EXISTENCE, ALGORITHMS, AND ASYMPTOTICS OF DIRECT PRODUCT DECOMPOSITIONS, I

JAMES B. WILSON

Abstract. Direct products of finite groups are a simple method to construct new groups from old ones. A difficult problem by comparison is to prove a generic group G is indecomposable, or locate a proper nontrivial direct factor. To solve this problem it is shown that in most circumstances G has a proper nontrivial subgroup M such that every maximal direct product decomposition $\mathcal{Q}$ of G/M induces a unique set $\mathcal{H}$ of subgroups of G where $|\mathcal{H}| \leq |\mathcal{Q}|$ and for each $H \in \mathcal{H}$, the nonabelian direct factors of H are direct factors of G. In particular, G is indecomposable if $|\mathcal{H}| = 1$ and M is contained in the Frattini subgroup of G. This "local-global" property of direct products can be applied inductively to M and G/M so that the existence of a proper nontrivial direct factor depends on the direct product decompositions of the chief factors of G. Chief factors are characteristically simple groups and therefore a direct product of isomorphic simple groups. Thus a search for proper direct factors of a group of size N is reduced from the global search through all $N^{O(\log N)}$ normal subgroups to a search of $O(\log N)$ local instances induced from chief factors.

There is one family of groups G where no subgroup M admits the local-global property just described. These are p-groups of nilpotence class 2. There are $p^{2n^3/27+\Omega(n^2)}$ isomorphism types of class 2 groups with order p^n [BNV], which prevents a case-by-case study. Also these groups arise in the course of the induction described above so they cannot be ignored. To identify direct factors for nilpotent groups of class 2, a functor is introduced to the category of commutative rings. The result being that indecomposable p-groups of class 2 are identified with local commutative rings. This relationship has little to do with the typical use of Lie algebras for p-groups and is one of the essential and unexpected components of this study.

These results are the by-product of an efficient polynomial-time algorithm to prove indecomposability or locate a proper nontrivial direct factor. The theorems also explain how many isomorphism types of indecomposable groups exists of a given order and how many direct factors a group can have. These two topics are explained in a second part to this paper.

Contents

Date: March 27, 2012.
Key words and phrases. direct product, group variety, p-group, bilinear map.
This research was supported in part by NSF Grant DMS 0242983.

1. Introduction

This paper is the first of two that seek to explain when a finite group has a proper nontrivial direct factor. Of the many ways to address this problem we consider three. First, we describe the structural properties of a group that expose a direct product decomposition into proper nontrivial subgroups. The second perspective estimates how often a group admits a proper nontrivial direct factor. The third direction is to provide a polynomial-time algorithm that, given generators of a group, locates a direct product decomposition into indecomposable subgroups. (The asymptotic estimates and the algorithm are explained in the next paper.) Our motivation is to further understand direct products, which despite being elementary to create are surprisingly difficult to recognize.

The existence of proper nontrivial direct factors of abelian groups is a well-known subject. If A is abelian and $|A| = mn$ where $\gcd(m, n) = 1$ then $A \cong B \times C$ where $|B| = m$ and $|C| = n$. Similarly, an abelian group $P = \langle a_1, a_2, \dots \rangle$ of prime power order is indecomposable if, and only if, P is cyclic. These results invite more questions than answers: How do we intend to factor $|A|$? How can we find a discrete logarithm ℓ with $a_1^\ell = a_2$ to prove P is cyclic? We will not offer new insights to these important questions in Number Theory, but instead generalize to nonabelian groups.

Existence of direct factors in nonabelian groups is perhaps most developed in the context of complete groups, i.e. groups with a trivial center and no nontrivial outer automorphisms. For if a normal subgroup is complete then it is a direct factor [R3, p. 413]. These groups appeared even as the definition of a direct product was being formalized in the treatises of v. Dyck (1883) [D2, p. 97], Hölder (1893) [H2, §18][1] and in Burnside's influential first edition of *Theory of groups of finite order* [B, §34]. They remain an area of active research; cf. [R2]. Yet it is difficult to compare our methods to this situation since complete groups are quite distinct from general groups.

Far less attention has been given to identifying direct factors of a nonabelian group without imposing properties on the direct factors. This is with good reason. In moving to incomplete groups we encounter finite p-groups of which there are enormous numbers – making it impossible to even loosely characterize the indecomposable groups. Also, individual finite p-groups can have huge numbers of normal subgroups that centralize one-another but are not direct factors. We consider our study of direct factors of p-groups to be the essential component in our new strategy. In particular we have departed from the usual connections to Lie algebras and instead called upon bilinear maps and a functorial relationship to commutative rings.

1.1. **Rethinking "Krull-Schmidt".** To explain our findings we first present some of our notation and we do this by considering our somewhat non-standard treatment of the "Krull-Schmidt" theorem. A full list of details is provided in Section 2.

We focus on finite Ω-groups G (Ω a possibly empty set of automorphisms). An Ω-*decomposition* $\mathcal{H}$ of G is a set of Ω-subgroups that generate G and where

$$(\forall H \in \mathcal{H}) \qquad\qquad G \neq \langle \mathcal{H} - \{H\} \rangle.$$

By a *direct* Ω-decomposition we mean an Ω-decomposition where

$$(\forall H \in \mathcal{H}) \qquad [H, \langle \mathcal{H} - \{H\} \rangle] = 1 \quad \& \quad H \cap \langle \mathcal{H} - \{H\} \rangle = 1.$$

The members of $\mathcal{H}$ are *direct* Ω-*factors* of G. Notice 1 is not a direct Ω-factor in our meaning and so G is Ω-indecomposable when it has only the *trivial* direct Ω-decomposition $\{G\}$. A *Remak* Ω-decomposition is a direct Ω-decomposition whose members are Ω-indecomposable. We wish only to consider Ω-decompositions of normal subgroups. The problem is that in passing to subgroups normality is an ambiguous label and so we are explicit and ask for $(\Omega \cup G)$-decompositions, where the implied action of G is by conjugation. With quotients this notation is also applicable but not required.

An Ω-decomposition $\mathcal{H}$ of G *refines* an Ω-decomposition $\mathcal{K}$ of G if for each $H \in \mathcal{H}$, there a unique $K \in \mathcal{K}$ such that $H \leq K$ and

$$(\forall K \in \mathcal{K}) \qquad\qquad K = \langle H \in \mathcal{H} : H \leq K \rangle.$$

When $\mathcal{K}$ is a direct Ω-decomposition, the uniqueness of K to H is immediate. Also, if $\mathcal{H}$ is a direct Ω-decomposition then $\mathcal{K}$ is a direct Ω-decomposition.

