofs and examples require some classical facts about symmetric bilinear forms over finite fields.

Let K be a finite field and $\omega \in K$ a non-square. By [4, p. 144], every n-dimensional non-degenerate symmetric bilinear K-form is isometric to $d : K^n \times K^n \to K$ defined by

$$d(u,v) := uDv^t, \forall u, v \in K^n; \tag{II.7}$$

where D is I_n or $I_{n-1} \oplus [\omega]$. If n is odd then these two forms are pseudo-isometric, but they are not pseudo-isometric if n is even. If $A \in \mathrm{GL}(n,K)$ then $d(uA, vA) = u(ADA^t)v^t$. The *discriminant* of d is

$$\operatorname{disc} d \equiv \det D \equiv \det ADA^t \pmod{(K^\times)^2}, \tag{II.8}$$

for any $A \in \mathrm{GL}(n,K)$ [4, (3.7)]. The discriminant distinguishes the two isometry classes of non-degenerate symmetric bilinear forms of a fixed dimension.

Lemma II.2.12. *Let $d : K^2 \times K^2 \to K$ be defined as in* (II.7).

(i) If $\operatorname{disc} d = [1]$ *then* $\left(\begin{bmatrix} \alpha & \beta \\ \beta & -\alpha \end{bmatrix}, \omega \right) \in \mathrm{Isom}^*(d)$, *where* $\omega = \alpha^2 + \beta^2 \in K$.

(ii) If $\operatorname{disc} d = [\omega]$ *then* $\left(\begin{bmatrix} 0 & 1 \\ \omega & 0 \end{bmatrix}, \omega \right) \in \mathrm{Isom}^*(d)$.

Proof. In both cases $ADA^t = \omega D$ for the given matrix and scalar pair (A, ω) and D as in (II.7). $\square$

Proposition II.2.13. *Let d be as in* (II.7). *Then (by definition)* $\mathrm{Isom}(d)$ *is the general orthogonal group* $\mathrm{GO}(d)$. *Also,*

(i) if n is odd then $\mathrm{Isom}^*(d) = \langle (\alpha, 1), (sI_n, s^2) \mid \alpha \in \mathrm{GO}(d), s \in K^\times \rangle$; *hence,* $\mathrm{Isom}^*(d)/\mathrm{Isom}(d) \cong (K^\times)^2$;

(ii) if n is even then $\mathrm{Isom}^*(d) = \langle(\alpha,1),(sI_n,s^2),(\varphi,\omega) \mid \alpha \in \mathrm{GO}(d), s \in K^\times\rangle$ *where* $\varphi := \phi \oplus \cdots \oplus \phi \oplus \mu$, (ϕ,ω) *is as in Lemma II.2.12.(i) and*

(a) if $\mathrm{disc}\, d = [1]$ *then* (μ,ω) *is as in Lemma II.2.12.(i); and*

(b) if $\mathrm{disc}\, d = [\omega]$ *then* (μ,ω) *is as in Lemma II.2.12.(ii).*

In particular, $\mathrm{Isom}^*(d)/\mathrm{Isom}(d) \cong K^\times$.

Therefore, $|\mathrm{Isom}^*(d)| = \varepsilon(q-1)|\mathrm{GO}(d)|$ *where* $q = |K|$, $\varepsilon = 1/2$ *if n is odd, and* $\varepsilon = 1$ *if n is even.*

Proof. By Proposition II.2.10.(ii) we start knowing $\mathrm{Isom}^*(d)/\mathrm{Isom}(d) \leq K^\times$. Furthermore, $\mathrm{Isom}^*(d) = \{(A,s) \in \mathrm{GL}(V) \times k^\times : ADA^t = sD\}$. Hence, for each $(A,s) \in \mathrm{Isom}^*(d)$ we must have $s^n = (\det A)^2$. (i). If n is odd then s must be a square. Hence, $\mathrm{Isom}^*(d)/\mathrm{Isom}(d) \cong (K^\times)^2$. As $(sI_n, s^2) \in \mathrm{Isom}^*(d)$ it follows that $\mathrm{Isom}^*(d) = \langle(\alpha,1),(sI_n,s^2) \mid \alpha \in \mathrm{GO}(d), s \in K^\times\rangle$. (ii). If n is even, then $(\varphi,\omega) \in \mathrm{Isom}^*(d)$. Thus $\mathrm{Isom}^*(d)/\mathrm{Isom}(d) = \langle s^2, \omega : s \in K^\times\rangle = K^\times$ and $\mathrm{Isom}^*(d) = \langle(\alpha,1),(sI_n,s^2),(\varphi,\omega) \mid \alpha \in \mathrm{GO}(d), s \in K^\times\rangle$. □

II.3 Bilinear Maps and p-groups

In this section we transform fully refined central decompositions into $\perp$-decompositions, automorphisms into pseudo-isometries, and back (Proposition II.3.3 and Theorem II.3.6).

The proofs use a well-known method to convert p-groups of class 2 into bilinear maps explored as early as [6], compare [28], and [58, Section 5]. The method is closely related to the Kaloujnine-Lazard-Mal'cev correspondence (see [32, Theorems 10.13,10.20]).

Our notation is additive when inside elementary abelian sections.

II.3.1 The Functor Bi

Let P be a p-group of class 2 and exponent p, $V := P/P'$, and $W := P'$. Then V and W are elementary abelian p-groups, that is, $\mathbb{Z}_p$-vector spaces. The commutator affords an alternating $\mathbb{Z}_p$-bilinear map $\mathsf{Bi}(P) : V \times V \to W$ where $b := \mathsf{Bi}(P)$ is defined by

$$b(P'x, P'y) := [x,y], \qquad \forall x, y \in P. \tag{II.9}$$

The radical of b is $Z(P)/P'$. If $\alpha : P \to Q$ is a homomorphism of p-groups of class 2 and exponent p, then

$$\mathsf{Bi}(\alpha) := (\alpha|_{P/P'} : P'x \mapsto Q'x\alpha, \alpha|_{P'} : x \mapsto x\alpha) \tag{II.10}$$

is a morphism from $\mathsf{Bi}(P)$ to $\mathsf{Bi}(Q)$ (cf. (II.4)).

Remark II.3.1. *We have refrained from using $V := P/Z(P)$ and $W := Z(P)$. A homomorphism $\alpha : P \to Q$ of p-groups need not map the center of P into the center of Q so with $W = Z(P)$ we cannot induce a morphism $\mathsf{Bi}(\alpha)$ of $\mathsf{Bi}(P) \to \mathsf{Bi}(Q)$. Moreover, using P' we have $W = b(V,V)$. The penalty is that b may be degenerate. We avoid this difficulty by means of Lemma II.2.3.(i).*

Given another homomorphism $\beta : Q \to R$ then $\mathsf{Bi}(\alpha\beta) = \mathsf{Bi}(\alpha)\mathsf{Bi}(\beta)$; so, Bi is a functor. Finally, if $\alpha, \beta : P \to Q$ are homomorphisms then $\mathsf{Bi}(\alpha) = \mathsf{Bi}(\beta)$ if, and only if, $\alpha|_{P/P'} = \beta|_{P/P'}$ (which forces also $\alpha|_{P'} = \beta|_{P'}$).

Finally, subgroups $Q \leq P$ are mapped to $b_{QP'/P'}$ (see (II.2)). If $Q' = Z(Q)$ (as in Lemma II.2.3.(i)) then $Q' \leq Q \cap P' \leq Q \cap Z(P) \leq Z(Q) = Q'$ so that $Q \cap P' = Q'$. Hence, $QP'/P' \cong Q/Q'$ and $b_{QP'/P'}$ is naturally pseudo-isometric to $\mathsf{Bi}(Q)$.

Proposition II.3.2. *If $\mathcal{H}$ is a central decomposition of P, then $\mathsf{Bi}(\mathcal{H}) := \{HP'/P' : H \in \mathcal{H}\}$ is a $\perp$-decomposition of b.*

Proof. Let H and K be distinct members of $\mathcal{H}$. As $[H,K] = 1$ it follows that $b(HP'/P', KP'/P') = 0$. Furthermore, $\mathcal{H}$ generates P and so $\mathcal{X} := \mathsf{Bi}(\mathcal{H})$ generates $V = P/P'$. Take a proper subset $\mathcal{Y} \subset \mathcal{X}$. Define $\mathcal{J} := \{H \in \mathcal{H} : HP'/P' \in \mathcal{Y}\} \subseteq \mathcal{H}$. Note $\mathcal{Y} = \mathsf{Bi}(\mathcal{J})$. Since $\mathcal{Y}$ is a proper subset of $\mathcal{X}$, it follows that $\mathcal{J}$ generates a proper subgroup Q of P and thus $\mathcal{Y}$ generates QP'/P'. We must show $QP'/P' \neq P/P'$, or rather, that $QP' \neq P$.

Suppose that $QP' = P$. For each $K \in \mathcal{H} - \mathcal{J}$, K is not contained in Q by the assumptions on $\mathcal{H}$. Now $[P : P'] = [Q : Q \cap P'] \leq [QK : Q \cap P'] \leq [P : P']$ so $QK = Q$ and $K \leq Q$. This is impossible. Hence Q is proper. □

II.3.2 The Functor Grp

Suppose $b : V \times V \to W$ is an alternating $\mathbb{Z}_p$-bilinear map. Equip the set $V \times W$ with the product

$$(u,w) * (v,x) := \left(u+v, w+x+\frac{1}{2}b(u,v)\right), \qquad \forall (u,w),(v,x) \in V \times W.$$

The result is a group denoted $\mathsf{Grp}(b)$. If $(\alpha, \hat{\alpha})$ is a morphism from b to $b' : V' \times V' \to W'$ (see (II.4)), then $\mathsf{Grp}(\alpha, \hat{\alpha}) : \mathsf{Grp}(b) \to \mathsf{Grp}(b')$ is $(v, w) \mapsto (v\alpha, w\hat{\alpha})$.

By direct computation we verify that $\mathsf{Grp}(b)$ is a p-group of class 2 and exponent p with center $\operatorname{rad} b \times W$ and commutator subgroup $0 \times W$. Furthermore, Grp is a functor. Compare with [58, Theorem 5.14] and [6, Theorem 2.1].

If $\varphi \in \operatorname{Aut}_\gamma P$ (cf. Definition II.2.2) then φ induces the identity on $V = P/P'$ and $W = P'$. So write $\varphi - 1$ for the induced $\mathbb{Z}_p$-linear map $V \to W$ defined by $P'x(\varphi - 1) = x^{-1}(x\varphi)$.

Proposition II.3.3. *Let $P = \mathsf{Grp}(b)$. All the following hold:*

(i) $\operatorname{Aut}_\gamma P \cong \hom(V, W)$ *via the isomorphism* $\varphi \mapsto \varphi - 1$, *for all* $\varphi \in \operatorname{Aut}_\gamma P$.

(ii) $\operatorname{Aut} P \cong \operatorname{Isom}^*(b) \ltimes \operatorname{Aut}_\gamma P$, *with* $(1 + \varphi)^{(\alpha, \hat{\alpha})} = 1 + \alpha^{-1}\varphi\hat{\alpha}$ *for each* $\varphi \in \hom(V, W)$ *and* $(\alpha, \hat{\alpha}) \in \operatorname{Isom}^*(b)$.

(iii) $C_{\operatorname{Aut} P}(P') \cong \operatorname{Isom}(b) \ltimes \operatorname{Aut}_\gamma P$.

Proof. These follow directly from the definition of $\mathsf{Grp}(b)$. □

If $U \leq V$ then define $\mathsf{Grp}(b_U)$ as $U \times b(U, U) \leq \mathsf{Grp}(b)$. It is evident that this determines a subgroup. Similarly, given a set of subspaces $\mathcal{X}$ of V define $\mathsf{Grp}(\mathcal{X}) = \{\mathsf{Grp}(b_U) : U \in \mathcal{X}\}$.

Proposition II.3.4. *If $\mathcal{X}$ is a $\perp$-decomposition of b then $\mathsf{Grp}(\mathcal{X})$ is a central decomposition of $\mathsf{Grp}(b)$.*

Proof. Let X and Y be distinct members of $\mathcal{X}$. Set $H := \mathsf{Grp}(b_X)$, $K := \mathsf{Grp}(b_Y)$ and $P = \mathsf{Grp}(b)$. Since $b(X, Y) = 0$ it follows that $[H, K] = 1$. Also, V is generated by $\mathcal{X}$, and $V \times 0$ generates P, so that P is generated by $\mathcal{H} := \mathsf{Grp}(\mathcal{X})$.

Let $\mathcal{J}$ be a proper subset of $\mathcal{H}$. Define $\mathcal{Y} = \{X \in \mathcal{X} : \mathsf{Grp}(b_X) \in \mathcal{J}\}$. As $\mathcal{J} \neq \mathcal{H}$ it follows that $\mathcal{X} \neq \mathcal{Y}$ and therefore $U := \langle \mathcal{Y} \rangle \neq V$. Furthermore, $\langle \mathcal{J} \rangle = \mathsf{Grp}(b_U) = U \times b(U, U) \neq V \times b(V, V) = P$. So indeed, $\mathcal{H}$ is a central decomposition. □

II.3.3 Equivalence of Central and Orthogonal Decompositions

Here we relate fully refined central decompositions to fully refined $\perp$-decompositions.

Proposition II.3.5. *Let $b : V \times V \to W$ be an alternating $\mathbb{Z}_p$-bilinear map and P a p-group of class 2 and exponent p.*

(i) There is a natural pseudo-isometry $(\tau, \hat{\tau})$ *from* b *to* $b' := \mathsf{Bi}(\mathsf{Grp}(b))$.

(ii) Every function $\ell : P/P' \to P$ *to a transversal of* P/P' *in* P, *with* $0\ell = 1$ *determines an isomorphism* $\varphi_\ell : P \to \tilde{P}$ *where* $\tilde{P} := \mathsf{Grp}(\mathsf{Bi}(P))$.

Proof. (i). Let $b : V \times V \to W$ be an alternating bilinear map. Set $P = \mathsf{Grp}(b)$ and $b' = \mathsf{Bi}(\mathsf{Grp}(b))$. Recall $P' = 0 \times W$ and define $\tau : V \to P/P'$ by $v\tau = (v, 0) + 0 \times W$ and $\hat{\tau} : W \to 0 \times W$ by $w\hat{\tau} = (0, w)$. This makes $(\tau, \hat{\tau})$ a pseudo-isometry from b to b'. It is straightforward to verify that $(\tau, \hat{\tau})$ is indeed a natural transformation.

(ii). Now let P be an arbitrary p-group of class 2 and exponent p. Set $V := P/P'$, $W := P'$, $b := \mathsf{Bi}(P)$ and $\tilde{P} := \mathsf{Grp}(\mathsf{Bi}(P))$. Given a lift $\ell : V \to P$ with $0\ell = 1$, define $x\varphi_\ell := (\bar{x}, x - \bar{x}\ell)$ where $\bar{x} := P'x$. The group P has the presentation

$$\langle V\ell, W \mid [u\ell, v\ell] = b(u, v),\ \text{exponent } p,\ \text{class } 2\rangle$$

and $\tilde{P}$ has the presentation

$$\langle V \times 0, 0 \times W \mid [(u, 0), (v, 0)] = (0, b(u, v)),\ \text{exponent } p,\ \text{class } 2\rangle.$$

Evidently φ_ℓ preserves the exponent relations. Furthermore,

$$[x, y]\varphi_\ell = [\bar{x}\ell, \bar{y}\ell]\varphi_\ell = b(\bar{x}, \bar{y})\varphi_\ell = (0, b(\bar{x}, \bar{y}))$$

for each $x, y \in P$. Hence, φ_ℓ preserves all the relations of the presentations and so φ_ℓ is a homomorphism, indeed, an isomorphism.

□

Theorem II.3.6. *Let* P *be a* p*-group of class* 2 *and exponent* p *such that* $P' = Z(P)$, *and let* $\mathcal{H}$ *be a central decomposition of* P.

(i) P *is centrally indecomposable if, and only if,* $\mathsf{Bi}(P)$ *is* $\perp$*-indecomposable.*

(ii) $\mathcal{H}$ *is a fully refined if, and only if,* $\mathsf{Bi}(\mathcal{H})$ *is fully refined.*

(iii) if $\mathcal{K}$ *is a central decomposition of* P, *then*

(a) there is an automorphism $\alpha \in \operatorname{Aut} P$ *such that* $(\mathcal{H}P')\alpha = \mathcal{K}P'$ *if, and only if, there is a* $(\beta, \hat{\beta}) \in \operatorname{Isom}^*(\mathsf{Bi}(P))$ *such that* $(\mathsf{Bi}(\mathcal{H}))\beta = \mathsf{Bi}(\mathcal{K})$.

(b) there is an automorphism $\alpha \in C_{\operatorname{Aut} P}(P')$ *such that* $(\mathcal{H}P')\alpha = \mathcal{K}P'$ *if, and only if, there is a* $\beta \in \operatorname{Isom}(\mathsf{Bi}(P))$ *such that* $(\mathsf{Bi}(\mathcal{H}))\beta = \mathsf{Bi}(\mathcal{K})$.

Proof. (i). Let P be a centrally indecomposable group and take $b := \mathsf{Bi}(P)$, $V = P/P'$, $W = P'$. Suppose that $\mathcal{X}$ is a $\perp$-decomposition of b. It follows that $\{X \times b(X,X) : X \in \mathcal{X}\}$ is central decomposition of $\mathsf{Grp}(\mathsf{Bi}(P))$ Proposition II.3.4. By Proposition II.3.5.(ii) we know P is isomorphic to $\mathsf{Grp}(\mathsf{Bi}(P))$ so that $\mathsf{Grp}(\mathsf{Bi}(P))$ must be centrally indecomposable. Therefore, $X \times b(X,X) = \mathsf{Grp}(\mathsf{Bi}(P)) = V \times W$ so that $X = V$, for each $X \in \mathcal{X}$. Since no proper subset of $\mathcal{X}$ generates V it follows that $\mathcal{X} = \{V\}$ and b is $\perp$-indecomposable.

Next suppose that b is $\perp$-indecomposable and that $P = \mathsf{Grp}(b)$. Suppose that $\mathcal{H}$ is a fully refined central decomposition of P. Then $\{HP'/P' : H \in \mathcal{H}\}$ is a $\perp$-decomposition of $\mathsf{Bi}(\mathsf{Grp}(b))$, Proposition II.3.2. Proposition II.3.5.(i) states that b is pseudo-isometric to $\mathsf{Bi}(\mathsf{Grp}(b))$ and so $HP'/P' = P/P'$, or rather $HP' = P$, for each $H \in \mathcal{H}$. Hence $H' = P'$ for each $H \in \mathcal{H}$. Since $P' \neq 1$ there is an $H \in \mathcal{H}$ which is non-abelian. Furthermore, H is centrally indecomposable so that by Lemma II.2.3.(i), $H' = Z(H)$. Therefore, $HP' = H \oplus A$ for some $A \leq Z(P)$ such that $H'A = P'$, Lemma II.2.3.(i). But $H' = P'$ forces $A = 1$. Thus $H = P$, and P is centrally indecomposable.

(ii). This follows from Proposition II.3.4, Proposition II.3.2 and (i). Finally, (iii) follows from Proposition II.3.3. □

Example II.3.7. *If* H *is* p*-group of class* 2 *and exponent* p *with* $b = \mathsf{Bi}(H)$ *then*

$$\mathsf{Bi}(\overbrace{H \circ \cdots \circ H}^{n}) = \overbrace{b \perp \cdots \perp b}^{n},$$

(cf. (II.1)*). Furthermore, the canonical central decomposition* $\{H_1, \ldots, H_n\}$ *of* $\overbrace{H \circ \cdots \circ H}^{n}$ *corresponds to the canonical* $\perp$*-decomposition* $\{V_1, \ldots, V_n\}$ *of* $\overbrace{b \perp \cdots \perp b}^{n}$.

II.4 Adjoint and Self-adjoint Operators

In this section a structure theorem for isometry groups (Theorem II.4.17) is proved. Also a criterion is introduced for groups/bilinear maps to be indecomposable (Theorem II.4.36), and a stronger version of the first part of Theorem II.1.1 (Theorem II.4.32) is proved.

Throughout this section let $b : V \times V \to W$ be a *non-degenerate Hermitian bilinear map over a field* k (cf. (II.3)). We associate to b a $*$-algebra, and a Hermitian Jordan algebra of *self-adjoint* elements. The isometry group of b is a subgroup of the group of units of the $*$-algebra and $\perp$-decompositions are represented by sets of pairwise orthogonal idempotents of the Jordan algebra.

II.4.1 The Adjoint $*$-algebra $\mathrm{Adj}(b)$

Definition II.4.1. *(i) A map $f \in \mathrm{End}\, V$ has an* adjoint *$f^* \in \mathrm{End}\, V$ for b if*

$$b(uf, v) = b(u, vf^*), \qquad \forall u, v \in V.$$

Write $\mathrm{Adj}(b)$ for the set of all endomorphisms with an adjoint for b.

(ii) A $*$-algebra is an associative k-algebra A with a linear bijection $* : A \to A$ such that $(ab)^* = b^*a^*$ and $(a^*)^* = a$ for all $a, b \in A$.

(iii) A homomorphism $f : A \to B$ of $*$-algebras is a $*$-homomorphism if $a^*f = (af)^*$ for all $a \in A$.

(iv) The trace *of A is $T(x) = x + x^*$ for all $x \in A$.*

(v) The norm *of A is $N(x) = xx^*$ for all $x \in A$.*

Proposition II.4.2. $\mathrm{Adj}(b)$ *is an associative unital $*$-algebra; in particular, adjoints are unique.*

Proof. Let $f \in \mathrm{Adj}(b)$ and $f', f'' \in \mathrm{End}\, V$ where $b(u, vf') = b(uf, v) = b(u, vf'')$ for all $u, v \in V$. As b is non-degenerate, $vf' = vf''$ so that $f' = f''$. If $f, g \in \mathrm{Adj}(b)$ then $b(u(fg), v) = b(uf, vg^*) = b(u, v(g^*f^*))$ for $u, v \in V$; so, $fg \in \mathrm{Adj}(b)$ with $(fg)^* = g^*f^*$. Since $b(u, v) = b(v, u)\theta$ for $u, v \in V$, it follows that $b(uf^*, v) = b(v, uf^*)\theta = b(vf, u)\theta = b(u, vf)$ for every $f \in \mathrm{Adj}(b)$. Hence, $f^* \in \mathrm{Adj}(b)$ and $(f^*)^* = f$. □

Proposition II.4.3. *Let $b : V \times V \to W$ and $b' : V' \times V' \to W'$ be non-degenerate Hermitian maps.*

(i) A pseudo-isometry (α, β) from b to b' (cf. (II.4)) induces a $*$-isomorphism

$$f \mapsto f^{(\alpha,\beta)} := \alpha^{-1} f \alpha$$

of $\mathrm{Adj}(b)$ *to* $\mathrm{Adj}(b')$. *In particular,* $\mathrm{Isom}^*(b)$ *acts on* $\mathrm{Adj}(b)$.

(ii) Let $\varphi \in \mathrm{GL}(V)$ and $s \in k^\times$. Then $(\varphi, s1_W) \in \mathrm{Isom}^*(b)$ if, and only if, $\varphi \in \mathrm{Adj}(b)$ and $\varphi\varphi^* = s1_V$. Hence,

$$\mathrm{Isom}(b) = \{\varphi \in \mathrm{Adj}(b) : \varphi\varphi^* = 1_V\}.$$

Proof. (i) We have

$$\begin{aligned} b'(uf^{(\alpha,\beta)}, v) &= b'(u\alpha^{-1}f\alpha, v\alpha^{-1}\alpha) = b(u\alpha^{-1}f, v\alpha^{-1})\beta \\ &= b(u\alpha^{-1}, v\alpha^{-1}f^*)\beta = b'(u, v(f^*)^{(\alpha,\beta)}), \end{aligned}$$

for each $u, v \in V'$ and $f \in \mathrm{Adj}(b)$. Hence $f^{(\alpha,\beta)} \in \mathrm{Adj}(b')$ with $(f^{(\alpha,\beta)})^* = (f^*)^{(\alpha,\beta)}$.

(ii) Take $(\varphi, s1_W) \in \mathrm{Isom}^*(b)$, $s \in k^\times$. Then

$$b(u\varphi, v) = b(u\varphi, v\varphi^{-1}\varphi) = sb(u, v\varphi^{-1}) = b(u, sv\varphi^{-1}), \qquad \forall u, v \in V.$$

Hence $\varphi \in \mathrm{Adj}(b)$ with $\varphi^* = s\varphi^{-1}$. Conversely, if $\varphi \in \mathrm{Adj}(b)$ with $\varphi\varphi^* = s1_V$ then

$$b(u\varphi, v\varphi) = b(u, v\varphi\varphi^*) = sb(u, v), \qquad \forall u, v \in V.$$

Thus $(\varphi, s1_W) \in \mathrm{Isom}^*(b)$. □

II.4.2 Simple $*$-algebras and Hermitian C-forms $d : V \times V \to C$

In this section we summarize in a uniform manner the known results of finite simple $*$-algebras (Theorem II.4.4) and the corresponding finite classical groups (Proposition II.4.13).

Theorem II.4.4. *For a finite simple $*$-algebra $(A, *)$ over a field k of odd characteristic, there is*

an $n \in \mathbb{N}$ and a field extension K/k such that $(A, *)$ is $*$-isomorphic to one of the following:

Orthogonal case *$M_n(K)$ with the $X \mapsto D^{-1}X^tD$ as the involution, for $X \in M_n(K)$, where D is either I_n or $I_{n-1} \oplus [\omega]$ and $\omega \in K$ is a non-square (compare* (II.7)*).*

Unitary case *$M_n(F)$ with involution $X \mapsto \bar{X}^t$, where F/K is a quadratic field extension with involutory field automorphism $x \mapsto \bar{x}$, $x \in F$, applied to the entries of $X \in M_n(F)$.*

Exchange case *$M_n(K \oplus K)$ with involution $X \mapsto \bar{X}^t$, where $\overline{(x,y)} := (y,x)$ for $(x,y) \in K \oplus K$, defines an involution on $K \oplus K$ which is applied to the entries of $X \in M_n(K \oplus K)$,*

Symplectic case *$M_n(M_2(K))$ with involution $X \mapsto \bar{X}^t$, where*

$$\overline{\begin{bmatrix} a & b \\ c & d \end{bmatrix}} := \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^{-1} \tag{II.11}$$

defines an involution on $M_2(K)$ which is applied to each entry of $X \in M_n(M_2(K))$.

Proof. See [25, p.178] restricting consideration to finite fields. (Compare with Theorem II.4.7, Proposition II.4.11, (II.7), and Corollary II.4.12.) □

The above description of these algebras will allow us to give uniform proofs later; however, there are simpler and more standard descriptions, for example:

Remark II.4.5. *The exchange type $*$-algebras can also be described as $M_n(K) \oplus M_n(K)$ with $(X,Y)^* = (Y^t, X^t)$ for $(X,Y) \in M_n(K) \oplus M_n(K)$.*

The symplectic type $*$-algebras are $*$-isomorphic to $M_{2n}(K)$ with involution $X^* = JX^tJ^{-1}$, for each $X \in M_{2n}(K)$, where $J := I_n \otimes \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ [25, p. 178].

Definition II.4.6. *[27, Definition 6.2.2] A $*$-algebra C is an associative* composition *algebra over a field K (where by convention x^* is denoted $\bar{x}$) if*

(i) $K = \{x \in C : x = \bar{x}\}$ and

(ii) $xax = 0$ for all $a \in C$ implies $x = 0$.

Theorem II.4.7. *[27, Theorem 6.2.3] Over a finite field K of odd characteristic each associative composition algebra C is $*$-isomorphic to one of the following:*

(i) K *with trivial involution,*

(ii) a quadratic field extension F/K *with the involutorial field automorphism,*

(iii) $K \oplus K$ *with the* exchange *involution* $\overline{(x,y)} = (y,x)$ *for* $(x,y) \in K \oplus K$, *or*

(iv) $M_2(K)$ *with the involution* (II.11).

In particular these algebras are simple $*$*-algebras and with the exception of (iii) also simple algebras. Norms (cf. Definition II.4.1.(v)) behave as follows:* $N(C) = K$ *if* $C > K$; *otherwise,* $N(K) = K^2$.

Definition II.4.8. *Let* C *be an associative composition algebra and* V *be a free left* C*-module. We call a* K*-bilinear map* $d : V \times V \to C$ *a* Hermitian C-form *if, for* $u, v \in V$ *and* $s \in C$, *it follows that:*

(i) $d(u,v) = \overline{d(v,u)}$, *and*

(ii) $d(su,v) = sd(u,v)$ *and* $d(u,sv) = d(u,v)\bar{s}$.

The rank *of* d *is the rank of* V *as a free left* C*-module.*

Note that a Hermitian C-form is also a Hermitian K-bilinear map and the usual definitions of (pseudo-)isometries apply. *It is most important to note that* $d(x,x) = \overline{d(x,x)}$; *hence,* $d(x,x) \in K$, *for all* $x \in V$.

Let C be an associative composition algebra over K and $D \in M_n(C)$ where $D = \bar{D}^t$. Then $d_D(u,v) := uD\bar{v}^t$, for $u, v \in C^n$, determines a Hermitian C-form $d_D : C^n \times C^n \to C$. Here adjoints $f, f^* \in \mathrm{Adj}(d_D)$ can be represented as matrices $F, F^* \in M_n(C)$ such that:

$$uFD\bar{v}^t = d_D(uf, v) = d_D(u, vf^*) = uD(\bar{F}^*)^t\bar{v}^t, \qquad \forall u, v \in C^n.$$

Hence, $FD = D(\bar{F}^*)^t$. As D is invertible, $\mathrm{Adj}(d_D)$ $*$-isomorphic to $M_n(C)$ with involution defined by

$$F^* := D\bar{F}^tD^{-1}, \qquad \forall F \in M_n(C). \tag{II.12}$$

Likewise, if $d : V \times V \to C$ is a Hermitian C-form and $\mathcal{X}$ is an ordered basis of V as a free left C-module, then setting $D_{xy} := d(x,y)$, for all $x, y \in \mathcal{X}$, determines a matrix D in $M_n(C)$, $n = |\mathcal{X}|$, such that $D = \bar{D}^t$ and the Hermitian C-form given by D is isometric to d. Furthermore, d is non-degenerate if, and only if, D is invertible. So we have:

Corollary II.4.9. *Every simple $*$-algebra is $*$-isomorphic to* $\mathrm{Adj}(d)$ *for a non-degenerate Hermitian C-form $d : V \times V \to C$.*

In the cases where C has orthogonal or unitary type we have the usual symmetric and Hermitian forms, respectively. Suppose instead the $C = M_2(K)$ and that $d : V \times V \to C$ is the non-degenerate Hermitian C-from $d(u, v) := u\bar{v}^t$, where $V = C^n$. There is a natural submodule U of V defined by:

$$U := \overbrace{\left\{\begin{bmatrix} * & * \\ 0 & 0 \end{bmatrix}\right\} \oplus \cdots \oplus \left\{\begin{bmatrix} * & * \\ 0 & 0 \end{bmatrix}\right\}}^{n} \leq V.$$

Furthermore, $d(U, U) \cong K$; hence, the restriction $d_U : U \times U \to K$ is a bilinear form. It is easily checked that d_U is alternating and non-degenerate. The case when C has exchange type is not usually handled as a form but for a uniform treatment we find it convenient. In particular we may state:

Definition II.4.10. *Given a non-degenerate Hermitian C-form $d : V \times V \to C$, an element $x \in V$ is* non-singular *if $d(v, v) \neq 0$ and $\dim Cv = \dim C$.*

Proposition II.4.11. *Every non-degenerate Hermitian C-form $d : V \times V \to C$ has an orthogonal C-basis $\mathcal{X}$ (i.e.: $\mathcal{X}$ is a C-basis for V and $d(x, y) = 0$ if $x \neq y$, $x, y \in \mathcal{X}$). Furthermore, every fully refined $\perp$-decomposition of d determines an orthogonal basis and so every $\perp$-indecomposable has rank* 1.

Proof. First we show that there is always a non-singular vector $x \in V$.

Suppose otherwise: $d(x, x) = 0$ for any $x \in V$ such that $\dim Cx = \dim C$. Immediately, $d(v, v) = 0$ for all $v \in V$ and thus $-d(v, u) = d(u, v) = \overline{d(v, u)}$ for $u, v \in V$.

For each $u \in V$, $Cd(u, V) + d(V, u)C$ is a bar-ideal of C. As C is a simple bar-algebra (Theorem II.4.7), $Cd(u, V) + d(V, u)C = 0$ or C. If $Cd(u, V) + d(V, u)C = 0$ then $Cd(u, V) = 0$ and $d(V, u)C = 0$; hence, $u \in \operatorname{rad} d = 0$. Thus, $C = Cd(u, V) + d(V, u)C$ for all $u \in V - \{0\}$. We divide into two cases.

If $C = Cd(u, V)$ then $1 = d(su, v)$ for some $s \in C$ and $v \in V$. Then $1 = \bar{1} = \overline{d(su, v)} = -d(su, v) = -1$, so $\operatorname{char} K = 2$, which we exclude. Similarly, $d(V, u)C \neq C$.

Now suppose $C \neq Cd(u,V), d(V,u)C$. Then $Cd(u,V)$ is a proper ideal of C. By Theorem II.4.7 we see that $C = K \oplus K$ with the exchange involution. Without loss of generality, take $Cd(u,V) = K \oplus 0$. Hence $(1,0) = sd(u,v)$ for some $s \in C$ and $v \in V$. Thus, $(1,1) = d(su,v) + \overline{d(su,v)} = d(su,v) - d(su,v) = 0$, which is false. Therefore, there exists a non-singular vector $x \in V$.

As $0 \neq d(x,x) = \overline{d(x,x)}$ it follows that $d(x,x) \in K^\times$. Then $d\left(v - \frac{d(v,x)}{d(x,x)}x, x\right) = d(v,x) - \frac{d(v,x)}{d(x,x)}d(x,x) = 0$, for $v \in V$. That is, $v - \frac{d(v,x)}{d(x,x)}x \in x^\perp$; hence, $v = \frac{d(v,x)}{d(x,x)}x + \left(v - \frac{d(v,x)}{d(x,x)}x\right)$ shows that $V = Cx + x^\perp$. Since $Cx \cap x^\perp = 0$ it follows that $V = Cx \oplus x^\perp$. Restrict d to $x^\perp$ and induct to exhibit an orthogonal basis $\mathcal{X}$ for d on $x^\perp$. Thus $\mathcal{X} \cup \{x\}$ is an orthogonal basis of d on V. □

Notice in the case of type symplectic type, if $\{x_1, \ldots, x_n\}$ is an orthogonal C-basis for d, then $V = Cx_1 \perp \cdots \perp Cx_n$. Translating to the associated alternating bilinear form d', the orthogonal basis becomes a hyperbolic basis: $U = H_1 \perp \cdots \perp H_n$ where each H_i is a hyperbolic line (cf. [4, Definition 3.5]). In the case of exchange type, a natural orthogonal basis is given by $\{(x,x) : x \in \mathcal{X}\}$ where $\mathcal{X}$ is a K-basis of U and $V = U \oplus U$, $U = K^n$.

Corollary II.4.12. *If C does not have orthogonal type then d has an orthonormal C-basis (i.e.: a basis $\mathcal{X}$ where $d(x,y) = \delta_{xy}$, for all $x, y \in \mathcal{X}$). In particular, d is pseudo-isometric to the C-dot product $d : C^n \times C^n \to C$ where $d(u,v) := u\bar{v}^t$, for all $u, v \in V$.*

Proof. From Theorem II.4.7, $N(C) = K$ whenever $C > K$. Therefore if $v \in V$ such that $d(v,v) \neq 0$ then $d(v,v) = N(s) = s\bar{s}$ for some $s \in C^\times$. Let $u = s^{-1}v$ so that $d(u,u) = s^{-1}d(v,v)\bar{s}^{-1} = s^{-1}N(s)\bar{s}^{-1} = 1$. By Proposition II.4.11, we have an orthogonal basis $\mathcal{X}$ for d. Replace each $x \in \mathcal{X}$ with $s_x^{-1}x$ so that $d(s_x^{-1}x, s_x^{-1}x) = 1$ and $\{s^{-1}x : x \in \mathcal{X}\}$ is still an orthogonal C-basis. □

Proposition II.4.13. *Let $d : V \times V \to C$ be a non-degenerate Hermitian C-form. Then* $\mathrm{Adj}(d) = \mathrm{End}\, V \cong M_n(C)$ *as an algebra, and the following hold:*

Orthogonal type $C = K$ *and* $\mathrm{Isom}(d) = \mathrm{GO}(d)$*;*

Unitary type $C = F$ *and* $\mathrm{Isom}(d) = \mathrm{GU}(d)$*;*

Exchange type $C = K \oplus K$, $\mathrm{Isom}(d) \cong \mathrm{GL}(U)$, $V = U \oplus U$*; and*

Symplectic type $C = M_2(K)$ *and* $\mathrm{Isom}(d) \cong \mathrm{Sp}(U)$, $V = U \oplus U$.

Proof. The first two cases are by definition alone. If $C = K \oplus K$ then $\mathrm{Adj}_C(d) \cong \mathrm{End}\, U \oplus \mathrm{End}\, U$ with $(f \oplus g)^* = g \oplus f$. Hence, the isometry group is:

$$\begin{aligned}\mathrm{Isom}(d) &= \{f \oplus g \in \mathrm{GL}(U) \oplus \mathrm{GL}(U) : (f \oplus g)(f \oplus g)^* = 1 \oplus 1\} \\ &= \{f \oplus f^{-1} : f \in \mathrm{GL}(U)\} \cong \mathrm{GL}(U).\end{aligned}$$

Finally, if $C = M_2(K)$ then $\mathrm{Adj}(d) \cong \mathrm{Adj}(d')$ where d' is the non-degenerate alternating K-bilinear form on U, Remark II.4.5. Therefore $\mathrm{Isom}(d) \cong \mathrm{Isom}(d')$ as both are the set of elements defined by $\varphi\varphi^* = 1$ (Proposition II.4.3.(*ii*)). The latter group is by definition $\mathrm{Sp}(U)$. □

II.4.3 Radical and Semi-simple Structure of $*$-algebras

Definition II.4.14. *(i) A* $*$-ideal *is an ideal I of a $*$-algebra A such that $I^* = I$.*

(ii) $\mathrm{spec}_0\, A$ *is the set of all maximal $*$-ideals of A.*

(iii) A $*$-simple *algebra is a $*$-algebra with exactly two $*$-ideals.*

(iv) A $*$-semi-simple *algebra is a direct product of simple $*$-algebras.*

(v) A $*$-ideal is nil *if it consists of nilpotent elements.*

Theorem II.4.15 ($*$-algebra structure theorem). *Let A be a $*$-algebra with Jacobson radical* $\mathrm{rad}\, A$. *Then*

(i) $\mathrm{rad}\, A$ *is a nil $*$-ideal,*

(ii) $A/\mathrm{rad}\, A$ *is $*$-semi-simple, and*

(iii) if A is $*$-simple then $A \cong \mathrm{Adj}(d)$ for a non-degenerate Hermitian C-form d.

Proof. (*i*) Since $*$ is an anti-automorphism of A, every left quasi-regular element is mapped to a right quasi-regular element. Thus $(\mathrm{rad}\, A)^* \subseteq \mathrm{rad}\, A$. Since A is finite dimensional, the Jacobson radical is nilpotent.

(*ii*) We induce $*$ on $A/\mathrm{rad}\, A$, so that $A/\mathrm{rad}\, A$ is a $*$-algebra which is product of uniquely determined minimal ideals. If I is a minimal ideal of $A/\mathrm{rad}\, A$ then either $I^* = I$ or $I \cap I^* = 0$ so that $\langle I, I^* \rangle = I \oplus I^*$ is a minimal $*$-closed ideal. Thus $A/\mathrm{rad}\, A$ is a product of simple $*$-algebras.

For (*iii*) see Section II.4.2. □

II.4.4 Isometry Groups are Unipotent-by-classical

We describe the structure of the isometry group of a Hermitian bilinear map. To do this we invoke the following generalization of the Wedderburn Principal Theorem for finite dimensional $*$-algebras over fields not of characteristic 2 (cf. [37]).

Theorem II.4.16. *[54, Theorem 1] Given a finite dimensional $*$-algebra A over a separable field k, there is a subalagebra B of A such that $B^* = B$, $A = B \oplus \operatorname{rad} A$ as a k-vector space, and $B \cong A/\operatorname{rad} A$.*

Recall that the *p-core* of a finite group G, denoted $O_p(G)$, is the largest normal p-subgroup of G.

Theorem II.4.17. *If* $\operatorname{Adj}(b)/\operatorname{rad}\operatorname{Adj}(b) \cong \operatorname{Adj}(d_1) \oplus \cdots \oplus \operatorname{Adj}(d_s)$ *where d_i is a non-degenerate Hermitian C_i-form, for some associative composition algebra C_i, for each $1 \leq i \leq s$, then*

$$\operatorname{Isom}(b) \cong (\operatorname{Isom}(d_1) \times \cdots \times \operatorname{Isom}(d_s)) \ltimes O_p(\operatorname{Isom}(b)),$$

where p is the characteristic of $\operatorname{Adj}(b)$.

Proof. Let $A := \operatorname{Adj}(b)$. By Theorem II.4.16 we have $A = B \oplus \operatorname{rad} A$ where the projection map $\pi : A \to B$ is a surjective $*$-homomorphism with kernel $\operatorname{rad} A$. Now set $G = \{\varphi \in B : \varphi\varphi^* = 1\}$ and $N = \{\varphi \in A : \varphi\varphi^* = 1, \varphi - 1 \in \operatorname{rad} A\}$. If $\varphi = 1 + z, \tau = 1 + z' \in N$, $z, z' \in \operatorname{rad} A$, then $\varphi\tau - 1 = z + z' + zz' \in \operatorname{rad} A$ so that $\varphi\tau \in N$. Hence, G and N are subgroups of $\operatorname{Isom}(b)$ and $G \cap N = 1$. As π is a $*$-homomorphism, $(\varphi\pi)(\varphi\pi)^* = (\varphi\varphi^*)\pi = 1$ for all $\varphi \in \operatorname{Isom}(b) \subset A$ (Proposition II.4.3.(*ii*)). Hence, $\operatorname{Isom}(b)\pi = G$. Finally, the kernel of π restricted to $\operatorname{Isom}(b)$ is N. Thus $\operatorname{Isom}(b) = G \ltimes N$. Since $B \cong A/\operatorname{rad} A \cong \operatorname{Adj}(d_1) \oplus \cdots \oplus \operatorname{Adj}(d_s)$ it follows that $G \cong \operatorname{Isom}(d_1) \times \cdots \times \operatorname{Isom}(d_s)$ (Proposition II.4.3.(*ii*)). By Proposition II.4.13, $O_p(G) = 1$. Thus, $O_p(\operatorname{Isom}(b)) = N$. □

II.4.5 The Jordan Algebra $\operatorname{Sym}(b)$ *of Self-adjoint Operators*

At last we introduce the Jordan algebras associated to our bilinear maps (and thus to our p-groups as well).