The main tool for direct products is the familiar "Krull-Schmidt" theorem. This theorem has been reproved and generalized many times. We opt for the following formulation.

[1]G.A. Miller [M1, p. 66] credits this work of Hölder for the name *direct product*.

Theorem ("Krull-Schmidt"). *If G is a finite Ω-group and $\mathcal{R}$ and $\mathcal{T}$ are Remak Ω-decompositions of G, then for every $\mathcal{X} \subseteq \mathcal{R}$, there is a $\varphi \in \mathrm{Aut}_{\Omega \cup G} G$ such that $\mathcal{X}\varphi \subseteq \mathcal{T}$ and φ is the identity on $\mathcal{R} - \mathcal{X}$. In particular, $\mathcal{R}\varphi = \mathcal{X}\varphi \sqcup (\mathcal{R} - \mathcal{X})$ is a Remak Ω-decomposition.*

(Note that we use $\sqcup$ to emphasize that the union is known to be disjoint.)

We have introduced the "Krull-Schmidt" theorem in the language we find most efficient for our purpose. However, it is worth a moment to restate this in the form found in references (e.g. [K2, Vol. II, p. 120]) so that its meaning is not obscured. We first enumerate our direct Ω-decompositions $\mathcal{R} = \{R_1, \ldots, R_s\}$ and $\mathcal{T} = \{T_1, \ldots, T_t\}$, i.e.

$$G = R_1 \times \cdots \times R_s = T_1 \times \cdots \times T_t.$$

Subject to re-indexing of $\mathcal{R}$ we take $\mathcal{X} = \{R_1, \ldots, R_i\}$ and since $\mathcal{X}\varphi \subseteq \mathcal{T}$ we can re-index $\mathcal{T}$ so that $\mathcal{X}\varphi = \{T_1, \ldots, T_i\}$. Hence, $\mathcal{R}\varphi = \mathcal{X}\varphi \sqcup (\mathcal{R} - \mathcal{X})$ is the familiar claim that:

$$G = T_1 \times \cdots \times T_i \times R_{i+1} \times \cdots \times R_s \tag{1.1}$$

Using $\mathcal{X} = \mathcal{R}$ we also find $s = t$. Our use of sets has the advantage of dismissing the ambiguity of re-indexing and this is critical in explaining the many complex exchanges used in proofs.

An unexpected benefit to our notation is that one more easily recognizes the structure of a matroid. A *matroid* is a finite nonempty set E and set $\mathcal{I}$ of subsets of E where (a) $\emptyset \in \mathcal{I}$, (b) for all $I \in \mathcal{I}$ and all $J \subseteq I$, $J \in \mathcal{I}$, and (c) if $I, J \in \mathcal{I}$ and $|J| < |I|$ then there exists an $x \in I - J$ with $J \cup \{x\} \in \mathcal{I}$. The sets in $\mathcal{I}$ are called *independent* and the maximal members of $\mathcal{I}$ are called *bases*; cf. [O2, p. 8, p. 16].

Corollary. *Fix a finite Ω-group G. The set $\mathcal{D}(G)$ of all indecomposable direct Ω-factors of G has the structure of a matroid whose bases are the Remak Ω-decompositions and whose independent sets are subsets of Remak Ω-decompositions.*

This perspective is quite useful but we add a caution. In our situation we presume not to know even on member of $\mathcal{D}(G)$ at the start. What we have instead is the entire modular lattice of $(\Omega \cup G)$-subgroups to begin with and our effort is to discover this hidden matroid $\mathcal{D}(G)$ from within the set of all subgroups.

Historical Remark. The "Krull-Schmidt" theorem first appears in an under-cited work of Wedderburn (1909) [MW] where he states (1.1) and concludes the indecomposable direct factors of a group are isomorphism invariants. This was followed by Remak (1911) [R1] who proved that the central automorphism group (i.e. $\mathrm{Aut}_G G$) acts transitively on the set of Remak decompositions, as they are now called.

Remak appears to have proved his result unaware of Wedderburn's work until publishing. In his closing remarks [R1, p. 308] Remak asserted a line in Wedderburn's proof was unsupported (specifically [MW, p.175, l.-4]). Later authors also refered to a 'gap' in Wedderburn's proof [K2, p. 83]. Schur reviewed both articles after both had appeared and mentioned regarding Wedderburn's work "... as indicated by Remak, the proof here is not complete" [S1, S2]. On the other hand, it should not be overlooked that Wedderburn read this result before the *American Mathematical Society* and the article appeared in the well-respected *Annals of Mathematics*, so it is possible that several contemporaries viewed this unsupported step as a permissible omission.

The issue concerns an isomorphism between two groups for which Wedderburn did not provide the isomorphism (indeed he used an equal sign instead of an isomorphism symbol). Wedderburn claimed his result was classically known for permutation groups and implied by work of Miller [M1, p.71] who in turn credited it to Hölder [H2, p. 330]. Perhaps this encouraged a terse treatment (his proof is a concise 5 pages). Indeed, there are other unsupported isomorphisms (some also indicated by equal signs) in Wedderburn's work that Remak did not protest, including one in the very same line. This suggests some acceptance of "self-evident" isomorphisms already at this stage in Group Theory. By current standards the omission is reasonable; compare [R4, p.81, l.-12].

In 1913 Schmidt [S3] condensed Remak's proof to 3 pages. Following the simplifications in the proof came the era of generalization. First in line was Krull (1925) [K1] who considered direct products of finite and infinite abelian Ω-groups. Fitting [F] invented the standard proof using idempotents, Ore [O1] grounded the concepts in Lattice Theory, and in several works Kurosh [K2, §17, §§42–47] and others unified the treatments and found counter-examples to extending the results further. By the 1930's direct decompositions of maximum length appear as "Remak decompositions" while at the same time the theorem is cited as "Krull-Schmidt".

It is not uncommon for theorems to bare names different from their original authors. In the case Wedderburn this appears to have been on account of a dispute in standards. A modest tribute remains. Most accounts of direct products now adopt Wedderburn's introduction of the symbol $\times$ which he re-appropriated from a non-group theoretic work of Hurwitz [MW, p. 173].