Definition II.4.18. *For a k-bilinear map $b : V \times V \to W$, define*

$$\mathrm{Sym}(b) := \{f \in \mathrm{End}\, V : b(uf, v) = b(u, vf), \forall u, v \in V\}$$

(The notation $\mathrm{Sym}(b)$ has no relationship to symmetric groups.) This is an instance of a broader class of objects (see Theorem II.4.20):

Definition II.4.19. *Given a $*$-algebra A, the* special Hermitian Jordan algebra *of A is the set*

$$\mathfrak{H}(A, *) = \{a \in A : a = a^*\}$$

equipped with the special Jordan product $x \bullet y = \frac{1}{2}(xy + yx)$ [25, pp. 12-13].

Special Hermitian Jordan algebras are part of the family of unital Jordan algebras, which are algebras J with a binary product $\bullet$ such that:

(i) $x \bullet y = y \bullet x$,

(ii) $x^{\bullet 2} \bullet (y \bullet x) = (x^{\bullet 2} \bullet y) \bullet x$ where $x^{\bullet 2} = x \bullet x$, and

(iii) $x \bullet 1 = 1 \bullet x = x$

for all $x, y \in J$ [25, Definition I.2]. *Unless stated otherwise, our use of Jordan algebras is restricted to finite special Hermitian Jordan algebras.* As we deal only with odd characteristic, the definitions we provide for ideals, powers, and related properties are in terms of the classical $x \bullet y$ product rather than the quadratic Jordan definitions. This said, we still have many uses for the *quadratic Jordan product* which in a special Hermitian Jordan algebra $J := \mathfrak{H}(A, *)$ is simply:

$$yU_x := xyx \in J, \qquad x, y \in J. \tag{II.13}$$

Evidently the Jordan product $\bullet$ need not be associative. However, we always have $x^i \bullet x^j = \frac{1}{2}(x^{i+j} + x^{j+i}) = x^{i+j}$, $i, j \in \mathbb{N}$ (cf. [25, p. 5]). As $J = \mathfrak{H}(A, *)$ and $1^* = 1$, the identity of J is the identity of A. Furthermore, if $x \in J$ is invertible in A then $(x^{-1})^* = (x^*)^{-1} = x^{-1}$ proving that $x^{-1} \in J$. Hence we omit the $\bullet$ notation in the exponents of our Jordan algebra products.

From our discussion thus far we have:

Theorem II.4.20. *For every non-degenerate Hermitian bilinear map b,* $\mathrm{Sym}(b)$ *is the special Hermitian Jordan algebra* $\mathfrak{H}(\mathrm{Adj}(b))$. *Furthermore,* $\mathrm{Isom}^*(b)$ *acts on* $\mathrm{Sym}(b)$ *as in Proposition II.4.3.*

Proof. This follows directly from the definitions. □

Definition II.4.21. *[27, 4.1-4.2] Let J be a Jordan algebra.*

(i) A subspace I of J is an ideal *if $I \bullet J \subseteq I$. Then, in the usual way, J/I becomes a Jordan algebra.*

(ii) A nil *ideal is an ideal that consists of nilpotent elements.*

(iii) A subspace I is an inner *ideal if $JU_I = \{aU_b : a \in J, b \in I\} \subseteq I$.*

(iv) The radical, *denoted* $\mathrm{rad}\, J$, *is the intersection of all maximal inner ideals [27, 4.4.10].*

(v) J is simple *if it has exactly two ideals, and* semi-simple *if it is a direct product of simple Jordan algebras.*

In Jordan algebras, the inner ideals often play the rôle that left/right ideals play for associative algebras. Every ideal of a Jordan algebra is also an inner ideal. As $J = \mathfrak{H}(A, *)$ (cf. Definition II.4.19) each ideal I of A determines an ideal $I \cap J$ of J. Likewise, if I is a left or right ideal of A then $I \cap J$ is an inner ideal. For further details see [27, 4.1-4.2].

We can account for all the special simple Hermitian Jordan algebras (also called *special Jordan matrix algebras*) in much the same way as we have describe the simple $*$-algebras.

Definition II.4.22. *[25, III.2] Let C be a finite associative composition algebra over a field K and $D = \mathrm{Diag}[\omega_1, \ldots, \omega_n]$ a matrix in $M_n(C)$ with entries in $K^\times$. Then the* special Jordan matrix algebra *with respect to D is*

$$\mathfrak{H}(D) = \{X \in M_n(C) : X = D\bar{X}^t D^{-1}\}$$

whose product is $X \bullet Y = \frac{1}{2}(XY + YX)$ and where $XU_Y = YXY$ for $X, Y \in \mathfrak{H}(D)$.

Following Section II.4.2 we know $d(u, v) := uD\bar{v}^t$, $u, v \in C^n$, determines a non-degenerate Hermitian C-form and

$$\mathfrak{H}(D) = \mathfrak{H}(\mathrm{Adj}(d)) = \mathrm{Sym}(d). \tag{II.14}$$

By [25, p.178-179], $\mathfrak{H}(D)$ is a special simple Hermitian Jordan algebra (though typically the case of $C = K \oplus K$ is not specified in this manner).

Theorem II.4.23 (Hermitian Jordan algebra structure theorem). *Let A be a finite $*$-algebra with Jacobson radical* $\operatorname{rad} A$, *and let* $J = \mathfrak{H}(A, *)$.

(i) $\operatorname{rad} J = J \cap \operatorname{rad} A$ *and is a nil ideal of* J,

(ii) $J/\operatorname{rad} J$ *is a semi-simple Jordan algebra,*

(iii) every special simple Hermitian Jordan algebra is isomorphic to $\operatorname{Sym}(d)$ *for some non-degenerate Hermitian C-form d.*

(iv) for every $I \in \operatorname{spec}_0 A$, $J \cap I$ *is a maximal ideal of* J.

Proof. (iii). This follows from [25, pp.178-179, Second Structure Theorem].

(ii). This follows from (iii) and Theorem II.4.15.(ii), $J/(J \cap \operatorname{rad} A) = \mathfrak{H}(A/\operatorname{rad} A, *)$ is semi-simple.

(i). By [25, p.161, First Structure Theorem] (interpreted in radical vocabulary in [27, 4.2.7,4.2.15]), $\operatorname{rad}(J/\operatorname{rad} J) = 0$ and also $\operatorname{rad} J = 0$ if, and only if, J is semi-simple. Thus, by (iii), it follows that $J \cap \operatorname{rad} A = \operatorname{rad} J$. By Theorem II.4.15.$(i)$, $\operatorname{rad} A$ is a nil ideal, and so $\operatorname{rad} J = J \cap \operatorname{rad} A$ is also a nil ideal.

(iv). This is immediate from (iii) and Theorem II.4.15.(iii). □

II.4.6 Decompositions, Idempotents, and Frames: $\mathcal{E}(\mathcal{X})$

We show how idempotents of $\operatorname{Sym}(b)$ parameterize $\perp$-decompositions of a Hermitian k-bilinear map $b : V \times V \to W$. We start with the elementary

Lemma II.4.24. *If* $f \in \operatorname{Sym}(b)$ *then* $b(\operatorname{im} f, \ker f) = 0$.

Proof. Let $u \in V$ and $v \in \ker f$. Then $b(uf, v) = b(u, vf) = 0$. □

By standard linear algebra, an idempotent e in $\operatorname{End} V$ decomposes V as $\operatorname{im} e \oplus \ker e$. In light of Lemma II.4.24, if $e \in \operatorname{Sym}(b)$ then $b(\operatorname{im} e, \ker e) = 0$, so we arrive at a $\perp$-decomposition $\{\ker f, \operatorname{im} f\}$.

Definition II.4.25. *[25, pp.117-118] Let J be a Jordan algebra.*

(i) An idempotent *is an element e in J such that $e^2 = e$. It is* proper *if it is neither* 0 *nor* 1.

(ii) The Peirce-1-space of an idempotent e is the subspace JU_e. The Peirce-0-space is JU_{1-e}. These are Jordan algebras (in fact inner ideals) with identity e and $1 - e$, respectively (cf. Proposition II.4.26).

Proposition II.4.26. *Let $e \in \operatorname{End} V$ with $e^2 = e$, $E := Ve$ and $F := V(1 - e)$.*

(i) $e \in \operatorname{Sym}(b)$ if, and only if, $b(E, F) = 0$.

(ii) If $e \in \operatorname{Sym}(b)$ then $\operatorname{Sym}(b)U_e$ is isomorphic as a Jordan algebra to $\operatorname{Sym}(b_E)$ via the restriction of $f \in \operatorname{Sym}(b)U_e$ to $(fU_e)|_E : E \to E$.

Proof. (i) Lemma II.4.24 proves the forward direction. For the converse, since $b(E, F) = 0$ it follows that $b(ue, v(1 - e)) = 0 = b(u(1 - e), ve)$ for all $u, v \in V$. Hence

$$b(ue, v) = b(ue, ve + v(1 - e)) = b(ue, ve) = b(ue + u(1 - e), ve) = b(u, ve),$$

for all $u, v \in V$; thus, $e \in \operatorname{Sym}(b)$.

For (ii), note that $\operatorname{Sym}(b)U_e \subseteq e \operatorname{Adj}(b) e$ and so $\operatorname{Sym}(b)U_e$ is faithfully represented in $\operatorname{End} E$ by restriction. Furthermore, $b(uexe, v) = b(u, vexe)$ for all $u, v \in E$ and $x \in \operatorname{Sym}(b)$. Thus the restriction of $\operatorname{Sym}(b)U_e$ is $\operatorname{Sym}(b_E)$. □

From Proposition II.4.26.(i) we see that $F = E^\perp$ (cf. Definition II.2.11.(ii)).

Definition II.4.27. *[25, pp.117-118] Let J be a Jordan algebra.*

(i) Two idempotents e, f in J are orthogonal *if $e \bullet f = fU_e = eU_f = 0$ [27, 5.1].*

(ii) An idempotent is primitive *if it is not the sum of two proper orthogonal idempotents.*

(iii) A set of idempotents is supplementary *if the idempotents are pairwise orthogonal and sum to* 1.

(iv) A frame *$\mathcal{E}$ of J is a set of primitive pairwise orthogonal idempotents which sum to* 1.

Idempotents in special Jordan algebras are idempotents in the associative algebra as well. If $e, f \in \operatorname{Sym}(b)$ then e and f are orthogonal idempotents in $\operatorname{Sym}(b)$ if, and only if, they are

orthogonal in Adj(b). To see this, if $0 = e \bullet f = \frac{1}{2}(ef + fe)$ and $efe = fU_e = 0$ then $ef = ef + efe = e(ef + fe) = 0$ and also $fe = 0$. If $ef = 0 = fe$ then $e \bullet f = \frac{1}{2}(ef + fe) = 0$ (cf. [27, p. 5.4]). However, if e is a primitive idempotent in Sym(b) it need not follow that e is primitive in Adj(b) since there may be orthogonal idempotents in Adj(b) which sum to e but do not lie in Sym(b).

The following definition is based on standard uses of idempotents in linear algebra.

Definition II.4.28. *Let V be a vector space over k.*

(i) Let $\mathcal{E}(\mathcal{Y})$ be the set of supplementary idempotents parameterizing a $\oplus$-decomposition $\mathcal{Y}$ of V.

(ii) Let $\mathcal{X}(\mathcal{F})$ be the $\oplus$-decomposition arising from a set of supplementary idempotents $\mathcal{F}$ of End V.

Theorem II.4.29. *Let $\mathcal{X}$ be a $\oplus$-decomposition of V and let $\mathcal{E} = \mathcal{E}(\mathcal{X})$.*

(i) $\mathcal{E}(\mathcal{X}) \subseteq$ Sym(b) if, and only if, $\mathcal{X}$ is a $\perp$-decomposition of b.

(ii) $\mathcal{X}$ is a fully refined $\perp$-decomposition if, and only if, $\mathcal{E}$ is a frame.

(iii) Let $\mathcal{X}$ be a $\perp$-decomposition. If $(\alpha, \hat{\alpha}) \in$ Isom$^*(b)$, then $\mathcal{X}\alpha = \mathcal{X}(\mathcal{E}^{(\alpha,\hat{\alpha})})$ and $\mathcal{E}^{(\alpha,\hat{\alpha})} = \mathcal{E}(\mathcal{X}\alpha)$. In particular, Isom$^*(b)$ *acts on the set of all frames of* Sym(b).

Proof. Part (i) follows from Proposition II.4.26. Part (ii) follows from observing that an idempotent $e \in$ Sym(b) is primitive if, and only if, b_{Ve} is $\perp$-indecomposable.

For part (iii), if $e \in \mathcal{E}$ and $x \in Ve\alpha$, then $x(e^{(\alpha,\hat{\alpha})}) = ((x\alpha^{-1})e)\alpha = x\alpha^{-1}\alpha = x$. Therefore $V(e^{(\alpha,\hat{\alpha})}) = Ve\alpha$. □

II.4.7 Linking Central Decompositions, $\perp$-Decompositions, Frames, and Orthogonal Bases: $\mathcal{H}_I$, $\mathcal{X}_I$, $\mathcal{E}_I$, and $\mathcal{X}_{d(I)}$.

We use the following notation repeatedly as a means to track the changes from p-groups, to bilinear maps, to $*$-algebras, to Hermitian forms, and then back. As usual, we assume that P has class 2, exponent p, and $P' = Z(P)$.

Let $\mathcal{H}$ be a fully refined central decomposition of P, $\mathcal{X}$ a fully refined $\perp$-decomposition of

$b := \mathsf{Bi}(P)$, $\mathcal{E}$ a frame of $J := \mathrm{Sym}(b)$, $A := \mathrm{Adj}(b)$, and $I \in \mathrm{spec}_0 A$. Define:

$$\mathcal{E}_I = \{e \in \mathcal{E} : e \notin I\}, \tag{II.15}$$

$$\mathcal{X}_I = \{X \in \mathcal{X} : e \in \mathcal{E}(\mathcal{X})_I, X = Ve\}, \tag{II.16}$$

$$\mathcal{H}_I = \{H \in \mathcal{H} : HP'/P' \in \mathsf{Bi}(\mathcal{H})_I\}. \tag{II.17}$$

Since $A/I \cong \mathrm{Adj}(d(I))$ for some non-degenerate Hermitian C-form $d := d(I)$, (Theorem II.4.15.(iii))), it follows that $J/(I \cap J) \cong \mathrm{Sym}(d)$. Hence, $I \cap J$ is a maximal ideal of J (Theorem II.4.23.(iii)). Therefore, $\mathcal{E}_I$ parameterizes a frame

$$\mathcal{E}_{J/(I\cap J)} := \{(I \cap J) + e : e \in \mathcal{E}_I\} \tag{II.18}$$

of $J/(I \cap J)$. Furthermore, this gives rise to a fully refined $\perp$-decomposition

$$\mathcal{X}_{d(I)} := \{Ue\tau : e \in \mathcal{E}_I\} \tag{II.19}$$

of $d(I)$ where $\tau : A/I \to \mathrm{Adj}(d(I))$ is a $*$-isomorphism. Certainly, $\mathcal{X}_{d(I)}$ depends on the choice of τ but we consider τ fixed. This influences the definition of address in Section II.5.1.

Proposition II.4.30. *Let $\mathcal{H}$ be a fully refined central decomposition of P, $\mathcal{X} := \mathsf{Bi}(\mathcal{H})$, and $\mathcal{E} := \mathcal{E}(\mathcal{X})$. The sets $\mathcal{H}_I$, $\mathcal{X}_I$, $\mathcal{E}_I$, $\mathcal{E}_{J/(I\cap J)}$, and $\mathcal{X}_{d(I)}$ are in bijection.*

Proof. This follows from Theorem II.3.6.(ii), Theorem II.4.29.(ii), Theorem II.4.23.(iii), and Proposition II.4.11. □

Proposition II.4.31. *For every fully refined central decomposition $\mathcal{H}$ of P with $P' = Z(P)$, the set $\{\mathcal{H}_I : I \in \mathrm{spec}_0 \mathrm{Adj}(\mathsf{Bi}(P))\}$ partitions $\mathcal{H}$. Furthermore, $|\mathcal{H}_I|$ depends only on P and $I \in \mathrm{spec}_0 \mathrm{Adj}(\mathsf{Bi}(P))$.*

Proof. By Proposition II.4.30 we know $\mathcal{H}_I$ is in bijection with $\mathcal{E}_I$ for each maximal $*$-ideal of $\mathrm{Adj}(\mathsf{Bi}(P))$. As $\mathcal{E}$ is partitioned by $\mathcal{E}_I$, as I ranges over the maximal $*$-ideals of $\mathrm{Adj}(\mathsf{Bi}(P))$, it follows that $\{\mathcal{H}_I : I \in \mathrm{spec}_0 \mathrm{Adj}(\mathsf{Bi}(P))\}$ partition $\mathcal{H}$. □

II.4.8 All Fully Refined Central Decompositions Have the Same Size

We now prove the first part of Theorem II.1.1.(i) – that fully refined central decompositions of a p-group P of exponent p and class 2 have the same size.

Theorem II.4.32. *Let P be a finite p-group of class 2 and exponent p and $\mathcal{H}$ a fully refined central decomposition. Let $Q := \langle \mathcal{K} \rangle$, $\mathcal{K} := \mathcal{H} - Z(\mathcal{H})$. Then $\mathcal{H}$ is partitioned into*

$$Z(\mathcal{H}) \sqcup \{\mathcal{K}_I : I \in \operatorname{spec}_0 \operatorname{Adj}(\operatorname{Bi}(Q))\}. \tag{II.20}$$

Furthermore, $|Z(\mathcal{H})|$ and $|\mathcal{K}|$ are uniquly determined by P, and $|\mathcal{H}|$ is uniquely determined by P.

Proof. By Lemma II.2.3 we know $P = Q \oplus A$ with $A \leq Z(P)$ and $Q' = P' = Z(Q)$. Furthermore, $|Z(\mathcal{H})| = |A| = [Z(P) : P']$. Therefore, Lemma II.2.5 and Proposition II.4.31 complete the proof. □

II.4.9 The Five Classical Indecomposable Families

By Theorem II.4.29, a bilinear map b has no proper $\perp$-decompositions if, and only if, 0 and 1 are the only idempotents of $\operatorname{Sym}(b)$. But more can be said if $\operatorname{Adj}(b)$ is considered as well:

Lemma II.4.33 (Fitting's Lemma for bilinear maps)**.** *If b is $\perp$-indecomposable then, for every $x \in \operatorname{Adj}(b)$, $T(x) = x + x^*$ is either invertible or nilpotent. In particular, every $x \in \operatorname{Sym}(b)$ is either invertible or nilpotent.*

Proof. Set $y = x + x^*$ and note $y^r \in \operatorname{Sym}(b)$ for all $r \in \mathbb{N}$. By Fitting's lemma there is some $r > 0$ such that $V = \operatorname{im} y^r \oplus \ker y^r$. By Lemma II.4.24, $b(\operatorname{im} y^r, \ker y^r) = 0$. So we have a $\perp$-decomposition of b. Since b is $\perp$-indecomposable, $y^r = 0$ so that y is nilpotent, or $\ker y^r = 0$ and $\operatorname{im} y^r = V$ so that y is invertible. □

Theorem II.4.34. *[47, Theorem 2] If $(A, *)$ is a $*$-algebra over a finite field of odd characteristic such that $T(x)$ is either invertible or nilpotent for each $x \in A$, then $A/\operatorname{rad} A$ is an associative composition algebra.*

Corollary II.4.35. *For a k-bilinear map b the following are equivalent:*

(i) b is $\perp$-indecomposable,

(ii) $\mathrm{Sym}(b)$ *has only trivial idempotents,*

(iii) $J/\operatorname{rad} J$ *is isomorphic to a field extension of* k*.*

(iv) $A = \mathrm{Adj}(b)$ *has* $A/\operatorname{rad} A$ *is isomorphic to an associative composition algebra.*

Theorem II.4.36. *A p-group* P *of class 2 and exponent* p *is centrally indecomposable if, and only if, one of the following holds with* $G := C_{\mathrm{Aut}\,P}(Z(P))/O_p(C_{\mathrm{Aut}\,P}(Z(P)))$*:*

Abelian $|P| = p$*,*

Orthogonal $G \cong O(1,p^e) \cong \mathbb{Z}_2$ *with* $p \neq 3$*, or* $p = 3$ *and*
$C_{\mathrm{Aut}\,P\circ P}(P')/O_p(C_{\mathrm{Aut}\,P\circ P}(P')) \cong \mathrm{GO}^{\pm}(2,3^e)$*;*

Unitary $G \cong U(1,p^e) \cong \mathbb{Z}_{p^e+1}$*,*

Exchange $|P| \neq p$ *and* $G \cong \mathrm{GL}(1,p^e) \cong \mathbb{Z}_{p^e-1}$*, or*

Symplectic $G \cong \mathrm{Sp}(2,p^e) \cong \mathrm{SL}(2,p^e)$*;*

for some $e > 0$*.*

Proof. This follows from Corollary II.4.35, Theorem II.4.17 and Theorem II.3.6. □

In Section II.7 we demonstrate that with the possible exception of the unitary type, each of these types can occur.

II.5 Isometry Orbits of $\perp$-decompositions

In this section we describe the orbits of $C_{\mathrm{Aut}\,P}(P')$ in its action on the set of fully refined central decompositions. To do this, we define a computable $C_{\mathrm{Aut}\,P}(P')$-invariant for each fully refined central decomposition called its *address*. Then we prove that any two fully refined central decompositions with the same address lie in the same orbit.

II.5.1 Addresses

Definition II.5.1. *Let* $d : V \times V \to C$ *be a non-degenerate Hermitian* C*-form.*

(i) Given a non-singular $x \in V$ (cf. Definition II.4.10), the address *of $X := Cx$ is*

$$X@ := d(x,x)N(C^\times),$$

as an element of $K^\times/N(C^\times)$.

(ii) $\mathcal{X}@ := \{X@ : X \in \mathcal{X}\}$ (as a multiset indexed by $\mathcal{X}$) for every fully refined $\perp$-decomposition $\mathcal{X}$ of d.

From Theorem II.4.7 we know $N(C) = K$ if $C > K$ and therefore the addresses of non-singular points of a non-symmetric non-degenerate Hermitian C-form are all equal to $K^\times$. Therefore we ignore this case. However, for non-degenerate symmetric bilinear forms, the address is a coset of $(K^\times)^2$.

Let $d : V \times V \to K$ be a non-degenerate symmetric bilinear form.

Fix $\omega \in K^\times - (K^\times)^2$. Every address of a non-singular point of V is either $[1] := (K^\times)^2$ or $[\omega] := \omega(K^\times)^2$. If $\mathcal{X}$ is an orthogonal basis of d, then for some $0 \le s \le n$,

$$\mathcal{X}@ = \{\overbrace{[1],\dots,[1]}^{n-s},\overbrace{[\omega],\dots,[\omega]}^{s}\}, \qquad n = \dim V.$$

We write $(n-s : s)$ for the address $\mathcal{X}@$.

The discriminant of Hermitian C-form d is

$$\operatorname{disc} d = \prod_{X \in \mathcal{X}} X@ \tag{II.21}$$

as an element of $K^\times/N(C^\times)$ (cf. (II.8)). In particular, if d is symmetric then $\operatorname{disc} d = [\omega^s]$. Otherwise we can regard the discriminant as trivial.

Let P be a p-group P of class 2, exponent p, and $P' = Z(P)$. Let $\mathcal{H}$ be a fully refined central decomposition of P, $\mathcal{X} := \mathsf{Bi}(\mathcal{H})$, and $\mathcal{E} := \mathcal{E}(\mathcal{X})$. Using the notation of Section II.4.7 and Proposition II.4.30, for each maximal $*$-ideal I of $\mathsf{Adj}(\mathsf{Bi}(P))$, assign the address of $\mathcal{H}_I$, $\mathcal{X}_I$, $\mathcal{E}_I$,

and $\mathcal{E}_{J/(I\cap J)}$ as the address of $\mathcal{X}_{d(I)}$. Finally,

$$\mathcal{E}@ := \{(I, \mathcal{E}_I@) : I \in \mathrm{spec}_0 \,\mathrm{Adj}(\mathrm{Bi}(P))\}, \tag{II.22}$$

$$\mathcal{X}@ := \{(I, \mathcal{X}_I@) : I \in \mathrm{spec}_0 \,\mathrm{Adj}(\mathrm{Bi}(P))\}, \tag{II.23}$$

$$\mathcal{H}@ := \{(I, \mathcal{H}_I@) : I \in \mathrm{spec}_0 \,\mathrm{Adj}(\mathrm{Bi}(P))\}. \tag{II.24}$$

Remark II.5.2. *Recall that $\mathcal{X}_{d(I)}$ depends on the choice of non-degenerate Hermitian C-form $d := d(I) : U \times U \to C$. Any other choice is pseudo-isometric to d. Suppose that $d' : U' \times U' \to C$ is pseudo-isometric to d via (α, β). Let $u \in U$ such that $d(u,u) \in K^\times$ (cf. Proposition II.4.11). Then*

$$d(u,u)\beta = d(u\alpha, u\alpha) = \overline{d(u\alpha, u\alpha)} = \bar{\beta} d(u,u). \tag{II.25}$$

Hence, $\beta = \bar{\beta}$; thus, $\beta \in K^\times$.

The affect is that $\mathcal{X}_{d'}@\beta = \mathcal{X}_d@$. Therefore the specific cosets in $K^\times/N(C^\times)$ are not significant. The pseudo-isometry invariant of $\mathcal{X}_{d(I)}@$ is the partition into equal cosets. For finite fields, the notation $(n-s:s)$ records this partition.

Proposition II.5.3. *(i) If $\mathcal{X}$ is a fully refined $\perp$-decomposition of b and $\varphi \in \mathrm{Isom}(b)$ then $X@ = X\varphi@$ for all $X \in \mathcal{X}$.*

(ii) If $\mathcal{H}$ is a fully refined central decomposition of P and $\varphi \in C_{\mathrm{Aut}\,P}(P')$ then $H@ = H\varphi@$ for all $H \in \mathcal{H}$.

Proof. (i). Let $I \in \mathrm{spec}_0 \,\mathrm{Adj}(b)$ and $\mathrm{Adj}(b)/I \cong \mathrm{Adj}(d)$, $d := d(I) : U \times U \to C$. By Proposition II.4.3.$(ii)$, $\mathrm{Isom}(b)$ maps into $\mathrm{Isom}(d)$. Let $X \in \mathcal{X}_I$ and Cx, $x \in U$, the corresponding member of $\mathcal{X}_{d(I)}$. The address of X is by definition the address of Cx. As $d(x,x) = d(x\varphi, x\varphi)$ it follows that $Cx\varphi@ = Cx@$ and $X\varphi@ = X@$. (ii). This follows from (i) and Theorem II.3.6. □

We now work towards the converse of Proposition II.5.3.

II.5.2 Orbits of Fully Refined $\perp$-decompositions of Non-degenerate Hermitian C-forms

The theorems of this section are undoubtedly known, though with different terminology.

Lemma II.5.4. *Let $d : V \times V \to C$ be a non-degenerate Hermitian C-form and $\mathcal{X}$ a fully refined*

$\perp$-decompositions of d. Then, for each $\varphi \in \mathrm{Isom}(d)$ there is a $\tau \in \mathrm{Isom}(d)$ which is a product of involutions and such that $X\varphi = X\tau$, for $X \in \mathcal{X}$.

Proof. If the rank of V is 1 then let $\tau = 1$. So assume the rank is greater than 1. By Proposition II.4.13, we have the four classical groups to consider. The orthogonal groups are generated by reflections so take $\tau := \varphi$. In the exchange, unitary, and symplectic cases, the rank of V excludes the case $GF(q)^\times$, $\mathrm{GU}(1,q)$ and $\mathrm{Sp}(2,q)$. Therefore the relevant symplectic groups are generated by their involutions and again $\tau := \varphi$. In the exchange and unitary cases the involutions generate a normal subgroup $N \geq \mathrm{Isom}(d) \cap \mathrm{SL}(V)$. Therefore $\varphi \equiv \mu \pmod{N}$ where μ is a diagonalizable. Without loss of generality, $\mathcal{X}\mu = \mathcal{X}$, so take $\tau := \mu^{-1}\varphi \in N$. □

Theorem II.5.5. *Let $d : V \times V \to C$ be a non-degenerate Hermitian C-form and $\mathcal{X}$ and $\mathcal{Y}$ fully refined $\perp$-decompositions of d. Then there is an isometry φ of d such that $\mathcal{X}\varphi = \mathcal{Y}$ if, and only if, $\mathcal{X}@ = \mathcal{Y}@$. Indeed, if $\phi : \mathcal{X} \to \mathcal{Y}$ is a bijection where $X\phi@ = X@$ for each $X \in \mathcal{X}$, then φ can be taken as a product of involutions where $X\varphi = X\phi$, for each $X \in \mathcal{X}$.*

Proof. Suppose $\mathcal{X}\varphi = \mathcal{Y}$ for some $\varphi \in \mathrm{Isom}(d)$. Given $X \in \mathcal{X}$, $d(x\varphi, x\varphi) = d(x,x)$ for each $x \in X$; hence, $X@$ equals $X\varphi@$. Thus, the addresses of $\mathcal{X}$ and $\mathcal{Y}$ agree.

For the converse, suppose we have a bijection ϕ as described above. Fix generators x and y_x for $X = Cx \in \mathcal{X}$ and $X\phi = Cy_x \in \mathcal{Y}$, respectively. By assumption, there is an $s_x \in C^\times$ such that $d(x,x) = N(s_x)d(y_x, y_x)$.

Define $\varphi : V \to V$ by $x\varphi = s_x y_x$ for each $X = Cx \in \mathcal{X}$. It follows that $d(x\varphi, x\varphi) = N(s_x)d(y_x,y_x) = d(x,x)$ for all $X = Cx \in \mathcal{X}$; thus, $\varphi \in \mathrm{Isom}(d)$. Furthermore, $\mathcal{X}\varphi = \mathcal{Y}$ and $X\varphi = X\phi$. To convert φ into a product of involutions, invoke Lemma II.5.4. □

We also require the following version of transitivity as well.

Theorem II.5.6. *Let $d : V \times V \to C$ be a non-degenerate Hermitian C-form. If $X, Y \in V$ are non-singular points (Definition II.4.10), then $X\varphi = Y$ for some $\varphi \in \mathrm{Isom}(d)$ if, and only if, $X@ = Y@$.*

Proof. If $X\varphi = Y$ then $X@ = Y@$.

For the reverse direction suppose that $X@ = Y@$. Since $X@\operatorname{disc} d_{X^\perp} = \operatorname{disc} d = Y@\operatorname{disc} d_{Y^\perp}$, it follows that $\operatorname{disc} d_{X^\perp} = \operatorname{disc} d_{Y^\perp}$. By (II.7) for the symmetric case and Proposition II.4.11 for all other cases, there are orthogonal bases $\mathcal{X}'$ of $d_{X^\perp}$ and $\mathcal{Y}'$ of $d_{Y^\perp}$ such

that $\mathcal{X}'@ = \{[1], \ldots, [1], [\operatorname{disc} d_{X^\perp}]\}$ and $\mathcal{X}'@ = \{[1], \ldots, [1], [\operatorname{disc} d_{Y^\perp}]\}$. Set $\mathcal{X} = \{X\} \sqcup \mathcal{X}'$ and $\mathcal{Y} := \{Y\} \sqcup \mathcal{Y}'$. Then $\mathcal{X}$ and $\mathcal{Y}$ are fully refined $\perp$-decompositions of d. Furthermore,

$$\mathcal{X}@ = \{X@, [1], \ldots, [1], [\operatorname{disc} d_{X^\perp}]\} = \{Y@, [1], \ldots, [1], [\operatorname{disc} d_{Y^\perp}]\} = \mathcal{Y}@.$$

Therefore, by Theorem II.5.5, there is a $\varphi \in \operatorname{Isom}(d)$ such that $\mathcal{X}\tau = \mathcal{Y}$ and $X\varphi = Y$. □

II.5.3 Orbits of Frames in Jordan Algebras

In this section we determine the orbits of $\operatorname{Isom}(b)$ acting on fully refined $\perp$-decompositions of b, for an arbitrary Hermitian bilinear map $b : V \times V \to W$. To do this we use frames, radicals, and the semi-simple structure of the Jordan algebra $\operatorname{Sym}(b)$. We caution that we make frequent use of results from Sections II.4.5 and II.4.6, at times without specific reference.

Suppose $\mathcal{X}$ is a fully refined $\perp$-decomposition of b. By Theorem II.4.29, $\mathcal{E} := \mathcal{E}(\mathcal{X})$ is a frame of $\operatorname{Sym}(b)$. We also know that $\operatorname{Isom}(b)$ acts on $\operatorname{Sym}(b)$ by conjugation (Theorem II.4.20) and that $\mathcal{E}^\varphi = \mathcal{E}(\mathcal{X}\varphi)$ for each $\varphi \in \operatorname{Isom}(b)$ (Theorem II.4.29). Therefore, it suffices to work with the orbits of frames of $\operatorname{Sym}(b)$ under the action of $\operatorname{Isom}(b)$. To make use of the Jordan algebra we also translate the action of $\operatorname{Isom}(b)$ into Jordan automorphisms of $\operatorname{Sym}(b)$ in the following way.

By Proposition II.4.3.(*ii*), every isometry φ has the defining property $\varphi\varphi^* = 1$. Hence, $\varphi \in \operatorname{Sym}(b) \cap \operatorname{Isom}(b)$ if, and only if, $\varphi^2 = 1$.

Definition II.5.7. *Define* $\operatorname{Inv}(J) = \langle U_x : x \in J, x^2 = 1 \rangle \leq \operatorname{GL}(J)$ *for a special Jordan algebra* J.

We consider only those Jordan algebras J which are subalgebras or quotient algebras of a special Hermitian Jordan algebra such as $\operatorname{Sym}(b)$. Note that if $x \in J$ with $x^2 = 1$ then $yU_x = x^{-1}yx = y^x$ for all $y \in J$. Therefore each element of $\operatorname{Inv}(J)$ acts both as a product of U-operators and as conjugation. So $\operatorname{Inv}(J)$ is a group of automorphisms of J built from elements of J.

Remark II.5.8. *The group* $\operatorname{Inv}(\operatorname{Sym}(b))$ *is not contained in* $\operatorname{Isom}(b)$ *and we are careful to distinguish the action on* $J := \operatorname{Sym}(b)$ *by the two groups as follows: if* $\varphi \in \operatorname{Isom}(b)$ *then write* y^φ *(cf. Proposition II.4.3.(i)), and if* $\varphi \in \operatorname{Inv}(J)$ *then use the usual function notation* $y\varphi$, *for* $y \in J$. *However,* $\operatorname{Inv}(\operatorname{Sym}(b))$ *embeds in* $\operatorname{Isom}(b)$ *by extending* $U_x \mapsto x$, $x \in \operatorname{Sym}(b)$, $x^2 = 1$.

By Definition II.4.25, if $e \in J$, $e^2 = e$ then $JU_e = eJe$ is a subalgebra with identity e.

Proposition II.5.9. *Let e be an idempotent in J. Then* $\mathrm{Inv}(JU_e)$ *embeds in* $\mathrm{Inv}(J)$ *acting as the identity on* JU_{1-e}.

Proof. It suffices to extend the generators of $\mathrm{Inv}(JU_e)$ to J. Let $v \in JU_e$ with $v^2 = e$. Set $u := (1-e)+v \in J$. As $v = vU_e = eve$ it follows that $u^2 = (1-e)^2+(1-e)eve+eve(1-e)+v^2 = 1$, so $U_u \in \mathrm{Inv}(J)$. Furthermore, if $x \in JU_e$, then $xU_u = xU_eU_u = ((1-e)+v)exe((1-e)+v) = xU_v$. Finally, if $x \in JU_{1-e}$, then $xU_u = xU_{1-e}U_u = ((1-e)+v)(1-e)x(1-e)((1-e)+v) = x$. □

Lemma II.5.10. *[25, III.7,Lemma 4] Let N be a nil ideal in J. If $N+u \in J/N$ with $u^2-1 \in N$, then there is a $v \in J$ such that $N+u = N+v$ and $v^2 = 1$.*

Proposition II.5.11. *(i) If $\varphi \in \mathrm{Inv}(J)$ then $(\mathrm{rad}\, J)\varphi = \mathrm{rad}\, J$ and $\varphi|_{J/\mathrm{rad}\, J} \in \mathrm{Inv}(J/\mathrm{rad}\, J)$.*

(ii) Suppose $N \trianglelefteq J$ and N is nil (in particular for $N \subseteq \mathrm{rad}\, J$). Then for each $\hat{\varphi} \in \mathrm{Inv}(J/N)$ there is a $\varphi \in \mathrm{Inv}(J)$ such that $\varphi|_{J/N} = \hat{\varphi}$.

Proof. (i) $\mathrm{Inv}(J)$ is a subgroup of the automorphism group of J and so maximal inner ideals are mapped to maximal inner ideals and the radical is preserved. Since involutions of J are sent to involutions of $J/\mathrm{rad}\, J$, it follows that $\mathrm{Inv}(J)|_{J/\mathrm{rad}\, J} \leq \mathrm{Inv}(J/\mathrm{rad}\, J)$.

(ii) By definition $\mathrm{Inv}(J/N)$ is generated by the $U_{\hat{v}}$ for which $\hat{v}$ is an involution of J/N. For each $\hat{v}$, by Lemma II.5.10 there is an involution $v \in J$ such that $\hat{v} = v+N$. Thus $U_{\hat{v}} = U_{v+N} = (U_v)|_{J/N}$, $U_v \in \mathrm{Inv}(J)$. □

Lemma II.5.12. *Let $e, e' \in J$ be orthogonal idempotents. If $z \in J$ such that $z^2 = 0$ and $e+z$ is an idempotent, then there is a $v \in J$ such that (i) $v^2 = 1$, (ii) $eU_v = e+z$ and (iii) $e'U_v = e' - 2e' \bullet z + e'U_z$.*

Proof. Let $v = 1-2e-z$.

(i). Since $e+z = (e+z)^2 = e+ez+ze$ it follows that $z = ez+ze$. Hence, $v^2 = 1-4e+4e^2-2z+2ez+2ze+z^2 = 1$. For *(ii)* note that $0 = z^2 = ez^2+zez$ so that $zez = 0$. Thus,

$$\begin{aligned}(1-2e-z)e(1-2e-z) &= ((1-2e-z)e)(e(1-2e-z)) \\ &= (e+ze)(e+ez) = e+ez+ze = e+z.\end{aligned}$$

So $eU_v = e + z$. Finally for (iii):

$$e'U_v = (1 - 2e - z)e'(1 - 2e - z) = (e' - ze')(e' - e'z) = e' - 2e' \bullet z + e'U_z.$$

□

Lemma II.5.13. *Let N be an ideal in J such that $N^2 = 0$. If $\mathcal{E}$ and $\mathcal{F}$ are both sets of supplementary idempotents of J such that $\mathcal{E} \equiv \mathcal{F} \pmod{N}$, then there is $\varphi \in \mathrm{Inv}(J)$ such that $\mathcal{E}\varphi = \mathcal{F}$.*

Proof. Take $e \in \mathcal{E} - \mathcal{F}$ and $f = e + z \in \mathcal{F}$, $z \in N$ so that $z^2 = 0$. By Lemma II.5.12.(i,ii), there is an involution $v \in J$ such that $eU_v = e + z = f$. Hence, $\mathcal{E}' := \mathcal{E}U_v$ is a supplementary set of idempotents of J. By Lemma II.5.12(iii), $\mathcal{E}' \equiv \mathcal{E} \pmod{N}$ so that $\mathcal{E}' \equiv \mathcal{F} \pmod{N}$. Also, $f \in \mathcal{E}' \cap \mathcal{F}$.

We now induct on the size of $\mathcal{E}$. In the base case $\mathcal{E} = \{e\}$ and $\mathcal{F} = \{f\}$, so $\mathcal{E}U_v = \mathcal{E}' = \mathcal{F}$. Otherwise, as $\mathcal{E}'$ is a set of supplementary idempotents, for all $e' \in \mathcal{E}' - \{f\}$, $e'U_{1-f} = e'$ so $\mathcal{E}' - \{f\} = \mathcal{E}'U_{1-f} - \{0\}$ and similarly $\mathcal{F} - \{f\} = \mathcal{F}U_{1-f} - \{0\}$. So $\mathcal{E}' - \{f\}$ and $\mathcal{F} - \{f\}$ are both sets of supplementary idempotents in JU_{1-f}, where $\mathcal{E}' - \{f\} \equiv \mathcal{F} - \{f\} \pmod{NU_{1-f}}$. By induction there is a $\tau' \in \mathrm{Inv}(JU_{1-f})$ such that $(\mathcal{E}' - \{f\})\tau' = \mathcal{F} - \{f\}$. By Proposition II.5.9 there is a $\tau \in \mathrm{Inv}(J)$ extending τ' to J so that τ is the identity on JU_f. So $\mathcal{E}'\tau = \mathcal{F}$. Thus $U_v\tau \in \mathrm{Inv}(J)$ with $\mathcal{E}U_v\tau = \mathcal{F}$. □

Proposition II.5.14. *Two sets of supplementary idempotents of J are equivalent under the action of $\mathrm{Inv}(J)$ if, and only if, their images in $J/\operatorname{rad} J$ are equivalent under the action of $\mathrm{Inv}(J/\operatorname{rad} J)$.*

Proof. The forward direction follows from Proposition II.5.11.(*i*). For the converse, let $\mathcal{E}$ and $\mathcal{F}$ be sets of supplementary idempotents of J such that $\mathcal{E}\bar{\varphi} \equiv \mathcal{F} \pmod{\operatorname{rad} J}$ for some $\bar{\varphi} \in \mathrm{Inv}(J/\operatorname{rad} J)$. By Proposition II.5.11.(*ii*) we can replace $\bar{\varphi}$ with some $\varphi \in \mathrm{Inv}(J)$.

We will induct on the dimension of $\operatorname{rad} J$. In the base case $\operatorname{rad} J = 0$ and the result is clear. Now suppose $N := \operatorname{rad} J > 0$. By [25, Lemma V.2.2] there is an ideal M of J such that $N^2 \subseteq M \subset N$. Then $\mathcal{E}\varphi \equiv \mathcal{F} \pmod{N/M}$ in J/M and $(N/M)^2 = 0$, so by Lemma II.5.13 there is a $\tilde{\mu} \in \mathrm{Inv}(J/M)$ such that $\mathcal{E}\varphi\tilde{\mu} \equiv \mathcal{F} \pmod{M}$. By Proposition II.5.11.(*ii*), $\tilde{\mu}$ lifts to some $\mu \in \mathrm{Inv}(J)$ such that $\mathcal{E}\varphi\mu \equiv \mathcal{F} \pmod{M}$. As M is a nil ideal properly contained in N, using M in the rôle of N and inducting we find a $\tau \in \mathrm{Inv}(J)$ such that $\mathcal{E}\varphi\mu\tau = \mathcal{F}$. □

Theorem II.5.15. $\mathrm{Inv}(J)$ *is transitive on the set of frames of* $\mathrm{Sym}(b)$ *which have any given address.*

Proof. By Proposition II.5.14 we may assume $\operatorname{rad} J = 0$. By Theorem II.4.23.(ii, iii), J is the direct product of a uniquely determined set $\mathcal{M}$ of simple Jordan matrix algebras. If e is a primitive idempotent of J then eJe is a minimal inner ideal of J (cf. [25, Theorem 1.III]), and so e lies in a minimal ideal of J, thus in a unique simple direct factor of J. Hence, if $\mathcal{E}$ is a frame of J then $M \cap \mathcal{E}$ is a frame of M, for each $M \in \mathcal{M}$. Furthermore, $\mathrm{Inv}(J)$ restricts to $\mathrm{Inv}(M)$ for each $M \in \mathcal{M}$. Thus Corollary II.5.5 and Remark II.5.8 show that $\mathrm{Inv}(J)$ is transitive on frames with the same address. □

Corollary II.5.16. *(i)* $\mathrm{Isom}(b)$ *acts transitively on the set of fully refined* $\perp$*-decompositions with a given address.*

(ii) If P *is a* p*-group of class* 2*, exponent* p*, and* $P' = Z(P)$*, then* $C_{\mathrm{Aut}\,P}(P')$ *acts transitively on the set of fully refined central decompositions with a given address.*

Proof. (i). This follows from Theorem II.5.15 and Remark II.5.8. (ii). This follows form part (i) and Theorem II.3.6. □

Corollary II.5.17. *Let* $b : V \times V \to W$ *be a non-degenerate Hermitian bilinear map. Suppose that* X *and* Y *are two* $\perp$*-factors of* b*.*

(i) Then there is a $\varphi \in \mathrm{Isom}(b)$ *such that* $X\varphi = Y$ *if, and only if,* $X@ = Y@$ *(which includes* $X \in \mathcal{X}_I$*,* $Y \in \mathcal{Y}_I$ *for the same maximal* $*$*-ideal* I *of* $\mathrm{Adj}(b)$*).*

(ii) b_X *is isometric to* b_Y *if, and only if,* $X@ = Y@$*.*

(iii) Let P *be a* p*-group of class* 2*, exponent* p*, and* $P' = Z(P)$ *with centrally indecomposable subgroups* H *and* K*. Then there is a* $\varphi \in C_{\mathrm{Aut}\,P}(P')$ *such that* $H\varphi = K$ *if, and only if,* $H@ = K@$*.*

Proof. The forward direction of (i) and (ii) are clear. For the reverse, use Theorem II.5.6, Lemma II.5.4, Remark II.5.8, and Proposition II.5.11.(ii) to arrange for $\mathcal{E}(\{X, X^\perp\}) \equiv \mathcal{E}(\{Y, Y^\perp\})$. Then Proposition II.5.14 completes the proof. (iii). This follows from (ii) and Theorem II.3.6. □

II.6 Semi-refinements and Proof of Theorem II.1.1.(i)

By Theorem II.5.16.(i), any two fully refined $\perp$-decompositions with the same address have the same multiset of isometry types. This section is concerned with strengthening this result by involving pseudo-isometries in order to prove Theorem II.1.1.(i).

II.6.1 The Orthogonal Bases of Symmetric Bilinear Forms

Let $d : V \times V \to K$ be a non-degenerate symmetric bilinear form and recall the notation $(n - s : s)$ for addresses, given in Section II.5.1.

Lemma II.6.1. *If $\mathcal{X}$ and $\mathcal{Y}$ are fully refined $\perp$-decompositions of d with $\mathcal{X}@ = (n - s : s)$ and $\mathcal{Y}@ = (n - r : r)$, then $2|s - r$.*

Proof. Recall that the discriminant is independent of the basis of V. Hence, we have $[\omega^s] = \operatorname{disc} d = [\omega^r]$ so that $\omega^{s-r} \equiv 1 \pmod{(K^\times)^2}$ and $2|s - r$. □

Theorem II.6.2. *Let $\mathcal{X}$ be a fully refined $\perp$-decomposition with address $(n - r : r)$. There is an involution $\rho \in \mathrm{Isom}(d)$ where $\mathcal{X}\rho = \mathcal{X}$ and such that, if $S := \{X \in \mathcal{X} : X\rho = X\}$ then*

(i) if $|\mathcal{X}| = 2m + 1$ then $S = \{X\}$ with $X@ = \operatorname{disc} d$,

(ii) if $|\mathcal{X}| = 2m$ and $\operatorname{disc} d = [\omega]$ then $S = \{X, X'\}$ with $X@ = [1]$, $X'@ = [\omega]$,

(iii) if $|\mathcal{X}| = 2m$ and $\operatorname{disc} d = [1]$ then $S = \emptyset$,

(iv) and for each $0 \leq s \leq n$, where $2|r - s$, there is a fully refined $\perp$-decomposition $\mathcal{Y}$ where

(a) $\mathcal{Y}@ = (n - s : s)$,

(b) $\langle X, X\rho\rangle = \langle \mathcal{Y} \cap \langle X, X\rho\rangle\rangle$ for each $X \in \mathcal{X}$.

Proof. We proceed by induction on the size of $\mathcal{X}$.

If $\mathcal{X} = \{X\}$ then let $\rho = 1$ and $\mathcal{Y} = \mathcal{X}$. Hence $S = \mathcal{X}$ and $\operatorname{disc} d = X@$, as required by (i). Also (iv) is satisfied trivially.

If $\mathcal{X} = \{X, X'\}$, $X \neq X'$ then $\operatorname{disc} d = X@X'@$. If $X@ \neq X'@$ then take $\rho = 1$ and $\mathcal{Y} = S = \mathcal{X}$ and up to relabeling, (ii) is satisfied. Once again, (iv) is satisfied trivially as $s = r = 1$.

Suppose that $X@ = X'@$. By Theorem II.5.5 there is a $\rho \in \mathrm{Isom}(d)$ where $X\rho = X'$ and $X'\rho = X$, and indeed we may take $\rho^2 = 1$. Notice $S = \emptyset$ and $\mathrm{disc}\, d = [1]$, as required by (iii). For (iv), either $s = r$ and we let $\mathcal{Y} = \mathcal{X}$ or $s = 2 - r$. By Lemma II.2.12 there is $(\varphi, \omega) \in \mathrm{Isom}^*(d)$; hence, $\mathcal{Y} := \mathcal{X}\varphi$ satisfies (iv).

If $n = |\mathcal{X}| > 2$ then there are distinct $X, X' \in \mathcal{X}$ with $X@ = X'@$. By induction on $\mathcal{Z} := \mathcal{X} - \{X, X'\}$ we have an isometry τ of $d_{\langle \mathcal{Z} \rangle}$ which permutes $\mathcal{Z}$. We also induct on S to locate an involution $\mu \in \mathrm{Isom}(d_{\langle S \rangle})$ such that $X\mu = X'$. Set $\rho = \tau \oplus \mu \in \mathrm{Isom}(d)$. Hence, $\rho^2 = 1$ and permutes $\mathcal{X}$. Moreover, $\{X \in \mathcal{X} : X\rho = X\} = S = \{Z \in \mathcal{Z} : Z\tau = Z\}$ and $\mathrm{disc}\, d = X@X'@\, \mathrm{disc}\, d_{\langle \mathcal{Z} \rangle} = \mathrm{disc}\, d_{\langle \mathcal{Z} \rangle}$. Therefore, each case of S is satisfied for $\mathcal{X}$ with ρ as it is satisfied for $\mathcal{Z}$ with τ. Therefore ρ satisfies (i), (ii), and (iii).

For (iv), let $2|r - s$. First assume $s \geq 2$. From the induction on $\mathcal{Z}$ there is a fully refined $\perp$-decomposition $\mathcal{W}$ of $\langle \mathcal{Z} \rangle$ of address $(n - 2 : s - 2)$ such that $\langle Z, Z\tau \rangle = \langle \mathcal{Y} \cap \langle Z, Z\rho \rangle \rangle$ for each $Z \in \mathcal{Z}$. If $X@ = [\omega]$ then set $\mathcal{Y} = \mathcal{W} \sqcup \{X, X'\}$ to complete (iv). If $X@ = [1]$ then use $(\varphi, \omega) \in \mathrm{Isom}^*(d_{\langle X, X' \rangle})$ from Lemma II.2.12 and set $\mathcal{Y} := \mathcal{W} \sqcup \{X\varphi, X'\varphi\}$. Finally, if $s < 2$ then take $\mathcal{W}$ to have address $(n - 2 : s)$ and define $\mathcal{Y} := \mathcal{W} \sqcup \{X\varphi, X'\varphi\}$ if $X@ = [\omega]$, and $\mathcal{Y} := \mathcal{W} \sqcup \{X, X'\}$ otherwise. □

Corollary II.6.3. *The set of addresses of orthogonal bases of d is*

$$\left\{(n - (c + 2k) : c + 2k) : 0 \leq k \leq \frac{n - c}{2}\right\}$$

where $\mathrm{disc}\, d = [\omega^c]$, $c = 0, 1$. *In particular, there are* $1 + \lfloor \frac{n-c}{2} \rfloor$ *addresses.*

Proof. From Theorem II.6.2.(iv), there is a fully refined $\perp$-decomposition of d for each address in the set. By Lemma II.6.1, these are the possible addresses of d. □

Corollary II.6.4. *Let $d : V \times V \to K$ be a non-degenerate symmetric bilinear form with $n = \dim V$ and let $\mathcal{X}$ and $\mathcal{Y}$ be orthogonal bases with addresses $(n - s : s)$ and $(n - r : r)$, respectively.*

(i) If n is odd then $\mathcal{X}\varphi = \mathcal{Y}$ for some $(\varphi, \hat{\varphi}) \in \mathrm{Isom}^*(d)$ if, and only if, $s = r$.

(ii) If n is even then $\mathcal{X}\varphi = \mathcal{Y}$ for some $(\varphi, \hat{\varphi}) \in \mathrm{Isom}^*(d)$ if, and only if, $s = r$ or $s = n - r$.

Proof. Let $\mathcal{X}\varphi = \mathcal{Y}$. Then as $\hat{\varphi} \in K^\times$, $\hat{\varphi} \equiv 1$ or $\omega \pmod{(K^\times)^2}$. If $x \in \mathcal{X}$, then

$$X\varphi@ \equiv d(x\varphi, x\varphi) \equiv d(x, x)\hat{\varphi} \equiv X@\hat{\varphi} \pmod{(K^\times)^2}, \qquad X = \langle x \rangle.$$

Thus $\mathcal{Y}@ = \mathcal{X}@\hat{\varphi}$. If $\hat{\varphi} \equiv 1 \pmod{(K^\times)^2}$ then $s = r$. If $\hat{\varphi} \equiv \omega$ then $s = n - r$, and

$$(\operatorname{disc} d)[\omega^n] = \prod_{X \in \mathcal{X}} X@\hat{\varphi} = \prod_{Y \in \mathcal{Y}} Y@ = \operatorname{disc} d.$$

So, $2|n$. This completes the proof of (i).

For the converse, by Theorem II.5.5 it remains only to consider $s = n - r$, which means $\mathcal{X}@ = \mathcal{Y}@[\omega]$, and from above also $n = 2m$. By Proposition II.2.13.(ii) there is a $(\varphi, \omega) \in \mathrm{Isom}^*(d)$. Therefore $\mathcal{X}\varphi@ = \mathcal{Y}@$. By Theorem II.5.5 there is a $\tau \in \mathrm{Isom}(d)$ such that $\mathcal{X}\varphi\tau = \mathcal{Y}$. This completes the proof of (ii). □

II.6.2 Semi-refinements

Definition II.6.5. *A bilinear map $b : V \times V \to W$ is* $\perp$-semi-indecomposable *if it is either $\perp$-indecomposable or b has orthogonal type with a fully refined $\perp$-decomposition $\{X, Y\}$ such that $X@ = Y@$.*

A $\perp$-decomposition is semi-refined *if it consists of $\perp$-semi-indecomposables and it has no coarser $\perp$-decomposition consisting of $\perp$-semi-indecomposables.*

Remark II.6.6. *Suppose that b is a $\perp$-semi-indecomposable bilinear map which is not $\perp$-indecomposable. Then, we have a fully refined $\perp$-decomposition $\{X, Y\}$ of b with $X@ = Y@$. By Corollary II.5.17.(ii), this is equivalent to having an isometry $\varphi \in \mathrm{Isom}(b)$ in which $X\varphi = Y$. Thus b_X is isometric to b_Y. Hence, if $c := b_X$ then b is isometric to $c \perp c$.*

Theorem II.6.7. *Let b be a non-degenerate Hermitian bilinear map.*

(i) Given a semi-refined $\perp$-decomposition $\mathcal{Z}$ and any fully refined $\perp$-decomposition $\mathcal{X}$, there is a fully refined $\perp$-decomposition $\mathcal{Y}$ with $\mathcal{X}@ = \mathcal{Y}@$ and

$$\mathcal{Z} = \mathcal{Y}^{[\rho]} := \{\langle Y, Y\rho\rangle : Y \in \mathcal{Y}\},$$

where $\rho \in \mathrm{Isom}(b)$ is an involution. In particular, $|\mathcal{Z}| \geq |\mathcal{X}|/2$.

(ii) $\mathrm{Isom}(b)$ acts transitively on the set of semi-refined $\perp$-decompositions.

(iii) Every fully refined $\perp$-decomposition of a bilinear map b determines a semi-refined $\perp$-decomposition (as in (i)). In particular, semi-refined $\perp$-decompositions exist.

Proof. (i). The idempotents associated to a semi-indecomposable b_Z, $Z \in \mathcal{Z}$, project to the same simple factor of $\mathrm{Adj}(b)$. By Proposition II.4.31, $\{\mathcal{Z}_I : I \lhd \mathrm{Adj}(b)$ a maximal $*$-ideal $\}$ partitions $\mathcal{Z}$. Hence, it suffices to consider $\mathcal{Z}_I$ for a fixed maximal $*$-ideal I of $\mathrm{Adj}(b)$.

For each $Z \in \mathcal{Z}_I$, either b_Z is $\perp$-indecomposable or it has a $\perp$-decomposition of size 2 with equal addresses. As $\mathcal{Z}_I$ is semi-refined, the set $S = \{Z \in \mathcal{Z} : b_Z$ is $\perp$-indecomposable$\}$ has size 1 if $|\mathcal{Z}_I|$ is odd, or size 2 with $S = \{Y, Y'\}$ and $Y@ \neq Y'@$, or $S = \emptyset$. It follows that $\mathcal{Z}_I$ is determines a fully refined $\perp$-decomposition

$$\mathcal{Y}_I := (\sqcup_{Z \in \mathcal{Z}_I} \{Y_Z, Y_Z'\}) \sqcup S$$

in which $Y_Z@ = Y_Z'@$ and $Z = \langle Y_Z, Y_Z' \rangle$, for each $Z \in \mathcal{Z} - S$. By Theorem II.6.2 and Lemma II.5.10, there is an involution $\rho \in \mathrm{Isom}(b)$ for which $\mathcal{Y}^{[\rho]} = \mathcal{Z}$ and furthermore, such that $\mathcal{X}_I@ = \mathcal{Y}_I@$.

(ii). Let $\mathcal{W}$ be another semi-refined $\perp$-decomposition of b. As in (i) we know $\mathcal{W} = \mathcal{U}^{[\tau]}$ where $\mathcal{U}$ is fully refined and has address equal to that of $\mathcal{Y}$. By Corollary II.5.16, the bijection $\phi : \mathcal{Y} \rightarrow \mathcal{U}$ induces a $\varphi \in \mathrm{Isom}(b)$ such that $Y\varphi = Y\phi$ so that $\mathcal{Y}\varphi = \mathcal{U}$ and $\mathcal{Y}^{[\rho]}\varphi = \mathcal{U}^{[\tau]}$.

(iii). Let $\mathcal{X}$ be a fully refined $\perp$-decompositions. From (i), any semi-refined $\perp$-decomposition can be fully refined to have the same address of $\mathcal{X}$. By (ii) is this unique up to an isometry. Therefore it remains only to prove that there is a semi-refined $\perp$-decomposition. This follows from Theorem II.6.2. □

Definition II.6.8. *A p-group P of class 2 and exponent p is centrally* semi-indecomposable *if it is either centrally indecomposable or $P = H \circ H$ where H is centrally indecomposable of orthogonal type.*

A central decomposition is semi-refined *if it consists of centrally semi-indecomposable subgroups and it has no coarser central decomposition consisting of centrally semi-indecomposable subgroups.*

Remark II.6.9. *If P is centrally semi-indecomposable and not centrally decomposable then $P = H \circ H$ where H is centrally indecomposable. Thus $\mathsf{Bi}(P) = \mathsf{Bi}(H) \perp \mathsf{Bi}(H)$. As in Remark II.6.6, this is equivalent to having a fully refined central decomposition $\{H, K\}$ of P where $H@ = K@$.*

Corollary II.6.10. *Every fully refined central decomposition $\mathcal{H}$ of a p-group P of class 2, exponent*

p, and $P' = Z(P)$, generates a semi-refined central decomposition

$$\mathcal{H}^{[\rho]} := \{\langle H, H\rho\rangle : H \in \mathcal{H}\},$$

for some $\rho \in C_{\mathrm{Aut}\,P}(P')$ in which $\mathcal{H}\rho = \mathcal{H}$. Furthermore, $C_{\mathrm{Aut}\,P}(P')$ acts transitively on the set of semi-refined central decompositions.

Proof. Let $\mathcal{H}$ be fully refined central decomposition of P.

As $P' = Z(P)$, $b := \mathsf{Bi}(P)$ is non-degenerate. Let $\mathcal{X} := \mathsf{Bi}(\mathcal{H})$ (cf. Section II.3.1). By Theorem II.3.6.(i) we know $\mathcal{X}$ is a fully refined $\perp$-decomposition of b. By Theorem II.6.7 there is an isometry ρ which permutes $\mathcal{X}$ such that $\mathcal{X}^{[\rho]}$ is semi-refined. Let τ be the automorphism on $\mathcal{H}$ induced by ρ (cf. Proposition II.3.3). Thus, $H\tau \neq H$ only if H is centrally indecomposable of orthogonal type (see Definition II.6.8 and Theorem II.4.36) and $H@ = H\tau@$ (cf. Corollary II.5.17.(iii)). Hence, $\langle H, H\tau\rangle \cong H \circ H$ for each $H \neq H\tau$, $H \in \mathcal{H}$. This makes $\mathcal{H}^{[\tau]}$ semi-refined.

Given any other fully refined central decomposition $\mathcal{K}$ of P it follows that $\mathcal{K}$ can be semi-refined by an automorphism μ which permutes $\mathcal{K}$. Thus, $\mathcal{H}^{[\tau]}$ and $\mathcal{K}^{[\mu]}$ have full refinements with a common address. Therefore Corollary II.5.16, Theorem II.3.6.$(ii.b)$, and Corollary II.2.9 prove the transitivity of $C_{\mathrm{Aut}\,P}(P')$. □

Proof of Theorem II.1.1.(i). First assume that $P' = Z(P)$. By Theorem II.4.32 we know all fully refined central decompositions have the same size. By Corollary II.6.10, we know that all semi-refinements of a fully refined central decomposition are equivalent under $\mathrm{Aut}\,P$. Furthermore, this also shows that a semi-refined central decomposition has the form $\mathcal{H}^{[\rho]} = \{\langle H, H\rho\rangle : H \in \mathcal{H}\}$ where $\rho \in \mathrm{Aut}\,P$. Therefore the multiset $\{|\langle H, H\rho\rangle| : H \in \mathcal{H}\}$ is uniquely determined by P. Indeed, $|H| = |\langle H, H\rho\rangle|/[H : Z(H)]$ is uniquely determined by H and P.

Let $\mathcal{K} := \{H \in \mathcal{H} : H\rho \neq H\}$. Then $\mathcal{H}$ is partitioned into

$$\{H \in \mathcal{H} : H\rho = H\} \sqcup \mathcal{K} \sqcup \mathcal{K}\rho. \tag{II.26}$$

Hence, the multiset $\{|H| : H \in \mathcal{H}\}$ equals

$$\{|H| : H \in \mathcal{H} : H\rho = H\} \sqcup \{|K| : K \in \mathcal{K}\} \sqcup \{|K| : K \in \mathcal{K}\}. \tag{II.27}$$

Thus, the multiset of orders of members of $\mathcal{H}$ is uniquely determined by P. The similar argument works for the multiset of orders of the centers of the members of $\mathcal{H}$.

Finally, for the case when $P' < Z(P)$ we invoke Lemma II.2.5 and Lemma II.2.3.(ii). □

II.7 Unbounded Numbers of Orbits of Central Decompositions

As indicated in the introduction, the proofs of our main theorem have depended on a study of $C_{\mathrm{Aut}\,P}(P')$. Whenever $C_{\mathrm{Aut}\,P}(P')$ is transitive on the set of fully refined central decompositions (Theorem II.3.6 and Corollary II.5.16) this approach is sufficient. However, $C_{\mathrm{Aut}\,P}(P')$ may have multiple orbits. This occurs only if there are centrally indecomposable p-groups of orthogonal type (cf. Theorem II.4.36).

In this section we have two principal aims: first to show how symmetric bilinear forms arise in the context of p-groups. Secondly, we develop examples of centrally indecomposable p-groups of the other types specified in Theorem II.4.36, with the exception of the unitary type.

Most the constructions and theorems in this section are subsumed by more general results in [63], but the proofs provided here are self-contained and require fewer preliminaries.

II.7.1 Centrally Indecomposable p-groups of Orthogonal Type

In [63] we prove that there are exponentially many p-groups of order p^n which have class 2, exponent p, and are centrally indecomposable of type 1. Indeed, we also show that a p-group of class 2 and exponent p with "randomly selected presentation" is "almost always" a centrally indecomposable group of type 1. Here we describe just one family of centrally indecomposable p-groups of type 1.

Lemma II.7.1. *Let V be a k-vector space of dimension $n > 2$. Define $b : V \times V \to V \wedge V$ by $b(u, v) := u \wedge v$, for all $u, v \in V$. Then b is alternating and* $\mathrm{Adj}(b) \cong k$ *with trivial involution, that is, b is $\perp$-indecomposable of type* 1.

Proof. Take $g \in \mathrm{Adj}(b)$. We show that g is a scalar matrix and thus $\mathrm{Adj}(b) \cong k$. Hence b is $\perp$-indecomposable of type 1 with respect to k.

Let $V = \langle e_1, \ldots, e_n \rangle$ so that $\{e_i \wedge e_j : 1 \leq i < j \leq n\}$ is a basis of $V \wedge V$. Fix $1 \leq i, j \leq n$,

$i \neq j$. We have

$$e_i g \wedge e_j = b(e_i g, e_j) = b(e_i, e_j g^*) = e_i \wedge e_j g^*, \qquad 1 \leq i < j \leq n. \tag{II.28}$$

If we take $e_i g = \sum_{s=1}^{n} g_{is} e_s$ and $e_j g^* = \sum_{t=1}^{n} g^*_{jt} e_t$, then

$$\begin{aligned} 0 = e_i g \wedge e_j - e_i \wedge e_j g^* &= \sum_{s=1}^{n} g_{is}(e_s \wedge e_j) - \sum_{t=1}^{n} g^*_{jt}(e_i \wedge e_t) \\ &= \sum_{s=1, s\neq i}^{n} g_{is}(e_s \wedge e_j) + (g_{ii} - g^*_{jj}) e_i \wedge e_j - \sum_{t=1, t\neq j}^{n} g^*_{jt}(e_i \wedge e_t). \end{aligned}$$

So we have $g_{is} = 0$ for all $s \neq i$ and $g^*_{jt} = 0$ for all $t \neq j$, $1 \leq s, t \leq n$ and furthermore $g_{ii} = g^*_{jj}$. As this is done for arbitrary $1 \leq i, j \leq n$, $i \neq j$, we have $g_{11} = g^*_{22} = g_{ii}$ for all $2 < i \leq n$. Finally, $g_{22} = g^*_{11} = g_{33} = g_{11}$ so in fact $g = g_{11} I_n$ and similarly $g^* = g_{11} I_n$. As g was arbitrary, $\mathrm{Adj}(b) = k$. □

If $\dim V = 2$ then $V \wedge V \cong k$ and the k-bilinear map b is simply the non-degenerate alternating k-bilinear form of dimension 2. This is indecomposable of symplectic type (Lemma II.7.11) and the corresponding group is the extra-special group of order p^3 and exponent p.

Corollary II.7.2. *Let V be an $\mathbb{F}_q$-vector space of dimension $n > 2$ and let $b : V \times V \to V \wedge V$ be defined by $b(u, v) = u \wedge v$ for all $u, v \in V$. Then $\mathsf{Grp}(b)$ is centrally indecomposable of orthogonal type (see Section II.3.2).*

Proof. This follows from Theorem II.3.6. □

When $q = p$, $\mathsf{Grp}(b) \cong \langle a_1, \ldots, a_n \mid \text{class 2, exponent } p \rangle$. Note that the smallest example of an orthogonal type group is $\langle a_1, a_2, a_3 \mid \text{class 2, exponent } p \rangle$ – the free class 2 exponent p-group of rank 3 and order p^6.

II.7.2 Direct Sums and Tensor Products

Direct sums and tensor products are two natural ways to construct bilinear maps from others. To use these we must demonstrate that the adjoint algebras of such products are determined by the adjoints of the components. A full account is given in [63] but here we give only the cases required and supply direct computational proofs.

Definition II.7.3. *Let $b : V \times V \to W$ and $b' : V' \times V' \to W'$ be k-bilinear maps. Let $b \oplus b' : V \oplus V' \times V \oplus V' \to W \oplus W'$ be the bilinear map defined by*

$$(b \oplus b')(u \oplus u', v \oplus v') = b(u, v) \oplus b'(u', v')$$

for all $u, v \in V$ and $u', v' \in V'$.

Proposition II.7.4. *Let b and b' be two non-degenerate bilinear maps. Then* $\mathrm{Adj}(b \oplus b') = \mathrm{Adj}(b) \oplus \mathrm{Adj}(b')$, *where the $*$-operator on the right hand side is componentwise. Hence also* $\mathrm{Sym}(b \oplus b') = \mathrm{Sym}(b) \oplus \mathrm{Sym}(b')$.

Proof. Evidently $\mathrm{Adj}(b) \oplus \mathrm{Adj}(b') \leq \mathrm{Adj}(b \oplus b')$. For the reverse, let $f \in \mathrm{Adj}(b \oplus b') \in \mathrm{End}(V \oplus V')$. Given $u, v \in V$, $v' \in V'$, take $(u \oplus 0)f = x \oplus x'$ and $(v \oplus v')f = y \oplus y'$ for some $x \oplus x', y \oplus y' \in V \oplus V'$. It follows that

$$\begin{aligned} b(x, v) \oplus b'(x', v') &= (b \oplus b')((u \oplus 0)f, v \oplus v') \\ &= (b \oplus b')(u \oplus 0, (v \oplus v')f^*) = b(u, y) \oplus b'(0, y') = b(u, y) \oplus 0. \end{aligned}$$

Therefore $b'(x', v') = 0$ for all $v' \in V'$. So $x' \in \mathrm{rad}\, b' = 0$. Thus $(u \oplus 0)f \in V \oplus 0$ for all $u \in V$. Similarly $(0 \oplus v')f \in 0 \oplus V'$. So $f \in (\mathrm{End}\, V) \oplus (\mathrm{End}\, V')$.

Let $f = g \oplus h$ and $f^* = g^* \oplus h^*$ for $g, g^* \in \mathrm{End}\, V$ and $h, h^* \in \mathrm{End}\, V'$. It follows that

$$\begin{aligned} b(ug, v) \oplus 0 = b(ug, v) \oplus b'(u', 0) &= (b \oplus b')((u \oplus u')f, v \oplus 0) \\ &= (b \oplus b')(u \oplus u', (v \oplus 0)f^*) = b(u, vg^*) \oplus b'(u', 0). \end{aligned}$$

Therefore $g \in \mathrm{Adj}(b)$ and similarly $h \in \mathrm{Adj}(b')$. So $f \in \mathrm{Adj}(b) \oplus \mathrm{Adj}(b')$. □

Given two bilinear maps $b : V \times V \to W$ and $b' : V' \times V' \to W'$ we induce a multi-linear map $(b \times b') : V \times V' \times V \times V' \to W \otimes W'$ defined by:

$$(b \otimes b')(u, u', v, v') := b(u, v) \otimes b'(u', v'), \qquad \forall u, v \in V, u', v' \in V'. \tag{II.29}$$

Let $\widehat{b \times b'}$ denote the induced linear map $V \otimes V' \otimes V \otimes V' \to W \otimes W'$. With this notation we give:

Definition II.7.5. *Let $b \otimes b' : V \otimes V' \times V \otimes V' \to W \otimes W'$ be the restriction of $\widehat{b \times b'}$ to $V \otimes V' \times V \otimes V'$, where $b : V \times V \to W$ and $b' : V' \times V' \to W'$ are bilinear maps.*

Evidently, $b \otimes b'$ is bilinear. Using tensor products and the following obvious result, we can convert symmetric bilinear maps to alternating bilinear maps.

Proposition II.7.6. *Let $b : U \times U \to W$ and $c : V \times V \to X$ be Hermitian maps over k with involutions θ and τ, respectively. Then $b \otimes c$ is Hermitian with involution $\theta \otimes \tau$. In particular, the tensor of two symmetric bilinear maps is symmetric, the tensor of a symmetric and an alternating bilinear map is alternating, and the tensor of two alternating bilinear maps is symmetric.*

Proposition II.7.7. *Let $d : U \times U \to C$ be a non-degenerate Hermitian C-form with $k = \{x \in C : \bar{x} = x\}$ and let $b' : V \times V \to W$ be a k-bilinear map. Then* $\mathrm{Adj}(d \otimes b) = \mathrm{Adj}(d) \otimes \mathrm{Adj}(b)$ *and* $\mathrm{Sym}(d \otimes b) = \mathrm{Sym}(d) \otimes \mathrm{Sym}(b)$.

Proof. Clearly $\mathrm{Adj}(d) \otimes \mathrm{Adj}(b) \leq \mathrm{Adj}(d \otimes b)$. For the reverse inclusion, let $\mathcal{X}$ be an orthogonal basis of d and $\mathcal{E} = \mathcal{E}(X)$. Take $g \in \mathrm{Adj}(d \otimes b)$. We show that $g \in \mathrm{Adj}(d) \otimes \mathrm{Adj}(b)$.

If $x, y \in \mathcal{X}$ with associated idempotents $e, f \in \mathcal{E}$, then $(e \otimes 1)g(f \otimes 1)$ restricts to $\langle x \rangle \otimes V \to \langle y \rangle \otimes V$, so there is a $g_{x,y} : V \to V$ defined by $vg_{x,y} = v'$, where $(x \otimes v)(e \otimes 1)g(f \otimes 1) = y \otimes v'$. Let (x, y) be the transposition interchanging x and y and identity on $\mathcal{X} - \{x, y\}$, treated as an element of $\mathrm{End}\, U = \mathrm{Adj}(d)$. Set $e_{x,y} = e(x, y)f$. Thus, $(e \otimes 1)g(f \otimes 1) = e_{x,y} \otimes g_{x,y}$. Since

$$g = \left(\sum_{e \in \mathcal{E}} e \otimes 1\right) g \left(\sum_{f \in \mathcal{E}} f \otimes 1\right) = \sum_{e,f \in \mathcal{E}} (e \otimes 1)g(f \otimes 1) = \sum_{x,y \in \mathcal{X}} e_{x,y} \otimes g_{x,y},$$

it suffices to prove that $g_{x,y} \in \mathrm{Adj}(b)$.

As $(e \otimes 1)g(f \otimes 1) \in \mathrm{Adj}(d \otimes b)$ with $((e \otimes 1)g(f \otimes 1))^* = (f \otimes 1)g^*(e \otimes 1)$ it follows that:

$$\begin{aligned} 1 \otimes b(v(d(y,y)g_{x,y}), v') &= d(y,y) \otimes b(vg_{x,y}, v') \\ &= (d \otimes b)((x \otimes v)(e \otimes 1)g(f \otimes 1), y \otimes v') \\ &= (d \otimes b)(x \otimes v, (y \otimes v')(f \otimes 1)g^*(e \otimes 1)) \\ &= d(x,x) \otimes b(v, v'g^*_{y,x}) = 1 \otimes b(v, v'(d(x,x)g^*_{y,x})). \end{aligned}$$

Notice we have used the fact that $d(x,x), d(y,y) \in k^\times$ and that the tensor product is taken over

k. Therefore $b(vg_{x,y}, v') = \frac{d(x,x)}{d(y,y)} b(v, v' g^*_{y,x})$ for all $v, v' \in V$. Hence $g_{x,y} \in \mathrm{Adj}(b)$ with adjoint $\frac{d(x,x)}{d(y,y)} g^*_{y,x}$. This completes the proof. □

It can be shown that $\mathrm{Adj}(b \otimes c) = \mathrm{Adj}(b) \otimes \mathrm{Adj}(c)$ for any two bilinear maps b and c [63].

II.7.3 Proof of Theorem II.1.1.(ii)

The best known examples of central products are the extra-special p-groups of exponent p and rank $2n$: $p^{1+2n} = \overbrace{p^{1+2} \circ \cdots \circ p^{1+2}}^{n}$, [15, Theorem 5.5.2]. It is customary to recognize $\mathsf{Bi}(p^{1+2n})$ as the non-degenerate alternating bilinear form $b : \mathbb{Z}_p^{2n} \times \mathbb{Z}_p^{2n} \to \mathbb{Z}_p$. We view this map as $d \otimes c$, where $d : \mathbb{Z}_p^n \times \mathbb{Z}_p^n \to \mathbb{Z}_p$ is the dot product $d(u, v) := uv^t$, and $c : \mathbb{Z}_p^2 \times \mathbb{Z}_p^2 \to \mathbb{Z}_p \wedge \mathbb{Z}_p$.

This construction generalizes. If H is a centrally indecomposable group then it has an associated associative composition algebra $C := \mathrm{Adj}(\mathsf{Bi}(H))/\operatorname{rad}\mathrm{Adj}(\mathsf{Bi}(H))$ (cf. Theorem II.4.36). Recall that $K := \{x \in C : x = \bar{x}\}$ is a field (cf. Definition II.4.6). Set $P := \overbrace{H \circ \cdots \circ H}^{n}$ and $b := \mathsf{Bi}(\overbrace{H \circ \cdots \circ H}^{n})$. As in Example II.3.7, $b = \overbrace{\mathsf{Bi}(H) \perp \cdots \perp \mathsf{Bi}(H)}^{n}$ which we can express compactly as $b = d \otimes_K \mathsf{Bi}(H)$, where $d : K^n \times K^n \to K$ is the usual dot product $d(u, v) := uv^t$, $u, v \in K^n$. Hence, by Proposition II.7.7, it follows that $\mathrm{Adj}(b) = \mathrm{Adj}(d) \otimes_K \mathrm{Adj}(\mathsf{Bi}(H))$ and thus $\mathrm{Adj}(b)/\operatorname{rad}\mathrm{Adj}(b) \cong \mathrm{Adj}(d) \otimes_K C$. Yet, $\mathrm{Adj}(d) \otimes_K C \cong \mathrm{Adj}(d')$, where $d' : C^n \times C^n \to C$ is defined by $d'(u, v) := u\bar{v}^t$, for $u, v \in C^n$. If $C > K$ then Corollary II.5.16 proves that all fully refined central decompositions are conjugate under automorphisms. We now demonstrate that the same is not generally possible with orthogonal type.

Lemma II.7.8. *Let $H = \langle X \rangle$ be a centrally indecomposable p-group of orthogonal type over $\mathbb{F}_q$ with X a minimal generating set of H. Set $P := \overbrace{H \circ \cdots \circ H}^{n}$ and let $\mathcal{H}_0 = \{H_1, \ldots, H_n\}$ be the canonical central decomposition given by the central product, so that $H_i = \langle x_i : x \in X \rangle$ where x_i denotes x in the i-th component.*

Let $\omega = \alpha^2 + \beta^2 \in \mathbb{Z}_p$ be a non-square. If $0 \le m \le n/2$ then define

$$\mathcal{H}_m = \{K_1, \ldots, K_{2m}, H_{2m+1}, \ldots, H_n\}$$

where

$$K_{2j-1} := \langle x_{2j-1}^{\alpha} x_{2j}^{\beta} : x \in X \rangle, \quad K_{2j} := \langle x_{2j-1}^{\beta} x_{2j}^{-\alpha} : x \in X \rangle,$$

for $1 \leq j \leq m$. Then every member of $\mathcal{H}_m$ is isomorphic to H and $\mathcal{H}_m$ is a fully refined central decompositions of P with address $(n-2m:2m)$, for $1 \leq m \leq n/2$.

Proof. As X is a minimal generating set of H, if $x, y \in X$ with $Z(H)x = Z(H)y$ then $x = y$. Therefore, $\overbrace{X \times \cdots \times X}^{n}$ is mapped injectively into P via the homomorphism $\pi : \prod_{H \in \mathcal{H}} H \to P$ described in Section II.2.1. This makes the groups H_i, K_{2j-1}, and K_{2j} well-defined, for each $1 \leq i \leq n$ and $1 \leq j \leq n/2$. Furthermore, $H_i \cong H$ for each $1 \leq i \leq n$ and $\mathcal{H}_0$ is a fully refined central decomposition of P.

Set $X_i = H_i/H_i' = H_iP'/P'$, $W = P' = H_i'$, $1 \leq i \leq n$. Also set $L_j := \langle H_{2j-1}, H_{2j} \rangle = \langle K_{2j-1}, K_{2j} \rangle$, $1 \leq j \leq n/2$. Then $L_j/L_j' = X_{2j-1} \oplus X_{2j}$ and $b|_{L_j/L_j'}$ is $b \perp b$ where $b = \mathsf{Bi}(H)$. Recall that $\mathsf{Bi}(P) = d \otimes b$ where $d : k^n \times k^n \to k$ is the dot product and $\mathcal{X} := \mathsf{Bi}(\mathcal{H}_0) = \{X_i : 1 \leq i \leq n\}$ is a fully refined $\perp$-decomposition of $\mathsf{Bi}(P)$. As $\mathrm{Adj}(\mathsf{Bi}(P)) = \mathrm{Adj}(d) \otimes \mathrm{Adj}(\mathsf{Bi}(H)) \cong \mathrm{Adj}(d)$, it follows that $\mathcal{X}_d = \{Y_1, \ldots, Y_n\}$ is fully refined $\perp$-decomposition of d. In fact, the implied isomorphism $\mathrm{Adj}(\mathsf{Bi}(P))$ to $\mathrm{Adj}(d)$ maps $f \otimes 1 \to f$, so $\mathcal{E}(\mathcal{X})$ is sent to the canonical frame $\{\mathrm{Diag}\{1, 0, \ldots\}, \ldots, \mathrm{Diag}\{\ldots, 0, 1\}\}$ of $\mathrm{Adj}(d)$. So, $\mathcal{H}_0@ = \mathcal{X}_d@ = (n:0)$.

Define

$$(\varphi_j, \hat{\varphi}_j) := \left(\begin{bmatrix} \alpha 1_{X_{2j-1}} & \beta 1_{X_{2j}} \\ \beta 1_{X_{2j-1}} & -\alpha 1_{X_{2j}} \end{bmatrix}, (\alpha^2 + \beta^2) 1_W \right) \in \mathrm{Isom}^*(b|_{L_j/L_j'}).$$

Set $\tau_j := \mathsf{Grp}(\varphi_j, \hat{\varphi}_j) \in \mathrm{Aut}\, L_j$. Then $K_{2j-1} = H_{2j-1}\tau_j$ and $K_{2j} = H_{2j}\tau_j$ for $1 \leq j \leq n/2$. Furthermore, $(\varphi_j, \hat{\varphi}_j)$ induces

$$\left(\begin{bmatrix} \alpha & \beta \\ \beta & -\alpha \end{bmatrix}, \omega \right) \in \mathrm{Isom}^*(\langle Y_{2j-1}, Y_{2j} \rangle).$$

Therefore, $K_{2j-1}@ = [\omega]$ and $K_{2j}@ = [\omega]$. Thus we have proved that $\mathcal{H}_m$ has address $(n-2m : 2m)$. □

At this point we know there are multiple $C_{\mathrm{Aut}\, P}(P')$-orbits of fully refined central decompositions of P, for any P satisfying the hypothesis of Lemma II.7.8. But we have not worked with $\mathrm{Aut}\, P$-orbits yet. We now show that there are multiple $\mathrm{Aut}\, P$-orbits as well.

Lemma II.7.9. *Given vector spaces U and V, the map $\alpha \oplus \beta \to \alpha \otimes \beta$ from $\mathrm{GL}(U) \oplus \mathrm{GL}(V) \to$*

$\mathrm{GL}(U \otimes V)$ *has kernel*

$$Z := \langle s1_U \oplus s^{-1}1_V \mid s \in k^\times \rangle.$$

and the image is isomorphic to $\mathrm{GL}(U) \circ \mathrm{GL}(V) = (\mathrm{GL}(U) \oplus \mathrm{GL}(V))/Z$.