1.2. **Existence theorems for direct product decompositions.** We start by identifying normal Ω-subgroups N of G that are especially amenable to the direct Ω-decompositions. We say N is Ω-*graded* if every finite direct Ω-decomposition $\mathcal{H}$ of G induces the following direct $(\Omega \cup G)$-decompositions of N and G/N respectively:

$$\mathcal{H} \cap N = \{H \cap N : H \in \mathcal{H}\} - \{1\} \tag{1.2}$$

$$\mathcal{H}N/N = \{HN/N : H \in \mathcal{H}\} - \{N/N\}. \tag{1.3}$$

Most normal subgroups are not graded (consider noncyclic elementary abelian groups), but several important subgroups are graded including the center $\zeta_1(G)$ and commutator subgroup $\gamma_2(G)$. We prove:

Theorem 1. *Every finite Ω-group has an Ω-graded chief series (i.e. a maximal $(\Omega \cup G)$-series of Ω-graded subgroups).*

Our approach to prove Theorem 1 (in Section 3.5) is more broad than simply constructing one such series. Indeed, we show that most of the obvious methods to construct a chief series are automatically graded. Indeed, each graded subgroup we consider is associated with a specific class of groups as follows.

Definition 1.4. A class $\mathfrak{X}$ of Ω-groups is *direct* if it is closed to isomorphic images, finite direct Ω-products, and also direct Ω-factors. An up (resp. down) Ω-*grader* for a direct class $\mathfrak{X}$ is an idempotent (resp. radical) function $G \mapsto \mathfrak{X}(G)$ of Ω-groups satisfying the following:

(a) $\mathfrak{X}(G) \in \mathfrak{X}$ (resp. $G/\mathfrak{X}(G) \in \mathfrak{X}$),
(b) $\mathfrak{X}(G)$ is Ω-graded in G, and
(c) if H is a direct Ω-factor of G then $\mathfrak{X}(H) = H \cap \mathfrak{X}(G)$.

The pair $\langle \mathfrak{X}, G \mapsto \mathfrak{X}(G) \rangle$ we call an Ω-*grading pair*.

There are many possibilities for grading pairs but the most evident seem to be varieties of groups, i.e. a class $\mathfrak{V}(\mathtt{W})$ of Ω-groups for which every member satisfies the words in a fixed set $\mathtt{W}$; cf. Section 3.2 & [N]. The words $\mathtt{W}$ not only define the class of groups but also describe up/down graders. E.g. in the class $\mathfrak{A}$ of abelian groups every member satisfies the commutator word $[x, y] = x^{-1}y^{-1}xy$ and for an arbitrary group the center is an up grader and the commutator is a down grader, with respect to $\mathfrak{A}$.

After settling on an Ω-graded subgroup N of G, we plan to reconstruct a direct Ω-decomposition $\mathcal{H}$ of G from a pair $(\mathcal{N}, \mathcal{Q})$ of direct $(\Omega \cup G)$-decompositions of N and $Q = G/N$. We say $\mathcal{H}$ *extends* (or is an *extension* of) $\mathcal{N}$ if $\mathcal{N}$ refines $\mathcal{H} \cap N$. We say $\mathcal{Q}$ *lifts* to $\mathcal{H}$ (or $\mathcal{H}$ is a *lift* of $\mathcal{Q}$) if $\mathcal{Q}$ refines $\mathcal{H}N/N$. Finally we say $\mathcal{H}$ *matches* (or is a *match* for) $(\mathcal{N}, \mathcal{Q})$ if $\mathcal{H}$ is an extension of $\mathcal{N}$ and a lift of $\mathcal{Q}$. Finding matches is usually difficult. Yet in most circumstances there is a unique coarsest direct $(\Omega \cup G)$-decomposition $\mathcal{N}$ (resp. $\mathcal{Q}$) of N (resp. Q) that extends (resp. lifts) to *every* Remak Ω-decomposition of G. Applying Remak's transitivity theorems [R1] we prove:

Theorem 2. *Fix $(\Omega \cup G)$-graded subgroups $1 \leq M \leq N \leq G$.*

(i) If $\zeta_1(G/M) \leq N/M$, then for all Remak Ω-decompositions $\mathcal{Q}$ of G/M, $\mathcal{Q}N/N$ is a direct Ω-decomposition of G/N that lifts to all Remak Ω-decompositions of G. Furthermore, $\mathcal{Q}N/N$ is independent of the choice of $\mathcal{Q}$.

(ii) If $M \leq \gamma_2(N)$ then for each Remak $(\Omega \cup G)$-decomposition $\mathcal{N}$ of N, $\mathcal{N} \cap M$ extends to every Remak Ω-decomposition of G. Furthermore, $\mathcal{N} \cap M$ is independent of the choice of $\mathcal{N}$.

Theorem 2 is proved in Section 4.1.

The pullback $\mathcal{H}$ of $\mathcal{Q}N/N$ to G is alluded to in the abstract. It is possible that G is indecomposable and $|\mathcal{H}| > 1$ since we know only that $\mathcal{Q}N/N$ refines $\mathcal{R}N/N$, for a Remak decomposition $\mathcal{R}$ of G. Identifying the unique refinement of $\mathcal{Q}N/N$ to $\mathcal{R}N/N$ is an issue will be addressed below. It is this unique refinement that we mention in the abstract. In any case we can sometimes setup a stronger result.

Corollary. *If a group G has a sequence of $(\Omega \cup G)$-graded subgroups*

$$1 \leq N_1 \leq \zeta_1(G/N_1)^{-1} \leq N_2 \leq \gamma_2(N_3) \leq N_3 \leq G,$$

(where $\zeta_1(G/N_1)^{-1}$ is the pull-back of $\zeta_1(G/N_1)$ to G) then for every Remak $(\Omega \cup G)$-decomposition $\mathcal{N}_3$ of N_3 and $\mathcal{Q}_1$ of G/N_1, it follows that $(\mathcal{N}_3 \cap N_2, \mathcal{Q}_3 N_2/N_2)$ is matched by every Remak Ω-decomposition of G.

Also notice that it is possible that the pull-back $\mathcal{H}$ of $\mathcal{Q}N/N$ in Theorem 2(i) equals $\{G\}$ without G being Ω-indecomposable. If $N = \mathfrak{X}(G)$ for an up Ω-grading pair $\langle \mathfrak{X}, G \mapsto \mathfrak{X}(G) \rangle$, this requires that G have a unique direct Ω-factor not contained in $\mathfrak{X}$. Hence, if $\mathfrak{X}(G) \leq \Phi(G)$ then it is not possible for G to have further direct factors as those would lie in $\mathfrak{X}$ and so in $\mathfrak{X}(G)$. Yet $\Phi(G)$ consists of non-generators of G so $\Phi(G)$ contains no proper nontrivial direct factors. So we obtain the following indecomposability criteria.