Proof. To verify that Z is the kernel, fix a basis for V and consider matrices. □

Theorem II.7.10. *Let* $H := \langle x, y, z |$ *class* 2, *exponent* $p\rangle$ *(which is centrally indecomposable by Corollary II.7.2),* $P := \overbrace{H \circ \cdots \circ H}^{2n}$ *and* $\mathcal{H}_m$ *be as in Lemma II.7.8. Then all the following hold:*

(i) every member of $\mathcal{H}_m$ *is isomorphic to* H.

(ii) $\mathcal{H}_m$ *is a fully refined central decomposition of* P.

(iii) For every fully refined central decomposition $\mathcal{K}$ *of* P, *there is is a unique* m *and some* $\alpha \in C_{\mathrm{Aut}\,P}(P')$ *such that* $\mathcal{K}^\alpha = \mathcal{H}_m$. *So there are* $1+n$ *orbits of fully refined central decomposition under the action of* $C_{\mathrm{Aut}\,P}(P')$.

(iv) $\mathcal{H}_m$ *and* $\mathcal{H}_{m'}$ *are in the same* $\mathrm{Aut}\,P$*-orbit if, and only if,* $m' = n - m$.

Hence there are exactly $1 + \lfloor n/2 \rfloor$ *orbits in the set of fully refined central decompositions of* P *under the action of* $\mathrm{Aut}\,P$.

Proof. Let $k := \mathbb{Z}_p$.

By definition, $\mathsf{Bi}(H)$ is the map $c : V \times V \to W$ where $U = k^3$, $W := k^3 \wedge k^3 \cong k^3$ and $c(u, v) = u \wedge v$, $u, v \in V$. Hence (i) and (ii) follow from Lemma II.7.8. Furthermore, every possible address (see Corollary II.6.3) of $\mathsf{Bi}(P)$ is given by one of the $\mathcal{H}_m$. Therefore (iii) follows from Corollary II.5.16 and Theorem II.3.6.

To prove (iv) we start by describing the structure of $\mathrm{Isom}^*(b)$. Set $b := \mathsf{Bi}(P)$ and recall that $b = d \otimes c$ where $d : U \times U \to k$ is the dot product on $U := k^n$. Following Lemma II.7.9 we find that

$$\mathrm{Isom}^*(d) \circ \mathrm{Isom}^*(c) = \mathrm{Isom}^*(d) \oplus \mathrm{Isom}^*(c)/\langle (s1_U \oplus s^{-1}1_V, 1_{k\otimes W}) : s \in k^\times \rangle$$

embeds in $\mathrm{Isom}^*(b)$. *We claim that* $\mathrm{Isom}^*(b)$ *equals this embedding.*

By Proposition II.7.7 we know that $\mathrm{Adj}(b) = \mathrm{Adj}(d) \otimes \mathrm{Adj}(c) \cong \mathrm{Adj}(d)$. Hence $\mathrm{Isom}(b) \cong \mathrm{Isom}(d) = \mathrm{GO}(d)$. Indeed this shows that

$$\mathrm{Isom}(b) = \{\alpha \otimes 1_V : \alpha \in \mathrm{GO}(d)\}.$$

In particular, $\mathrm{Isom}(b)$ embeds in $\mathrm{Isom}^*(d) \circ \mathrm{Isom}^*(c)$.

Therefore, following Lemma II.2.13 we have

$$[\mathrm{Isom}^*(d) \circ \mathrm{Isom}^*(c) : \mathrm{Isom}(b)] = \frac{(p-1)|\,\mathrm{GO}(d)||\,\mathrm{GL}(3,p)|}{(p-1)|\,\mathrm{GO}(d)|} = |\,\mathrm{GL}(3,p)|.$$

As $\mathrm{Isom}^*(b)/\mathrm{Isom}(b) \leq \mathrm{GL}(k \otimes W) \cong \mathrm{GL}(3,p)$, we conclude by orders that $\mathrm{Isom}^*(b) = \mathrm{Isom}^*(d) \circ \mathrm{Isom}^*(c)$. Hence the orbits of $\mathrm{Isom}^*(b)$ on fully refined central decompositions are those of $\mathrm{Isom}^*(d) \circ \mathrm{Isom}^*(c)$, that is, the orbits described in Corollary II.6.4. □

Theorem II.1.1.(ii). This follows from Theorem II.7.10. □

II.7.4 Centrally Indecomposable p-groups of Non-orthogonal Type

Centrally indecomposable families of type symplectic are the easiest to construct by classical methods. Already the extraspecial p-groups p^{1+2} of exponent p serve as examples. We generalize the extraspecial example to include field extensions of $\mathbb{Z}_p$. We let k be an arbitrary field.

Lemma II.7.11. *The k-bilinear form $d : k^2 \times k^2 \to k$ defined by $d(u,v) = \det \begin{bmatrix} u \\ v \end{bmatrix}$, for all $u, v \in k^2$, has $\mathrm{Adj}(d) = M_2(k)$ with the adjugate involution, thus d is $\perp$-indecomposable of symplectic type.*

Corollary II.7.12. *Let $d : \mathbb{F}_q^2 \times \mathbb{F}_q^2 \to \mathbb{F}_q$ be the non-degenerate alternating bilinear form of dimension 2. Then $\mathsf{Grp}(d)$ is centrally indecomposable of symplectic type.*

Proof. This follows from Theorem II.3.6. □

Presently we are not aware of any alternating bilinear maps which are centrally indecomposable of unitary type. We expect infinite families over any field $\mathbb{F}_{q^2}$ to exist. Our search for such examples is on-going.

We next construct a family of centrally indecomposable p-groups of exchange type. This family furthermore illustrates that there can be a non-trivial $O_p(C_{\mathrm{Aut}\,P}(P'))$. There are families of exchange type without this feature but we choose this family for the ease of proof.

Lemma II.7.13. *Let V be a k-vector space of dimension $n > 1$. Define the k-bilinear map $b : (k \oplus V) \times (k \oplus V) \to V$ by*

$$b(\alpha \oplus u, \beta \oplus v) := \alpha v - \beta u. \tag{II.30}$$

Then b is alternating and

$$\mathrm{Adj}(b) \cong \left\{ \begin{bmatrix} \alpha 1_k & h \\ 0 & \beta 1_V \end{bmatrix} : h \in \hom(k, V), \alpha, \beta \in k \right\},$$

where the multiplication and the action on $k \oplus V$ is interpreted as matrix multiplication and where the involution is defined by

$$\begin{bmatrix} \alpha 1_k & h \\ 0 & \beta 1_V \end{bmatrix}^* := \begin{bmatrix} \beta 1_k & -h \\ 0 & \alpha 1_V \end{bmatrix}.$$

In particular, $\mathrm{Adj}(b)/\operatorname{rad}\mathrm{Adj}(b) \cong k \oplus k$ with the exchange involution and the radical is

$$\left\{ \begin{bmatrix} 0 & h \\ 0 & 0 \end{bmatrix} : h \in \hom(k, V) \right\}.$$

Thus b is $\perp$-indecomposable of exchange type.

Proof. It is easily checked that $e := 1_k \oplus 0_V, f := 0_k \oplus 1_V \in \mathrm{End}(k \oplus V)$ are both in $\mathrm{Adj}(b)$ and furthermore $e^* = f$, $e^2 = e$, $f^2 = f$. Fix $g \in \mathrm{Adj}(b)$. Then ege, egf, fge and fgf lie in $\mathrm{Adj}(b)$.

Let $u, v \in V$ be linearly independent. Since $(0 \oplus u)fge = \lambda \oplus 0$ and $(0 \oplus v)fg^*e = \tau \oplus 0$ for some $\lambda, \tau \in k$, it follows that

$$\begin{aligned} \lambda v &= b(\lambda \oplus 0, 0 \oplus v) = b((0 \oplus u)g, 0 \oplus v) = b(0 \oplus u, (0 \oplus v)g^*) \\ &= b(0 \oplus u, \tau \oplus 0) = -\tau u. \end{aligned}$$

However, u and v are linearly independent, and hence $\lambda = 0 = \tau$ so $fge = 0 = fg^*e$.

Next let $(1 \oplus 0)ege = \alpha \oplus 0$ and $(0 \oplus u)fg^*f = 0 \oplus v$ for some $\alpha \in k$ and $v \in V$. Then

$$\begin{aligned} \alpha u &= b(\alpha \oplus 0, 0 \oplus u) = b((1 \oplus 0)ege, 0 \oplus u) = b(1 \oplus 0, (0 \oplus u)g^*) \\ &= b(1 \oplus 0, 0 \oplus v) = v. \end{aligned}$$

Thus $fg^*f = 0 \oplus \alpha 1_V$ where $ege = \alpha 1_k \oplus 0_V$. Setting $(0 \oplus u)fgf = 0 \oplus v$ and $(1 \oplus 0)eg^*e = \beta \oplus 0$ we similarly find $fgf = 0 \oplus \beta 1_V$ where $eg^*e = \beta 1_k \oplus 0_V$.

Finally, set $(1 \oplus 0)egf = 0 \oplus u$ and $(1 \oplus 0)eg^*f = 0 \oplus v$. Then

$$\begin{aligned} -u &= b(0 \oplus u, 1 \oplus 0) = b((1 \oplus 0)egf, 1 \oplus 0) = b(1 \oplus 0, (1 \oplus 0)eg^*f) \\ &= b(1 \oplus 0, 0 \oplus v) = v. \end{aligned}$$

So egf is induced by a k-linear map $h : k \to V$ and eg^*f is induced by $-h$. □

Corollary II.7.14. *Let $b : (\mathbb{F}_q \oplus \mathbb{F}_q^n) \times (\mathbb{F}_q \oplus \mathbb{F}_q^n) \to \mathbb{F}_q^n$ be as in* (II.30) *with $n > 1$. Then* $\mathsf{Grp}(b)$ *is centrally indecomposable of exchange type.*

Proof. This follows from Theorem II.3.6. □

If $n = 1$ then b is simply the non-degenerate alternating bilinear k-form of dimension 2. The smallest example of a p-group with exchange type is in fact of order p^5 with rank 3.

We can use this example as evidence that the radicals accounted for in Section II.5.3 do arise for the setting of p-groups. We emphasize that instances of non-trivial radicals are known in far more general settings than $\perp$-indecomposable bilinear maps of exchange type.

The radical in of $\mathrm{Adj}(b)$, for b as in (II.30), intersects $\mathrm{Sym}(b)$ trivially. However, if we define $c : (k \oplus V) \times (k \oplus V) \to V$ by

$$c(\alpha \oplus u, \beta \oplus v) := \alpha v + \beta u, \qquad \forall \alpha, \beta, \in k, u, v \in V; \tag{II.31}$$

then $\mathrm{Adj}(c)/\operatorname{rad}\mathrm{Adj}(c) \cong k \oplus k$ with the exchange involution. Here $\operatorname{rad}\mathrm{Adj}(c) \leq \mathrm{Sym}(c)$. To make this example alternating we may simply tensor by the alternating bilinear map from Lemma II.7.1. To further make a $\perp$-decomposable bilinear map we may tensor with a dot-product. By Proposition II.7.7, the result has a non-trivial radical in $\mathrm{Sym}(b)$.

II.8 Closing Remarks

II.8.1 Conjecture on Uniqueness of Fully Refined Central Decompositions

It remains open whether or not the multiset of isomorphism types of fully refined central decompositions of a p-group P of class 2 and exponent p is uniquely determined. It suffices to answer the following:

> Let H and K be centrally indecomposable p-groups of class 2, exponent p, and of orthogonal type. Is it true that whenever $H \circ H \cong K \circ K$ then $H \cong K$?

We conjecture this is true. Because such groups involve symmetric bilinear forms, it is possible that a solution will divide along the congruence of p modulo 4. Some evidence of this has been uncovered while attempting to develop counter-examples. It appears that a counter-example would have order at least 5^{30}.

II.8.2 Further directions

The condition that an endomorphism $f \in \operatorname{End} V$ lies in $\operatorname{Adj}(b)$ (or $\operatorname{Sym}(b)$) is determined by a system of linear equations. This is the source of polynomial time algorithms for computing central decompositions of p-groups found in [60]. In contrast, the equations to determine if $f \in \operatorname{Isom}(b)$ or $\operatorname{Isom}^*(b)$ (and hence to determine the automorphism group of a p-group) are quadratic and generally difficult to solve.

Our theorems apply (at least over finite fields) to central decompositions of class 2 nilpotent Lie algebras. See also [3] and [9, pp. 608-609].

II.8.3 Other fields

The use of finite fields removed the need to consider Hermitian forms over non-commutative division rings in the classification of $*$-simple algebras, and consequently also the related simple Jordan algebras (Theorem II.4.15 and Theorem II.4.23); therefore, this assumption affects Section II.5.2. Furthermore, as finite fields are separable, we are able to apply Taft's $*$-algebra version of the Wedderburn Principal theorem (Theorem II.4.16) in proving Theorem II.4.36. Evidently our proofs apply also to bilinear maps over algebraically closed fields of characteristic not 2.

II.8.4 2-*groups of exponent* 4

The omission of 2-groups of exponent 4 in the proof of Theorem II.3.6 can be relaxed [60]. The known obstacles for 2-groups of class 2 and exponent 4 derive from the usual complications of symmetric bilinear forms in characteristic 2. We are presently investigating whether or not these are indeed the only limitations.

CHAPTER III

FINDING CENTRAL DECOMPOSITIONS OF p-GROUPS

III.1 Introduction

An algorithm is given to find a fully refined central decomposition of a finite p-group of class 2. The number of algebraic operations used by the algorithm is bounded by a polynomial in the log of the size of the group. The algorithm uses a Las Vegas probabilistic algorithm to compute the structure of a finite ring and the Las Vegas MeatAxe is also used. However, when p is small, the probabilistic methods can be replaced by deterministic polynomial time algorithms.

A set $\mathcal{H}$ of subgroups of a group G is a *central decomposition* of G if $\mathcal{H}$ generates G but no proper subset does, and distinct members of $\mathcal{H}$ commute. We say that G is *centrally indecomposable* if it has only the trivial central decomposition. A *fully refined* central decomposition of G is a central decomposition consisting of centrally indecomposable groups. Such decompositions arise from to central products in which the centers of the factors need not be the same.

For computational purposes, we assume groups are input and output via generators in a useful computational representation, such as a set of permutations, a set of matrices, or a polycyclic presentation (see Section III.2.1). We prove:

Theorem III.1.1. *Assuming a discrete log oracle module p, there is a Las Vegas polynomial time algorithm which, given a p-group P of class 2, returns a fully refined central decomposition. The algorithm uses in $O(\log^6[P : P'])$ time. When $p \leq \log^c |P|$, for some constant c, there is also a deterministic polynomial time algorithm for the same task.*

The discrete log oracle in our algorithm is unavoidable (Proposition III.7.1). Although Theorem III.1.1 concerns groups, most of the work of the algorithm is concentrated on computing the semisimple and radical structure of certain finite rings. Our algorithm introduces methods to compute the structure of $*$-rings and constructive recognition of simple $*$-algebras.

At a high level, the algorithm proceeds by passing from P to a related bilinear map b; and it is shown that central decompositions of P correspond to orthogonal decompositions of b, see Proposition III.3.1 and Theorem III.3.2. To find a fully refined orthogonal decomposition of b, a ring with involution (i.e. a *$*$-ring*) $\mathrm{Adj}(b)$ is introduced and shown to parameterize orthogonal decompositions of b via sets of suitable idempotents; see Corollary III.4.3.

In Section III.5 we find such sets of idempotents using the semisimple and radical structure of $\mathrm{Adj}(b)$. This structure can be computed efficiently by reducing to rings of characteristic p and applying the algorithms of Ronyai, Friedl, and Ivanyos for finite $\mathbb{Z}_p$-algebras [51, 22, 24]. This stage uses a Las Vegas polynomial time algorithm for factoring polynomials over finite fields of characteristic p, such as the methods of Berlekamp or Cantor-Zassenhaus [57, Chapter 14]. We select [22] as the specific approach to compute the structure of the rings we encounter. This leads us to use of the Las Vegas MeatAxe [21, 23] in one stage of our algorithm, cf. Theorem III.5.3. However, for a deterministic algorithm (for small p), both of these Las Vegas algorithms can be avoided (Section III.7.2).

Having found a fully refined orthogonal decomposition of b we convert this to a fully refined central decomposition of P using straightforward group theory (Corollary III.3.4).

The methods of Theorem III.1.1 took root in [59] where central decompositions of p-groups P of class 2 and exponent p were studied. There the $*$-ring $\mathrm{Adj}(b)$ and its associated Jordan algebra $\mathrm{Sym}(b)$ were used to describe the $\mathrm{Aut}\,P$-orbits of the set of fully refined central decompositions of P. Here, the algorithms apply in all exponents and include 2-groups.

A result in a different direction is the development of efficient algorithms to find direct product decomposition not only of p-groups, but general groups [61]. That work illustrates how decompositions of p-groups of arbitrary class can be reduced to the case of p-groups of class 2, where once again bilinear and ring theory methods are introduced to solve the problem.

III.2 Background

Throughout this work we assume p is a prime. Unless otherwise obvious, all our groups, rings, modules, and algebras (i.e.: rings over a field) are finite. All our rings are associative and unital. We express all abelian groups additively and refrain from indicating this elsewhere.

We use $A \sqcup B$ for the disjoint union of sets A and B, and $A - B$ for the complement of

$A \cap B$ in A. We measure the efficiency of our algorithms by bounding the total number of algebraic operations (in a group, module, or ring) by a polynomial in the size of the input, roughly $\log |P|$. The probabilistic aspects of our algorithm are of *Las Vegas* type, which means they return correct result but with probability $\epsilon > 0$ they may fail to return in the alloted number of steps.

III.2.1 Representing Groups for Computation

We assume throughout that P is a finite p-group for a known prime p. We allow P to be input by various means including via a polycyclic presentation, as a permutation group, or as a matrix group [20, Section 3.1]. In all cases we assume that P is specified with generators; a method to multiply, invert, and test equality of elements in P; and a method to test if an element $g \in P$ lies in a subgroup $\langle T \rangle$, where $T \subseteq P$. That is, we may consider P to be a *black-box* group with a *membership test* oracle [20, Section 3.2]. For large primes p, membership testing already assumes an instance of the discrete log problem (cf. Section III.7.1). We count each of these tasks as a single algebraic operation though we are mindful that each requires more than constant time.

The assumptions on P give rise to deterministic algorithms which use a polynomial number of group operations and which: find $|\langle T \rangle|$ for any $T \subseteq P$; find generators for the normal closure $\langle T^G \rangle$ of the subgroup $\langle T \rangle$, $T \subseteq P$; find generators for the commutator subgroup P' of P; and find generators for the center $Z(P)$ of P [20, Section 3.3].

Remark III.2.1. *(i) Though in practice most p-groups are input by polycyclic presentations, the current methods to multiply in such groups, and to test membership, have exponential complexity (even when $p = 2, 3$) within the collection process [35, p. 670].*

(ii) Permutation groups use fast multiplication and membership testing, but various p-groups have no small degree faithful permutation representations [45, Example 1.1].

(iii) For matrix p-groups, multiplication is efficient and membership testing can be done if p is small or if p is the characteristic of the ground field [38, Theorem 3.2].

III.2.2 Abelian p-groups, Bases, Effective Homomorphisms, and Solving Systems of Equations

A *basis* of a finite abelian p-group V is a subset $\mathcal{X}$ of V such that $V = \bigoplus_{x \in \mathcal{X}} \langle x \rangle$. Every basis of V gives a natural isomorphism to $\mathbb{Z}_{p^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{e_s}}$ for $e_1 \leq \cdots \leq e_s \in \mathbb{Z}^+$. Operating in the latter representation is preferable to V's original representation and we assume all abelian

groups are handled in this way. Each endomorphism f of V can be represented by an integer matrix $F = [F_{ij}]$ such that $p^{e_j - e_i} | F_{ij}$, $1 \leq i \leq j \leq s$, and furthermore, every such matrix induces an endomorphism of V (with respect to $\mathcal{X}$) [19, Theorem 3.3].

We have need in various places to apply homomorphisms and isomorphisms between finite abelian p-groups, rings, and algebras. We say a homomorphism is *effective* when it can be evaluated efficiently – for instance with the same cost as matrix multiplication – and a coset representative for the preimage of a point in the codomain can also be found efficiently. This means that effective isomorphisms are easily evaluated and inverted.

Suppose we have a system of $\mathbb{Z}_{p^e}$ linear equations with solutions in a $\mathbb{Z}_{p^e}$-module V. There are efficient deterministic methods to solve for a basis of the solution space of the system [39, Theorem 8.3]; however, it is essential to note that for large p, this process assumes a discrete log oracle of p and we must do the same. For simplicity, we use the usual cubic polynomial-time methods of Gaussian elimination and traditional matrix multiplication.

III.2.3 Bilinear Maps, $\perp$-decompositions, and Isometry

A *$\mathbb{Z}_{p^e}$-bilinear map* $b : V \times V \to W$ is a function of $\mathbb{Z}_{p^e}$-modules V and W where

$$b(su + u', tv + v') = stb(u, v) + sb(u, v') + tb(u', v) + b(u', v'), \tag{III.1}$$

for each $u, u', v, v' \in V$ and $s, t \in \mathbb{Z}_{p^e}$. A *$\perp$-decomposition* of b is a decomposition $\mathcal{V}$ of V into a direct sum of submodules which are pairwise orthogonal relative to b, i.e. $b(X, Y) = 0$ for distinct $X, Y \in \mathcal{V}$.

Let $\mathcal{X}$ and $\mathcal{Z}$ be ordered bases of V and W respectively. We define $B_{xy}^{(z)} \in \mathbb{Z}_{p^e}$ by

$$b\left(\sum_{x \in \mathcal{X}} s_x x, \sum_{y \in \mathcal{X}} t_y y\right) = \sum_{x,y \in \mathcal{X}} \sum_{z \in \mathcal{Z}} s_x t_y B_{xy}^{(z)} z, \quad \forall s_x, s_y \in \mathbb{Z}_{p^e}, x, y \in \mathcal{X}. \tag{III.2}$$

Set

$$B_{xy} = \sum_{z \in \mathcal{Z}} B_{xy}^{(z)} z, \qquad \forall x, y \in \mathcal{X};$$

so that $B = [B_{xy}]_{x,y \in \mathcal{X}}$ is an $n \times n$-matrix with entries in W, where $n = |\mathcal{X}|$. Writing the elements

of V as row vectors with entries in $\mathbb{Z}_{p^e}$ with respect to the basis $\mathcal{X}$ we can then write:

$$b(u,v) = uBv^t, \qquad \forall u,v \in V. \tag{III.3}$$

Take $f,g \in \operatorname{End} V$ represented as matrices F and G with respect to the basis $\mathcal{X}$ above. Define FB and BG^t by the usual matrix multiplication, but notice the results are matrices with entries in W. Evidently, $(F+G)B = FB+GB$, $F(GB) = (FG)B$, and similarly for the action on the right. The significance of these operations is seen by their relation to b:

$$b(uf,v) = uFBv^t \text{ and } b(u,vg) = uBG^tv^t; \tag{III.4}$$

for all $u,v \in V$.

An isometry between two bilinear maps $b : V \times V \to W$ and $b' : V' \times V' \to W$ is an isomorphism $\alpha : V \to V'$ such that $b'(u\alpha, v\alpha) = b(u,v)$ for all $u,v \in V$. Evidently, isometries map $\perp$-decompositions of b to $\perp$-decomposition of b'.

Finally, we call a bilinear map *Hermitian* if there is $\theta \in \mathrm{GL}(W)$ of order at most 2 such that

$$b(u,v) = b(v,u)\theta, \qquad \forall u,v \in V. \tag{III.5}$$

This meaning of Hermitian includes the usual *symmetric*, $b(u,v) = b(v,u)$; and *skew symmetric*, $b(u,v) = -b(v,u)$ flavors of bilinear maps. If $W = \langle b(u,v) : u,v \in V\rangle$ then θ is uniquely determined by b and so in that case we make no effort to specify θ explicitly.

III.2.4 Rings

All our rings will have characteristic a power of p and so they are input with a generating set. Furthermore, each of our rings will be represented in $\operatorname{End} V$ for some abelian p-group V and thus multiplication is done by the usual matrix multiplication.

III.3 Reducing Central Decompositions to Orthogonal Decompositions

In this section we reduce the problem of finding a central decomposition of a p-group of class 2 to the related problem of finding a $\perp$-decomposition of an associated bilinear map.

III.3.1 Bilinear Maps and p-groups

Let P be a p-group of class 2 and $P' \leq M \leq Z(P)$. Associated to P are various bilinear maps $b := \mathsf{Bi}(P, M)$ defined by $b : P/M \times P/M \to P'$ where $b(Mx, My) := [x, y]$, for each $x, y \in P$. We will express the operations in P/M, P', and b additively. Notice that b is alternating and skew-symmetric: $b(Mx, Mx) = 0$ and $b(Mx, My) = -b(My, Mx)$ for all $x, y \in P$.

III.3.2 Central Decompositions from Orthogonal Decompositions

We recall some ideas from [59, Section 4] involving class 2 and exponent p and modify them to p-groups P of class 2 of general exponent, including 2-groups.

Let $\mathcal{H}$ be a set of subgroups of P. Given a normal subgroup M of P we define:

$$\mathcal{H}M := \{HM : H \in \mathcal{H}\} - \{M\}, \tag{III.6}$$

$$\mathcal{H}M/M := \{HM/M : H \in \mathcal{H}\} - \{M/M\}. \tag{III.7}$$

A central decomposition $\mathcal{H}$ is an *M-central decomposition* if $H \cap \langle \mathcal{H} - \{H\} \rangle \leq M$ for each $H \in \mathcal{H}$. We may assume that $M \leq Z(P)$ as every central decomposition of P is a $Z(P)$-central decomposition. Given an M-central decomposition $\mathcal{H}$, it follows that $\mathcal{H}M/M$ is a direct decomposition of P/M.

Suppose that $\mathcal{V}$ is a direct decomposition of P/M. Define

$$\mathcal{H}(\mathcal{V}) := \{H \leq P : M \leq H, H/M \in \mathcal{V}\}. \tag{III.8}$$

Note that $\mathcal{V}$ and $\mathcal{H}(\mathcal{V})$ are in a natural bijection.

Proposition III.3.1. *Let P be a p-group of class 2, $P' \leq M \leq Z(P)$, and $b := \mathsf{Bi}(P, M)$.*

(i) If $\mathcal{H}$ is an M-central decomposition of P then $\mathcal{H}M/M$ is a $\perp$-decomposition of b.

(ii) If $\mathcal{V}$ is a $\perp$-decomposition of b then $\mathcal{H}(\mathcal{V})$ is an M-central decomposition of P where $\mathcal{H}(\mathcal{V})M = \mathcal{H}(\mathcal{V})$ and $\mathcal{H}(\mathcal{V})/M = \mathcal{V}$.

Proof. (i). If $\mathcal{H}$ is an M-central decomposition of P then $\mathcal{H}M/M$ is a direct decomposition of $V := P/M$. Furthermore, if H and K are distinct members of $\mathcal{H}$ then $[H, K] = 1$, which proves that $b(HM/M, KM/M) = 0$. Thus, $\mathcal{H}M/M$ is a $\perp$-decomposition of b.

(*ii*). Let $\mathcal{V}$ be a $\perp$-decomposition of b and set $\mathcal{K} := \mathcal{H}(\mathcal{V})$. By definition, $\mathcal{K} = \mathcal{K}M$ and $\mathcal{K}/M = \mathcal{V}$, so that $K \cap \langle \mathcal{K} - \{K\} \rangle = M$ for all $K \in \mathcal{K}$. Therefore, it remains to show that $\mathcal{K}$ is a central decomposition of P. As $\mathcal{V} \neq \emptyset$ it follows that $\mathcal{K} \neq \emptyset$. Furthermore, $V = \langle \mathcal{V} \rangle$ so $P = \langle \mathcal{K}, M \rangle = \langle \mathcal{K} \rangle$, as $M \leq K$ for any $K \in \mathcal{K}$. Since $\mathcal{K}$ is in bijection with $\mathcal{V}$, if $\mathcal{J}$ is a proper subset of $\mathcal{K}$ then $\mathcal{J}/M$ is a proper subset of $\mathcal{V}$ and as $\mathcal{J}/M$ does not generate V it follows that $\mathcal{J}$ does not generate P. Finally, if H and K are distinct members of $\mathcal{K}$ then $0 = b(H/M, K/M) = [H, K]$. Thus, $\mathcal{K}$ is a central decomposition of P. □

Theorem III.3.2. *If P is a p-group of class 2, then P is centrally indecomposable if, and only if,* $\mathsf{Bi}(P, Z(P))$ *is $\perp$-indecomposable and $Z(P) \leq \Phi(P)$.*

Proof. Assume that P is centrally indecomposable.

Let $\mathcal{V}$ be a $\perp$-decomposition of $\mathsf{Bi}(P, Z(P))$. By Proposition III.3.1.(*ii*), $\mathcal{H}(\mathcal{V})$ is a central decomposition of P and therefore $\mathcal{H}(\mathcal{V}) = \{P\}$. Hence, $\mathcal{V} = \mathcal{H}(\mathcal{V})/Z(P) = \{P/Z(P)\}$. As $\mathcal{V}$ was an arbitrary $\perp$-decomposition of $\mathsf{Bi}(P, Z(P))$, it follows that $\mathsf{Bi}(P, Z(P))$ is $\perp$-indecomposable.

Next let $\Phi(P) \leq Q \leq P$ be such that $P/\Phi(P) = Q/\Phi(P) \oplus Z(P)\Phi(P)/\Phi(P)$ as $\mathbb{Z}_p$-vector spaces. Set $\mathcal{H} = \{Q, Z(P)\}$. Clearly $[Q, Z(P)] = 1$ and P is generated by $\mathcal{H}$. Therefore, $\mathcal{H}$ contains a subset which is a central decomposition of P. As P is centrally indecomposable and $P \neq Z(P)$, it follows that $P = Q$, and so $1 = Z(P)\Phi(P)/\Phi(P)$, which proves that $Z(P) \leq \Phi(P)$.

For the reverse direction we assume that $\mathsf{Bi}(P, Z(P))$ is $\perp$-indecomposable and that $Z(P) \leq \Phi(P)$. Let $\mathcal{H}$ be a central decomposition of P.

By Proposition III.3.1.(*i*) we know $\mathcal{H}Z(P)/Z(P)$ is a $\perp$-decomposition of $\mathsf{Bi}(P, Z(P))$. Thus, $\mathcal{H}Z(P)/Z(P) = \{P/Z(P)\}$ so that $\mathcal{H}Z(P) = \{P\}$. Hence, for all $H \in \mathcal{H}$, either $H \leq Z(P)$ or $HZ(P) = P$. As $Z(P) \leq \Phi(P) < P$, it follows that at least one $H \in \mathcal{H}$ is not contained in $Z(P)$ and furthermore, $P = HZ(P) = H$ as $Z(P)$ consists of non-generators. Since no proper subset of $\mathcal{H}$ generates P and $P \in \mathcal{H}$, it follows that $\mathcal{H} = \{P\}$. Since $\mathcal{H}$ was an arbitrary central decomposition of P it follows that P is centrally indecomposable. □

Proposition III.3.3. *Suppose P is a p-group of class 2 such that* $\mathsf{Bi}(P, Z(P))$ *is $\perp$-indecomposable. Then*

(i) every central decomposition of P has exactly one nonabelian member, and

(ii) there is deterministic algorithm using $O(\log^4[P : P'])$ algebraic operations which returns a nonabelian centrally indecomposable group Q such that $P = Q$ or $\{Q, Z(P)\}$ is a central decomposition of P.

Proof. (i). Let $\mathcal{H}$ be a central decomposition of P. Since $P \neq Z(P)$ and $\mathsf{Bi}(P, Z(P))$ is $\perp$-indecomposable, there is a nonabelian $H \in \mathcal{H}$ and $\mathcal{H}Z(P) = \{P\}$ proves that $P = HZ(P)$. If $K \in \mathcal{H} - \{H\}$ then $[K, P] = [K, HZ(P)] = [K, H] = 1$, since distinct members of $\mathcal{H}$ commute. Thus $K \leq Z(P)$, which proves that H is the *only* nonabelian group in $\mathcal{H}$.

(ii). If $Z(P) \leq \Phi(P)$ then the algorithm returns P. Otherwise, compute generators for a vector space complement $Q/\Phi(P)$ to $Z(P)\Phi(P)/\Phi(P)$ in $P/\Phi(P)$, $\Phi(P) \leq Q < P$. Recurse with Q in the rôle of P and return the result of this recursive call.

If we find that $Z(P) \leq \Phi(P)$ then Theorem III.3.2 proves that P is centrally indecomposable. Otherwise, $Z(P)\Phi(P)/\Phi(P)$ is a proper subspace of the vector space $P/\Phi(P)$. The group Q satisfies $P = QZ(P)$. Hence, $P' = [QZ(P), QZ(P)] = Q'$ (so Q is nonabelian) and $[Z(Q), P] = [Z(Q), QZ(P)] = 1$, so that $Z(Q) = Q \cap Z(P) \geq P'$. In particular, the isomorphism of $P/Z(P) = QZ(P)/Z(P) \cong Q/Z(P) \cap Q = Q/Z(Q)$ gives an isometry between $\mathsf{Bi}(P, Z(P))$ and $\mathsf{Bi}(Q, Z(Q))$ which implies that $\mathsf{Bi}(Q, Z(Q))$ is $\perp$-indecomposable. Thus we may recurse with Q. By induction, the return of a recursive call is a centrally indecomposable subgroup $P' \leq R \leq P$ such that $Q = RZ(Q)$ and so $P = RZ(P)$, which proves that $\{R, Z(P)\}$ is a central decomposition of P.

For the timing we note that $[Q : Q'] < [P : P']$. Thus the number of recursive calls is bounded by $\log[P : P']$. To find a vector space complement amounts to finding a basis of $Z(P)\Phi(P)/\Phi(P)$ and extending the basis to one for $P/\Phi(P)$ and so it uses $O(\log^3[P : P'])$ algebraic operations. Hence, the algorithm uses $O(\log^4[P : P'])$ algebraic operations. □

Corollary III.3.4. *Let P be a p-group of class 2 and $\mathcal{V}$ a fully refined $\perp$-decomposition of $\mathsf{Bi}(P, Z(P))$. There is a deterministic algorithm using $O(\log^5[P : P'])$ algebraic operations, which returns a fully refined central decomposition $\mathcal{H}$ of P such that $\mathcal{H}Z(P)/Z(P) = \mathcal{V}$.*

Proof. Algorithm. Computing $\mathcal{H} := \mathcal{H}(\mathcal{V})$. Set $\mathcal{K} = \emptyset$. Then, for each $H \in \mathcal{H}$, use the algorithm of Proposition III.3.3.(ii) to find a nonabelian centrally indecomposable subgroup $K \leq H$ such that $H = KZ(P)$ and add K to $\mathcal{K}$. Next, given $Z(P) = \langle S \rangle$, set $\mathcal{J} := \mathcal{K} \sqcup \{\langle x \rangle : x \in S - \langle \mathcal{K} \rangle\}$. Using a greedy algorithm, remove the abelian members from $\mathcal{J}$ until no proper subset of $\mathcal{J}$ generates P.

Correctness. By Proposition III.3.1 we know that $\mathcal{H}$ is a central decomposition of P in which every member H has $Z(H) = Z(P)$ and $\mathrm{Bi}(H, Z(H))$ is $\perp$-indecomposable. Thus the algorithm of Proposition III.3.3.(*ii*) can be applied to H and so the set $\mathcal{K}$ consists of nonabelian centrally indecomposable subgroups where distinct members pairwise commute. Furthermore, $\mathcal{K}Z(P) = \mathcal{H}$. Let $Q := \langle \mathcal{K} \rangle$. We now have $P = QZ(P)$. Thus, at every stage of the greedy algorithm, the set $\mathcal{J}$ generates P, distinct members pairwise commute, and every member is centrally indecomposable. Thus $\mathcal{J}$ contains a central decomposition of P (i.e.: a subset which generates P and no proper subset does). If $\mathcal{L} \subset \mathcal{J}$ and generates P, then given $H \in \mathcal{J} - \mathcal{L}$ it follows that $1 = [H, \langle \mathcal{L} \rangle] = [H, P]$ so that $H \leq Z(P)$. Hence, the greedy algorithm need only consider the abelian members of $\mathcal{J}$. The algorithm halts when a central decomposition is found.

Timing. There are $|\mathcal{V}|$ calls made to the algorithm of Proposition III.3.3.(*ii*), which uses $O(\log^4[H : H'])$ algebraic operations for each $H \in \mathcal{H}$. The greedy algorithm halts after $|S|$ steps as then it has tested each abelian member of $\mathcal{J}$. □

III.4 The $*$-ring of Adjoints of a Bilinear Map

We have discussed the necessary group theory and now concentrate on the ring theory required in proving Theorem III.1.1. In this section we introduce a ring with involution (i.e. a $*$-ring [37]) as a means to compute $\perp$-decompositions of a Hermitian bilinear map.

Throughout this section we assume that $b : V \times V \to W$ is a $\mathbb{Z}_{p^e}$-bilinear map.

III.4.1 Adjoints

The ring of *adjoints* of b is:

$$\mathrm{Adj}(b) := \{(f, g) \in \mathrm{End}\, V \oplus (\mathrm{End}\, V)^{op} : b(uf, v) = b(u, vg), \forall u, v \in V\}. \tag{III.9}$$

There is a natural subset of $\mathrm{Adj}(b)$ of *self-adjoint* elements:

$$\mathrm{Sym}(b) := \{(f, f) \in \mathrm{End}\, V \oplus (\mathrm{End}\, V)^{op} : b(uf, v) = b(u, vf), \forall u, v \in V\}. \tag{III.10}$$

Remark III.4.1. *Notice that* $\mathrm{Sym}(b)$ *is not an associative subring but rather a Jordan algebra, quadratic in the case of characteristic* 2*, cf. [59, Section 4.5]. This is a vital observation for an-*

swering questions surrounding $\perp$-decompositions; however, for algorithmic purposes this perspective is not necessary.

If b is Hermitian then $(f,g) \in \mathrm{Adj}(b)$ if, and only if, $(g,f) \in \mathrm{Adj}(b)$. Hence, $(f,g) \mapsto (g,f)$ is an anti-isomorphism $*$ (which uses multiplication in $(\mathrm{End}\, V)^{op}$ in the second variable). Indeed, $*$ has order 1 or 2 so that $\mathrm{Adj}(b)$ is a $*$-ring.

In general, for a $*$-ring $(R,*)$ and additive subgroup $S \subseteq R$, we define $\mathfrak{H}(S,*) = \{s \in S : s^* = s\}$ which is again a subgroup of S, as $*$ is additive. ($\mathfrak{H}$ is for Hermitian and is a notation encouraged by Jacobson.)

III.4.2 Self-adjoint Idempotents

Recall that an endomorphism $e \in \mathrm{End}\, V$ is an *idempotent* if $e^2 = e$. Hence, $V = Ve \oplus V(1-e)$. Indeed, every direct decomposition $\mathcal{V}$ of V is parameterized by the set of projection idempotents $\mathcal{E} := \mathcal{E}(\mathcal{V})$; that is, for each $U \in \mathcal{V}$, $e_U \in \mathcal{E}$ where e_U projects V onto U with kernel $\langle \mathcal{V} - \{U\} \rangle$. It follows that distinct members e and f of $\mathcal{E}$ are *orthogonal* (i.e. $ef = 0 = fe$) and $1 = \sum_{e \in \mathcal{E}} e$.

Note that $1 \in \mathrm{Sym}(b)$. All idempotents in $\mathrm{Sym}(b)$ are self-adjoint and vice-versa, but to emphasize this requirement we call these *self-adjoint idempotents*. The significance of $\mathrm{Sym}(b)$ is the following:

Theorem III.4.2. *A direct decomposition $\mathcal{V}$ of V is a $\perp$-decomposition of $b : V \times V \to W$ if, and only if, $\mathcal{E}(\mathcal{V}) \subseteq \mathrm{Sym}(b)$.*

Proof. See [59, Proposition 4.30, Theorem 4.33.(i)] (whose proof applies in any characteristic). □

A self-adjoint idempotent $e \in \mathrm{Sym}(b)$ is *self-adjoint-primitive* if it is not the sum of proper (i.e.: not 0 nor 1) pairwise orthogonal self-adjoint idempotents in $\mathrm{Sym}(b)$. Such idempotents need not be primitive in $\mathrm{Adj}(b)$. A set of pairwise orthogonal self-adjoint primitive idempotents of $\mathrm{Sym}(b)$ which sum to 1 is called a *frame* of $\mathrm{Sym}(b)$. More generally, in a $*$-ring $(R,*)$, a (self-adjoint) frame is a set of self-adjoint-primitive pairwise orthogonal idempotents which sum to 1.

Corollary III.4.3. *There is a natural bijection between the set of fully refined $\perp$-decompositions of b and the set of all frames of* $\mathrm{Sym}(b)$.

Proof. See [59, Theorem 4.33.(*ii*)]. □

III.4.3 Computing Adj(b) *and* Sym(b)

Let V and W be finite abelian p-groups specified with bases $\mathcal{X}$ and $\mathcal{Z}$ respectively. Take $b : V \times V \to W$ to be a $\mathbb{Z}_{p^e}$-bilinear map. Assume that b is input with structure constant matrix B with respect to the bases $\mathcal{X}$ and $\mathcal{Z}$ (cf. (III.3)).

If $\operatorname{End} V$ is expressed as matrices (see Section III.2.2) with respect to $\mathcal{X}$ then

$$\operatorname{Adj}(B) = \{(X, Y) \in \operatorname{End} V \oplus \operatorname{End} V : XB = BY^t\}. \tag{III.11}$$

To find a basis for $\operatorname{Adj}(B)$ we solve for X and Y such that:

$$0 = \sum_{x \in \mathcal{X}} X_{xx'} B^{(z)}_{x'y} - \sum_{y \in \mathcal{X}} Y_{yy'} B^{(z)}_{xy'}, \qquad \forall x, y \in \mathcal{X}, z \in \mathcal{Z}. \tag{III.12}$$

This amounts to solving $|\mathcal{X}|^2|\mathcal{Z}|$ linear equations over $\mathbb{Z}_{p^e}$, each in $2|\mathcal{X}|$ variables and can be done using $O(|\mathcal{X}|^4|\mathcal{Z}|)$ operations in $\mathbb{Z}_{p^e}$ (cf. Section III.2.2). Computing a basis of Sym(b) can be done in similar fashion.

Remark III.4.4. *If b is Hermitian then the number of equations determining* Adj(b) *can be decreased by 2 by considering the ordering of the basis $\mathcal{X}$ and using only the equations* (III.12) *for $x \leq y$, $x, y \in \mathcal{X}$ and $z \in \mathcal{Z}$.*

III.5 Algorithms for $*$-rings

In this section we prove effective versions of the classical semisimple and radical structure theorems for finite $*$-rings. Most of the work reduces to known algorithms for the semisimple and radical structure theorems of finite algebras over $\mathbb{Z}_p$.

III.5.1 A Fast Skolem-Noether Algorithm

Let K be a field of characteristic p. The Skolem-Noether theorem states that every ring automorphism φ of $M_n(K)$ has the form $X\varphi = D^{-1}X^\sigma D$ for $(D, \sigma) \in \mathrm{GL}_n(K) \rtimes \mathrm{Gal}(K/\mathbb{Z}_p)$, for $X \in M_n(K)$, [10, (3.62)]. Given an effective automorphism φ, there is a straightforward method

to find (D, σ) which involves solving a system of n^2 linear equations over K and thus uses $O(n^6)$ field operations. We offer the following improvement by analyzing the proof of the Skolem-Noether theorem in [26, Chapter VIII].

Proposition III.5.1. *Given an effective ring automorphism φ of $M_n(K)$, K a finite field of characteristic p, there is a deterministic algorithm using $O(n^4 + \dim_{\mathbb{Z}_p} K)$ algebraic operations which finds $(D, \sigma) \in \mathrm{GL}_n(K) \rtimes \mathrm{Gal}(K/\mathbb{Z}_p)$ such that $X\varphi = D^{-1}X^{\sigma}D$, for all $X \in M_n(K)$.*

Proof. Define $g : K^n \to M_n(K)$ by $x \mapsto \begin{bmatrix} x \\ 0 \\ \vdots \end{bmatrix}$ and $\tau : K^n \to M_n(K)$ by $x\tau = xg\varphi$. Fix a basis $\{x_1, \ldots, x_n\}$ of K^n and find the first $1 \leq i \leq n$ such that $x_i(x_j\tau) \neq 0$ for all $1 \leq j \leq n$. Set $D := \begin{bmatrix} x_i(x_1\tau) \\ \vdots \\ x_i(x_n\tau) \end{bmatrix} \in M_n(K)$. Induce $\sigma : K \to K$ by $\alpha \mapsto [(\alpha I_n)\varphi]_{11}$, then return (D, σ).

We summarize how the steps in this algorithm perform the various stages of the proof of Skolem-Noether, given in [26, Chapter VIII].

Let I be the image of g. As I is a minimal right ideal, the image $J := I\varphi$ is also a minimal right ideal. Thus, there is an $1 \leq i \leq n$ such that $x_iJ \neq 0$. Since x_iJ is a simple right $M_n(K)$-module, it follows that $x_iJ \cong K^n$. As $\{x_1g, \ldots, x_ng\}$ is a K-basis of I, $\{x_1\tau, \ldots, x_n\tau\}$ is a K-basis of J and so $\{x_i(x_1\tau), \ldots, x_i(x_n\tau)\}$ is a basis of x_iJ. Thus D is an invertible matrix in $M_n(K)$. Finally, $(\alpha I_n)\varphi = (\alpha\sigma)I_n$, for $\alpha \in K$, defines a field automorphisms of K. It follows that $X\varphi = D^{-1}X^{\sigma}D$ for each $X \in M_n(K)$.

The algorithm searches over the set of all $1 \leq i, j \leq n$ and tests whether $x_i(x_j\tau) \neq 0$, a test which uses $O(n^2)$ field operations in K. The additional task of inducing σ uses $O(\dim_{\mathbb{Z}_p} K)$ operations in $\mathbb{Z}_p$. □

III.5.2 Constructive Recognition of Simple $*$-algebras

Let A be a finite simple $*$-algebra of characteristic p. There is an elementary yet highly useful observation that:

> every simple $*$-algebra is either simple as an algebra, or
> the sum of two simple algebras with the involution exchanging (III.13)
> the two simple factors.

We call the second case a simple $*$-algebra with *exchange involution*, that is, $(M_n(K) \oplus M_n(K), \bullet)$ where $(X,Y)^\bullet = (Y^t, X^t)$ for each $(X,Y) \in M_n(K) \oplus M_n(K)$. (Note, we could have treated this simple $*$-algebra as $\mathrm{Adj}(d)$ for a nondegenerate Hermitian bilinear map $d : K^{2n} \times K^{2n} \to K \oplus K$ as in [59, Corollary 4.11].)

When A is a simple algebra it is $*$-isomorphic to $\mathrm{Adj}(d)$ where $d : K^n \times K^n \to K$ is a nondegenerate Hermitian form (recall from Section III.2.3 that our meaning of Hermitian includes alternating and symmetric as well). The proof of this follows from [26, IX.10-11] and adapts well to an algorithm:

Theorem III.5.2. *Given a $*$-algebra $(A,*)$ with an effective (easily evaluated and inverted) ring isomorphism $\varphi : A \to M_n(K)$ for some field extension $K/\mathbb{Z}_p$, there is a deterministic algorithm using $O(n^4 + \dim_{\mathbb{Z}_p} K)$ algebraic operations which returns an effective $*$-isomorphism $\mu : (A,*) \to \mathrm{Adj}(d)$ for some nondegenerate Hermitian form $d : K^n \times K^n \to K$.*

Proof. Define the ring anti-automorphism $\bullet : X \mapsto ((X\varphi^{-1})^*)\varphi$, and the ring automorphism $\tau : X \mapsto (X^\bullet)^t$ on $M_n(K)$. Apply the algorithm of Proposition III.5.1 to τ to find $(D,\sigma) \in \mathrm{GL}_n(K) \rtimes \mathrm{Gal}(K/\mathbb{Z}_p)$ such that $X\tau = D^{-1}X^\sigma D$, for $X \in M_n(K)$. Define $d : K^n \times K^n \to K$ by $d(u,v) := uDv^{\sigma t}$, $u,v \in K^n$. Return $\mu : (A,*) \to \mathrm{Adj}(d)$ defined by $a\mu := (a\varphi, a\varphi^\bullet)$.

To see that the algorithm is correct, notice that φ is now a $*$-isomorphism from $(A,*)$ to $(M_n(K),\bullet)$. Furthermore, it is easy to check that $d(uX,v) = d(u,vX^\bullet)$ for each $X \in M_n(K)$ and $u,v \in K^n$. Thus $(M_n(K),\bullet)$ is $*$-isomorphic to $\mathrm{Adj}(d)$ via $X \mapsto (X,X^\bullet)$. Hence the return μ is a $*$-isomorphism.

For timing we note that the only computation is in apply the Skolem-Noether theorem which uses $O(n^4 + \dim_{\mathbb{Z}_p} K)$ algebraic operations. □

III.5.3 Computing the $*$-semisimple and $*$-radical Structure of $\mathrm{Adj}(b)$

We require the following generalization of the algorithm of [22] using effective homomorphism (Section III.2.2).

Theorem III.5.3. *There is a Las Vegas algorithm using which, given $R \subseteq \mathrm{End}\, V$, for a finite abelian p-group V, returns a set Ω of effective ring epimorphisms such that:*

(i) for each $\pi : R \to \mathrm{End}_K W$ in Ω, W is a K-vector space so that $\mathrm{End}_K W$ is a simple ring and $\ker \pi$ is a maximal ideal of R;

(ii) for each maximal ideal M of R there is a unique $\pi \in \Omega$ such that $M = \ker \pi$, and

(iii) if $x, y \in R$ such that $x\pi = y\pi$ then the representatives $x', y' \in R$ of the pullbacks to R of $x\pi$ and $y\pi$ given by the effective $\pi \in \Omega$, satisfy $x' \equiv y' \pmod{pR}$. Each evaluation or computation of preimages of π uses $O(\mathrm{rank}^3 R)$ operations.

The algorithms use $O(\mathrm{rank}^5 V)$ algebraic operations.

Proof. Pass to $\bar{R} := R/pR \subseteq \mathrm{End}\, \bar{V}$, $\bar{V} = V/pV$, and using [22, Corollary 1.5] compute a Wedderburn complement decomposition $\bar{R} = \bar{S} \oplus \mathrm{rad}\, \bar{R}$, where $\bar{S}$ is a subring of $\bar{R}$ and $\bar{S} \cong \bar{R}/\mathrm{rad}\, \bar{R}$ as rings (note that the direct decomposition is as vector spaces not necessarily as rings).

Now apply the MeatAxe, [21, 23], to $\bar{S}$ to find a decomposition of $\bar{V} := V/pV$ into a sum of irreducible $\bar{S}$-modules $\bar{V} = \bar{V}_1 \oplus \cdots \oplus \bar{V}_l$, and express $\bar{R}$ in a basis exhibiting this decomposition so that $\bar{R}$ is block lower triangular. Use an obvious greedy algorithm to find a minimal subset $\mathcal{W}$ of $\{\bar{V}_1, \ldots, \bar{V}_l\}$ such that $\bar{S}$ acts faithfully on $\langle \mathcal{W} \rangle$. Let $\tau : \bar{R} \to \bar{S}$ be the projection of $\bar{x} \in \bar{R}$ to $\bar{S}$ given by the vector space decomposition $\bar{R} = \bar{S} \oplus \mathrm{rad}\, \bar{R}$. For each $\bar{W} \in \mathcal{W}$, define $\pi_{\bar{W}} : R \to \mathrm{End}\, \bar{W}$ by $x\pi_{\bar{W}} := (x + pR)\tau|_{\bar{W}}$, for $x \in R$. The coset representative of the inverse image of $\bar{t} \in \mathrm{End}\, \bar{W}$ is created by extending $\bar{t}$ to V as $\bar{s}$ acting as 0 on each $\bar{V}_i \neq \bar{W}$, $1 \leq i \leq l$ (i.e., $\bar{s}$ has $\bar{t}$ in the $\bar{W}$ diagonal block of the matrix and 0's elsewhere), and then returning a coset representative of $\bar{s}\tau^{-1}$. Thus π is an effective homomorphism. The algorithm returns the set $\{\pi_{\bar{W}} : \bar{W} \in \mathcal{W}\}$.

First we validate the algorithm. If M is a maximal ideal of R then $R/M \cong \mathrm{End}_K W$ for some field extension $K/\mathbb{Z}_p$ and K-vector space W. Hence, R/M is a $\mathbb{Z}_p$-vector space and so $R/\mathrm{rad}\, R$ is a $\mathbb{Z}_p$-vector space, which proves that $pR \leq \mathrm{rad}\, R$ and $\mathrm{rad}\, \bar{R} = (\mathrm{rad}\, R)/pR$. Therefore, it suffices to find the projections of $\bar{R}$ onto its simple factors.

Since $R/pR \subseteq \operatorname{End} \bar{V}$ we can apply [22, Corollary 1.5]. Hence, we obtain a Wedderburn complement decomposition $\bar{R} = \bar{S} \oplus \operatorname{rad} \bar{R}$. As $\bar{S}$ is semisimple its action on $\bar{V}$ is completely reducible and the MeatAxe [21, 23] finds a decomposition $\bar{V} = \bar{V}_1 \oplus \cdots \oplus \bar{V}_l$ as above. For each $\bar{W} \in \mathcal{W}$, the map $\pi_{\bar{W}}$ is a ring homomorphism as τ is a ring homomorphism and $\bar{W}$ is an S-module. Since $\bar{W}$ is also irreducible it follows that $\bar{T} := R\pi_{\bar{W}} \leq \bar{S}$ is a simple subring of $\operatorname{End}_{\mathbb{Z}_p} \bar{W}$. The appropriate field of scalars is the center K of $\bar{T}$. Thus $\bar{W}$ is a K-vector space and $\pi_{\bar{W}}$ is a ring epimorphism onto $\operatorname{End}_K \bar{W}$ with kernel a maximal ideal of R, proving (i). Since $\mathcal{W}$ is minimal with respect to having $\bar{S}$ represented faithfully on $\langle \mathcal{W} \rangle$, the returned set of epimorphism has one epimorphism for each maximal ideal of R, thus proving (ii).

Finally, for (iii) we note that the representative matrix for the inverse image under $\pi \in \Omega$, of a point in $\operatorname{End}_K \bar{W}$ is trivial in every block except the block on which π is projected. Furthermore, to evaluate π, we compute $(x + pR)\tau$ which is done by writing $x + pR$ in the bases of the block decomposition given by $\{V_1, \ldots, V_l\}$ and uses $O(\dim^3 \bar{V})$ operations. To compute a preimage of $\bar{t}$ under π requires we write $\bar{t}$ in the basis $\mathcal{X}\tau$ where $\mathcal{X}$ is the fixed basis of R. Therefore the algorithm returns correctly.

For the timing, we note the significant tasks are computing the Wedderburn decomposition and the use of the MeatAxe, which use $O(\dim^5 \bar{V})$ and $O(\dim^4 \bar{V})$ algebraic operations, respectively [22, Corollary 1.4], [21, 23]. □

Corollary III.5.4. *Given a $*$-ring $(R, *)$ where $R \subseteq \operatorname{End} V$ for an abelian p-group V, there is a Las Vegas algorithm using $O(\operatorname{rank}^5 V)$ algebraic operations which returns a set $\Gamma = \{\gamma : (R, *) \to (T, *)\}$ of $*$-ring epimorphisms.*

(i) There is exactly one $\gamma \in \Gamma$ for each maximal $*$-ideal M of $(R, *)$, and $\ker \gamma = M$.

(ii) For each $\gamma : (R, *) \to (T, *) \in \Gamma$ either:

(a) $T = (M_m(K) \oplus M_m(K), \bullet)$ a simple $*$-algebra with exchange involution, or

(b) $T = \operatorname{Adj}(d)$ for a nondegenerate Hermitian form $d : K^m \times K^m \to K$.

(iii) If $x, y \in (R, *)$ such that $x\gamma = y\gamma$ then the representatives $x', y' \in (R, *)$ of the pullbacks to $(R, *)$ of $x\gamma$ and $y\gamma$ given by the effective $\gamma \in \Gamma$, satisfy $x' \equiv y' \pmod{pR}$.

Proof. We build Γ recursively.

Let $\Gamma = \emptyset$. Using the algorithm of Theorem III.5.3, compute a representative set of ring epimorphisms $\Omega = \{\pi : R \to \mathrm{End}_K W\}$ corresponding to the maximal ideals of R. Take $\pi \in \Omega$ and set $M := \ker \pi$. Test if $M^* = M$. If so then apply Theorem III.5.2 to construct an effective isomorphism $\varphi : \mathrm{End}_K W \to \mathrm{Adj}(d)$. Add φ to Γ and continue. Otherwise, find $\pi' \in \Omega$ where $\ker \pi' = M^*$. Then remove π' from Ω and define $\gamma : R \to (\mathrm{End}_K W \oplus \mathrm{End}_K W, \bullet)$ by $r\gamma := (r\pi, r\pi')$. Add γ to Γ and continue.

Theorem III.5.3 and (III.13) prove that the algorithm returns correctly and the number of operations is dominated by the algorithm for Theorem III.5.3. □

III.5.4 Self-adjoint Pullbacks

We need an improvement over Corollary III.5.4.(*iii*) which allows us to pull back elements which are *self-adjoint* in the $*$-simple factors to *self-adjoint* elements of our $*$-ring.

Lemma III.5.5. *Assume a discrete log oracle for $\mathbb{Z}_p$. Let $\gamma : (R, *) \to (T, *)$ be an effective epimorphism and R a ring of characteristic a power of p. Given $t \in T$ such that $t^* = t$, there is an $O(\mathrm{rank}^3 R)$ algorithm which finds an $s \in R$ such that $s\gamma = t$ and $s^* = s$.*

Proof. Set $M := \ker \gamma$ and compute bases for $\mathfrak{H}(M, *)$, $\mathfrak{H}(R, *)$, and the abelian group $J := \mathfrak{H}(R, *)/\mathfrak{H}(M, *)$. The map $\iota : \mathfrak{H}(M, *) + x \mapsto M + x$ embeds J isomorphically into $\mathfrak{H}(R/M, *)$. Fix a basis $\mathcal{X}$ for J and note that images and inverse images of ι are completely determined by the basis and require $O(\mathrm{rank}^3 \mathcal{H}(R/M, *))$ operations to compute. Therefore, ι is an effective isomorphism.

Now take $t \in \mathfrak{H}(T, *)$. As γ is effective, compute a coset representative $r \in R$ of the preimage $t\gamma^{-1}$, that is, $t = r\gamma$. Hence, $M + r \in \mathfrak{H}(R/M, *)$ and so $(M + r)\iota^{-1} \in \mathfrak{H}(R, *)/\mathfrak{H}(M, *)$. As ι^{-1} is effective we have $(M + r)\iota^{-1} = \mathcal{H}(M, *) + s$ for some $s \in \mathfrak{H}(R, *)$. Thus, $s^* = s$ and $s\gamma = r\gamma = t$.

The timing of the algorithm is dominated by computing bases for the various abelian subgroups and quotient groups. This uses $O(\mathrm{rank}^3 R)$ algebraic operations and a discrete log oracle for $\mathbb{Z}_p$ (cf. Section III.2.2). □

III.5.5 Finding Self-adjoint Frames

Let $(R, *)$ be a finite ring with involution $*$. We outline how to find a self-adjoint frame of $\mathfrak{H}(R, *) = \{r \in R : r^* = r\}$. To do this we require the following lemma:

Lemma III.5.6 (Lifting idempotents). *Suppose that $e \in R$ such that $e^2 - e \in \operatorname{rad} R$. Then there is an $n \in \mathbb{N}$ such that $(e^2 - e)^n = 0$, and setting*

$$\hat{e} := e^n \sum_{j=0}^{n-1} \binom{2n-1}{j} e^{n-1-j}(1-e)^j \tag{III.14}$$

it follows that:

(i) $\hat{e}^2 = \hat{e}$,

(ii) $e \equiv \hat{e} \pmod{\operatorname{rad} R}$,

(iii) $\widehat{1-e} = 1 - \hat{e}$, *and*

(iv) If $*$ is an involution on R and $e^* = e$ then $\hat{e}^* = \hat{e}$.

Proof. (i) through (iii) can be verified directly, compare [10, (6.7)]. For (iv) notice that $\hat{e}$ is a polynomial in $\mathbb{Z}[e]$. As $1^* = 1$ and $e^* = e$ it follows that $\hat{e}^* = \hat{e}$. □

Proposition III.5.7. *(i) Given* $\operatorname{Adj}(d)$ *for a nondegenerate Hermitian form $d : K^n \times K^n \to K$, there is a deterministic algorithm using $O(n^3)$ operations in K which finds a frame of* $\operatorname{Sym}(d)$.

(ii) If $(M_n(K) \oplus M_n(K), \bullet)$ a simple $*$-ring with exchange involution, then $\mathcal{E} = \{(E_{ii}, E_{ii}) : 1 \leq i \leq n\}$ is a frame of $\mathfrak{H}(M_n(K) \oplus M_n(K), \bullet)$.

Proof. (i). By Corollary III.4.3 we know that the set of frames of $\operatorname{Sym}(d)$ is in bijection with the fully refined $\perp$-decompositions of d. As d is a bilinear form the fully refined $\perp$-decomposition of d are parameterized by standard bases; i.e. a bases $\mathcal{X}$ of d such that for each $x \in \mathcal{X}$ there is a unique $y \in \mathcal{X}$ such that $d(x, y) \neq 0$. Finding a standard basis of d can be done by standard linear algebra at a cost of $O(n^3)$ operations in K. Given a standard basis $\mathcal{X}$ of d, create the fully refined $\perp$-decomposition $\mathcal{V} := \{\langle x \rangle : x \in \mathcal{X}\}$ and compute associated projection idempotents $\mathcal{E} := \mathcal{E}(\mathcal{V})$. This is the return of the algorithm.

(ii). This is obvious from Section III.5.2. □

Theorem III.5.8. *Given a $*$-ring $(R, *)$ with $R \leq \operatorname{End} V$, V an abelian p-group, there is a Las Vegas algorithm using $O(\operatorname{rank}^6 R)$ algebraic operations which finds a frame of $\mathfrak{H}(R, *)$.*

Proof. Using Corollary III.5.4 we compute a set Γ of $*$-epimorphisms onto simple $*$-algebras, one for each maximal $*$-ideal of $(R,*)$. Given $\gamma : (R,*) \to (T,*) \in \Gamma$, use Proposition III.5.7 to compute a self-adjoint frame $\mathcal{E}_\gamma$ of $(T,*)$. By Corollary III.5.4.(*iii*), we pullback $\mathcal{E}_\gamma$ to a set

$$\mathcal{F}_\gamma = \{e + pR : e^2 \equiv e \pmod{pR}, e^* \equiv e \pmod{pR}\}$$

such that $\mathcal{F}$ maps to $\mathcal{E}$ via $e + pR \mapsto e\gamma + pR$. Next, using Lemma III.5.5, choose coset representatives $f \in R$ for each $e + pR \in \mathcal{F}$ such that $f^* = f$ so that now:

$$\mathcal{F}'_\gamma = \{f + pR : f^2 \equiv f \pmod{pR}, f^* = f\}$$

and $\mathcal{F}_\gamma\gamma = \mathcal{E}_\gamma$. Apply Lemma III.5.6 to the members of $\mathcal{F}_\gamma$ to create $\widehat{\mathcal{E}} = \{\hat{f} : f \in \mathcal{F}_\gamma\}$, which is a set of pairwise orthogonal self-adjoint primitive idempotents.

Since $\mathcal{F}_\gamma$ projects onto a unique $*$-simple factor of $(R,*)$, and there is exactly one $\gamma \in \Gamma$ for each maximal $*$-ideal of $(R,*)$, it follows that $\mathcal{F} := \sqcup_{\gamma\in\Gamma}\mathcal{F}_\gamma$ is a self-adjoint frame of $(R,*)$.

Now we consider the number of operations. By using Corollary III.5.4 we use $O(\operatorname{rank}^5 V)$ algebraic operations. Now fix $\gamma : (R,*) \to (T_\gamma,*) \in \Gamma$ with $T_\gamma = \operatorname{End}_K W_\gamma$. Proposition III.5.7 uses $O(\operatorname{rank}^3 W_\gamma)$ operations. Since $\sum_{\gamma\in\Gamma} \operatorname{rank} W_\gamma$ is at most $\operatorname{rank} V$, it follows that this stage takes at most $O(\operatorname{rank}^3 V)$ operations.

Next, the computation applies Lemma III.5.5 which uses $O(\operatorname{rank}^3 T_\gamma)$ operations. Since the bases computed in Lemma III.5.5 can be reused for each application with respect to a fixed γ, it follows that the total cost of this stage is $O\left(\sum_{\gamma\in\Gamma} \operatorname{rank}^3 T_\gamma\right) = O\left(\sum_{\gamma\in\Gamma} \operatorname{rank}^6 W_\gamma\right) = O(\operatorname{rank}^6 V)$ operations. □

III.6 Proof of Theorem III.1.1

Given a finite p-group P of class 2, compute bases for $P/Z(P)$ and P' and compute a structure constant representation of $b := \mathsf{Bi}(P, Z(P))$ (which is straightforward from the definitions in Section III.3.1 and (III.3)).

Next, compute a basis for $\operatorname{Adj}(b)$ (Section III.4.3). Apply Theorem III.5.8 to find a self-adjoint frame $\mathcal{E}$ of $\operatorname{Adj}(b)$. Induce a fully refined $\perp$-decomposition $\mathcal{V} = \{(P/Z(P))e : e \in \mathcal{E}\}$ of b (cf. Corollary III.4.3).

Apply Corollary III.3.4 to produce a fully refined central decomposition of P.

Since $\operatorname{rank}\mathrm{Adj}(b) \leq \log_p^2[P : Z(P)]^2 \leq \log^2[P : P']$, the total number of algebraic operations is at most $O(\log^6[P : P'])$. □

III.7 Closing Remarks.

III.7.1 Discrete Logs are Required

The *discrete log problem* for $\mathbb{Z}_p$, is: given two elements x, y in an elementary abelian p-group, determine if $y \in \langle x \rangle$ [20, Section 7.1]. That is, can we decide if $\langle x, y \rangle$ is isomorphic to $\mathbb{Z}_p$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

This problem occurs in many fields of computational mathematics. It has no known polynomial-time solution and is generally regarded as a hard problem. A stronger version of the discrete log problem asks further for an exponent e such that $x^e = y$ and this is the version required in Section III.2.2 to use [39, Theorem 8.3] for large primes.

Since the abelian centrally indecomposable p-groups are the cyclic p-groups, we cannot test if an abelian p-group is centrally indecomposable without solving the discrete log problem, i.e.: determining if $\langle x, y \rangle$ is $\mathbb{Z}_p$ or $\mathbb{Z}_p \times \mathbb{Z}_p$. For p-groups of general class the situation does not improve:

Proposition III.7.1. *The discrete log problem for $\mathbb{Z}_p$ is polynomial-time reducible to testing if a central decomposition of finite p-group of class 2 is fully refined.*

Proof. Let $V = \langle x, y \rangle$ be an instance of the discrete log problem for $\mathbb{Z}_p$. Set $P := p^{1+2} \times V$, where p^{1+2} is the extraspecial p-group of order p^3 and exponent p, in particular, p^{1+2} is centrally indecomposable of class 2.

Evidently P is a p-group of class 2 and $\mathcal{H} = \{p^{1+2} \times 1, 1 \times V\}$ is a central decomposition of P. Furthermore, $\mathcal{H}$ is fully refined if, and only if, $V = \langle x, y \rangle$ is cyclic. □

A version of Proposition III.7.1 for p-groups P of any class c shows that there exists a centrally indecomposable p-group of any class c.

III.7.2 Deterministic Version

Suppose that p is small, for instance bounded by $\log^c |P|$. In this case the discrete log problem can be solved by brute force. Furthermore, by replacing the Las Vegas method of [22] with the original deterministic methods of [24] in the algorithm of Theorem III.5.3, we can avoid all use of nondeterministic methods.

III.7.3 A Faster Las Vegas Algorithm

Suppose that we are only interested in testing if a p-group P of class 2 is centrally indecomposable. By Theorem III.3.2, the key step is to prove that $\mathsf{Bi}(P, Z(P))$ is $\perp$-indecomposable. This means that we must prove that $\mathrm{Sym}(b)/(\mathrm{Sym}(b) \cap \mathrm{rad}\,\mathrm{Adj}(b))$ is a field. This can be done without polynomial factorization as we must only verify that various polynomials are irreducible (see the algorithm of [24, Corollary 5.2]). Testing irreducibility can be done deterministically [57, Theorem 14.37]. The use of discrete log oracles could also be avoided in this constrained setting as we use this only in our pullback algorithm Lemma III.5.5. So it appears possible that a deterministic method can prove that a p-group of class 2 is centrally indecomposable. (Note, the same is impossible for abelian p-groups by Section III.7.1.)

If we can test if a p-group of class 2 is centrally indecomposable in a deterministic and efficient manner then there is an alternative approach to proving Theorem III.1.1, with discrete logs reserved only to determine if abelian central factors are centrally indecomposable. The algorithm would replace Theorem III.5.8 by a random search for self-adjoint idempotents in $\mathrm{Sym}(b)$. Unfortunately, $\mathrm{Sym}(b)$ is a (quadratic) Jordan algebra, and there are presently no known estimates on the the number of zero-divisors in $\mathrm{Sym}(b)$ and therefore finding idempotents at random may not be easy. These questions are being investigated.

III.7.4 Parallel Implementation

The algorithm described here is sequential. Recent investigations have revealed alternative parallel algorithms for associative algebras, and the algorithms added here can be modified to a parallel setting [64].

III.7.5 Finding Orbits of Central Decompositions

In [59], the action of the automorphism group of a p-group P of class 2 and exponent p was studied. Though not presented in detail, it is clear that the methods here can be used to find a representative fully refined central decomposition for each $C_{\mathrm{Aut}\,P}(P')$-orbit as described in [59, Corollary 5.23.(iii)]. The necessary step is to choose an orthogonal basis in Proposition III.5.7 with the desired address in the sense of [59, Definition 5.1].

CHAPTER IV

FINDING DIRECT PRODUCT DECOMPOSITIONS

IV.1 Introduction

A polynomial-time algorithm is provided which, given a group of permutations, matrices, or a polycyclic presentation; returns a Remak decomposition of the group: a fully refined direct decomposition. The method uses group varieties to reduce to the case of p-groups of class 2. Bilinear and ring theory methods are employed there to complete the process.

One of the most elementary methods to create a group is through a direct product of other groups. This immediately suggests the problem of decomposing a group into a direct product of nontrivial subgroups or proving that no such decomposition exists. By the classical Krull-Remak-Schmidt theorem, finding one direct decomposition with maximal size is sufficient to understand all other direct decompositions, as any two maximal direct decompositions are equivalent up to an automorphism of the group. However, this does not resolve the problem of finding even one proper direct factor, should one exist. For finite groups G this is a finite problem, but surprisingly algorithms to accomplish this task use $|G|^{\log|G|+O(1)}$ steps, see Section IV.6.1.[1] Thus such methods are impractical and here we present a substantial improvement as seen in the following special case of our main theorem:

Theorem IV.1.1. *There is a polynomial-time algorithm which, given $G = \langle T \rangle \leq S_n$, returns a direct decomposition of G into nontrivial subgroups: $G = H_1 \times \cdots \times H_\ell$, with ℓ maximal.*

As every group G can be represented as a permutation group of degree $|G|$, this leads to a polynomial-time, in $|G|$, algorithm to find a direct decomposition of any group. With a careful analysis we prove that in fact such an algorithm is nearly optimal:

[1] In this work, all logs are with base 2.

Corollary IV.1.2. *There is a nearly linear-time, $O^{\sim}(N)$, algorithm which, given the multiplication table of a group G of order N, returns a direct decomposition into nontrivial subgroups $G = H_1 \times \cdots \times H_\ell$, with ℓ maximal.*

We have not pursued every notable optimization in the algorithm of Theorem IV.1.1. However, much of that algorithm adapts to matrix groups and groups given by polycyclic presentations. To explain this some vocabulary is required.

Groups and subgroups are given by sets of generators. To decompose a group into a direct product of nontrivial subgroups it suffices to provide a set of generating sets for the members of the *direct decomposition.* A group G is *directly indecomposable* if its only direct decomposition is $\{G\}$ – owing to the fact that we do not allow 1 as a direct factor. A *Remak decomposition* is a direct decomposition consisting of directly indecomposable subgroups.

We let $\mathbb{G}_n$ denote a class of groups suitable for computation, together with a list of hypothesized routines available for members of $\mathbb{G}_n$ which are described in Section IV.2.2. If $G = \langle S \rangle \in \mathbb{G}_n$ then G is input by $O(|S|n)$ bits of data, and the algorithm's complexity is measured in terms of $|S|n + \log|G|$. In some domains $\mathbb{G}_n$, there are no efficient deterministic algorithms for some of the hypothesized routines, but often there are Las Vegas algorithms or the inherent obstacles appear infrequently in practical settings. Section IV.2.2 expands on these issues. We can now present our main theorem:

Theorem IV.1.3. *There is a deterministic polynomial time algorithm which, given a group $G \in \mathbb{G}_n$, returns a Remak decomposition of G.*

IV.1.1 Outline of the Algorithm of Theorem IV.1.3

The algorithm works recursively through the following characteristic series of the given finite group $G \neq 1$:

$$1 \leq \zeta_1(G) \leq \zeta_2(G) \leq \cdots \leq O_{\mathfrak{S}}(G) \leq S(G) \leq G, \tag{IV.1}$$

where $\zeta_i(G)$ represents the upper central series of G, $i \in \mathbb{Z}^+$, $O_{\mathfrak{S}}(G)$ is the solvable radical, and $S(G)/O_{\mathfrak{S}}(G) = \mathrm{soc}(G/O_{\mathfrak{S}}(G))$ is the pullback of the socle of $G/O_{\mathfrak{S}}(G)$. Using this series we describe the stages of the algorithm.

- **Case:** $G > O_{\mathfrak{S}}(G) = 1$. This case is settled in Section IV.5.4, utilizing the unique Remak decomposition of the socle of G to build the unique Remak decomposition of G.

- **Case:** $G = O_{\mathfrak{S}}(G) > 1$. This case is settled in Sections IV.5.1- IV.5.3 and breaks into five subcases.

  - **Subcase:** $G > \zeta_1(G) = 1$. This case is settled in Theorem IV.5.4, reducing to the case of p-groups by means of a Sylow system for the group.

  - **Subcase:** $G = \zeta_1(G) > 1$. This case is settled in Section IV.2.3. Here G is a direct product of cyclic groups of prime power order. To find such a decomposition is routine but in general relies on factoring and discrete logs.

  - **Subcase:** $G > \zeta_2(G) = \zeta_1(G) > 1$. This is settled in Section IV.5.3, using a recursive call to find a Remak decomposition of $G/\zeta_1(G)$. Using the algorithm for abelian groups, the algorithm lifts and reduces that decomposition to a Remak decomposition of G.

  - **Subcase:** $G = \zeta_2(G) > \zeta_1(G) > 1$. This is settled in Sections IV.4.9 and IV.5.1. This stage of the algorithm uses the bilinear map of commutation of the group G and the structure of a certain commutative ring. This translates the problem to one of factoring polynomials over finite fields.

  - **Subcase:** $G > \zeta_2(G) > \zeta_1(G) > 1$. This is settled in Sections IV.5.2 and IV.5.3, using a recursive call to find a Remak decomposition of $G/\zeta_1(G)$. Using the algorithm for nilpotent groups of class 2, the algorithm lifts and reduces that decomposition to a Remak decomposition of G.

- **Case:** $G > O_{\mathfrak{S}}(G) > 1$. This is settled in Section IV.5.5 making a recursive call to find a Remak decomposition of $G/O_{\mathfrak{S}}(G)$. Then using the algorithm for solvable groups, the algorithm lifts and reduces that decomposition to a Remak decomposition of G.

The recursive calls in the third and fifth subcases, and the final case, use the same framework. Indeed, the algorithm handles them uniformly through the use of group varieties. That is carried out in Section IV.4.1.

IV.2 Background

IV.2.1 Notation

Unless otherwise obvious, we assume all groups, rings, and modules are finite. We use $A - B$ for the complement of $A \cap B$ in A, and $A \sqcup B$ denotes a union of disjoint sets. In general p denotes a prime.

Groups, rings, and modules will be denoted by capital Roman letters, i.e.: G, H, etc. Sets of subgroups, subrings, and submodules will be denoted with calligraphy, for instance, $\mathcal{H}$, $\mathcal{X}$, etc. Varieties will be denoted in Gothic letters, i.e: $\mathfrak{V}$, $\mathfrak{N}$, etc.

The direct product of groups A and B is denoted by $A \times B$, whereas the direct product of rings or modules A and B is denoted by $A \oplus B$. Given a set $\mathcal{H}$ of groups we let $\prod_{H \in \mathcal{H}} H$ denote the direct product of the members of $\mathcal{H}$. *Given a set $\mathcal{H}$ of normal subgroups of G, we use only the notation $\langle \mathcal{H} \rangle := \langle H : H \in \mathcal{H} \rangle$ for the product of the members in $\mathcal{H}$ and thus avoid confusion with the notation $\prod_{H \in \mathcal{H}} H$.* As we contend with many notions of "product" we take care to include the adjective "direct" whenever appropriate.

Given a group G, our convention is that $g^h := h^{-1}gh$ and $[g,h] = g^{-1}g^h$, for $g, h \in G$. Also, $[H,K] := \langle [h,k] : h \in H, k \in K \rangle$ and $C_H(K) := \{h \in H : [h,K] = 1\}$, for $H, K \leq G$. We make repeated implicit use of the following: given normal subgroups A, B, C of G: $[A,B] \trianglelefteq G$, $[A,B] \leq A \cap B$, $[A,B] = [B,A]$, and $[A,BC] = [A,B][A,C]$.

Set $\zeta_1(G) := C_G(1)$ and inductively define $\zeta_{i+1}(G) \geq \zeta_i(G)$ so that $\zeta_{i+1}(G)/\zeta_i(G) = \zeta_1(G/\zeta_i(G))$, $i \in \mathbb{Z}^+$; that is the usual *upper central series* of G. We say that G is *nilpotent of class c* if $\zeta_c(G) = G > \zeta_{c-1}(G)$.

The *derived series* begins with $G^{(0)} := G$ and recursively $G^{(i+1)} = [G^{(i)}, G^{(i)}]$, $i \in \mathbb{N}$. We call G *solvable of derived length d* if $G^{(d-1)} > G^{(d)} = 1$. The *solvable radical* of G, $O_{\mathfrak{S}}(G)$, is the largest solvable normal subgroup of G.

The *socle* of G, $\operatorname{soc} G$, is the subgroup generated by all minimal normal subgroups of G.

IV.2.2 $\mathbb{G}_n$ and its Hypothesized Routines

For $\mathbb{G}_n$ we have in mind permutation groups, matrix groups, and groups given by polycyclic presentations. More generally, $\mathbb{G}_n$ is a class of groups for which:

(i) given $G = \langle S \rangle \in \mathbb{G}_n$ is input using $O(|S|n)$ bits,

(ii) if $H = \langle T \rangle \leq G$, $G \in \mathbb{G}_n$, then $H \in \mathbb{G}_n$, and

(iii) the list of hypothesized routines (IV.2.3-IV.2.12) below, are available for members of $\mathbb{G}_n$.

The complexity of all algorithms is with respect to $|S|n+\log|G|$. The additional $\log|G|$ term allows for recursion through chains of subgroups of G (which have length at most $\log|G|$). In the examples of $\mathbb{G}_n$ above, this is implicit since $\log|G| \in O^{\sim}(n)$. Though we discuss current implementation and complexities for (IV.2.3-IV.2.12), these algorithm can be taken as oracles in that the algorithm of Theorem IV.1.3 is a deterministic polynomial-time reduction to these hypothesized routines. In the context of permutation groups, (IV.2.3-IV.2.12) has a deterministic polynomial-time solution, which leads to Theorem IV.1.1.

Quotients of Permutation Groups: $\mathbb{G}_n = \text{QPERM}_n$. Here $\mathbf{G} \in \text{QPERM}_n$ if, and only if, $\mathbf{G} = G/M$ where $G = \langle S \rangle \leq \text{Sym}(\Omega)$, $|\Omega| = n$, and $M = \langle T^G \rangle \trianglelefteq G$.

Remark IV.2.1. *Theorem IV.1.1 references permutation groups but the algorithm applies also to quotients of permutation groups. In fact, it* requires *this generality (actually the quotients in IV.2.7). But a benefit of this requirement is that it allows for larger families of groups. For example, extraspecial 2-groups of order 2^{1+2m} have no faithful permutation representations of degree less than 2^m. However, such groups are obvious quotients of a permutation group of degree $8m$.*

"Proto" Matrix groups: $\mathbb{G}_n = \text{PRMAT}(d, q)$ with $n = d^2 \log q$, and q a power of a known prime p. Here $\mathbf{G} \in \text{PRMAT}(d, q)$ if, and only if, $\mathbf{G} = G/\zeta_i(G)$ for some $i \in \mathbb{N}$ or $\mathbf{G} = G/O_{\mathfrak{S}}(G)$, where $G = \langle S \rangle \leq \text{GL}(V)$, V a d dimensional vector space over $\mathbb{F}_q$.

Remark IV.2.2. *Working with general quotients of matrix groups would seem the appropriate context here; however, algorithms for such general settings do not exist. As they are not required, this generality suffices, and indeed, it this generality alone that is required for permutation group setting.*

Polycyclic groups: $\mathbb{G}_n = \text{PC}(p_1, \ldots, p_d)$ with $n = \binom{d+1}{3} \log \max\{p_1, \ldots, p_d\}$, and p_i not necessarily distinct primes, for $1 \leq i \leq d$. Here

$$\begin{aligned} G = \langle x_1, \ldots, x_d | x_i^{p_i} = x_{i+1}^{e_{i(i+1)}} \cdots x_d^{e_{id}}, 0 \leq e_{ij} < p_j, \\ x_i^{x_j} = x_{i+1}^{c_{i(i+1)}^{(j)}} \cdots x_d^{c_{id}^{(j)}}, 0 \leq c_{ik}^{(j)} < p_k, 1 \leq i < j \leq d \rangle, \end{aligned} \tag{IV.2}$$

It follows that every $g \in G$ can be written as

$$g = x_1^{g_1} \cdots x_d^{g_d}, \qquad 0 \leq g_i \leq p_i, 1 \leq i \leq d. \tag{IV.3}$$

Hypothesized Routines.

IV.2.3. *Given $x, y \in G = \langle S \rangle \in \mathbb{G}_n$, compute xy, x^{-1}, and test if $x = y$.*

IV.2.4. *Given $G = \langle S \rangle \in \mathbb{G}_n$, return $|G|$.*

IV.2.5. *Given $H = \langle T \rangle \leq G = \langle S \rangle \in \mathbb{G}_n$ and $x \in G$, test if $x \in H$. If $x \in H$ then also return x as a word (or straight line program) in T.*

The routines (IV.2.3-IV.2.5) are interrelated. For QPERM_n and $\text{PRMAT}(d, q)$ both xy and x^{-1} can be computed efficiently by obvious means. To test $x = y$ requires testing equality of cosets in some instances, and is thus essentially equivalent to (IV.2.4) and (IV.2.5).

Deterministic polynomial-time algorithms for (IV.2.3-IV.2.5) for QPERM are in [29, P1]. For $\text{PRMAT}(d, q)$, these problems presently require many of the methods of the ongoing matrix group project, [46]. Many of those methods are nondeterministic Monte Carlo and Las Vegas routines, and also require large integer factorization and discrete logs (see [57, Chapter 19, p. 569]) – though in practice these are reportedly of little concern.[2] Deterministic polynomial time algorithms are known for restricted classes of matrix groups including solvable groups involving only small primes [38, Theorem 3.2] and other generalizations as in [41].

For groups in PC, none of these problems have polynomial-time solutions at present. The most popular method to test equality is through (IV.3). However, the known methods to write words $w(x_1, \ldots, x_d)$ as a words of the form (IV.3) have exponential complexity, even in the average case [35]. An improvement was given for p-groups in [36], but the complexity of that algorithm is not established. However, the domain PC has a great deal of successful uses in practice. and is often the easiest method to input solvable groups. In this case the algorithm of Theorem IV.1.3 will not be polynomial-time but rather will use a polynomial number of group multiplications.