Corollary. *A finite Ω-group G is indecomposable if there is an up Ω-grader $\langle \mathcal{X}, G \mapsto \mathfrak{X}(G) \rangle$ where $\zeta_1(G) \leq \mathfrak{X}(G) \leq \Phi(G)$ and $G/\mathfrak{X}(G)$ is Ω-indecomposable.*

Theorem 2(i) (and dually part (ii)) narrows the location of indecomposable direct Ω-factors. *A priori* the indecomposable direct Ω-factors of G where known only as one of the $|G|^{O(\log|G|)}$ possible $(\Omega \cup G)$-subgroups of G.[2] Under the hypothesis of Theorem 2(i) we know each indecomposable direct Ω-factor of G lies in some subgroup $H \geq N$ where H/N is a product of elements in the unique set $\mathcal{Q}N/N$. There are at most $2^{|\mathcal{Q}N/N|} \leq |G|$ choices for H, which is still too large for a practical algorithm but a substantial improvement over $|G|^{O(\log|G|)}$. Assume we locate a correct choice for H and ask how we might recover a direct Ω-factor of G from H. We answer this with a local-global treatment of direct factors which relies on Wedderburn's exchange results [MW]. In Section 4.3 we prove:

Theorem 3. *Fix an Ω-grading pair $\langle \mathfrak{X}, G \mapsto \mathfrak{X}(G)\rangle$ and an Ω-group G. If $H = R\mathfrak{X}(G)$ for a direct Ω-factor R of G then every direct $(\Omega \cup G)$-factor of H that does not lie in $\mathfrak{X}$ is a direct Ω-factor of G.*

Now we describe the main step in lifting. Let us suppose that $\langle \mathfrak{X}, G \mapsto \mathfrak{X}(G)\rangle$ is an up Ω-grading pair. Assume $\mathcal{Q}$ is a direct Ω-decomposition of $G/\mathfrak{X}(G)$ that lifts to a Remak Ω-decomposition $\mathcal{R}$ of G and let $\mathcal{H}$ be the pull-back of $\mathcal{Q}$, i.e. $\mathcal{H}/\mathfrak{X}(G) = \mathcal{Q}$ (cf. Theorem 2(i)). To understand this essential process of lifting we abstract the problem to lattices in manner related to Ore's treatment of direct products [O1]. We have two atomic boolean lattices ordered by set inclusion:

$$\mathscr{L} := \mathscr{L}(\mathcal{H}) = \{\langle \mathcal{J}\rangle : \mathcal{J} \subseteq \mathcal{H}\} \cong 2^{\mathcal{H}} \text{ and} \tag{1.5}$$

$$\mathscr{M} := \mathscr{L}(\mathcal{R}\mathfrak{X}(G)) = \{\langle \mathcal{J}\rangle : \mathcal{J} \subseteq \mathcal{R}\mathfrak{X}(G)\} \cong 2^{\mathcal{R}\mathfrak{X}(G)}. \tag{1.6}$$

Because $\mathcal{H}$ refines $\mathcal{R}\mathfrak{X}(G)$ it follows that $\mathscr{M} \subseteq \mathscr{L}$. We have the atoms, $\mathcal{H}$, of $\mathscr{L}$ but (probably) none of the atoms for $\mathscr{M}$. So we refer to $\mathscr{M}$ as a "hidden sublattice". Our goal is to obtain the atoms of the hidden sublattice $\mathscr{M}$ in $\mathscr{L}$. The idea is to employ Theorem 3 progressively through a chain in $\mathscr{L}$.

Definition 1.7. A *direct $(\Omega \cup G)$-chain* of $(\Omega \cup G)$-subgroups is a proper chain

$$\mathfrak{X}(G) = C_0 < C_1 \cdots < C_\ell = G$$

for which there exists a direct Ω-decomposition $\mathcal{R}$ (called *directions*) of G with:

(i) for all $0 \leq i \leq \ell$, $C_i = \langle \mathcal{R} \cap C_i\rangle$, and
(ii) for each $0 \leq i < \ell$, there is a unique $R \in \mathcal{R}$ (called *the direction of C_i*) where

$$R\mathfrak{X}(G) \cap C_i < R\mathfrak{X}(G) \cap C_{i+1}.$$

Indeed all maximal chains in $\mathscr{L}$ are direct so there is no concern for the chain we choose.

Theorem 4. *If $\mathcal{H} = \mathcal{H}\mathfrak{X}(G)$ is an $(\Omega \cup G)$-decomposition of G and $\mathcal{R}$ is a direct Ω-decomposition of G such that $\mathcal{H}$ refines $\mathcal{R}\mathfrak{X}(G)$, then every maximal proper chain $\mathscr{C}$ of subsets of $\mathcal{H}$ induces a direct $(\Omega \cup G)$-chain $\{\langle \mathcal{C}, \mathfrak{X}(G)\rangle : \mathcal{C} \in \mathscr{C}\}$.*

The point of a direct $(\Omega \cup G)$-chain is that by (i) we know for each C_i the directions $\mathcal{R}$ induce a direct $(\Omega \cup G)$-decomposition of C_i, but by (ii) if $R \in \mathcal{R}$ is the direction of C_i then for all $S \in \mathcal{R} - \{R\}$, $C_i \cap S$ remains a direct factor of C_{i+1}.

[2]The number of $(\Omega \cup G)$-subgroups of an Ω-group G is bounded above by the number of subgroups of G. If $|G| = p_1^{a_1} \cdots p_t^{a_t}$, with each p_i a distinct prime, then the number of subgroups of G is at most $|G|^t p_1^{O(a_1^2)} \cdots p_t^{O(a_t^2)} = |G|^{O(\log|G|)}$; see [W1, (1.5)]. This upper bound is attained by nilpotent groups.

Hence, if we have built a direct $(\Omega \cup G)$-decomposition $\mathcal{K}_i$ of C_i where $\mathcal{K}_i\mathfrak{X}(G)$ refines $\mathcal{R}\mathfrak{X}(G) \cap C_i$ then we can invoke Theorem 3 repeatedly to guarantee most of the members of $\mathcal{K}_i$ remain direct $(\Omega \cup G)$-factors of C_{i+1}. To obtain a Remak Ω-decomposition from this process we start with a Remak $(\Omega \cup G)$-decomposition $\mathcal{K}_0$ of $\mathfrak{X}(G)$ and then move up the chain. At each stage not only does $\mathcal{K}_i\mathfrak{X}(G)$ refine $\mathcal{R}\mathfrak{X}(G) \cap C_i$, but indeed $\mathcal{K}_i$ is a direct $(\Omega \cup G)$-decomposition of C_i in which every member of $\mathcal{K}_i$ in $\mathfrak{X}$ is indecomposable and every member outside of $\mathfrak{X}$ has no direct $(\Omega \cup G)$-factor in $\mathfrak{X}$. We call such a direct $(\Omega \cup G)$-decomposition $\mathfrak{X}$-*refined*. We prove:

Theorem 5. *Fix a direct $(\Omega \cup G)$-chain $\mathfrak{X}(G) = C_0 < \cdots < C_\ell = G$ with directions $\mathcal{R}$. Fix i with $0 \leq i < \ell$ and let $R \in \mathcal{R}$ be the direction of C_i. If $\mathcal{K}_i$ is an $\mathfrak{X}$-refined direct $(\Omega \cup G)$-decomposition of C_i and $\mathcal{K}_i\mathfrak{X}(G)$ refines $\mathcal{R}\mathfrak{X}(G) \cap C_i$, then*

$$\mathcal{L}_i = \left\{K \in \mathcal{K}_i - \mathfrak{X} : K \leq \langle \mathcal{R} - \{R\}\rangle \mathfrak{X}(G)\right\}$$

lies in an $\mathfrak{X}$-refined direct $(\Omega \cup G)$-decomposition $\mathcal{K}_{i+1}$ of C_{i+1} where $\mathcal{K}_{i+1}\mathfrak{X}(G)$ refines $\mathcal{R} \cap C_{i+1}$. Indeed, we can insist $|(\mathcal{K}_{i+1} - \mathfrak{X}) - \mathcal{L}_i| = 1$

There are many details necessary to produce an algorithm form Theorems 1–5, such as constructing graded subgroups, finding direct complements, and mechanizing the existences results. Furthermore we must handle certain base cases. We leave the details of the algorithm to the next note but close this portion by describing the relevant properties of the cases that cannot be handled recursively.

First we encounter finite characteristically simple $(\Omega \cup G)$-groups. Such groups are direct products of isomorphic simple groups. If these groups are abelian then they are elementary abelian so we treat these as $(\mathbb{Z}/p\mathbb{Z})[\Omega]$-modules, for some prime p. Otherwise the group is a direct product of nonabelian simple groups and there the set of minimal $(\Omega \cup G)$-subgroups is the unique Remak Ω-decomposition of the group. Indeed, the following theorem is a evident in the work of Krull [K1] and Fitting [F] and proved in Section 6.1.

Theorem 6. *Fix a finite characteristically simple Ω-group G.*

(i) If G is abelian it is an elementary abelian p-group for some prime p. Also, every $\mathcal{E} \subset \mathrm{End}_{(\mathbb{Z}/p\mathbb{Z})[\Omega]}(G)$ of pairwise orthogonal primitive idempotents that sum to 1 determines a Remak Ω-decomposition $\{Ge : e \in \mathcal{E}\}$ of G.

(ii) If G is nonabelian then the set of minimal $(\Omega \cup G)$-subgroups of G is the Remak Ω-decomposition of G.

Next we have groups with a 2-step Ω-graded chief series $1 < N < G$. Consequently $\zeta_1(G)$ is 1 or N (since the general abelian case is handled similar to Theorem 6(i)). Likewise $\gamma_2(G)$ is N or G. All but one of these cases is handled by the following result.

Theorem 7. *Fix a finite Ω-group G.*

(i) If $\zeta_1(G) = 1$ then G has a unique Remak Ω-decomposition $\mathcal{R}$ and the set $\mathcal{N}$ of minimal $(\Omega \cup G)$-subgroups is a direct $(\Omega \cup G)$-decomposition of the socle of G and $\mathcal{N}$ extends to $\mathcal{R}$.

(ii) If $\gamma_2(G) = G$ then G has a unique Remak Ω-decomposition $\mathcal{R}$ and the set $\mathcal{Q}$ of Ω-subgroups of G that are minimal over the completely reducible Ω-radical $CR(G)$ are a direct Ω-decomposition of $G/CR(G)$. Also, $\mathcal{Q}$ lifts to $\mathcal{R}$.

This leaves us with the case $1 < \gamma_2(G) = \zeta_1(G) < G$. This makes G a nilpotent group of nilpotence class 2; indeed, we can also assume G is a p-group for some prime p. Though this setting is the most difficult, its solution is also quite pleasing. Not only do we succeed in finding situations where we can lift and extend, we actually find matchings and sometimes *perfect* matchings in the sense that we can replace refinement in the definitions of lifting and extending with equality as sets. To achieve this we make a radical departure from standard Group Theoretic methods. Mimicking a recent study of central products of p-groups [W4, W5], we introduce a new group isomorphism invariant

$$C(G) \subseteq \mathrm{End}_{(\mathbb{Z}/p\mathbb{Z})[\Omega]}(G/\gamma_2(G)) \times \mathrm{End}_{(\mathbb{Z}/p\mathbb{Z})[\Omega]}(\gamma_2(G))$$

which is a commutative ring. Furthermore, the idempotents of this ring determine direct Ω-decompositions of G. This replaces the similar role of Jordan algebras for central products in [W4]. The definition of $C(G)$ is provided later in Definition 6.7. It enables us to prove:

Theorem 8. *If G is a finite Ω-group where $\gamma_2(G) = \zeta_1(G)$, then there is a unique $\mathcal{E} \subseteq C(\mathsf{Bi}(G))$ of pairwise orthogonal primitive idempotents that sum to 1. Furthermore, every Remak Ω-decomposition of G matches $(\mathcal{N}, \mathcal{Q})$ where*

$$\mathcal{N} = \{\gamma_2(G)\hat{e} : (e, \hat{e}) \in \mathcal{E}\} \qquad \& \qquad \mathcal{Q} = \{(G/\gamma_2(G))e : (e, \hat{e}) \in \mathcal{E}\}.$$

If we are to interpret this another way we discover an indecomposability test.

Corollary. *If P is an Ω-group of prime p power order, $C(P)$ is a local $(\mathbb{Z}/p\mathbb{Z})[\Omega]$-algebra and $\gamma_2(P) \leq \zeta_1(P) \leq \Phi(P)$, then P is directly Ω-indecomposable. The converse holds if $P^p = 1$.*

Theorems 1–8 comprise the scaffolding for recovering direct product decompositions. With these theorems in place it is possible to make claims about the efficiency of finding a Remak Ω-decomposition of a group and to prove when a group is Ω-indecomposable. We can also use this structure to estimate the number of groups that are Ω-indecomposable. These topics are taken up in the second half of this project.

2. Background

We begin with a survey of the background we use throughout the paper. Much of the preliminaries can be found in standard texts on Group Theory, consider [K2, Vol. I §§15–18; Vol. II §§45–47].

Typewriter fonts $\mathtt{X}, \mathtt{R}$, etc. denote sets without implied properties; Roman fonts G, H, etc., denote groups; Calligraphic fonts $\mathcal{H}, \mathcal{X}$, etc. denote sets and multisets of groups; and the Fraktur fonts $\mathfrak{X}$, $\mathfrak{N}$, etc. denote classes of groups.