IV.2.6. *Given $|G|$ for $G = \langle S \rangle \in \mathbb{G}_n$, return the primary factorization of $|G|$.*

For $G \in \text{QPERM}_n$, the prime divisors of $|G|$ are at most n and so the factorization is always easy. For $G \in \text{PC}(p_1, \ldots, p_d)$, following (IV.3), $|G|$ divides $p_1 \cdots p_d$. To factor $|G|$ is

[2] Thanks to C.R. Leedham-Green for communicating the state of these at Groups and Computation V.

straight forward as the primes $\{p_1, \ldots, p_d\}$ are known. If $G \in \text{PRMAT}(d, q)$ this routine can involve the difficult problem of factoring $q^i - 1$ for various $1 \leq i \leq d$.

IV.2.7. *Given $G = \langle S \rangle \in \mathbb{G}_n$ and $M \in \{\zeta_1(G), \zeta_2(G), \ldots, O_{\mathfrak{S}}(G)\}$, return $H = \langle T \rangle \in \mathbb{G}_{f(n)}$ and an isomorphism $\varphi : G/M \to H$, where $f(n)$ is a polynomial in n independent of G.*

For the domains QPERM_n, $\text{PRMAT}(d, q)$, and $\text{PC}(p_1, \ldots, p_d)$, this routine is trivial, with $f(n) = n$, as these classes are closed to quotients by these subgroups. If we consider simply the class of permutation groups (without quotients) then it is not even clear that quotients of this form have faithful permutation representations of degree a polynomial in n.

IV.2.8. *Given $M = \langle T^G \rangle \trianglelefteq G = \langle S \rangle \in \mathbb{G}_n$, return $C_G(M)$. Consequently, given $G = \langle S \rangle \in \mathbb{G}_n$ and $i \in \mathbb{Z}^+$, return the i-th upper central series term $\zeta_i(G)$.*

For QPERM see [29, P7]. This presently depends upon the classification of finite simple groups. For PRMAT we have not found a treatment of this problem; however, for solvable matrix groups this is solved in [38, Theorem 3.2.(8)] under the assumption that all primes in the order of the group are small. That condition can be removed by hypothesizing routines for integer factorization and discrete logs, and it is possible that methods from the matrix group project apply for the general matrix group setting. For PC see [20, Section 8.8.2].

IV.2.9. *Given $G = \langle S \rangle \in \mathbb{G}_n$, return the solvable radical: $O_{\mathfrak{S}}(G)$.*

For QPERM see [29, P29]. As the groups in PC are solvable, there $G = O_{\mathfrak{S}}(G)$ so the problem is trivial. For PRMAT this problem has long been studied as part of the matrix group project, but has not been resolved in general, though in many situations this can be computed; see [46, Section 1.3].

IV.2.10. *Given $G = \langle S \rangle \in \mathbb{G}_n$ with $O_{\mathfrak{S}}(G) = 1$, return a minimal normal subgroup of G. Consequently, also find the socle of G: $\operatorname{soc} G$.*

See [29] for QPERM and [46, Section 1.3] for PRMAT. For groups $G > 1$ in PC, $O_{\mathfrak{S}}(G) = G > 1$ so this problem is not applicable..

IV.2.11. *Given a solvable group $G = \langle S \rangle \in \mathbb{G}_n$, return a Sylow system $\mathcal{P} = \{P_1, \ldots, P_t\}$ of G: P_i a Sylow subgroup of G for $1 \leq i \leq t$, $G = P_1 \cdots P_t$, and $P_i P_j = P_j P_i$ for $1 \leq i, j \leq t$.*

For details on the existence and uniqueness of Sylow systems see [11, Section I.4].

For PC see [13], for QPERM [29, P13], and for PRMAT [31].

IV.2.12. *Given $H = \langle T \rangle \leq G = \langle S \rangle \in \mathbb{G}_n$, return $K \leq G$ such that $G = H \times K$, or prove that no such K exists.*

(IV.2.12) was solved independently by E. M. Luks and C.R.B. Wright in 2004 in a back to back lectures given at the University of Oregon. Earlier Holt and Luks independently produced polynomial-time algorithms to find a complement K to H in G, though possibly not a direct complement; see for instance [30, Proposition 3.8]. Their methods are essentially the same and can be viewed as applications of 1-cohomology. Coupled with the (IV.2.8), this leads to:

Theorem IV.2.13 (Luks,Wright; 2004 (unpublished)). *Given a method to find general complements and solutions to (IV.2.5) and (IV.2.8) in $\mathbb{G}_n$, there is a deterministic polynomial time algorithm which solves (IV.2.12).*

Proof. Let $G \in \mathbb{G}_n$.

Algorithm. Use (IV.2.5) to determine if $H \trianglelefteq G$. If not, then report that H is not a direct factor of G. Otherwise, use (IV.2.8) to compute $C_G(H)$ and $Z(H)$. Use (IV.2.5) to test if $G \leq HC_G(H)$ and if not, report that H is not a direct factor of G. Next, find a general complement $K \leq C_G(H)$ to $Z(H)$, if one exists, and return K; otherwise, report that H is not a direct factor of G.

Correctness. Evidently, $G = H \times J$, for some $J \leq G$, requires that $H \trianglelefteq G$, $C_G(H) = Z(H) \times J$, and $G = HC_G(H)$. Therefore, a negative return is given only if H is not a direct factor.

Now suppose that H is a direct factor of G. Then every direct complement of H lies in $C_G(H)$. Furthermore, a direct complement of H is also a direct complement of $Z(H)$ in $C_G(H)$. As $Z(H)$ is central in G, so also in $C_G(H)$, a complement $K \leq C_G(H)$ to $Z(H)$ is a direct complement to $Z(H)$. Furthermore, $H \cap K \leq H \cap C_G(H) = Z(H)$, so $H \cap K \leq Z(H) \cap K = 1$. Also, $HK \geq HZ(H)K = HC_G(H) = G$. Finally, $[H, K] = 1$ so $G = H \times K$.

Timing. The algorithm makes a bounded number of calls to assumed routines. □

Remark IV.2.14. *For clarity we point out that the only computational domains considered here which have deterministic polynomial time algorithms for each of the hypothesized routines are quotients of permutation groups and solvable matrix groups whose orders involves small primes.*

IV.2.3 Abelian p-groups, Bases, Effective Homomorphisms, and Solving Systems of Equations

A *basis* of a finite abelian p-group V is a subset $\mathcal{X}$ of V such that $V = \bigoplus_{x\in\mathcal{X}}\langle x\rangle$. Every basis of V gives a natural isomorphism to $\mathbb{Z}_{p^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{e_s}}$ for $e_1 \leq \cdots \leq e_s \in \mathbb{Z}^+$. Operating in the latter representation is preferable to V's original representation and we assume all abelian groups are handled in this way. Each endomorphism f of V can be represented by an integer matrix $F = [F_{ij}]$ such that $p^{e_j - e_i} | F_{ij}$, $1 \leq i \leq j \leq s$, and furthermore, every such matrix induces an endomorphism of V (with respect to $\mathcal{X}$) [19, Theorem 3.3].

In various places we apply homomorphisms and isomorphisms between finite abelian p-groups, rings, and algebras. We say a homomorphism is *effective* when it can be evaluated efficiently – for instance with the same cost as matrix multiplication – and a coset representative for the preimage of an element in the codomain can also be found efficiently. This means that effective isomorphisms are easily evaluated and inverted.

Suppose we have a system of $\mathbb{Z}_{p^e}$-linear equations with solutions in a $\mathbb{Z}_{p^e}$-module V. There are efficient deterministic methods to find a basis of the solution space of the system [39, Theorem 8.3]; however, it is essential to note that for a large p, this process assumes a discrete log oracle mod p. However, we have elected to assume (IV.2.5) which incapsulates this problem for large p and so we do not make explicit mention of the discrete log problem below.

Proposition IV.2.15. *There is a deterministic polynomial time algorithm which, given an abelian group in $\mathbb{G}_n$, returns a Remak decomposition of the group.*

Proof. Let $G \in \mathbb{G}_n$ be abelian.

Algorithm. Use (IV.2.4) and (IV.2.6) to compute and factor $N := |G|$. For each prime $p|N$, let m_p be the p' part of N, and set $G_p := G^{m_p}$. Use [39, Theorem 8.3] to find a basis $\mathcal{X}_p$ for G_p. Return $\bigsqcup_{p|N} \{\langle x\rangle : x \in \mathcal{X}_p\}$.

Correctness. The subgroups G_p are the p-primary components of G and so [39, Theorem 8.3] applies. Furthermore, $G = \prod_{p|N}\langle\mathcal{X}_p\rangle$, and $\langle\mathcal{X}\rangle = \prod_{x\in\mathcal{X}}\langle x\rangle$ by the definition of a basis.

Timing. The algorithm applies deterministic polynomial time methods. As $\log|G| \leq n$, the number of applications of these routines is polynomial in n. □

IV.2.4 Rings, Idempotents, and Frames

All our rings will have characteristic a power of p and are input with a basis. Furthermore, each of our rings will be represented in $\operatorname{End} V$ for some abelian p-group V and thus multiplication is the usual matrix multiplication.

Let R be a finite ring. An element $e \in R$ is an idempotent if $e^2 = e$. The trivial idempotents are 0 and 1 and all other idempotents are called *proper*. Two idempotents e and f are *orthogonal* when $ef = 0 = fe$. Given any idempotent e, $1 - e$ is also an idempotent and is orthogonal to e, and if f is orthogonal to e then $f(1-e) = f = (1-e)f$. A set $\mathcal{E}$ of pairwise orthogonal idempotents is *supplementary* if $1 = \sum_{e \in \mathcal{E}} e$. An idempotent is *primitive* if it is not the sum of proper pairwise orthogonal idempotents. Finally, a *frame* is a supplementary set of primitive pairwise orthogonal idempotents.

As R is finite, it follows that R has a frame and any two frames of R are conjugate under a unit of R [10, p. 141]. The unique size of a frame we call the *capacity* of R. If R has capacity 1 then we say R is a *local ring*. As idempotents are not quasi-regular, they lie outside of the Jacobson radical $J(R)$ of R. Thus, a frame of R induces a frame of $R/J(R)$. We have occasion to use the following classic formula for the lifting of idempotents:

Lemma IV.2.16 (Lifting idempotents). *Suppose that $e \in R$ such that $e^2 - e \in J(R)$. Then there is an $n \in \mathbb{N}$ such that $(e^2 - e)^n = 0$, and setting*

$$\hat{e} := e^n \sum_{j=0}^{n-1} \binom{2n-1}{j} e^{n-1-j}(1-e)^j \tag{IV.4}$$

it follows that:

(i) $\hat{e}^2 = \hat{e}$,

(ii) $e \equiv \hat{e} \pmod{J(R)}$, *and*

(iii) $\widehat{1-e} = 1 - \hat{e}$.

(iv) If $\mathcal{E}$ is a frame of $R/J(R)$, then $\hat{\mathcal{E}} := \{\hat{e} : e \in \mathcal{E}\}$ is a frame of R.

Proof. (i)–(iii) are verified directly, compare [10, (6.7)]. For (iv) note that $J(R)$ consists of nilpotent elements as R is finite. By (i), $\hat{\mathcal{E}}$ is a set of idempotents of R. Given $e \in \mathcal{E}$, we have assumed that $1 - e = \sum_{f \in \mathcal{E} - \{e\}} f$, and so by (iii) $\hat{e}$ is orthogonal to $\hat{f}$ for all $f \in \mathcal{E} - \{e\}$. Finally, by (ii),

if $\hat{e}$ is not primitive in R then e is not primitive in $R/J(R)$, which contradicts our assumptions. Thus $\hat{\mathcal{E}}$ is a frame of R. □

Consequently, if R is a finite commutative ring, then $R/J(R)$ is a product of fields and so there is a unique frame $\mathcal{E}$ of R; that is, $\{Re : e \in \mathcal{E}\}$ is the unique direct decomposition of R into commutative local subrings.

Let R be a finite ring and V a finite (left) R-module. If S is a subring of $\mathrm{End}_R V$ then every idempotent $e \in S$ decomposes V into R-modules: $V = Ve \oplus V(1-e)$. In general a direct decomposition $\mathcal{X}$ of V determines a supplementary set $\mathcal{E}(\mathcal{X})$ of pairwise orthogonal idempotents which are the projection endomorphisms to the various components. If instead we start with a set $\mathcal{E} \subset \mathrm{End}_R V$ of supplementary pairwise orthogonal idempotents then the associated direct decomposition is denoted $\mathcal{X}(\mathcal{E}) := \{Ve : e \in \mathcal{E}\}$. Notice that $\mathcal{E}(\mathcal{X}(\mathcal{E})) = \mathcal{E}$ and $\mathcal{X}(\mathcal{E}(\mathcal{X})) = \mathcal{X}$.

IV.2.5 Biadditive and Bilinear Maps

Let V and W denote finite abelian groups. A map $b : V \times V \to W$ is *biadditive* if

$$b(u+u', v+v') = b(u,v) + b(u',v) + b(u,v') + b(u',v'), \tag{IV.5}$$

for all $u, u'v, v' \in V$. Define

$$b(X,Y) := \langle b(x,y) : x \in X, y \in Y \rangle \tag{IV.6}$$

for $X, Y \subseteq V$. If $X \leq V$ then define

$$b_X : X \times X \to b(X,X) \tag{IV.7}$$

as the restriction of b to inputs from X. The *radical* of b is

$$\mathrm{rad}\, b := \{v \in V : b(v,V) = 0 = b(V,v)\}. \tag{IV.8}$$

We say that b is *nondegenerate* if $\mathrm{rad}\, b = 0$.

If R is a ring, then a biadditive map $b : V \times V \to W$ is *R-bilinear* if V and W are (left)

R-modules such that

$$b(ru, v) = rb(u, v) = b(u, rv), \qquad \forall u, v \in V, \text{ and } r \in R. \tag{IV.9}$$

We say b is *faithful* R-bilinear when $\operatorname{Ann}_R V \cap \operatorname{Ann}_R W = 0$, where the *annihilator* of an R-module V is $\operatorname{Ann}_R V = \{r \in R : rV = 0\}$. Every biadditive map is also $\mathbb{Z}$-bilinear. More generally, if R is a subring of S and b is S-bilinear then b is also R-bilinear. In that case $\operatorname{rad} b$ and $b(V, V)$ are both R- and S-modules.

IV.2.6 Representing Bilinear Maps for Computations

Assume that $b : V \times V \to W$ is a $\mathbb{Z}_{p^e}$-bilinear map. Let $\mathcal{X}$ and $\mathcal{Z}$ be ordered bases of V and W respectively. We define $B_{xy}^{(z)} \in \mathbb{Z}_{p^e}$ by

$$b\left(\sum_{x\in\mathcal{X}} s_x x, \sum_{y\in\mathcal{X}} t_y y\right) = \sum_{x,y\in\mathcal{X}} \sum_{z\in\mathcal{Z}} s_x t_y B_{xy}^{(z)} z, \quad \forall s_x, s_y \in \mathbb{Z}_{p^e}, x, y \in \mathcal{X}. \tag{IV.10}$$

Set

$$B_{xy} = \sum_{z\in\mathcal{Z}} B_{xy}^{(z)} z, \qquad \forall x, y \in \mathcal{X};$$

so that $B = [B_{xy}]_{x,y\in\mathcal{X}}$ is an $n \times n$-matrix with entries in W, where $n = |\mathcal{X}|$. Writing the elements of V as row vectors with entries in $\mathbb{Z}_{p^e}$ with respect to the basis $\mathcal{X}$ we can then write:

$$b(u, v) = uBv^t, \qquad \forall u, v \in V. \tag{IV.11}$$

Take $F, G \in \operatorname{End} V$, represented as matrices with respect to the ordered basis $\mathcal{X}$. Define FB and BG^t by the usual matrix multiplication, but notice the result is a matrix with entries in W. Evidently, $(F+G)B = FB + GB$, $F(GB) = (FG)B$, and similarly for the action on the other side of B. If $H \in \operatorname{End} W$ then define B^H by $[B^H]_{x,y} := B_{xy}H$ for each $x, y \in \mathcal{X}$. The significance of these operations is seen by their relation to b:

$$b(uF, v) = uFBv^t, \quad b(u, vG) = uBG^t v^t, \text{ and } b(u, v)H = u(B^H)v^t \tag{IV.12}$$

for all $u, v \in V$.

IV.3 Direct Decompositions

In this section we develop various properties of direct decompositions. Our principal aim is to establish when direct products can be lifted from direct products of a quotient (Subsection IV.4).

IV.3.1 Normal, Central, and Direct Decompositions

A set $\mathcal{H}$ of normal subgroups of a group G is a *(normal) decomposition* of G if $\mathcal{H}$ generates G but no proper subset does. Evidently, $1 \notin \mathcal{H}$. Thus, if $G = 1$, its the only decomposition is $\emptyset$.

A decomposition $\mathcal{H}$ is *central* if $[H, \langle \mathcal{H} - \{H\}\rangle] = 1$ for each $H \in \mathcal{H}$, or *direct* if $H \cap \langle \mathcal{H} - \{H\}\rangle = 1$ for each $H \in \mathcal{H}$. Direct decompositions are also central decompositions.

If $\mathcal{H}$ is a decomposition where $[H, K] = 1$ for distinct $H, K \in \mathcal{H}$, then $[H, \langle \mathcal{H} - \{H\}\rangle] = 1$ so $\mathcal{H}$ is a central decomposition.

A subgroup $H \leq G$ is a *direct factor* of G if there is a direct decomposition $\mathcal{H}$ of G with $H \in \mathcal{H}$. Notice $H \neq 1$.

Remark IV.3.1. *Central decompositions are in the internal description of central products while direct decompositions are the internal description of direct products.*

Remark IV.3.2. *Suppose that $G = \langle \mathcal{H}\rangle = \langle \mathcal{J}\rangle$ for some sets of subgroups $\mathcal{J} \subseteq \mathcal{H}$.*

(i) If $[H, \langle \mathcal{H} - \{H\}\rangle] = 1$ for each $H \in \mathcal{H}$, then $K \leq Z(G)$ for each $K \in \mathcal{H} - \mathcal{J}$.

(ii) If $H \cap \langle \mathcal{H} - \{H\}\rangle = 1$ for each $H \in \mathcal{H}$, then $K = 1$ for any $K \in \mathcal{H} - \mathcal{J}$. Thus, the definition of direct decompositions given in the introduction agrees with definition just given.

Proposition IV.3.3. *If $\mathcal{H}$ is a normal, central, or direct decomposition of G and $\mathcal{K}$ is a subset of $\mathcal{H}$, then $\mathcal{K}$ is a normal, central, or direct decomposition of $\langle \mathcal{K}\rangle$, respectively.*

IV.3.2 Finer and Coarser Decompositions

A set $\mathcal{H}$ of subgroups of a group G is *finer* than another set $\mathcal{K}$ of subgroups of G if

$$K = \langle H \in \mathcal{H} : H \leq K\rangle, \qquad \forall K \in \mathcal{K}. \tag{IV.13}$$

Note this is not the same as $\mathcal{H} \subseteq \mathcal{K}$. Evidently this gives a partial ordering on the decompositions of G with top element $\{G\}$. We also say that $\mathcal{K}$ is *coarser* than $\mathcal{H}$, or that $\mathcal{H}$ *refines* $\mathcal{K}$.

Remark IV.3.4. *Note that we have not required that* $\mathcal{H}$ *and* $\mathcal{K}$ *be decompositions in the definition of refinement. This allows us to speak of refinements of induced sets as in* (IV.14)-(IV.16)*, below.*

Proposition IV.3.5. *Suppose that* $\mathcal{H}$ *is a finer decomposition than* $\mathcal{K}$. *If* $\mathcal{H}$ *is normal, central, or direct, then* $\mathcal{K}$ *is central or direct, respectively.*

Proof. If every member of $\mathcal{H}$ is normal then any group generated by a subset of $\mathcal{H}$ is normal; thus, the members of $\mathcal{K}$ are normal. Now assume $\mathcal{H}$ is central and fix $K \in \mathcal{K}$. As $\langle \mathcal{K} - \{K\} \rangle = \langle H \in \mathcal{H} : H \not\leq K \rangle$ it follows that

$$\begin{aligned} [K, \langle \mathcal{K} - \{K\} \rangle] &= \langle [H, \langle H \in \mathcal{H} : H \not\leq K \rangle] : H \in \mathcal{H}, H \leq K \rangle \\ &\leq \langle [H, \langle \mathcal{H} - \{H\} \rangle] : H \in \mathcal{H}, H \leq K \rangle = 1. \end{aligned}$$

So $\mathcal{K}$ is a central decomposition. Finally assume that $\mathcal{H}$ is a direct decomposition. Note that

$$K \cap \langle \mathcal{K} - \{K\} \rangle = \langle H \in \mathcal{H} : H \leq K \rangle \cap \langle H \in \mathcal{H} : H \not\leq K \rangle.$$

As $\mathcal{H}$ is a direct decomposition, each $g \in G$ is expressed uniquely as $g = \prod_{H \in \mathcal{H}} g_H$, $g_H \in H$. If $g \in K \cap \langle \mathcal{K} - \{K\} \rangle$ then $g \in K$ so $g_H = 1$ for all $H \not\leq K$, $H \in \mathcal{H}$. Also, $g \in \langle \mathcal{K} - \{K\} \rangle$ so $g_H = 1$ for all $H \leq K$, $H \in \mathcal{H}$. Hence, $g = 1$. □

IV.3.3 Induced Decompositions and Generically Split Subgroups

Let M be a normal subgroup of a group G and $\mathcal{H}$ a set of subgroups of G. The following notation is convenient (coincidences can occur, but the resulting objects are sets so coincidences are ignored):

$$\mathcal{H} \cap M := \{H \cap M : H \in \mathcal{H}\} - \{1\}, \tag{IV.14}$$

$$\mathcal{H}M := \{HM : H \in \mathcal{H}\} - \{M\}, \text{ and} \tag{IV.15}$$

$$\mathcal{H}M/M := \{HM/M : H \in \mathcal{H}\} - \{M/M\}. \tag{IV.16}$$

Remark IV.3.6. *If $\mathcal{H}$ is a decomposition, it is generally possible to that $\mathcal{H} \cap M$, $\mathcal{H}M$, or $\mathcal{H}M/M$ is not a decomposition of M, G, or G/M, respectively.*

Proposition IV.3.7. *Let G be a group with a direct decomposition $\mathcal{H}$. If $M \trianglelefteq G$ and $M = \langle \mathcal{H} \cap M \rangle$ then:*

(i) $\mathcal{H} \cap M$ is a direct decomposition of M;

(ii) $HM = KM$ for $H, K \in \mathcal{H}$ implies $H, K \leq M$ (so $\mathcal{H}M$, $\mathcal{H}M/M$, and $\mathcal{H} - \{H \in \mathcal{H} : H \leq M\}$ are in bijection);

(iii) $\mathcal{H}M/M$ is a direct decomposition of G/M; and

(iv) if $N \trianglelefteq G$ with $N = \langle \mathcal{H} \cap N \rangle$ then $M \cap N = \langle \mathcal{H} \cap M \cap N \rangle$ and $MN = \langle \mathcal{H} \cap MN \rangle$.

Proof. (i). Suppose that $M = \langle \mathcal{H} \cap M \rangle$. If $H \cap M \in \mathcal{H} \cap M$, then $H \cap M \trianglelefteq M$. Furthermore, $(H \cap M) \cap \langle \mathcal{H} \cap M - \{H \cap M\} \rangle \leq H \cap \langle \mathcal{H} - \{H\} \rangle = 1$. By definition, $1 \notin \mathcal{H} \cap M$, and so $\mathcal{H} \cap M$ is a direct decomposition of M.

(ii). Fix $H, K \in \mathcal{H}$, $H \neq K$. Set $J := \langle \mathcal{H} - \{H, K\} \rangle$. By Proposition IV.3.5, $G = H \times K \times J$ and by (i), $M = (H \cap M) \times (K \cap M) \times (J \cap M)$. Thus,

$$\begin{aligned} HM &= H \times (K \cap M) \times (J \cap M), \\ KM &= (H \cap M) \times K \times (J \cap M). \end{aligned}$$

If $HM = KM$ then $H = H \cap M$ and $K = K \cap M$.

(iii). As $G = \langle \mathcal{H} \rangle = \langle \mathcal{H}, M \rangle$ it follows that G/M is generated by $\mathcal{H}M/M$ and the members of $\mathcal{H}M/M$ are normal in G/M.

Fix $H \in \mathcal{H}$. Clearly $M \leq HM \cap \langle \mathcal{H} - \{H\} \rangle M$. Next we reverse the inequality. Set $J := \langle \mathcal{H} - \{H\} \rangle$, so $G = H \times J$. So $HM = H \times (J \cap M)$ and $JM = (H \cap M) \times J$. Thus $HM \cap JM = (H \cap M) \times (J \cap M) = M$. Furthermore, $\mathcal{H}M$ is in bijection with $\mathcal{H} - \{H \in \mathcal{H} : H \leq M\}$. So

$$(\mathcal{H} - \{H\})M = \{KM : K \in \mathcal{H}, K \not\leq M, K \neq H\} = \mathcal{H}M - \{HM\}.$$

Thus, $(HM/M) \cap (JM/M) = M/M$ implies $(HM/M) \cap \langle \mathcal{H}M/M - \{HM/M\} \rangle = 1$. As $M/M \notin \mathcal{H}M/M$ (by (IV.16)) it follows that $\mathcal{H}M/M$ is a direct decomposition of G/M.

(iv). Let $g \in M \cap N$. By (i), $\mathcal{H} \cap M$ is a direct decomposition of M and since $g \in M$, it follows that $g = \prod_{H \in \mathcal{H}} h_H$ for unique $h_H \in H \cap M$, $H \in \mathcal{H}$. Similarly, $\mathcal{H} \cap N$ is a direct decomposition of N and by the uniqueness of the h_H, it follows that $h_H \in H \cap N$, and so $h_H \in H \cap M \cap N$. Thus $M \cap N \leq \langle \mathcal{H} \cap M \cap N \rangle \leq M \cap N$.

The argument for $MN = \langle \mathcal{H} \cap MN \rangle$ is equally transparent. □

Definition IV.3.8. *A subgroup $M \trianglelefteq G$ is* generically split *if given any direct decomposition $\mathcal{H}$ of G, then $\mathcal{H} \cap M$ is a direct decomposition of M.*

Evidently 1 and G are always generically split. Furthermore, Proposition IV.3.7.(iv) show that the set of all generically split subgroups of G form a lattice. In Section IV.4.3 we uncover a great number of generically split subgroups but for now we give some simpler examples.

Example IV.3.9. *(i) If $G \cong \mathbb{Z}_p^n$ then the only generically split subgroups are 1 and G.*

(ii) In any group, the subgroups $\zeta_i(G)$ are generically split; see Proposition IV.4.11.(i).

(iii) In any finite group, the solvable radical is generically split; see Proposition IV.4.11.(ii).

Proposition IV.3.10. *If $M \leq N$ are normal subgroups of G such that M is generically split in N and N is generically split in G, then M is generically split in G. In particular, every characteristic generically split subgroup of N is generically split in G.*

Proof. Let $\mathcal{H}$ be a direct decomposition of G. As N is generically split in G, $N \cap \mathcal{H}$ is a direct decomposition of N. As M is generically split in N, also $M \cap (N \cap \mathcal{H}) = M \cap \mathcal{H}$ is a direct decomposition of M. Thus, M is generically split in G. □

IV.3.4 Krull-Remak-Schmidt Redux

We make crucial use of the classical theorem for direct products of groups:

Theorem IV.3.11 (Krull-Remak-Schmidt). *Let G be a finite group with Remak decompositions $\mathcal{H}$ and $\mathcal{K}$. Then for each $\mathcal{J} \subseteq \mathcal{H}$, there is a $\varphi \in C_{\mathrm{Aut}\, G}(\mathrm{Inn}\, G)$ such that $\mathcal{J}\varphi \subseteq \mathcal{K}$ and $\mathcal{H}\varphi = (\mathcal{H} - \mathcal{J}) \sqcup \mathcal{J}\varphi$. In particular, there is a $\varphi \in C_{\mathrm{Aut}\, G}(\mathrm{Inn}\, G)$ with $\mathcal{H}\varphi = \mathcal{K}$.*

Proof. See [49, (3.3.8)]. □

Remark IV.3.12. *Theorem IV.3.11 was proved by Remak in his 1911 thesis [48]. Over the next two years, Remak and Schmidt exchanged successive improvements in the proof concluding in Schmidt's 3 page proof [52].*

Krull was 12 years old at the time of these results, but 14 years later contributed a version for modules [33], a simpler but widely used version of the theorem. Modern group theory texts synthesize both versions into one statement involving operator groups. Incomprehensibly, Remak's name is sometimes dropped from the title.

Remark IV.3.13. *The Krull-Remak-Schmidt theorem is a hybrid of an exchange theorem (in the sense of a matroid) and a transitivity theorem. Both of these interpretations are used in the proof of Theorem IV.1.3.*

We need the following consequence:

Corollary IV.3.14. *Let G be a finite group, $\mathcal{H}$ a direct decomposition of G, and $\mathcal{R}$ a Remak decomposition of G. Then*

(i) $\mathcal{R}M$ refines $\mathcal{H}M$ whenever $Z(G) \leq M \trianglelefteq G$, and

(ii) $\mathcal{R} \cap M$ refines $\mathcal{H} \cap M$ whenever $M \trianglelefteq G$, $M \leq G'$.

Hence, $\mathcal{R}Z(G)$ and $\mathcal{R} \cap G'$ are uniquely determined by G, and $\operatorname{Aut} G$ acts on both sets.

Proof. (i). Let $\mathcal{K}$ be a Remak decomposition which refines $\mathcal{H}$ (there always is one). By Theorem IV.3.11, there is some $\varphi \in C_{\operatorname{Aut} G}(\operatorname{Inn} G)$ such that $\mathcal{R}\varphi = \mathcal{K}$. As $\varphi \in C_{\operatorname{Aut} G}(\operatorname{Inn} G)$, $[x, \varphi] \in Z(G) \leq M$ (see [49, 3.3.6]) and we have that $xM\varphi = xM$ for all $x \in G$. So $\mathcal{R}M = \mathcal{R}M\varphi = \mathcal{K}M$. As $\mathcal{K}M$ refines $\mathcal{H}M$, so does $\mathcal{R}M$.

(ii). The argument is identical to (i) except that it relies on the fact that $[x, y]\varphi = [x, y]$ for all $x, y \in G$. So $\mathcal{R} \cap M = \mathcal{K} \cap M$. □

Remark IV.3.15. *The sets $\mathcal{R}M$, $\mathcal{H}M$, $\mathcal{R} \cap M$, and $\mathcal{H} \cap M$ in Corollary IV.3.14 need not be decompositions in our strict sense; see Remark IV.3.4 and Remark IV.3.6. The special cases $M = Z(G)$ or $M = G'$ lead to direct decompositions in the respective subgroups or quotient groups by Proposition IV.4.11.*

Proposition IV.3.16. *Let G be a group and $Z(G) \leq M \leq G$ such that M is generically split.*

(i) $\mathcal{D}(M) := \{\mathcal{H}M : \mathcal{H}$ *a direct decomposition of* $G\}$ *is a boolean lattice under the partial ordering of refinement; see* (IV.13).

(ii) If $\mathcal{H} = \mathcal{H}M$ *is a normal decomposition of* G*, then there is a direct decomposition* $\mathcal{K}$ *of* G *such that* $\mathcal{H}$ *refines* $\mathcal{K}M$ *and so that if* $\mathcal{H}$ *refines* $\mathcal{J}M$ *for a direct decomposition* $\mathcal{J}$ *of* G*, then* $\mathcal{K}M$ *refines* $\mathcal{J}M$*.*

Proof. (i). Let $\mathcal{R}$ be a Remak decomposition of G. As M is generically split, $\mathcal{R}M$ is in a bijection with $\mathcal{R}(M) := \mathcal{R} - \{R \in \mathcal{R} : R \leq M\}$, Proposition IV.3.7.$(ii)$. By Corollary IV.3.14.$(i)$, this bijection is induces a lattice isomorphism between $\mathcal{D}(M)$ and the boolean lattice of partitions of $\mathcal{R}(M)$.

(ii). Let $\mathcal{S} = \{\mathcal{K} \in \mathcal{D}(M) : \mathcal{H}$ refines $\mathcal{K}\}$. Evidently $\{G\} \in \mathcal{S}$ so $\mathcal{S} \neq \emptyset$. The meet $\mathcal{K}M$ of the members of $\mathcal{S}$ satisfies the conclusion. □

IV.4 Pulling Back Direct Decompositions of Quotient Groups

In this section we develop a method to create direct decompositions of a group G from direct decompositions of G/M, for selected $M \trianglelefteq G$. The quotients required by the algorithm for Theorem IV.1.3 (as outlined in Section IV.1.1) are handled uniformly using group varieties. Sections IV.4.1 and IV.4.2 introduce necessary vocabulary and objects. Sections IV.4.3 and IV.4.4 develop the relationship between direct decompositions of G/M and direct decompositions of G. Finally, Section IV.4.6 provides the algorithms to pullback direct decompositions of G/M to direct decomposition of G.

IV.4.1 Group Varieties $\mathfrak{V}$*, Verbal Subgroups* $W(G)$*, and Marginal Subgroups* $W^*(G)$

In this section we review group varieties, verbal, and marginal subgroups.

Throughout this section let X be a countable set and $W \neq \emptyset$ a subset of the free group $F(X)$ on X. Given a group G and a function $f : X \to G$, define $\bar{f} : F(X) \to G$ as the induced homomorphism with $x\bar{f} = xf$, $x \in X$. If X is enumerated as $X = \{x_1, x_2, \dots\}$ then we may treat $w \in F(X)$ as a function in the variables X, denoted $w(x_1, x_2, \dots)$, and $f : X \to G$ as a sequence $(g_1, g_2, \dots)$ of elements in G where $x_i f = g_i$, $i \in \mathbb{Z}^+$. In this way $w\bar{f} = w(g_1, g_2, \dots)$, compare [44, pp.3-4].

The *W-verbal* subgroup of G is

$$W(G) := \langle w\bar{f} \mid w \in W, f : X \to G \rangle. \tag{IV.17}$$

This is the subgroup generated by all evaluations of the words in W with elements from G.

Given $f, f' : X \to G$ we form the product $ff' : X \to G$ pointwise. Thus, in the indexed sequence notation above we have:

$$w\overline{ff'} = w(g_1 g_1', g_2 g_2', \dots) \tag{IV.18}$$

for $w \in F[X]$, $g_i = x_i f$ and $g_i' = x_i f'$, $i \in \mathbb{Z}^+$.

The counterpart to verbal subgroups are the *W-marginal* subgroups introduced by P. Hall [17].

$$\begin{aligned} W^*(G) := \{a \in G \mid w(g_1, \dots, g_{i-1}, ag_i, g_{i+1}, \dots) = w(g_1, \dots, g_{i-1}, g_i, g_{i+1}, \dots), \\ \forall g_i \in G, i \in \mathbb{Z}^+, w \in W\} \end{aligned} \tag{IV.19}$$

However, we will prefer the definition in the following equivalent formulation:

$$\mathrm{Null}_{X \to G}(W) := \{f' : X \to G \mid w\overline{f'f} = w\bar{f}, \forall f : X \to G, \forall w \in W\}, \tag{IV.20}$$

$$W^*(G) = \bigcup_{f \in \mathrm{Null}_{X \to G}(W)} \mathrm{im}\, f. \tag{IV.21}$$

Notice $f' : X \to G$ has $\mathrm{im}\, f' \subseteq W^*(G)$ if, and only if, $f' \in \mathrm{Null}_{X \to G}(W)$.

Verbal subgroups are fully-invariant (F. Levi, [17]) while marginal subgroups are in general only characteristic (P. Hall, [17]).

Example IV.4.1. *(i) Let* $[x_1] := x_1$ *and* $[x_1, \dots, x_{c+1}] := [[x_1, \dots, x_c], x_{c+1}]$, $c \in \mathbb{N}$. *If* $W_c = \{[x_1, \dots, x_{c+1}]\}$, *then* $W(G) = \gamma_{c+1}(G)$, *the* $(c+1)$*-st term in the lower central series. Also,* $W_c^*(G) = \zeta_c(G)$, *the c-th term in the upper central series of G [49, 2.3].*

(ii) Let $\delta(x_1) := x_1$ *and* $\delta(x_1, \dots, x_{2^{d+1}}) = [\delta(x_1, \dots, x_{2^d}), \delta(x_{2^d+1}, \dots, x_{2^{d+1}})]$, $d \in \mathbb{N}$. *If* $W_d = \{\delta(x_1, \dots, x_{2^d})\}$, *then* $W_{(d)}(G) = G^{(d)}$ *is the d-th derived group of G. It appears that* $W^*(G)$ *is not generally encountered and has no associated name. However, a philo-*

sophically appropriate title might be the d-th upper derived *subgroup of G, since $W_d^*(G)$ is a solvable group of derived length d. However, it is not generally true that the quotients of the series $W_{(1)}^*(G) \geq W_{(2)}^*(G) \geq \cdots$ are abelian.* [3]

Proposition IV.4.2. *Given a class $\mathfrak{V}$ of groups, the following are equivalent:*

(i) there is a countable nonempty set W of words such that $G \in \mathfrak{V}$ if, and only if, $W(G) = 1$;

(ii) (P. Hall) there is a countable nonempty set W of words such that $G \in \mathfrak{V}$ if, and only if, $W^*(G) = 1$;

(iii) (G. Birkhoff) $1 \in \mathfrak{V}$ and $\mathfrak{V}$ is closed to homomorphic images, subgroups, and direct products.

If $\mathfrak{V}$ satisfies any of these properties then $\mathfrak{V}$ is called a variety *of groups. Given a set of words, the associated variety is denoted $\mathfrak{V}(W)$.*

Proof. See [49, 2.3]. □

Remark IV.4.3. *Given sets of words $W, W' \subseteq F[X]$, it is be possible that $\mathfrak{V}(W) = \mathfrak{V}(W')$ with $W \neq W'$. Therefore, the subgroups $W(G)$ and $W^*(G)$ are not necessarily determined by the variety $\mathfrak{V}(W)$, but rather by set of words W.*

Example IV.4.4. *(i) The variety $\mathfrak{N}_c := \mathfrak{V}([x_1, \ldots, x_{c+1}])$ is the class of nilpotent groups of class at most c [32, Theorem 3.9].*

(ii) The variety $\mathfrak{S}_d := \mathfrak{V}(\delta(x_1, \ldots, x_{2^d}))$ is the class of solvable groups of derived length at most d [32, Theorem 3.20].

Definition IV.4.5. *A $\mathfrak{V}$-subgroup H of a group G is a subgroup contained in the variety $\mathfrak{V}$.*

Proposition IV.4.6. *Let $\mathfrak{V} := \mathfrak{V}(W)$ be a group variety and G a group. If H is a $\mathfrak{V}$-subgroup of G then so is $W^*(G)H$, that is: $W^*(G)H \in \mathfrak{V}$.*

Proof. Let $f : X \to G$ with $\operatorname{im} f \subseteq W^*(G)H$. As each element of $W^*(G)H$ has the form ah for $a \in W^*(G)$ and $h \in H$, choose functions f', f'' from X to G where $\operatorname{im} f' \subseteq W^*(G)$, $\operatorname{im} f'' \subseteq M$, and $f = f'f''$ (pointwise). By the definition of $W^*(G)$, $w\bar{f} = w\overline{f'f''} = w\overline{f''}$ for all $w \in W$. As $H \in \mathfrak{V}$, $W(H) = 1$ and so $w\overline{f''} = 1$ for all $w \in W$. Thus, $w\bar{f} = 1$ for all $w \in W$ and all $f : X \to G$ with $\operatorname{im} f \subseteq W^*(G)H$; that is, $W(W^*(G)H) = 1$ and hence, $W^*(G)H \in \mathfrak{V}$. □

[3] Peter Neumann informs me that for reasons such as this, marginal subgroups are not generally used except in the context of nilpotent groups. Indeed, they do not appear in [11].

IV.4.2 $\mathfrak{V}$-cores: $O_{\mathfrak{V}}(G)$

Following Remark IV.4.3 we know that $W^*(G)$ may depend on the choice of W and might not be uniquely determined by the variety $\mathfrak{V}(W)$. In this section we define a characteristic subgroup $O_{\mathfrak{V}}(G)$ of G with properties similar to $W^*(G)$ which depends only on $\mathfrak{V}(W)$, not W.

Definition IV.4.7. *Fix a variety $\mathfrak{V}$ and a group G.*

(i) A subgroup $M \trianglelefteq G$ is a maximal normal $\mathfrak{V}$-subgroup *if whenever $M \leq N \trianglelefteq G$ and $N \in \mathfrak{V}$, then $M = N$.*

(ii) The $\mathfrak{V}$-core, $O_{\mathfrak{V}}(G)$, of G is the intersection of all maximal normal $\mathfrak{V}$-subgroups of G.

As $1 \in \mathfrak{V}$, the set of maximal normal $\mathfrak{V}$-subgroups of a group G is always nonempty. It can be a singleton set, Examples .*(ii)*-*(iii)*, but it need not be, Example .*(i)*. Also note that $\mathfrak{V}$ is closed to subgroups so $O_{\mathfrak{V}}(G) \in \mathfrak{V}$.

Example IV.4.8. *(i) $O_{\mathfrak{N}_1}(G)$ is the intersection of all maximal normal abelian subgroups of G. Generally there can be any number of maximal normal abelian subgroups of G so $O_{\mathfrak{N}_1}(G)$ is not a trivial intersection.*

(ii) $O_{\mathfrak{N}_c}(G)$ is the intersection of all maximal normal nilpotent subgroups of G with class at most c. If $c > \log|G|$ then all nilpotent subgroups of G have class at most c and therefore $O_{\mathfrak{N}_c}(G)$ is the Fitting subgroup of G: the unique maximal normal nilpotent subgroup of G.

(iii) Similar to (ii), $O_{\mathfrak{S}_d}(G)$, $d > \log|G|$, is the unique maximal normal solvable subgroup of G, i.e.: the solvable radical $O_{\mathfrak{S}}(G)$ of G.

Proposition IV.4.9. *Let $\mathfrak{V} := \mathfrak{V}(W)$ be a group variety and G a group. Then*

(i) $W^*(G) \leq O_{\mathfrak{V}(W)}(G)$, and

(ii) if $M \trianglelefteq G$ then $O_{\mathfrak{V}}(G)O_{\mathfrak{V}}(M)$ is a normal $\mathfrak{V}$-subgroup of G.