With few exceptions we consider only finite groups. Functions are evaluated on the right and group actions are denoted exponentially. We write $\mathrm{End}\, G$ for the set of endomorphisms of G and $\mathrm{Aut}\, G$ for the group of automorphisms. The *centralizer* of a subgroup $H \leq G$ is $C_G(H) = \{g \in G : \forall h \in H, hg = gh\}$. The *upper central series* is $\{\zeta_i(G) : i \in \mathbb{N}\}$ where $\zeta_0(G) = 1$, $\zeta_i(G) \lhd \zeta_{i+1}(G)$ and $\zeta_{i+1}(G)/\zeta_i(G) = C_{G/\zeta_i(G)}(G/\zeta_i(G))$, for all $i \in \mathbb{N}$. The commutator of subgroups H and K of G is $[H, K] = \langle [h, k] = h^{-1}k^{-1}hk : h \in H, k \in K\rangle$. The *lower central series* is $\{\gamma_i(G) : i \in \mathbb{Z}^+\}$ where $\gamma_1(G) = G$ and $\gamma_{i+1}(G) = [G, \gamma_i(G)]$ for all $i \in \mathbb{Z}^+$. The *Frattini* subgroup $\Phi(G)$ is the intersection of all maximal subgroups. The *socle* $\mathrm{soc}(G)$ is the subgroup generated by all minimal normal subgroups.

2.1. **Operator groups.** An Ω-group G is a group, a possibly empty set Ω, and a function $\theta : \Omega \to \operatorname{End} G$. Throughout the paper we write g^ω for $g(\omega\theta)$, for all $g \in G$ and all $\omega \in \Omega$.

In a natural way, Ω-groups have all the usual definitions of Ω-subgroups, quotient Ω-groups, and Ω-homomorphisms. Call H *fully invariant*, resp. *characteristic* if it is an $(\operatorname{End} G)-$, resp. $(\operatorname{Aut} G)-$, subgroup. *With the exception of modules, we will insist that* $\Omega\theta \subseteq \operatorname{Aut} G$. In most places this is not a necessary requirement. However, this means that in this work every characteristic subgroup of G is automatically an Ω-subgroup. Let $\operatorname{Aut}_\Omega G$ denote the Ω-automorphisms of G. We describe normal Ω-subgroups M of G simply as $(\Omega \cup G)$-subgroup of G.

The following characterization is critical to our proofs; cf. [R3, (3.3.6)].

$$\operatorname{Aut}_{\Omega\cup G} G = \{\varphi \in \operatorname{Aut}_\Omega G : \forall g \in G, g\varphi \equiv g \pmod{\zeta_1(G)}\}. \tag{2.1}$$

It is also evident that $\operatorname{Aut}_{\Omega\cup G} G$ acts as the identity on $\gamma_2(G)$. Such automorphisms are called *central* but for uniformity we described them as $(\Omega \cup G)$-automorphisms.

We repeatedly use the following property of the $(\Omega \cup G)$-subgroup lattice.

Lemma 2.2 (Modular law)**.** [K2, Vol. II §44: pp. 91-92] *If M, H, and R are $(\Omega \cup G)$-subgroups of an Ω-group G and $M \leq H$, then $H \cap RM = (H \cap R)M$.*

2.2. **Free groups, varieties, and verbal and marginal subgroups.** In various places we use free groups. Fix a set $\mathtt{X} \neq \emptyset$ and a group G. Let $G^{\mathtt{X}}$ denote the set of functions from $\mathtt{X}$ to G, equivalently, the set of all $\mathtt{X}$-tuples of G.

Every $\bar{g} = (g_x : x \in \mathtt{X}) \in G^{\mathtt{X}}$ is the restriction of a unique homomorphism $\hat{g}$ from the free group $F(\mathtt{X})$ into G, that is:

$$(\forall x \in \mathtt{X}) \qquad\qquad x\hat{g} = g_x. \tag{2.3}$$

We use $\hat{g}$ exclusively in that manner. As usual we call $\langle \mathtt{X} | \mathtt{R} \rangle$ a *presentation* for a group G with respect to $\bar{g} \in G^{\mathtt{X}}$ if $G = \langle g_x : x \in \mathtt{X} \rangle$ and $\ker \hat{g}$ is the smallest normal subgroup of $F(\mathtt{X})$ containing $\mathtt{R}$.

A *variety of groups* $\mathfrak{V} = \mathfrak{V}(\mathtt{W})$ is a class of groups defined by a set $\mathtt{W}$ of words in a free group $F(\mathtt{X})$, known as *laws*. Explicitly, $G \in \mathfrak{X}$ if, and only if, every $\bar{g} \in G^{\mathtt{X}}$ and every $w \in \mathtt{W}$, $w(\bar{g}) = 1$. We say that $w \in F(\mathtt{X})$ is a *consequence* of the laws $\mathtt{W}$ if for every $G \in \mathfrak{V}$ and every $\bar{g} \in G^{\mathtt{X}}$, $w\hat{g} = 1$. A detailed study of varieties can be found in [N]. Our interest in varieties is summarized by the following well-known result.

Theorem 2.4 (Birkhoff [N, 15.53])**.** *A class of Ω-groups is a variety if, and only if, it is nonempty and is closed to homomorphic images, subgroups, and direct products (including infinite products).*

Corollary. *Varieties of Ω-groups are a direct classes.*

Fix a word $w \in F(\mathtt{X})$. We regard w as a function $G^{\mathtt{X}} \to G$, where $\bar{g} \mapsto w\hat{g}$, i.e. $w(\bar{g}) = w\hat{g}$. For example, if $w = [x_1, x_2]$, then $w : G^2 \to G$ can be defined as $w(g_1, g_2) = [g_1, g_2]$, for all $g_1, g_2 \in G$. Levi and Hall separately introduced two natural subgroups to associate with the function $w : G^{\mathtt{X}} \to G$. First, to approximate the image of w with a group, we have the *verbal* subgroup

$$w(G) = \langle w(\bar{g}) : \bar{g} \in G^{\mathtt{X}} \rangle. \tag{2.5}$$

Secondly, to mimic the radical of a multilinear map, we use the *marginal* subgroup

$$w^*(G) = \{h \in G \ : \ \forall \bar{g}' \in \langle h^\Omega \rangle^{\mathtt{X}}, \forall \bar{g} \in G^{\mathtt{X}}, \ w(\bar{g}\bar{g}') = w(\bar{g})\}. \tag{2.6}$$

(To be clear, $\bar{g}\bar{g}' \in G^{\mathtt{X}}$ is the pointwise product.) An alternative characterization is that $w(G)$ is the smallest subgroup of G containing the image of w and $w^*(G)$ is the largest normal Ω-subgroup of G for which $w : G^{\mathtt{X}} \to G$ factors through $w : (G/w^*(G))^{\mathtt{X}} \to w(G)$, similar to how the radical of bilinear form can be characterized. For a set $\mathtt{W}$ of words, the $\mathtt{W}$-verbal subgroup is $\mathtt{W}(G) = \langle w(G) : w \in \mathtt{W}\rangle$ and the $\mathtt{W}$-marginal subgroup is $\mathtt{W}^*(G) = \bigcap\{w^*(G) : w \in \mathtt{W}\}$. Observe that for finite sets $\mathtt{W}$, a single word may be used instead, e.g. replace $\mathtt{W} = \{[x_1, x_2], x_1^2\} \subseteq F(\{x_1, x_2\})$ with $w = [x_1, x_2]x_3^2 \in F(\{x_1, x_2, x_3\})$.

The verbal and marginal groups are dual in the following sense [H1]:

$$\mathtt{W}(G) = 1 \quad \Leftrightarrow \quad G \in \mathfrak{V}(\mathtt{W}) \quad \Leftrightarrow \quad \mathtt{W}^*(G) = G. \tag{2.7}$$

Hence, the verbal subgroups are *radical* in the sense that $W(G/W(G)) = 1$ and marginal subgroups are *idempotent* in the sense that $W^*(W^*(G)) = W^*(G)$. In particular, if $\mathfrak{V}(\mathtt{U}) \subseteq \mathfrak{V}(\mathtt{W})$ for two sets $\mathtt{W}$ and $\mathtt{U}$ of words, then $\mathtt{W}(G/\mathtt{U}(G)) = 1$ so that $\mathtt{W}(G) \leq \mathtt{U}(G)$. Likewise, $\mathtt{W}^*(\mathtt{U}^*(G)) = \mathtt{U}^*(G)$ so that $\mathtt{U}^*(G) \leq \mathtt{W}^*(G)$. In particular, if $\mathfrak{V}(\mathtt{W}) = \mathfrak{V} = \mathfrak{V}(\mathtt{U})$ then the verbal and marginal subgroups are independent of the choice of defining laws of $\mathfrak{V}$ which justifies the notation

$$\mathfrak{V}(G) = \mathfrak{V}(\mathtt{W})(G) = \mathtt{W}(G),$$
$$\mathfrak{V}^*(G) = \mathfrak{V}(\mathtt{W})^*(G) = \mathtt{W}^*(G).$$

Example 2.8. (i) The class $\mathfrak{A}$ of abelian groups is a group variety defined by $[x_1, x_2]$. The $\mathfrak{A}$-verbal subgroup of a group is the commutator subgroup and the $\mathfrak{A}$-marginal subgroup is the center.

(ii) The class $\mathfrak{N}_c$ of nilpotent groups of class at most c is a group variety defined by $[x_1, \ldots, x_{c+1}]$ (i.e. $[x_1] = x_1$ and $[x_1, \ldots, x_{i+1}] = [[x_1, \ldots, x_i], x_{i+1}]$, for all $i \in \mathbb{N}$). Also, $\mathfrak{N}_c(G) = \gamma_{c+1}(G)$ and $\mathfrak{N}_c^*(G) = \zeta_c(G)$ [R3, 2.3].

(iii) The class $\mathfrak{S}_d$ of solvable groups of derived length at most d is a group variety defined by $\delta_d(x_1, \ldots, x_{2^d})$ where $\delta_1(x_1) = x_1$ and for all $i \in \mathbb{N}$,

$$\delta_{i+1}(x_1, \ldots, x_{2^{i+1}}) = [\delta_i(x_1, \ldots, x_{2^i}), \delta_i(x_{2^i+1}, \ldots, x_{2^{i+1}})].$$

Predictably, $\mathfrak{S}_d(G) = G^{(d)}$ is the d-th derived group of G. It appears that $\mathfrak{S}_d^*(G)$ is not often used and has no name.[3]

Verbal and marginal subgroups are characteristic in G and verbal subgroups are also fully invariant [H1]. So if G is an Ω-group then so is $\mathfrak{V}(G)$. Moreover,

$$G \in \mathfrak{V}^\Omega \text{ if, and only if, } G \text{ is an } \Omega\text{-group and } \mathfrak{V}(G) = 1. \tag{2.9}$$

Unfortunately, marginal subgroups need not be fully invariant (e.g. the center of a group). In their place, we use the Ω-invariant marginal subgroup $(\mathfrak{V}^\Omega)^*(G)$, i.e. the largest normal Ω-subgroup of $\mathfrak{V}^*(G)$. Since $\mathfrak{V}$ is closed to subgroups it follows that $(\mathfrak{V}^\Omega)^*(G) \in \mathfrak{V}$. Furthermore, if G is an Ω-group and $G \in \mathfrak{V}$ then $\mathfrak{V}^*(G) = G$ and so the Ω-invariant marginal subgroup is G. (This explains our use of h^Ω in (2.6).) Thus,

$$G \in \mathfrak{V}^\Omega \text{ if, and only if, } G \text{ is an } \Omega\text{-group and } \mathfrak{V}^*(G) = G. \tag{2.10}$$

[3]This series behaves differently from the related upper central series. Whereas the derived series of a solvable group is strictly decreasing, the dual ascending marginal series is not always strictly increasing, even for solvable groups. However, it is always the case that a solvable group G with a derived series of length d also has an ascending marginal series reaching G in d steps.

In our special setting we can insist that all operators act as automorphisms and so the invariant marginal subgroup is indeed the marginal subgroup. Nevertheless, to avoid confusion we assume the marginal subgroup of a variety of Ω-groups refers to the Ω-invariant marginal subgroup.

2.3. **Rings, frames, and modules.** We involve some standard theorems for associative unital finite rings and modules; compare [CR, Chapter 6]. Throughout this section R denotes a finite associative unital ring.

An $e \in R - \{0\}$ is *idempotent* if $e^2 = e$. An idempotent is *proper* if it is not 1 (as we have excluded 0 as an idempotent). Two idempotents $e, f \in R$ are *orthogonal* if $ef = 0 = fe$. An idempotent is *primitive* if it is not the sum of two orthogonal idempotents. Finally, a *frame* $\mathcal{E} \subseteq R$ is a set of pairwise orthogonal primitive idempotents of R which sum to 1. We use the following properties.