Proof. *(i)*. By Proposition IV.4.6, every maximal normal $\mathfrak{V}$-subgroup of G contains $W^*(G)$.

(ii). As $M \trianglelefteq G$ and $O_{\mathfrak{V}}(M)$ is characteristic in M, it follows that $O_{\mathfrak{V}}(M)$ is a normal $\mathfrak{V}$-subgroup of G. Thus, $O_{\mathfrak{V}}(M)$ lies in a maximal normal $\mathfrak{V}$-subgroup N of G. As $O_{\mathfrak{V}}(G) \leq N$ we have $O_{\mathfrak{V}}(G)O_{\mathfrak{V}}(M) \leq N \in \mathfrak{V}$. As $\mathfrak{V}$ is closed to subgroups, it follows that $O_{\mathfrak{V}}(G)O_{\mathfrak{V}}(M)$ is in $\mathfrak{V}$. □

Remark IV.4.10. *(i) If $W, W' \subseteq F[X]$ with $\mathfrak{V}(W) = \mathfrak{V}(W')$, then $O_{\mathfrak{V}(W)}(G) = O_{\mathfrak{V}(W')}(G)$ and $(W')^*(G) \leq O_{\mathfrak{V}(W)}(G)$.*

(ii) It is possible to have $W^*(G) < O_{\mathfrak{V}(W)}(G)$. For instance, with $\mathfrak{N}_1 = \mathfrak{V}([x_1, x_2])$ and $G = S_3 \times C_2$, the marginal subgroup is the center $1 \times C_2$, whereas the $\mathfrak{N}_1$-core is $C_3 \times C_2$.

IV.4.3 Induced Decompositions with Margins and Cores

We now prove that marginal and core subgroups behave well when considering direct decompositions. Throughout we assume $W \subseteq F[X]$ and $\mathfrak{V} = \mathfrak{V}(W)$ as defined in Section IV.4.1.

Proposition IV.4.11. *Let G be a finite group with a direct decomposition $\mathcal{H}$. Then*

(i) $\mathcal{H} \cap W^*(G) = \{W^*(H) : H \in \mathcal{H}\}$, this is a direct decomposition of $W^*(G)$, and $\mathcal{H}W^*(G)/W^*(G)$ is a direct decomposition of $G/W^*(G)$; and

(ii) $\mathcal{H} \cap O_{\mathfrak{V}}(G) = \{O_{\mathfrak{V}}(H) : H \in \mathcal{H}\}$, this is a direct decomposition of $O_{\mathfrak{V}}(G)$, and $\mathcal{H}O_{\mathfrak{V}}(G)/O_{\mathfrak{V}}(G)$ is a direct decomposition of $G/O_{\mathfrak{V}}(G)$.

In particular, margins and cores are generically split subgroups for any set of words and any variety.

Proof. (i). We must show that $\mathcal{H} \cap W^*(G) = \{W^*(H) : H \in \mathcal{H}\}$ and by Proposition IV.3.7 that $W^*(G) = \langle \mathcal{H} \cap W^*(G) \rangle$. If $\mathcal{H} = \{G\}$ then these are true trivially. Fix $H \in \mathcal{H}$ and set $K := \langle \mathcal{H} - \{H\} \rangle$. By induction we may assume that $(\mathcal{H} - \{H\}) \cap W^*(K) = \{W^*(K) : K \in \mathcal{H} - \{H\}\}$ and this is a direct decomposition of $W^*(K)$.

As $G = H \times K$, every $f : X \to G$ decomposes uniquely as $f = f_H \times f_K$, where $f_H : X \to H$, $f_K : X \to K$. Moreover, if $w \in W$, then $w\overline{f} = w\overline{f_H} \times w\overline{f_K}$. Take $f'_H : X \to H$ with $\operatorname{im} f'_H \subseteq W^*(H)$, and $f'_K : X \to K$ with $\operatorname{im} f'_K \subseteq W^*(K)$, and define $f' : X \to G$ by $f' = f'_H \times f'_K$. Thus, by the definition of $W^*(H)$ and $W^*(K)$, for each $w \in W$:

$$w\overline{f'f} = w\overline{(f'_H \times f'_K)(f_H \times f_K)} = (w\overline{f'_H f_H}) \times (w\overline{f'_K f_K}) = (w\overline{f_H}) \times (w\overline{f_K}) = w\bar{f}. \qquad \text{(IV.22)}$$

Thus $\operatorname{im} f' \subseteq W^*(G)$ and hence $W^*(H) \times W^*(K) \leq W^*(G)$. Whence, $W^*(H) \leq H \cap W^*(G)$ and $W^*(K) \leq K \cap W^*(G)$. We now reverse these last three inclusions.

Fix $f' : X \to W^*(G)$. So $f' = f'_H \times f'_K$ where $f'_H : X \to H$, $f'_K : X \to K$ with $\operatorname{im} f'_H \subseteq H \cap W^*(G)$ and $\operatorname{im} f'_K \subseteq K \cap W^*(G)$. Take $f_H : X \to H$, $f_K : X \to K$, and $w \in W$, and

compute:

$$(w\overline{f'_H f_H}) \times (w\overline{f'_K f_K}) = w\overline{f'(f_H \times f_K)} = w\overline{f_H \times f_K} = w\overline{f_H} \times w\overline{f_K}. \qquad \text{(IV.23)}$$

As $G = H \times K$, it follows that $w\overline{f'_H f_H} = w\overline{f_H}$ and $w\overline{f'_K f_K} = w\overline{f_K}$. Thus, $H \cap W^*(G) \leq W^*(H)$, $K \cap W^*(G) \leq W^*(K)$, and $W^*(G) \leq W^*(H) \times W^*(K)$. So $H \cap W^*(G) = W^*(H)$, $K \cap W^*(G) = W^*(K)$, and $W^*(G) = W^*(H) \times W^*(K)$. Thus, by induction (i) is proved.

(ii). Let $H \in \mathcal{H}$ and $K := \langle \mathcal{H} - \{H\} \rangle$. Let M be a maximal normal $\mathfrak{V}$-subgroup of $G = H \times K$. Let M_H be the projection of M to the H-component. As $\mathfrak{V}$ is closed to homomorphic images, $M_H \in \mathfrak{V}$. Furthermore, $M_H \trianglelefteq H$ so there is a maximal normal $\mathfrak{V}$-subgroup N of H such that $M_H \leq N$.

We claim that $MN \in \mathfrak{V}$.

As $G = H \times K$, every $g \in M$ has the unique form $g = hk$, $h \in H$, $k \in K$. As M_H is the projection of M to H, $h \in M_H \leq N$. Thus, $g, h \in MN$ so $k \in MN$. Thus, $MN = N \times M_K$, where M_K is the projection of M to K. Now let $\mathfrak{V} = \mathfrak{V}(W)$ and fix $w \in W$. For each $f : X \to MN$, write $f = f_N \times f_K$ where $f_N : X \to N$ and $f_K : X \to M_K$. Hence, $w\bar{f} = w\overline{f_N \times f_K} = w\overline{f_N} \times w\overline{f_K}$. However, $W(N) = 1$ and $W(M_K) = 1$ as $N, M_K \in \mathfrak{V}$. Thus, $w\bar{f} = 1$, which proves that $W(MN) = 1$. So $MN \in \mathfrak{V}$ as claimed.

As M is a maximal normal $\mathfrak{V}$-subgroup of G, $M = MN$ and $N = M_H$. Hence, $H \cap M = N$ is a maximal normal $\mathfrak{V}$-subgroup of H. So we have characterized the maximal normal $\mathfrak{V}$-subgroups of G as the direct products of maximal normal $\mathfrak{V}$-subgroups of members $H \in \mathcal{H}$. Thus, $\mathcal{H} \cap O_{\mathfrak{V}}(G) = \{O_{\mathfrak{V}}(H) : H \in \mathcal{H}\}$ and this generates $O_{\mathfrak{V}}(G)$. By Proposition IV.3.7, $\mathcal{H} \cap O_{\mathfrak{V}}(G)$ is a direct decomposition of $O_{\mathfrak{V}}(G)$. □

IV.4.4 $\mathfrak{V}$-separated Direct Decompositions

In this section we define $\mathfrak{V}$-separated direct decompositions. These decompositions are direct decompositions which can be partitioned into subgroups lying in $\mathfrak{V}$, together with subgroups with no direct factors in $\mathfrak{V}$. This is the key organizational device for the proof of Theorem IV.1.3, through the use of Theorem IV.4.22.

Definition IV.4.12. *Let $\mathfrak{V}$ be a variety and G a group with a direct decomposition $\mathcal{H}$.*

(i) $\mathfrak{V} \cap \mathcal{H} := \{H \in \mathcal{H} : H \in \mathfrak{V}\}$.

(ii) $\mathcal{H} - \mathfrak{V} := \{H \in \mathcal{H} : H \notin \mathfrak{V}\} = \mathcal{H} - (\mathfrak{V} \cap \mathcal{H})$.

(iii) $\mathcal{H}$ *is* $\mathfrak{V}$-separated *if each* $H \in \mathcal{H} - \mathfrak{V}$ *has no direct factor in* $\mathfrak{V}$ *(note* $1 \notin \mathcal{H}$*).*

(iv) $\mathcal{H}$ *is* $\mathfrak{V}$*-refined if it is* $\mathfrak{V}$*-separated and every member of* $\mathcal{H} \cap \mathfrak{V}$ *is directly indecomposable.*

Example IV.4.13. *(i) For the variety* $\mathfrak{N}_1$ *of abelian groups, an* $\mathfrak{N}_1$*-separated direct decomposition is a decomposition in which all nonabelian members have no abelian direct factors (recalling* 1 *is not a direct factor).*

(ii) Given a group G *and the variety* $\mathfrak{S}_d$*,* $d > \log|G|$*, an* $\mathfrak{S}_d$*-separated direct decomposition of* G *is a decomposition in which the nonsolvable members have no solvable direct factors.*

Proposition IV.4.14. *Let* $\mathfrak{V}$ *be a variety and* G *a finite group.*

(i) Every Remak decomposition of G *is* $\mathfrak{V}$*-separated and so every direct decomposition can be refined to a* $\mathfrak{V}$*-separated decomposition of* G*.*

(ii) If $\mathcal{H}$ *is a* $\mathfrak{V}$*-separated direct decomposition of* G *then* $\{\langle \mathcal{H} - \mathfrak{V}\rangle, \langle \mathfrak{V} \cap \mathcal{H}\rangle\}$ *is a* $\mathfrak{V}$*-separated direct decomposition of* G*.*

(iii) If $\mathcal{H}$ *and* $\mathcal{K}$ *are* any *two* $\mathfrak{V}$*-separated direct decompositions of* G *then* $(\mathcal{H} - \mathfrak{V}) \sqcup (\mathfrak{V} \cap \mathcal{K})$ *is a* $\mathfrak{V}$*-separated direct decomposition of* G*.*

(iv) If $\mathfrak{V} = \mathfrak{V}(W)$ *and* $\mathcal{H}$ *is a* $\mathfrak{V}$*-separated decomposition of* G *then* $\langle \mathfrak{V} \cap \mathcal{H}\rangle \leq W^*(G)$*.*

Proof. (i). Let $\mathcal{H}$ be a Remak decomposition of G. As every $H \in \mathcal{H}$ is directly indecomposable, the only direct factor of H is H. Thus, the members of $\mathcal{H} - \mathfrak{V}$ have no direct factors in $\mathfrak{V}$. So $\mathcal{H}$ is $\mathfrak{V}$-separated.

(ii). Let $\mathcal{K}$ be a Remak decomposition of G which refines $\mathcal{H}$. As $\mathfrak{V}$ is closed to subgroups,

$$\mathcal{J} := \{K \in \mathcal{K} : \exists H \in \mathfrak{V} \cap \mathcal{H} \text{ with } K \leq H\} \subseteq \mathfrak{V} \cap \mathcal{K}. \tag{IV.24}$$

Furthermore, every $K \in \mathcal{K} - \mathcal{J}$ lies in some $H \in \mathcal{H} - \mathfrak{V}$ and so is a direct factor of H. As $\mathcal{H}$ is $\mathfrak{V}$-separated it follows that $K \notin \mathfrak{V}$, for any $K \in \mathcal{K} - \mathfrak{V}$. Thus $\mathcal{J} = \mathfrak{V} \cap \mathcal{K}$. Set $L := \langle \mathcal{H} - \mathfrak{V}\rangle = \langle \mathcal{K} - \mathfrak{V}\rangle = \langle \mathcal{K} - \mathcal{J}\rangle$ and $V = \langle \mathfrak{V} \cap \mathcal{K}\rangle = \langle \mathfrak{V} \cap \mathcal{H}\rangle$. We claim $\{L, V\}$ is $\mathfrak{V}$-separated.

If L has a direct factor which lies in $\mathfrak{V}$ then, as $\mathfrak{V}$ is closed to subgroups, it follow that L has a directly indecomposable direct factor M which lies in $\mathfrak{V}$. However, $\mathcal{K} - \mathfrak{V}$ is a Remak

decomposition of L (Proposition IV.3.3) and so M is isomorphic to a member of $\mathcal{K} - \mathfrak{V}$ (Theorem IV.3.11) and $M \in \mathfrak{V}$ by assumption. This is impossible as no member of $\mathcal{K} - \mathfrak{V}$ lies in $\mathfrak{V}$. Finally, as $\mathfrak{V}$ is closed to direct products it follows that $V \in \mathfrak{V}$. Thus $\{L, V\}$ is $\mathfrak{V}$-separated.

(iii). Let $\mathcal{H}$ and $\mathcal{K}$ be two $\mathfrak{V}$-separated decompositions. Choose Remak decompositions $\mathcal{J}$ and $\mathcal{L}$ which refine $\mathcal{H}$ and $\mathcal{K}$, respectively.

Without loss of generality, assume that $|\mathfrak{V} \cap \mathcal{J}| \geq |\mathfrak{V} \cap \mathcal{L}|$ (we will see shortly these are equal). By Theorem IV.3.11 applied to $\mathfrak{V} \cap \mathcal{J} \subseteq \mathcal{J}$ and $\mathcal{L}$, there is $\mathcal{W} \subseteq \mathcal{L}$ such that $\mathcal{I} := (\mathcal{J} - \mathfrak{V}) \sqcup \mathcal{W}$ is a Remak decomposition of G. Thus, $\mathcal{I}$ is $\mathfrak{V}$-separated by *(i)*. Theorem IV.3.11 provides a $\varphi \in \operatorname{Aut} G$ such that $(\mathfrak{V} \cap \mathcal{J})\varphi = \mathcal{W}$. As $\mathfrak{V}$ is closed to isomorphic images, it follows that $\mathcal{W} \subseteq \mathfrak{V} \cap \mathcal{L}$. As $|\mathfrak{V} \cap \mathcal{L}| \leq |\mathfrak{V} \cap \mathcal{J}| = |\mathcal{W}|$, $\mathfrak{V} \cap \mathcal{L} = \mathcal{W}$. Thus, $\mathcal{I} = (\mathcal{J} - \mathfrak{V}) \sqcup (\mathfrak{V} \cap \mathcal{L})$.

As shown in the proof of *(ii)*, $\mathcal{J} - \mathfrak{V}$ refines $\mathcal{H} - \mathfrak{V}$, and $\mathfrak{V} \cap \mathcal{L}$ refines $\mathfrak{V} \cap \mathcal{K}$. Thus, Proposition IV.3.5 proves that $(\mathcal{H} - \mathfrak{V}) \sqcup (\mathfrak{V} \cap \mathcal{K})$ is a direct decomposition of G, and it is $\mathfrak{V}$-separated.

(iv). Let $V := \langle \mathfrak{V} \cap \mathcal{H} \rangle$ and $H := \langle \mathcal{H} - \mathfrak{V} \rangle$. Fix $w \in W$, $f, f' : X \to G$ with $\operatorname{im} f' \subseteq V$. As $G = H \times V$ we write $f = f_V \times f_H$ for unique $f_H : X \to H$ and $f_V : X \to V$. As $V \in \mathfrak{V}$, $1 = W(V) = \{w\bar{g} : g : X \to V, w \in W\}$ so that $w\overline{f'_V f_V} = 1 = w\overline{f_V}$ for each $w \in W$. Hence,

$$w\overline{f'f} = w\overline{(f'_V \times 1_H)(f_V \times f_H)} = w\overline{f'_V f_V} \times w\overline{f_H} = w\overline{f_H} = w\overline{f_H} \times w\overline{f_V} = w\bar{f}.$$

Hence, $\operatorname{im} f' \subseteq W^*(G)$ so that $V \leq W^*(G)$. □

Proposition IV.4.15. *Let $\mathfrak{V} = \mathfrak{V}(W)$, G be a group, such that $Z(G) \leq W^*(G) \leq M \trianglelefteq G$ where M is generically split in G. If $\mathcal{X}$ is a Remak decomposition of M, then then either $\{G\}$ is $\mathfrak{V}$-separated or there is a nonempty subset $\mathcal{W} \subseteq \mathcal{X}$ and a subgroup $H \leq G$, such that $G = H \rtimes \langle \mathcal{W} \rangle$. Furthermore, if $\mathcal{H}$ is a $\mathfrak{V}$-refined direct decomposition of G, then $(\mathcal{H} \cap \mathfrak{V})Z(M) = \mathcal{W}Z(M)$.*

Proof. If $G \in \mathfrak{V}$ then $G = W^*(G) = M$ and so any $\mathcal{X}$ is a $\mathfrak{V}$-separated direct decomposition of G. Thus we assume that $G \notin \mathfrak{V}$.

Suppose that $\{G\}$ is not $\mathfrak{V}$-separated. Then by Proposition IV.4.14.*(ii)* there is a direct decomposition $\{H, V\}$ of G which is $\mathfrak{V}$-separated and $1 \neq V \in \mathfrak{V}$. Since M is generically split, $\{H \cap M, V \cap M\}$ is a direct decomposition of M. By Proposition IV.4.14.*(iv)*, $V \leq W^*(G) \leq M$ so that $\{H \cap M, V\}$ is a direct decomposition of M. Let $\mathcal{H}$ be a Remak decomposition of G. Set $\mathcal{Z} := \{Y \in \mathcal{H} : Y \leq V\}$, and then extend $\mathcal{Z}$ to a Remak decomposition $\mathcal{Y}$ of M. From Theorem

IV.3.11, applied to M and $\mathcal{Z} \subseteq \mathcal{Y}$, there is $\mathcal{W} \subseteq \mathcal{X}$ such that $(\mathcal{Y}-\mathcal{Z}) \sqcup \mathcal{W}$ is a Remak decomposition of M. As $V \neq 1$, $0 < |\mathcal{Z}| = |\mathcal{W}|$. Also, $G = \langle H, V \rangle = \langle H, \mathcal{Y} - \mathcal{Z}, \mathcal{W} \rangle$. As, $H \cap \langle \mathcal{W} \rangle \leq M$, it follows that $H \cap \langle \mathcal{W} \rangle = (H \cap M) \cap \langle \mathcal{W} \rangle = \langle \mathcal{Y} - \mathcal{Z} \rangle \cap \langle \mathcal{W} \rangle = 1$. So $G = H \rtimes \langle \mathcal{W} \rangle$. By Corollary IV.3.14.$(i)$, $\mathcal{Y}Z(M) = ((\mathcal{Y} - \mathcal{Z}) \sqcup \mathcal{W})Z(M)$, so $\mathcal{Z}Z(M) = \mathcal{W}Z(M)$. □

IV.4.5 Central Reduction Algorithms

Definition IV.4.16. *A* centrally-refined *direct decomposition $\mathcal{H}$ of a group G is a direct decomposition in which every abelian member is cyclic of prime power order, and every nonabelian member has no abelian direct factor.*

Theorem IV.4.17. *There is a deterministic polynomial-time algorithm which, given a group in $\mathbb{G}_n$, returns a centrally-refined direct decomposition of G.*

Proof. Let $G \in \mathbb{G}_n$.

Algorithm. Use the algorithm for Definition IV.4.19.(i) to compute $Z(G)$. If $Z(G) = 1$ then return $\{G\}$. If $Z(G) > 1$, use the algorithm for Definition IV.4.19.(ii), find a Remak decomposition $\mathcal{X}$ for $Z(G)$. Use (IV.2.12) to build $\mathcal{W} := \{W \in \mathcal{X} : \exists K \leq G, G = K \times W\}$. Use (IV.2.12) to find $K \leq G$ such that $G = K \times \langle \mathcal{W} \rangle$. Return $\{K\} \sqcup \mathcal{W}$.

Correctness. If $Z(G) = 1$ then G has no abelian direct factors and so $\{G\}$ is a centrally-refined direct decomposition of G. Now assume $Z(G) > 1$ and that $\mathcal{X}$ is Remak decomposition of G. By Proposition IV.4.15, $\mathcal{W}$, $G = H \rtimes \langle \mathcal{W} \rangle$ with H having no central direct factor. As $\langle \mathcal{W} \rangle \leq Z(G)$ it follows that $G = H \times \langle \mathcal{W} \rangle$ and $\{H\} \sqcup \mathcal{W}$ is a centrally-refined direct decomposition of G.

Timing. The algorithm uses $O(\log |G|)$ calls to polynomial-time algorithms for $\mathbb{G}_n$. □

Theorem IV.4.18. *There is a deterministic polynomial-time algorithm which, given $G \in \mathbb{G}_n$ and a decomposition $\mathcal{H}$ of G, returns a centrally-refined direct decomposition $\mathcal{K}$ of G such that if $\mathcal{H}M$ refines $\mathcal{J}M$ for a generically split abelian subgroup $M \geq Z(G)$ and a direct decomposition $\mathcal{J}$ of G, then $\mathcal{K}M$ refines $\mathcal{J}M$.*

Proof. Algorithm. Begin with $\mathcal{K} := \emptyset$ and $J := 1 \leq G$. Now loop over each $H \in \mathcal{H}$ and perform the following steps. Set $J := \langle J, H \rangle$ and use (IV.2.12) to construct $\mathcal{L} := \{K \in \mathcal{K} : \exists X \leq J, J = K \times X\}$. Use (IV.2.12) to compute $X \leq J$ such that $J = \langle \mathcal{L} \rangle \times X$. Let $\mathcal{X}$ be the return of the algorithm

for Theorem IV.4.17 applied to X, and set $\mathcal{K} := \mathcal{L} \sqcup \mathcal{X}$. Then continue with the next term in the loop. When the loop ends, return $\mathcal{K}$.

Correctness. We claim the following loop invariants: J is generated by a subset of $\mathcal{H}$, $\mathcal{K}$ is a centrally-refined direct decomposition of $\langle \mathcal{K} \rangle$. At the end of each loop iteration, $\langle \mathcal{K} \rangle = J$ and so at the end of the loop, $J = G$ and so $\mathcal{K}$ is a centrally-refined direct decomposition of G.

The loop invariants are initially true. It is also clear that J is generated by a subset of $\mathcal{H}$ and the loop ends once $J = G$. Within the loop, $\mathcal{L} \subseteq \mathcal{K}$ and so $\mathcal{L}$ is a centrally-refined direct decomposition of $\langle \mathcal{L} \rangle$. By assumption, $\mathcal{X}$ is also a centrally-refined direct decomposition of X. As $J = \langle \mathcal{L} \rangle \times X$, it follows that $\mathcal{L} \sqcup \mathcal{X}$ is a centrally-refined direct decomposition of J. Hence, $\mathcal{K}$ is maintained as a centrally-refined direct decomposition of $\langle \mathcal{K} \rangle$.

Now suppose that $\mathcal{H}M$ refines $\mathcal{J}M$ for some direct decomposition $\mathcal{J}$ of G. Suppose that $H \in \mathcal{H}$ is the current iterate. By induction we assume that $\mathcal{K}$ refines $\langle \mathcal{K} \rangle \cap \mathcal{J}$. By assumption, there is a unique $J_H \in \mathcal{J}$ such that $H \leq J_H M$. Since H is not contained in $\langle \mathcal{K} \rangle$ it is also not contained in $\langle \mathcal{L} \rangle$. As J_H is a direct factor of G, $J \cap J_H$ is a direct factor of J. Furthermore, $Z(G) \leq M \leq HM \leq JM$ so $Z(G) \leq Z(JM)$. Thus, $H \leq (J \cap J_H)Z(JM)$. Therefore H lies in $YZ(JM)$ for some (unique) direct factor Y of J; see Corollary IV.3.14.(i). By Corollary IV.3.14.(i) applied to $J = \langle \mathcal{L} \rangle \times X$, and the fact that H does not lie in $\mathcal{L}Z(JM)$, it follows that $H \leq XZ(JM)$. As the members of $\mathcal{K} - \mathcal{L}$ satisfy (IV.13), it follows that $XZ(J) \leq (J \cap J_H)Z(JM)$ (inequality is possible). Thus, the updated $\mathcal{K} := (\mathcal{L} \sqcup \mathcal{X})Z(JM)$ refines $(J \cap \mathcal{J})Z(JM)$. At the end of the loop, $G = J$ and so $\mathcal{K}M$ refines $\mathcal{J}M$.

Timing. The algorithm uses polynomial time methods with $|\mathcal{H}| \leq \log |G|$ recursive calls.

□

IV.4.6 Reduction Algorithms

In this section we provide the algorithms to reduce a direct decomposition of $G/M(G)$, $M \in \{W^*, O_{\mathfrak{V}(W)}\}$ to a direct decomposition of G, see Theorem IV.4.23.

Throughout this section, we assume that $\mathfrak{V} := \mathfrak{V}(W)$ is a group variety (Section IV.4.1) and that $\mathbb{G}_n$ is a computational domain (Section IV.2.2).

Definition IV.4.19. *A computational domain $\mathbb{G}_n$ is W-computable if there are polynomial-time algorithms (in n) for each of the following:*

(i) given $G \in \mathbb{G}_n$, return generators for $M(G)$, where $M(G)$ is either $W^*(G)$ or $O_{\mathfrak{V}(W)}(G)$, and

(ii) given $G \in \mathbb{G}_n$ with $G \in \mathfrak{V}(W)$, return a Remak decomposition of G.

Example IV.4.20. *Let $W = [x_1, x_2]$, so $\mathfrak{V} := \mathfrak{V}(W)$ is the group variety of abelian groups and the marginal subgroups $W^*(G)$ are the center of groups $G \in \mathbb{G}_n$; see Example IV.4.4.(i). Then any computational domain $\mathbb{G}_n$ with the hypothesized routines of Section IV.2.2 (for example:* QPERM, PRMAT, *and* PC*) are W-computable; see (IV.2.8) and Proposition IV.2.15.*

Remark IV.4.21. *It is possible that for some words W and computational domains $\mathbb{G}_n$, generators can be obtained for both $W^*(G)$ and $O_{\mathfrak{V}(W)}(G)$. In such a case either subgroup can be used as $M(G)$ for the algorithms of this section.*

Theorem IV.4.22. *Let $\mathbb{G}_n$ be W-computable and $V := \mathfrak{V}(W)$. Then there is a deterministic polynomial-time algorithm which: given $G \in \mathbb{G}_n$, returns a $\mathfrak{V}$-separated direct decomposition $\mathcal{H}$ of G in which $|\mathcal{H} - \mathfrak{V}| \leq 1$ and each member of $\mathfrak{V} \cap \mathcal{H}$ is directly indecomposable.*

Proof. Algorithm. Use the algorithm for Definition IV.4.19.(i) to compute $M(G)$. If $M(G) = 1$ then return $\{G\}$. If $M(G) > 1$, use the algorithm for Definition IV.4.19.(ii), find a Remak decomposition $\mathcal{X}$ for $M(G)$. Use (IV.2.12) to build

$$\mathcal{W} := \{W \in \mathcal{X} : \exists Z(G) \leq K \leq G, G/Z(G) = K/Z(G) \times WZ(G)/Z(G)\}. \tag{IV.25}$$

Use (IV.2.12) to find $Z(G) \leq K \leq G$ such that $G/Z(G) = K/Z(G) \times \langle \mathcal{W} \rangle Z(G)/Z(G)$. Now apply the algorithm for Theorem IV.4.18 to $\{K\} \sqcup \mathcal{W}$ and return the output of that algorithm.

Correctness. If $M(G) = 1$ then either $1 = O_{\mathfrak{V}}(G) \geq W^*(G)$ (Proposition IV.4.9.(i)) or $1 = W^*(G)$; in any case, $W^*(G) = 1$. By Proposition IV.4.14.(iv), if G has a direct factor which lies in $\mathfrak{V}$ then that factor lies in $W^*(G) = 1$. Hence, G has no direct factor which lies in $\mathfrak{V}$ and so $\{G\}$ is $\mathfrak{V}$-separated.

Now let $M(G) > 1$ and $\mathcal{X}$ be a Remak decomposition of $M(G)$. The set $\mathcal{H} := \{K\} \sqcup \mathcal{W}$ is a normal decomposition of G where $\mathcal{H} = \mathcal{H}Z(G)$. Therefore, the algorithm of Theorem IV.4.18 can be applied. Furthermore, $Z(M)$ is characteristic in M and generically split in $Z(M)$. As M is generically split in G, it follows by Proposition IV.3.10 that $Z(M)$ is generically split in G. Thus, Theorem IV.4.18 guarantees that the return is a centrally-refined direct decomposition $\mathcal{K}$ of G such

that if $\mathcal{H}Z(M)$ refines $\mathcal{J}Z(G)$ for a direct decomposition $\mathcal{J}$ of G, then $\mathcal{K}Z(M)$ refines $\mathcal{J}Z(M)$. By Proposition IV.4.15, we know $\mathcal{H}Z(M)$ refines $\mathcal{J}Z(M)$ for some $\mathfrak{V}$-refined direct decomposition of G, and thus the return is indeed $\mathfrak{V}$-refined.

Timing. The algorithm applies polynomial-time algorithms $O(\log|G|)$ times. □

Theorem IV.4.23. *Let $\mathbb{G}_n$ be a W-computable computational domain where $W^*(G) \geq Z(G)$ for each $G \in \mathbb{G}_n$, and $\mathfrak{V} := \mathfrak{V}(W)$. Then, there is a deterministic polynomial-time algorithm which: given $G \in \mathbb{G}_n$ and a normal decomposition $\mathcal{H}$ of G, returns a $\mathfrak{V}$-refined direct decomposition $\mathcal{K}$ of G such that if $\mathcal{H}N$ refines $\mathcal{J}N$ for $M(G) \leq N \leq G$ with N generically split in G, and $\mathcal{J}$ a direct decomposition of G, then $\mathcal{K}N$ refines $\mathcal{J}N$.*

Proof. Algorithm. Begin with $\mathcal{K} := \emptyset$ and $J := 1 \leq G$. Now loop over each $H \in \mathcal{H}$ and perform the following steps. Set $J := \langle J, H\rangle$ and use (IV.2.12) to construct $\mathcal{L} := \{K \in \mathcal{K} : \exists X \leq J, J = K \times X\}$. Use (IV.2.12) to compute $X \leq J$ such that $J = \langle\mathcal{L}\rangle \times X$. Let $\mathcal{X}$ be the return of the algorithm for Theorem IV.4.22 applied to X, and set $\mathcal{K} := \mathcal{L} \sqcup \mathcal{X}$. Then continue with the next term in the loop. When the loop ends, return $\mathcal{K}$.

Correctness. We claim the following loop invariants: J is generated by a subset of $\mathcal{H}$ and $\mathcal{K}$ is a $\mathfrak{V}$-refined direct decomposition of $\langle\mathcal{K}\rangle$. At the end of each loop iteration, $\langle\mathcal{K}\rangle = J$ and so at the end of the loop, $J = G$ and so $\mathcal{K}$ is a $\mathfrak{V}$-refined direct decomposition of G.

The loop invariants are initially true. It is also clear that J is generated by a subset of $\mathcal{H}$ and the loop ends once $J = G$. Within the loop, $\mathcal{L} \subseteq \mathcal{K}$ and so $\mathcal{L}$ is a $\mathfrak{V}$-refined direct decomposition of $\langle\mathcal{L}\rangle$. By assumption, $\mathcal{X}$ is also a $\mathfrak{V}$-refined direct decomposition of X. As $J = \langle\mathcal{L}\rangle \times X$, it follows that $\mathcal{L} \sqcup \mathcal{X}$ is a $\mathfrak{V}$-refined direct decomposition of J. Hence, $\mathcal{K}$ is maintained as again $\mathfrak{V}$-refined.

Now suppose that $\mathcal{H}M$ refines $\mathcal{J}M$ for some direct decomposition $\mathcal{J}$ of G. Suppose that $H \in \mathcal{H}$ is the current iterate. By induction we assume that $\mathcal{K}$ refines $\langle\mathcal{K}\rangle \cap \mathcal{J}$. By assumption, there is a unique $J_H \in \mathcal{J}$ such that $H \leq J_H M$. Since H is not contained in $\langle\mathcal{K}\rangle$ it is also not contained in $\langle\mathcal{L}\rangle$. As J_H is a direct factor of G, $J \cap J_H$ is a direct factor of J. Furthermore, $Z(G) \leq M(G) \leq N$ so $Z(G) \leq Z(JN)$. Thus, $H \leq (J \cap J_H)Z(JN)$. Therefore H lies in $YZ(JN)$ for some (unique) direct factor Y of J; see Corollary IV.3.14.(i). By Corollary IV.3.14.(i) applied to $J = \langle\mathcal{L}\rangle \times X$, and the fact that H does not lie in $\mathcal{L}Z(JN)$, it follows that $H \leq XZ(JN)$. As the members of $\mathcal{K} - \mathcal{L}$ satisfy (IV.13), it follows that $XZ(J) \leq (J \cap J_H)Z(JN)$. Thus, the updated $\mathcal{K} := (\mathcal{L} \sqcup \mathcal{X})Z(JN)$ refines $(J \cap \mathcal{J})Z(JN)$. At the end of the loop, $G = J$ and so $\mathcal{K}N$ refines $\mathcal{J}N$.

Timing. The algorithm loops over the elements of $\mathcal{H}$ and within each loop it uses polynomial-time methods on a set of size at most $|\mathcal{H}|$. Thus, the algorithm uses $O(|\mathcal{H}|)$ polynomial-time methods. □

IV.4.7 Enrichment

In this section we define the largest ring over which a biadditive map b is faithfully bilinear. In the next section, we show how this ring parameterizes the direct decompositions of b. This technique arose in [42, 43] to study the model theory of bilinear maps. Here the definitions are different (and apply more generally) but they are ultimately equivalent.

Throughout this section let $b : V \times V \to W$ be a biadditive map of abelian p-groups V and W.

Definition IV.4.24. *Define*

$$\mathrm{Rich}(b) := \{(f,g) \in \mathrm{End}\, V \oplus \mathrm{End}\, W : b(uf,v) = b(u,v)g = b(u,vf), \forall u,v \in V\}.$$

This is the enrichment ring *of* b.

The title of "enrichment" is justified by the following:

Theorem IV.4.25. *Let $b : V \times V \to W$ be a biadditive map. Then the following hold:*

(i) $\mathrm{Rich}(b)$ *is a subring of* $\mathrm{End}\, V \oplus \mathrm{End}\, W$, *and V and W are (right)* $\mathrm{Rich}(b)$*-modules.*

(ii) If b is K-bilinear, for a commutative ring K, then $K/(\mathrm{Ann}_K V \cap \mathrm{Ann}_K W)$ embeds in $\mathrm{Rich}(b)^{op}$. *Whence,* $\mathrm{Rich}(b)$ *is the largest ring over which b is "faithful" bilinear, i.e.:* $\mathrm{Ann}_{\mathrm{Rich}(b)} V \cap \mathrm{Ann}_{\mathrm{Rich}(b)} W = 0$.

Proof. (i). Set $S := \mathrm{Rich}_R(b)$. Evidently S is closed to sums. For composition, let $(f,g),(f',g') \in S$. Then for all $u,v \in V$ we have

$$b(uff',v) = b(uf,v)g' = b(u,vf)g' = b(u,v)gg'$$
$$b(uff',v) = b(uf,v)g' = b(u,vf)g' = b(u,vff').$$

Hence $(ff',gg') \in S$.

(*ii*). Let b be K-bilinear. As V and W are K-modules, there are $\rho : K \to \operatorname{End} V$ and $\hat{\rho} : K \to \operatorname{End} W$ such that $rv = \rho(r)v$ and $rw = \hat{\rho}(r)w$ for $v \in V$, $w \in W$, and $r \in K$. As b is K-bilinear, $b(ru, v) = rb(u, v) = b(u, rv)$ so $(\rho(r), \hat{\rho}(r)) \in \operatorname{Rich}(b)^{op}$. □

Proposition IV.4.26. *If* $\operatorname{rad} b = 0$ *and* $b(V, V) = W$ *then* $\operatorname{Rich}(b)$ *is commutative.*

Proof. For all $(f, g), (f', g') \in \operatorname{Rich}(b)$ and $u, v \in V$ we have

$$\begin{aligned} b(u[f, f'], v) &= b(u, vff') - b(u, vf'f) = b(u, vff') - b(u, vf')g \\ &= b(u, vff') - b(uf', v)g = b(u, vff') - b(uf', vf) \\ &= b(u, vff') - b(u, vff') = 0. \end{aligned}$$

This is easily repeated in the second variable to show that $v[f, f'] \in \operatorname{rad} b = 0$, for all $v \in V$. Thus, $[f, f'] = 0$. Also,

$$\begin{aligned} b(u, v)[g, g'] &= b(u, v)gg' - b(u, v)g'g = b(u, vff') - b(u, vf'f) \\ &= b(u, v[f, f']) = 0. \end{aligned}$$

As W is generated by $b(u, v)$, $u, v \in V$, and $b(u, v)[g, g'] = 0$, it follows that $[g, g'] = 0$. □

Remark IV.4.27. *If* $\operatorname{rad} b = 0$ *and* $(f, g), (f', g) \in \operatorname{Rich}(b)$ *then* $f = f'$. *If* $W = b(V, V)$ *and* $(f, g), (f, g') \in \operatorname{Rich}(b)$ *then* $g = g'$. *So if* $\operatorname{rad} b = 0$ *and* $W = b(V, V)$ *then the first variable determines the second and vice-versa. In this setting we write* $(f, \hat{f})$ *for elements in* $\operatorname{Rich}(b)$.

IV.4.8 Direct Products of Bilinear Maps

In this section we define the direct product of bilinear maps and then use the enrichment ring to parameterize the direct decompositions of a bilinear map.

Let $b : V \times V \to W$ and $b' : V' \times V' \to W'$ be two K-bilinear maps. Then form $b \oplus b' : V \oplus V' \times V \oplus V' \to W \oplus W'$ by

$$(b \oplus b')(u \oplus u', v \oplus v') := b(u, v) \oplus b(u', v'). \tag{IV.26}$$

This makes $b \oplus b'$ an K-bilinear map. This is the product in the category of K-bilinear maps.

We also have a natural internal description. Suppose that $b : V \times V \to W$ is an K-bilinear map. Then a *direct decomposition* of b is a set $\mathcal{B} \subseteq PG(V) \times PG(W)$ (here $PG(X)$ denotes the set of K-submodules of an K-module X) such that

$$V = \bigoplus_{(U,Z)\in\mathcal{B}} Z, \quad W = \bigoplus_{(U,Z)\in\mathcal{B}} Z, \text{ and } b(U,U) \leq Z, \quad \forall (U,Z) \in \mathcal{B}. \tag{IV.27}$$

This makes b naturally isomorphic (in the category of bilinear maps) to $\bigoplus_{(U,Z)\in\mathcal{B}} c_{(U,Z)}$, where $c_{(U,Z)} : U \times U \to Z$ is defined by $c(u,v) := b(u,v)$ for all $u, v \in U$. (Note that $b(U,U') \leq Z \cap Z' = 0$ for distinct $(U,Z), (U',Z') \in \mathcal{B}$ so that U and U' are perpendicular.)

By standard linear algebra, given a direct decomposition $\mathcal{X}$ of an R-module V there is a corresponding set of pairwise orthogonal supplementary idempotents $\mathcal{E}(\mathcal{X})$ which are the projections of the decomposition. Therefore given a direct decomposition $\mathcal{B}$ of an K-bilinear map $b : V \times V \to W$, we define $\mathcal{E}(\mathcal{B})$ as the set of ordered pairs (e, ε) of projection endomorphisms $e \in \operatorname{End}_K V$, $\varepsilon \in \operatorname{End}_K W$ resulting from the direct factors in $\mathcal{B}$. Likewise, given a set $\mathcal{E}$ of supplementary idempotents of $\operatorname{End}_K V \times \operatorname{End}_K W$, then $\mathcal{B}(\mathcal{E}) := \{(Ve, W\varepsilon) : (e,\varepsilon) \in \mathcal{E}\}$.

Theorem IV.4.28. *Let b be a non-degenerate bilinear map and $\mathcal{B}$ a direct decomposition of b.*

(i) $\mathcal{E}(\mathcal{B})$ is a set of pairwise orthogonal supplementary idempotents of $\operatorname{Rich}(b)$ *and $\mathcal{B}(\mathcal{E}(\mathcal{B})) = \mathcal{B}$.*

(ii) $\mathcal{B}(\mathcal{E})$ is a direct decomposition of b and $\mathcal{E}(\mathcal{B}(\mathcal{E})) = \mathcal{E}$.

(iii) $\mathcal{B}$ is fully refined if, and only if, $\mathcal{E}(\mathcal{B})$ is a frame of $\operatorname{Rich}(b)$.

(iv) b is directly indecomposable if, and only if, $\operatorname{Rich} b$ *is a local ring.*

Proof. These are readily verified, compare [42, Section 3]. □

Corollary IV.4.29. *Given a biadditive map $b : V \times V \to W$ where* $\operatorname{rad} b = 0$ *and $W = b(V,V)$, there is a unique fully refined direct decomposition of b.*

Proof. By Proposition IV.4.26, $\operatorname{Rich}(b)$ is commutative. Thus it has a unique direct decomposition into a product of local commutative rings, that is, it has a unique frame. Thus, by Theorem IV.4.28.*(iii)*, b has a unique fully refined direct decomposition. □

IV.4.9 Finding Direct Decompositions of Bilinear Maps

In this section we give an algorithm to find a direct decomposition of a bilinear map. The general setting depends on the work of Ronyai [50] on algorithms for associative algebras. However, the setting we require for Theorem IV.1.3 requires only the work of Berlekamp to factor polynomials over finite fields [8]. Thus the method is deterministic if the characteristic is small, otherwise, the method is only Las Vegas.

Let $b : V \times V \to W$ be a $\mathbb{Z}_{p^e}$-bilinear map for which bases $\mathcal{X}$ and $\mathcal{Z}$ are known for V and W. Thus $b(u, v) = uBv^t$ as in (IV.11). In this notation we have:

$$\mathrm{Rich}(B) = \{(F, G) \in \mathrm{End}\, V \times \mathrm{End}\, W : FB = B^G = BF^t\}. \tag{IV.28}$$

We recognize $FB = B^G = BF^t$ is a system of linear equations over $\mathbb{Z}_{p^e}$ in the variables $F_{x,x'}$ and $G_{z,z'}$, for $x, x' \in \mathcal{X}$, and $z, z' \in \mathcal{Z}$. This can be solved deterministically, see Section IV.2.3. Thus we have:

Proposition IV.4.30. *There is is a deterministic polynomial time algorithm which, given a $\mathbb{Z}_{p^e}$-bilinear map $b : V \times V \to W$ specified by bases $\mathcal{X}$ for V, $\mathcal{Z}$ for W, and structure constants matrix B with respect to these bases, returns a basis for* $\mathrm{Rich}(b)$ *as a subring of* $\mathrm{End}\, V \times \mathrm{End}\, W$.

Theorem IV.4.31. *There is a deterministic polynomial time algorithm, assuming an oracle for polynomial factorization of a field of characteristic p, which given a $\mathbb{Z}_{p^e}$-bilinear map b as in Proposition IV.4.30, returns a fully refined direct decomposition of b.*

Proof. Algorithm. Use Proposition IV.4.30 to compute $\mathrm{Rich}(b)$. Then use the algorithm of [50, 5.1] to find a frame $\bar{\mathcal{E}}$ of $\mathrm{Rich}(b)/J(\mathrm{Rich}(b))$ and apply the lifting of idempotents formula, Lemma IV.2.16, to $\bar{\mathcal{E}}$ to obtain a frame $\mathcal{E}$ of $\mathrm{Rich}(b)$. Return $\{b_{Ve} : Ve \times Ve \to W\varepsilon : (e, \varepsilon) \in \mathcal{E}\}$.

Correctness. Let $R := \mathrm{Rich}(b)$. As $R/J(R)$ is a semisimple of characteristic dividing p^e, it is in fact of characteristic p and a $\mathbb{Z}_p$-vector space. Thus $pR \subseteq J(R)$. Hence, R/pR is a $\mathbb{Z}_p$-algebra, so [50, Section 5.1] can be applied to find a frame of $\bar{\mathcal{E}}$. As R is finite, $J(R)$ is nilpotent and so we can apply the lifting of idempotents lemma to produce a frame of R. By Theorem IV.4.28, the return is a fully refined direct decomposition of b.

Timing. The algorithms of [50, 5.1] are deterministic polynomial-time, up to the factoring of polynomials over finite fields of characteristic p. □

Remark IV.4.32. *(i) Berlekamp [7] provided a deterministic polynomial time algorithm to factor polynomials over finite fields if the characteristic is small compared to the degree. His later Las Vegas method works in all characteristics, and subsequent algorithms have improved the timing, see [57, Chapter 14].*

(ii) The method of [50, 5.1] can be replaced by the nearly optimal Monte Carlo method of [12]. For Las Vegas speedup, observe that $\mathrm{Rich}(b)/p\,\mathrm{Rich}(b)$ *embeds in* $M_d(\mathbb{Z}_p) \oplus M_f(\mathbb{Z}_p)$ *where* $d = \operatorname{rank} V$ *and* $f = \operatorname{rank} W$. *Thus, [22] can be applied as well.*

(iii) If $\operatorname{rad} b = 0$ *and* $W = b(V, V)$, *then by Proposition IV.4.26,* $\mathrm{Rich}(b)$ *is commutative and there is a unique fully refined direct decomposition of b, (Corollary IV.4.29). Thus, instead of [50, 5.1] we may use [14], and in fact the entire problem is naturally equivalent to factoring polynomials, that is, it does not require the reductions used in [50] using general associative algebras.*

IV.5 The Remak Decomposition Algorithms

In this section we prove Theorem IV.1.3. This relies on five distinct stages. First, in Section IV.5.1, a proof is given for p-groups of class 2. In Section IV.5.2 the algorithm is extended to p-groups of any class. Section IV.5.3 addresses solvable groups. Section IV.5.4 deals with almost semisimple groups, and Section IV.5.5 puts these methods together to prove Theorem IV.1.3.

IV.5.1 p-groups of Class 2

In this section we prove Theorem IV.1.3 for the case of p-groups P of class 2. The algorithm depends on a bilinear map associated to P, the algorithm of Theorem IV.4.31, and the algorithm of Theorem IV.4.22 where the variety is $\mathfrak{N}_1$, the variety of abelian groups (Corollary ??).

Write the operations of $P/Z(P)$ and P' additively. A result of Baer [6] associates to P a biadditive map $b := \mathsf{Bi}(P/Z(P), P')$ defined by $b : P/Z(P) \times P/Z(P) \to P'$ where $b(Z(P)x, Z(P)y) := [x, y]$, for each $x, y \in P$. Note that $\operatorname{rad} b = 0$ and $b(P/Z(P), P/Z(P)) = [P, P]$. Also, b is naturally $\mathbb{Z}_{p^e}$-bilinear where $P^{p^e} = 1$.

Theorem IV.5.1. *There is a deterministic polynomial time algorithm which, given a p-group of class 2 in* $\mathbb{G}_n$, *returns a Remak decomposition of the group.*

Proof. Let P be a p-group of class 2 in $\mathbb{G}_n$.

Algorithm. Let $b := \mathsf{Bi}(P/Z(P), P')$. Use the algorithm of Theorem IV.4.31 to find a central decomposition $\mathcal{H} = \mathcal{H}Z(P)$ of P such that $\{b_{H/Z(P)} : H \in \mathcal{H}\}$ is the fully refined direct decomposition of b. Apply Corollary ?? and return the output of that algorithm.

Correctness. Suppose that $\mathcal{R}$ is a Remak decomposition of P. Then $[RZ(P), \langle \mathcal{R} - \{R\}Z(P)\rangle] = [R, \langle \mathcal{R} - \{R\}\rangle] = 1$, for $R \in \mathcal{R}$. By Proposition IV.4.11, $\mathcal{R}Z(G)/Z(G)$ and $\mathcal{R} \cap P'$ are direct decompositions of $P/Z(P)$ and P', respectively. Hence, $\mathcal{D} := \{b_{RZ(P)/Z(P)} : R \in \mathcal{R}\}$ is a direct decomposition of b. As b is nondegenerate and $P' = b(P/Z(P), P/Z(P))$, it has a unique fully refined direct decomposition (Corollary IV.4.29). Thus the return of Theorem IV.4.31 is this unique direct decomposition of b and so it refines $\mathcal{D}$. Therefore, $\mathcal{H}$ refines $\mathcal{R}Z(P)$ for any (thus by all, Corollary IV.3.14) Remak decomposition of P. Hence, Theorem IV.4.18 applies and returns a Remak decomposition of P.

Timing. The algorithm uses a constant number of polynomial time subroutines. □

Corollary IV.5.2. *There is a deterministic polynomial time algorithm which, given $G \in \mathbb{G}_n$ and a decomposition $\mathcal{H}$ of G such that $\mathcal{H} = \mathcal{H}\zeta_2(G)$ and $\mathcal{H}$ refines $\mathcal{J}\zeta_2(G)$ for some $\mathfrak{N}_2$-separated direct decomposition $\mathcal{J}$ of G, returns an $\mathfrak{N}_2$-separated direct decomposition $\mathcal{K}$ of G where $\mathcal{J}\zeta_2(G) = \mathcal{K}\zeta_2(G)$ and in which the members of $\mathfrak{N}_2 \cap \mathcal{K}$ are all directly indecomposable.*

Proof. Use Theorem IV.5.1 (together with the obvious decomposition of a nilpotent group into its Sylow subgroups) and (IV.2.8) to compute $\zeta_2(G)$ to satisfy the hypothesis of Theorem IV.4.23. □

IV.5.2 p-groups of General Class

In this section we prove Theorem IV.1.3 for the case of p-groups. The algorithm is a recursive use of Theorem IV.4.22 and uses Theorem IV.5.1 as the base case.

Theorem IV.5.3. *There is a deterministic polynomial time algorithm which: given a p-group group in $\mathbb{G}_n$, returns a Remak decomposition of the group.*

Proof. Let P be a p-group in $\mathbb{G}_n$.

Algorithm. If $\zeta_2(P) = P$ then apply the algorithm of Theorem IV.5.1 to P and return the result. Otherwise, make a recursive call with $P/\zeta_1(P)$ in the rôle of P to obtain a decomposition $\mathcal{H}$ of P in which $\mathcal{H} = \mathcal{H}\zeta_1(P)$ and $\mathcal{H}/\zeta_1(P)$ is a Remak decomposition of $P/\zeta_1(P)$. Use the algorithm of Corollary IV.5.2 on $\mathcal{H}\zeta_2(P)$, and return the output of that algorithm.

Correctness. Theorem IV.5.1 validates the return for the case were P has class c at most 2. So assume that $c > 2$. Thus, $P/\zeta_1(P)$ has class $c-1$ and by induction the recursive call returns a decomposition $\mathcal{H}$ of P where $\mathcal{H} = \mathcal{H}\zeta_1(P)$ and $\mathcal{H}/\zeta_1(P)$ is a Remak decomposition of $P/\zeta_1(P)$. Let $\mathcal{R}$ be a Remak decomposition of P. By Proposition IV.4.11, $\mathcal{R}\zeta_1(P)/\zeta_1(P)$ is a direct decomposition of $P/\zeta_1(P)$. Hence, $\mathcal{H}\zeta_1(P/\zeta_1(P))/\zeta_1(P)$ refines $\mathcal{R}\zeta_1(P/\zeta_1(P))/\zeta_1(P)$ by Corollary IV.3.14.(i) (applied to $P/\zeta_1(P)$). That is, $\mathcal{H}\zeta_2(P)$ refines $\mathcal{R}\zeta_2(P)$. Therefore, Corollary IV.5.2 applies and returns a $\mathfrak{N}_2$-separated direct decomposition $\mathcal{K}$ of G in which $\mathcal{K}\zeta_2(P) = \mathcal{R}\zeta_2(P)$ and every member of $\mathfrak{N}_2 \cap \mathcal{K}$ is directly indecomposable. We now show that $\mathcal{K}$ is a Remak decomposition of P.

As $\mathcal{R}$ is a Remak decomposition of P it is $\mathfrak{N}_2$-separated. By Proposition IV.4.14.(iii), it follows that $\mathcal{J} := (\mathcal{R} - \mathfrak{N}_2) \sqcup (\mathfrak{N}_2 \cap \mathcal{K})$ is a direct decomposition of P. As the members of $\mathcal{J}$ are directly indecomposable it follows that $\mathcal{J}$ is a Remak decomposition of P. In particular, $|\mathcal{R} \cap \mathfrak{N}_2| = |\mathcal{K} \cap \mathfrak{N}_2|$.

Next, as $\mathcal{K}\zeta_2(P) = \mathcal{R}\zeta_2(P)$ and both are $\mathfrak{N}_2$-separated, it follows from Proposition IV.3.7.(ii) that $|\mathcal{K} - \mathfrak{N}_2| = |\mathcal{R} - \mathfrak{N}_2|$. Thus,

$$|\mathcal{K}| = |\mathcal{K} - \mathfrak{N}_2| + |\mathfrak{N}_2 \cap \mathcal{K}| = |\mathcal{R} - \mathfrak{N}_2| + |\mathfrak{N}_2 \cap \mathcal{R}| = |\mathcal{R}|.$$

Hence, $\mathcal{K}$ is a direct decomposition of G of size equal to the size of a Remak decomposition of P: $\mathcal{K}$ is a Remak decomposition of P by Theorem IV.3.11.

Timing. The algorithm depends on polynomial time algorithms in a recursion of depth $c-2$. □

IV.5.3 Solvable Groups

In this section we prove Theorem IV.1.3 for solvable groups. The algorithm has two phases. First if the group has a trivial center then the algorithm uses Sylow system to reduce to the case of a p-group, where it uses Theorem IV.5.3. The second phase uses a recursion to the centerless case together with Theorem IV.4.18 and Corollary IV.5.2.

Theorem IV.5.4. *There is a deterministic polynomial time algorithm which: given a solvable group in $\mathbb{G}_n$ with trivial center, returns a Remak decomposition of the group.*

Proof. Let G be a solvable group in $\mathbb{G}_n$.

Algorithm. If $G = 1$ then return $\emptyset$. Otherwise, use (IV.2.11) to find a Sylow system $\mathcal{S}$ of G. For each $P \in \mathcal{S}$, use Theorem IV.5.3 to find a Remak decomposition $\mathcal{P}(P)$ of P. Set $\mathcal{K} := \bigcup_{P\in\mathcal{S}} \mathcal{P}(P)$. Then while there are distinct $X, Y \in \mathcal{K}$ such that $[X, Y] \neq 1$, set $\mathcal{K} := (\mathcal{K} - \{X, Y\}) \sqcup \{\langle X, Y\rangle\}$. When this loop completes, return $\mathcal{K}$.

Correctness. Assume $G \neq 1$ and note that $|\mathcal{S}| > 1$ since G is not nilpotent ($Z(G) = 1$). By Theorem IV.5.3 we know $\mathcal{P}(P)$ is a Remak decomposition of P for each $P \in \mathcal{S}$. Let $\mathcal{V} := \bigcup_{P\in\mathcal{S}} \mathcal{P}(P)$ be the set of vertices in a graph where edges are defined between members X and Y if, and only if, $[X, Y] \neq 1$. If $X, Y, Z \in \mathcal{V}$ are vertices where X and Y lie in the same connected component and Z does not, then $[Z, \langle X, Y\rangle] = 1$. Throughout the loop, $\mathcal{K}$ generates G. The loop ends when the distinct members of $\mathcal{K}$ pairwise centralize each other; that is, the loop returns the subgroups spanned by the connected components of the graph. Therefore, $[H, K] = 1$ for $H, K \in \mathcal{K}$, $H \neq K$. Furthermore,

$$G = \langle \mathcal{S}\rangle = \langle \mathcal{P}(P) : P \in \mathcal{S}\rangle = \langle \mathcal{K}\rangle.$$

Thus, some $\mathcal{J} \subseteq \mathcal{K}$ is a central decomposition of G. However, $Z(G) = 1$ and $1 \notin \mathcal{K}$ so $\mathcal{J} = \mathcal{K}$. Furthermore, as $H \cap \langle \mathcal{H} - \{H\}\rangle \leq Z(G) = 1$ for all $H \in \mathcal{K}$, we conclude that $\mathcal{K}$ is a direct decomposition of G.

Now we prove that each $K \in \mathcal{K}$ are directly indecomposable. Recall $K = \langle Q \in \mathcal{V} : Q \leq K\rangle$.

Suppose that $K = A \times B$, $A, B \neq 1$ and take $P \in \mathcal{S}$. As A and B are normal in K, $\{P \cap A, P \cap B\}$ is a direct decomposition of $P \cap K$. Let $\mathcal{Q}$ be a Remak decomposition of $P \cap K$ refining $\{P \cap A, P \cap B\}$. Notice that $\mathcal{P}_K(P) := \{Q \in \mathcal{P}(P) : Q \leq K\}$ is a direct decomposition of $P \cap K$ consisting of directly indecomposable groups, thus, also a Remak decomposition of $P \cap K$. As $\mathcal{P}_K(P)$ and $\mathcal{Q}$ are conjugate under a central automorphism of $P \cap K$, we can partition $\mathcal{P}_K(P)$ to create a coarser direct decomposition $\{\tilde{A}(P), \tilde{B}(P)\}$ which is conjugate under a central automorphism to $\{P \cap A, P \cap B\}$. As this is done for arbitrary $P \in \mathcal{S}$ it can be done for all $P \in \mathcal{S}$. Now take $Q, R \in \{Q \in \mathcal{V} : Q \leq K\}$ such that $Q \leq \tilde{A}(P_A)$ and $R \leq \tilde{B}(P_B)$ for $P_A, P_B \in \mathcal{S}$. Then $[Q, R] \leq [A, B] = 1$. Letting R range over all possibilities we see that $\{Q \in \mathcal{V} : Q \leq K\}$ has at least two connected components, which contradicts the assumption of how K was built.

Timing. Evidently we require integer factorization to find the primes dividing $|G|$, but

this is handled by an oracle. The recursion has depth equal to the number of prime divisors of $|G|$. Finally, the loop is a transitive closure and so it terminates in polynomial time. □

Corollary IV.5.5. *There is a deterministic polynomial time algorithm which: given a solvable group in $\mathbb{G}_n$, returns a Remak decomposition of the group.*

Proof. Let $G \in \mathbb{G}_n$ be a solvable group.

Algorithm. If G is nilpotent then find the unique Sylow system $\mathcal{S}$ of G and apply the algorithm of Theorem IV.5.3 on each $P \in \mathcal{S}$ to obtain a Remak decomposition $\mathcal{P}(P)$ for each $P \in \mathcal{S}$. Return $\bigcup_{P \in \mathcal{S}} \mathcal{P}(P)$.

Now G is not nilpotent. If $Z(G) = 1$ then use Theorem IV.5.4 and return the output of that algorithm. Else, if $\zeta_2(G) = \zeta_1(G)$ then use Theorem IV.5.4 to find a set $\mathcal{H} = \mathcal{H}\zeta_1(G)$ such that $\mathcal{H}/\zeta_1(G)$ is a Remak decomposition of $G/\zeta_1(G)$. Then apply Theorem IV.4.18 to return a Remak decomposition of G. Finally, if $\zeta_2(G) > \zeta_1(G)$, use a recursive call to find $\mathcal{H} = \mathcal{H}\zeta_1(G)$ such that $\mathcal{H}/\zeta_1(G)$ is a Remak decomposition of $G/Z(G)$. Then apply the algorithm of Corollary IV.5.2 to $\mathcal{H}\zeta_2(G)$ and return the result.

Correctness. If G is nilpotent this is clear, as is the case when $\zeta_1(G) = 1$. If $\zeta_2(G) = \zeta_1(G)$ then there is a unique Remak decomposition of $G/\zeta_1(G)$ and so $\mathcal{H}$ refines $\mathcal{R}\zeta_1(G)$ for any Remak decomposition $\mathcal{R}$ of G. Thus, Corollary IV.4.18 applies to return a Remak decomposition of G. Otherwise, $G > \zeta_2(G) > \zeta_1(G)$ and by induction $\mathcal{H}/\zeta_1(G)$ is a Remak decomposition of $G/\zeta_1(G)$. So $\mathcal{H}\zeta_2(G)$ refines $\mathcal{R}\zeta_2(G)$ and so Corollary IV.5.2 returns a Remak decomposition of G.

Timing. The algorithm makes at most $\log |G|$ recursions using polynomial time algorithms in the base cases. □

IV.5.4 Almost Semisimple Groups

In this section we prove Theorem IV.1.3 for *almost semisimple groups*, that is groups G with no proper normal abelian subgroups, equivalently $O_{\mathfrak{S}}(G) = 1$. The proof given is just one of many natural approaches for this case. Though it is not explicitly necessary in the following proofs, note that a group with trivial solvable radical has trivial center; hence, by Theorem IV.3.11, the group has a unique Remak decomposition.

The socle, $\mathrm{soc}(G)$, of G is the subgroup generated by all minimal normal subgroups.

Lemma IV.5.6. *If G is a finite group with $O_{\mathfrak{S}}(G) = 1$, then the set of minimal normal subgroups of G is a direct decomposition of* $\mathrm{soc}(G)$.

Proof. See [49, pp. 85-88]. □

Theorem IV.5.7. *Let G be a finite group with $O_{\mathfrak{S}}(G) = 1$ and direct decomposition $\mathcal{H}$. Then*

(i) $H \cap \mathrm{soc}(G) = \mathrm{soc}(H)$ *for all* $H \in \mathcal{H}$,

(ii) $\mathcal{H} \cap \mathrm{soc}(G) = \{\mathrm{soc}(H) : H \in \mathcal{H}\}$ *is a direct decomposition of* $\mathrm{soc}(G)$,

(iii) if $\mathcal{M}$ is the set of minimal normal subgroups of G, then $\mathcal{M}$ refines $\mathcal{H} \cap \mathrm{soc}(G)$; and

(iv) $\mathcal{H} = \{C_G(C_G(\mathrm{soc}(H))) : H \in \mathcal{H}\}$.

Proof. Since $\mathcal{H}$ is a direct decomposition of G, if $H \in \mathcal{H}$ and M is a minimal normal subgroup of H, then M is a minimal normal subgroup of G. Thus $\mathrm{soc}(H) \leq H \cap \mathrm{soc}(G)$.

Now suppose that M is a minimal normal subgroup of G. Since each $H \in \mathcal{H}$ is normal in G it follows that $H \cap M$ is normal in G; hence, $H \cap M$ is 1 or M. Suppose that $H \cap M = 1$ for all $H \in \mathcal{H}$. Hence, $[H, M] \leq H \cap M = 1$ for all $H \in \mathcal{H}$. Thus, $[G, M] = [\langle \mathcal{H} \rangle, M] = \langle [H, M] : H \in \mathcal{H} \rangle = 1$. This proves that $M \leq Z(G) = 1$. This is impossible as $M > 1$. Thus, there exists some $H_M \in \mathcal{H}$ such that $H_M \cap M = M$, that is, $M \leq H_M$. Since $H_M \cap K = 1$ for all $K \in \mathcal{H} - \{H_M\}$, it follows that M is not contained in any $K \in \mathcal{H} - \{H\}$ and so H_M is uniquely determined by M.

To prove (i), note that $H \cap \mathrm{soc}(G)$ is normal in G and therefore generated by minimal normal subgroups of G contained in H. Thus $H \cap \mathrm{soc}(G) \leq \mathrm{soc}(H)$.

For (ii) and (iii), $\mathcal{H} \cap \mathrm{soc}(G) = \{\mathrm{soc}(H) : H \in \mathcal{H}\} = \{\langle M \in \mathcal{M} : M \leq H \rangle : H \in \mathcal{H}\}$, and by Lemma IV.5.6, $\mathcal{M}$ is a direct decomposition of $\mathrm{soc}(G)$. As $\mathcal{M}$ refines $\mathcal{H} \cap \mathrm{soc}(G)$, $\mathcal{H} \cap \mathrm{soc}(G)$ is a direct decomposition of $\mathrm{soc}(G)$, by Proposition IV.3.5.

For (iv), fix $H \in \mathcal{H}$. Since $G = H \times \langle \mathcal{H} - \{H\} \rangle$ it follows that $C_G(\mathrm{soc}(H)) = C_H(\mathrm{soc}(H)) \times \langle \mathcal{H} - \{H\} \rangle$. As $\mathrm{soc}(H) \trianglelefteq H$, $C_H(\mathrm{soc}(H)) \trianglelefteq H$ and thus $C_H(\mathrm{soc}(H)) = 1$ or $C_H(\mathrm{soc}(H))$. The later means that $C_H(\mathrm{soc}(H))$ contains a minimal normal subgroup of H and $1 < C_H(\mathrm{soc}(H)) \cap \mathrm{soc}(H) \leq Z(\mathrm{soc}(H)) = 1$, which is impossible. So $C_G(\mathrm{soc}(H)) = \langle \mathcal{H} - \{H\} \rangle$ and $C_G(C_G(\mathrm{soc}(H)) = H$, by reapplying the argument interchanging the rôles of H and $\langle \mathcal{H} - \{H\} \rangle$. □

Theorem IV.5.8. *There is a deterministic polynomial time algorithm which: given an almost semisimple group in $\mathbb{G}_n$, returns a Remak decomposition of the group.*

Proof. Let G be an almost semisimple group in $\mathbb{G}_n$.

Algorithm. Use (IV.2.10) to find a minimal normal subgroup N of G. Use (IV.2.8) to compute $C_G(N)$. If $C_G(N) = 1$ then return $\{G\}$. Otherwise, recurse with $C_G(N)$ in the rôle of G to find a Remak decomposition $\mathcal{K}$ of $C_G(N)$. Use (IV.2.12) to create the set $\mathcal{L} := \{K \in \mathcal{K} : \exists X \leq G, G = K \times X\}$. Then (IV.2.12) to find $H \leq G$ such that $G = H \times \langle \mathcal{L} \rangle$. Return $\{H\} \sqcup \mathcal{L}$.

Correctness. Let $\mathcal{R}$ be the Remak decomposition of G. As N is a minimal normal subgroup of G as $\mathrm{soc}(G)$ is semisimple, it follows that N is a directly indecomposable direct factor of $\mathrm{soc}\, G$. As $\mathcal{R} \cap \mathrm{soc}\, G$ is a direct decomposition of $\mathrm{soc}\, G$, it follows that $N \leq R_N$ for a unique $R_N \in \mathcal{R}$. If $C_G(N) = 1$ then $\mathcal{R} = \{R_N\}$. As $\mathcal{R}$ generates G it follows that $G = R_N$, or rather that $\{G\}$ is the Remak decomposition of G. So now we assume that $C_G(N) > 1$.

As N is a direct product of nonabelian simple groups it follows that $N \not\leq C_G(N)$ and so $C_G(N)$ is smaller than G. If $M \lhd C_G(N)$ is abelian, then as $[N, M] = 1$, $M \trianglelefteq G$ and so G has a proper normal abelian subgroup, which is excluded by assumption. Thus, $C_G(N)$ is almost semisimple as well. Thus by induction the recursive call returns the Remak decomposition $\mathcal{K}$ of $C_G(N)$ which therefore refines the direct decomposition $C_G(N) = C_{R_N}(N) \times \langle \mathcal{R} - \{R_N\} \rangle$. In particular, $\mathcal{R} - \{R_N\} \subseteq \mathcal{K}$ as the members of $\mathcal{R} - \{R_N\}$ are directly indecomposable.

We claim that $\mathcal{L} = \mathcal{R} - \{R_N\}$. Clearly $\mathcal{R} - \{R_N\} \leq \mathcal{L}$. However, if $K \in \mathcal{L} - (\mathcal{R} - \{R_N\})$ then K is a direct factor of G and also directly indecomposable. Thus K lies in the Remak decomposition of G, that is, $K \in \mathcal{R} - (\mathcal{R} - \{R_N\})$. Thus, $K = R_N$ which contains N. Yet $K \leq C_G(N)$, which does not contain N. Thus no such K exists. This proves the claim.

As $\mathcal{L} = \mathcal{R} - \{R_N\}$ it follows that $\langle \mathcal{L} \rangle$ has a direct complement and it is R_N. So the algorithm returns the Remak decomposition $\mathcal{R}$.

Timing. The algorithm relies on polynomial time routines in a recursion of depth equal to the number of minimal normal subgroups of G. As the minimal normal subgroups are products of finite nonabelian simple groups and form a direct decomposition of $\mathrm{soc}(G)$, it follows that the recursion depth is bounded above by $\log_{60} |\mathrm{soc}(G)|$. □

IV.5.5 Proof of Theorem IV.1.3

In this section we prove Theorem IV.1.3 for all groups.

Proof. Let $G \in \mathbb{G}_n$.

Algorithm. Use (IV.2.9) to find $O_{\mathfrak{S}}(G)$. Use the algorithm of Theorem IV.5.8 to find a decomposition $\mathcal{H} = \mathcal{H}O_{\mathfrak{S}}(G)$ of G such that $\mathcal{H}/O_{\mathfrak{S}}(G)$ is a Remak decomposition of $G/O_{\mathfrak{S}}(G)$. Then apply the algorithm of Theorem IV.4.23 to $\mathcal{H}$ and return the result.

Correctness. $G/O_{\mathfrak{S}}(G)$ is almost semisimple, so Theorem IV.5.8 can be applied and the return is a decomposition $\mathcal{H}$ with the properties stated. If $\mathcal{R}$ is a Remak decomposition of G, then $\mathcal{R}O_{\mathfrak{S}}(G)/O_{\mathfrak{S}}(G)$ is a direct decomposition of $G/O_{\mathfrak{S}}(G)$, by Proposition IV.3.7. As $Z(G/O_{\mathfrak{S}}(G)) = 1$ and $\mathcal{H}/O_{\mathfrak{S}}(G)$ is the Remak decomposition of $G/O_{\mathfrak{S}}(G)$, by Corollary IV.3.14.(i), $\mathcal{H}/O_{\mathfrak{S}}(G)$ refines $\mathcal{R}O_{\mathfrak{S}}(G)/O_{\mathfrak{S}}(G)$, that is, $\mathcal{H}$ refines $\mathcal{R}O_{\mathfrak{S}}(G)$. As the class of solvable groups has an algorithm to find Remak decompositions (Corollary IV.5.5), Theorem IV.4.23 can be applied. The return is a direct decomposition $\mathcal{K}$ of G in which $\mathcal{K}O_{\mathfrak{S}}(G) = \mathcal{R}O_{\mathfrak{S}}(G)$ and every solvable member of $\mathcal{K}$ is directly indecomposable. Therefore $|\mathcal{K}| = |\mathcal{R}|$ and so $\mathcal{K}$ is a Remak decomposition of G.

Timing. The algorithm uses a constant number of polynomial time algorithms. □

IV.5.6 Proof of Theorem IV.1.1 and Corollary IV.1.2

Proof of Theorem IV.1.1. Let $\mathbb{G}_n = \text{QPERM}_n$ in Theorem IV.1.3. □

IV.6 Closing Remarks

IV.6.1 Nearly Linear-time Algorithm: Corollary IV.1.2

The previous algorithms for finding direct decompositions are part of a family of similar "$N^{\log N}$-problems", $N = |G|$, such as group isomorphism; see [40].[4] One such algorithm lists all n-tuples $(g_1, \ldots, g_n) \in G^n$, $n = \lfloor \log |G| \rfloor$, and tests if

$$G = \langle g_1, \ldots, g_i \rangle \times \langle g_{i+1}, \ldots, g_n \rangle \tag{IV.29}$$

for some $1 \leq i \leq n$. That method uses miniscule amounts of group theory and requires $|G|^{\log |G| + O(1)}$ steps to prove G is directly indecomposable. Asymptotically the same number of steps can be expected if G is directly decomposable. For example, a direct product G of two extraspecial p-groups of order 2^{1+2m} has fewer than $1/|G|^{\log |G| - 6}$ elements of G^n which satisfy (IV.29).

[4] Thank you to E. M. Luks and G.L. Miller for sharing the folklore of this problem.

Proof of Corollary IV.1.2. For a polynomial time algorithm for a group given by its Cayley table it suffices to use the regular representation of the group in Theorem IV.1.1. To achieve a nearly linear time bound it suffices to show the hypothesized routines in Section IV.2.2 have deterministic nearly linear time solutions. Our use of those methods in Theorem IV.1.3 proceeds through loops and recursions which are a polynomial in $\log |G|$, and therefore do not affect the soft-O asymptotic estimates in the timing.

(IV.2.3-IV.2.5) have straight-forward nearly linear time implementation. As we can list the order of G, we can also factor G in N-steps, thus handling (IV.2.6).

For (IV.2.7) we simply handle an arbitrary quotient of G by listing its multiplication table via cosets. To find the centralizer of any subgroup $H \leq G$ can be done from the definition, thus (IV.2.8) has a nearly linear times solution.

Finding a minimal normal subgroup requires considering the subgroups generated by the conjugacy class of G, all of which can be listed. Thus the socle can be found in nearly linear time which handles (IV.2.10). For (IV.2.9), a greedy algorithm can be used which begins with a minimal normal abelian group, passes to the quotient to recursively find the solvable radical of the quotient, then pulls back to the whole group.

To find a Sylow system of a solvable group G, we note that Sylow and Hall subgroups can be built (in nearly linear time) from their usual proofs of existence; see [49, Chapter 9]. This handles (IV.2.11).

Finally, Theorem IV.2.13 also handles (IV.2.12) in nearly linear time. □

IV.6.2 Decompositions of Nonassociative Rings

The algorithm to find a direct decomposition of a bilinear map can be modified to provide an algorithm which finds a direct decomposition of a nonassociative ring. For, a nonassociative finite ring is simply a biadditive map $b : A \times A \to A$. Define:

$$\mathrm{Rich}(A) := \{f \in \mathrm{End}\, A : b(uf, v) = b(u, v)f = b(u, vf), u, v \in A\}.$$

(End A here means additive endomorphisms only.) The algorithm of Theorem IV.4.31 can be applied to the bilinear map of multiplication in b. It is evident that a direct sum decomposition of b is also direct sum of A as ring. Thus we have:

Theorem IV.6.1. *There is a polynomial-time algorithm which, given a nonassociative finite ring, returns a Remak decomposition of the ring. The algorithm is deterministic in the characteristic of the ring plus the size of the input, and Las Vegas for all characteristics, with an oracle to factor the characteristic.*

This result is known for semisimple associative and semisimple Lie algebras over fields [51]. However, those techniques rely on specific theorems about associative and Lie algebras and do not provide a general purpose algorithm such as Theorem IV.6.1. As a tradeoff, they are far more efficient.

IV.6.3 A Top-down Approach

The method just used depends on a bottom-up approach proceed from the trivial group up a characteristic series of marginal subgroups. That method depends on Corollary IV.3.14.(*i*). It appears possible (at least for solvable groups) that Corollary IV.3.14.(*ii*) can be used along with verbal subgroups to provide a "top-down" approach from the top of the group proceeding recursively down a characteristic series. This would likely improve the efficiency of the algorithm as verbal subgroups are often easier to compute than marginal subgroups.

BIBLIOGRAPHY

[1] G. K. Abbasi, Central decompositions of finite p-groups with an abelian second center and a center of order p, Vestnik Moskov. Univ. Ser. I Mat. Mekh. (2) (1985) 75–78, 96.

[2] G. Q. Abbasi, Extraspecial q-groups and central decompositions, Punjab Univ. J. Math. (Lahore) 17/18 (1984/85) 63–68.

[3] G. Q. Abbasi, Central decompositions of nilpotent Lie algebras, Math. Japon. 34 (6) (1989) 841–846.

[4] E. Artin, Geometric algebra, Interscience Publishers, Inc., New York-London, 1957.

[5] M. Aschbacher, Finite group theory, vol. 10 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 1986.

[6] R. Baer, Groups with abelian central quotient group, Trans. Amer. Math. Soc. 44 (3) (1938) 357–386.

[7] E. R. Berlekamp, Algebraic coding theory, McGraw-Hill Book Co., New York, 1968.

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

[9] J. Bond, Lie algebras of genus one and genus two, Pacific J. Math. 37 (1971) 591–616.

[10] C. W. Curtis, I. Reiner, Methods of representation theory. Vol. I, John Wiley & Sons Inc., New York, 1981.

[11] K. Doerk, T. Hawkes, Finite soluble groups, vol. 4 of de Gruyter Expositions in Mathematics, Walter de Gruyter & Co., Berlin, 1992.

[12] W. Eberly, M. Giesbrecht, Efficient decomposition of associative algebras over finite fields, J. Symbolic Comput. 29 (3) (2000) 441–458.

[13] B. Eick, C. R. B. Wright, Computing subgroups by exhibition in finite solvable groups, J. Symbolic Comput. 33 (2) (2002) 129–143.

[14] P. Gianni, V. Miller, B. Trager, Decomposition of algebras, in: Symbolic and algebraic computation (Rome, 1988), vol. 358 of Lecture Notes in Comput. Sci., Springer, Berlin, 1989, pp. 300–308.

[15] D. Gorenstein, Finite groups, 2nd ed., Chelsea Publishing Co., New York, 1980.

[16] P. Hall, The classification of prime-power groups, J. Reine Angew. Math. 182 (1940) 130–141.

[17] P. Hall, Verbal and marginal subgroups, J. Reine Angew. Math. 182 (1940) 156–157.

[18] G. Higman, Enumerating p-groups. I. Inequalities, Proc. London Math. Soc. (3) 10 (1960) 24–30.

[19] C. J. Hillar, D. Rhea, Automorphisms of finite abelian groups, Amer. Math. Mon.

[20] D. F. Holt, B. Eick, E. A. O'Brien, Handbook of computational group theory, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2005.

[21] D. F. Holt, S. Rees, Testing modules for irreducibility, J. Austral. Math. Soc. Ser. A 57 (1) (1994) 1–16.

[22] G. Ivanyos, Fast randomized algorithms for the structure of matrix algebras over finite fields (extended abstract), in: Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation (St. Andrews), ACM, New York, 2000.

[23] G. Ivanyos, K. Lux, Treating the exceptional cases of the MeatAxe, Experiment. Math. 9 (3) (2000) 373–381.

[24] G. Ivanyos, L. Rónyai, Computations in associative and Lie algebras, in: Some tapas of computer algebra, vol. 4 of Algorithms Comput. Math., Springer, Berlin, 1999, pp. 91–120.

[25] N. Jacobson, Structure and representations of Jordan algebras, American Mathematical Society Colloquium Publications, Vol. XXXIX, American Mathematical Society, Providence, R.I., 1968.

[26] N. Jacobson, Lectures in abstract algebra, Springer-Verlag, New York, 1975, volume II: Linear algebra, Reprint of the 1953 edition [Van Nostrand, Toronto, Ont.], Graduate Texts in Mathematics, No. 31.

[27] N. Jacobson, Structure theory of Jordan algebras, vol. 5 of University of Arkansas Lecture Notes in Mathematics, University of Arkansas, Fayetteville, Ark., 1981.

[28] L. Kaloujnine, Zum Problem der Klassifikation der endlichen metabelschen p-Gruppen, Wiss. Z. Humboldt-Univ. Berlin. Math.-Nat. Reihe 4 (1955) 1–7.

[29] W. M. Kantor, E. M. Luks, Computing in quotient groups, in: STOC '90: Proceedings of the twenty-second annual ACM Symposium on Theory of Computing, ACM, New York, NY, USA, 1990.

[30] W. M. Kantor, E. M. Luks, P. D. Mark, Sylow subgroups in parallel, Journal of Algorithms 31 (1999) 132–195.

[31] W. M. Kantor, E. M. Luks, J. B. Wilson, Sylow subgroups of solvable matrix groups (in preparation).

[32] E. I. Khukhro, p-automorphisms of finite p-groups, vol. 246 of London Mathematical Society Lecture Note Series, Cambridge University Press, Cambridge, 1998.

[33] W. Krull, Über verallgemeinerte endliche Abelsche Gruppen, M. Z. 23 (1925) 161–196.

[34] C. R. Leedham-Green, oral communication (2008).

[35] C. R. Leedham-Green, L. H. Soicher, Collection from the left and other strategies, J. Symbolic Comput. 9 (5-6) (1990) 665–675, computational group theory, Part 1.

[36] C. R. Leedham-Green, L. H. Soicher, Symbolic collection using Deep Thought, LMS J. Comput. Math. 1 (1998) 9–24 (electronic).

[37] D. W. Lewis, Involutions and anti-automorphisms of algebras, Bull. London Math. Soc. 38 (4) (2006) 529–545.

[38] E. M. Luks, Computing in solvable matrix groups, in: Proceedings 33rd IEEE Symposium on the Foundations of Computer Science, 1992.

[39] P. McKenzie, S. A. Cook, The parallel complexity of abelian permutation group problems, SIAM J. Comput. 16 (5) (1987) 880–909.

[40] G. L. Miller, On the $n^{log}\, n$ isomorphism technique: A preliminary report, Tech. Rep. TR17, Rochester, Rochester (March 1977).

[41] T. Miyazaki, Deterministic algorithms for management of matrix groups, in: Groups and computation, III (Columbus, OH, 1999), vol. 8 of Ohio State Univ. Math. Res. Inst. Publ., de Gruyter, Berlin, 2001, pp. 265–280.

[42] A. G. Myasnikov, Definable invariants of bilinear mappings, Sibirsk. Mat. Zh. 31 (1) (1990) 104–115, 220.

[43] A. G. Myasnikov, The theory of models of bilinear mappings, Sibirsk. Mat. Zh. 31 (3) (1990) 94–108.

[44] H. Neumann, Varieties of groups, Springer-Verlag New York, Inc., New York, 1967.

[45] P. Neumann, Some algorithms for computing with finite permutation groups, in: Proceedings of groups—St. Andrews 1985, vol. 121 of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, 1986.

[46] E. A. O'Brien, Towards effective algorithms for linear groups, in: Finite geometries, groups, and computation, Walter de Gruyter, Berlin, 2006, pp. 163–190.

[47] J. M. Osborn, Jordan and associative rings with nilpotent and invertible elements., J. Algebra 15 (1970) 301–308.

[48] R. Remak, Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren., J. f ur Math. 139 (1911) 293–308.

[49] D. J. S. Robinson, A course in the theory of groups, vol. 80 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1993.

[50] L. Rónyai, Computing the structure of finite algebras, J. Symbolic Comput. 9 (3) (1990) 355–373.

[51] L. Rónyai, Computations in associative algebras, in: Groups and computation (New Brunswick, NJ, 1991), vol. 11 of DIMACS Ser. Discrete Math. Theoret. Comput. Sci., Amer. Math. Soc., Providence, RI, 1993, pp. 221–243.

[52] O. Schmidt, Sur les produits directs, S. M. F. Bull. 41 (1913) 161–164.

[53] C. C. Sims, Enumerating p-groups, Proc. London Math. Soc. (3) 15 (1965) 151–166.

[54] E. J. Taft, Invariant Wedderburn factors, Illinois J. Math. 1 (1957) 565–573.

[55] C. Y. Tang, On uniqueness of generalized direct decompositions, Pacific J. Math. 23 (1967) 171–182.

[56] C. Y. Tang, On uniqueness of central decompositions of groups, Pacific J. Math. 33 (1970) 749–761.

[57] J. von zur Gathen, J. Gerhard, Modern computer algebra, 2nd ed., Cambridge University Press, Cambridge, 2003.

[58] R. B. Warfield, Jr., Nilpotent groups, Springer-Verlag, Berlin, 1976, lecture Notes in Mathematics, Vol. 513.

[59] J. B. Wilson, Decomposing p-groups via Jordan algebras (submitted), `http://arxiv.org/abs/0711.0201`.

[60] J. B. Wilson, Finding central decompositions of p-groups (submitted), `http://arxiv.org/abs/0801.3434`.

[61] J. B. Wilson, Finding direct product decompositions (in preparation).

[62] J. B. Wilson, Lie equivalent p-groups (in preparation).

[63] J. B. Wilson, p-groups, bilinear maps, and their algebras (in preparation).

[64] J. B. Wilson, Parallel algorithms for rings (in preparation).