Lemma 2.11 (Lifting idempotents)**.** *Let R be a finite ring.*

(i) If $e \in R$ such that $e^2 - e \in J(R)$ (the Jacobson radical) then for some $n \leq \log_2 |J(R)|$, $(e^2 - e)^n = 0$ and

$$\hat{e} = \sum_{i=0}^{n-1} \binom{2n-1}{i} e^{2n-1-i}(1-e)^i$$

is an idempotent in R. Furthermore, $\widehat{1-e} = 1 - \hat{e}$.

(ii) $\mathcal{E}$ is a frame of $R/J(R)$ then $\hat{\mathcal{E}} = \{\hat{e} : e \in \mathcal{E}\}$ is a frame of R.

(iii) Frames in R are conjugate by a unit in R; in particular, if R is commutative then R has a unique frame.

Proof. Part (i) is verified directly, compare [CR, (6.7)]. Part (ii) follows from induction on (i). For (iii) see [CR, p. 141]. □

If M is an R-module and e is an idempotent of $\operatorname{End}_R M$ then $M = Me \oplus M(1-e)$. Furthermore, if $M = E \oplus F$ as an R-module, then the projection $e_E : M \to M$ with kernel F and image E is an idempotent endomorphism of M. Thus, every direct R-decomposition $\mathcal{M}$ of M is parametrized by a set $\mathcal{E}(\mathcal{M}) = \{e_E : E \in \mathcal{M}\}$ of pairwise orthogonal idempotents of $\operatorname{End}_R M$ which sum to 1. Remak R-decompositions of M correspond to frames of $\operatorname{End}_R M$.

2.4. **Bimaps and homotopisms.** Here we introduce Ω-bimaps and direct Ω-decompositions of Ω-bimaps.

Let U, V, and W denote abelian Ω-groups. An Ω-bimap $B : U \times V \to W$ is a function with the distributive-type properties: for all $u, u' \in U$, and all $v, v' \in V$,

$$(u+u')Bv = uBv + u'Bv \qquad uB(v+v') = uBv + uBv'$$

and the property: for all $u \in U$, all $v \in V$, and all $r \in \Omega$

$$(ur)Bv = (uBv)r = uB(vr)$$

Every Ω-bimap is also $\mathbb{Z}[\Omega]$-bimap. For $X \subseteq U$ and $Y \subseteq V$, set

$$\begin{aligned} XBY &= \langle xBy : x \in X, y \in Y \rangle, \\ X^\perp &= \{v \in V : XBv = 0\}, \text{ and} \\ Y^\top &= \{u \in U : uBY = 0\}. \end{aligned}$$

If $X \leq U$ and $Y \leq V$ then define the *submap*

$$B_{X,Y} : X \times Y \to XBY \tag{2.12}$$

as the restriction of B to inputs from $X \times Y$. The *radicals* of B are $U^\perp$ and $V^\top$. We say B is *nondegenerate* if both radicals are trivial.

Bimaps $B : U \times V \to W$ are found throughout algebra (e.g. as products of rings, actions of modules, dot-products, commutation in p-groups, etc). This makes it impossible to fix a single morphism type from which to build a category of bimaps. A study of these categories can be found in [W6]. In our special context we consider the category of bimaps up to *homotopisms*.[4] Homotopisms between bimaps $B : U \times V \to W$ and $B' : U' \times V' \to W'$ are triples $f = (f^\curvearrowleft, f^\curvearrowright; f^\uparrow)$ of homomorphisms where

$$(\forall u \in U, \forall v \in V) \qquad (uf^\curvearrowleft)B'(vf^\curvearrowright) = (uBv)f^\uparrow.$$

Two homotopisms $f = (f^\curvearrowleft, f^\curvearrowright; f^\uparrow)$ and $g = (g^\curvearrowleft, g^\curvearrowright; g^\uparrow)$ are composed pointwise: $fg = (f^\curvearrowleft g^\curvearrowleft, f^\curvearrowright g^\curvearrowright; f^\uparrow g^\uparrow)$. This is indeed a category with the expected notions of epitopisms, monotopisms, and isotopisms.

2.5. **Low class p-groups.** A group G is called *nilpotent* if for some $c > 0$, $\gamma_{c+1}(G) = 1$. The smallest such c is called the *nilpotence class* of G.

The bimaps we consider appeared in several early works on p-groups and were studied in detail by Baer [B; W2, Section 5].

Fix an Ω-group G where $\gamma_2(G) \leq \zeta_1(G)$ (again $\zeta_1(G)$ is an Ω-subgroup as Ω acts on G as automorphisms). There we define $V = G/\zeta_1(G)$, $W = \gamma_2(G)$, and denote operations additively in these groups. For $x \in G$ write $\bar{x} = x\zeta_1(G)$. Finally define $B = \mathsf{Bi}(G) : V \times V \to W$ where

$$(\forall x, y \in G) \qquad \bar{x}B\bar{y} = [x, y]. \tag{2.13}$$

The choice of coset representatives differ by a central element so that B is in fact well-defined. The commutator relations

$$[xy, z] = [x, z]^y[y, z] \qquad [x, yz] = [x, z][x, y]^z.$$

imply that B is a nondegenerate Ω-bimap, in fact a $\mathbb{Z}_{p^e}[\Omega]$-bilinear if $G^{p^e} = 1$. An Ω-bimap $B : U \times V \to W$ is *alternating* if $U = V$ and for all $v \in V$, $vBv = 0$. Notice $\mathsf{Bi}(G)$ is always alternating. Since $\zeta_1(G)$ is characteristic, Bi is a functor from groups of class 2 to the isotopism category of bimaps; cf. [W4, Section 3.3].

In many situations bimaps determine groups. This is subsumed by the Lazard correspondence but the version we need is simpler and due to Baer. Given an alternating bimap $B : V \times V \to W$ with V and W of odd order then we define product on $V \times W$ by:

$$(u, w) * (v, x) = \left(u + v, w + x + \frac{1}{2}uBv\right)$$

This makes $V \times W$ into a nilpotent group of class 2 with commutator $(0, VBV)$ and center $(V^\perp, W)$. We denote this group by $\mathsf{Grp}(B)$. For further details see [W2, W4]. In particular, if a group G has $\gamma_2(G) \leq \zeta_1(G)$ and $G^p = 1$, then $G \cong \mathsf{Grp}(\mathsf{Bi}(G))$ [W4, Proposition 3.10(ii)].

[4]The name homotopism comes from a similar definition of A. Albert for nonassociative algebras.

3. Graded subgroups

Our task in this section is to discover graded subgroups. Recall from Section 1.2 that an $(\Omega \cup G)$-subgroup N of an Ω-group G is Ω-graded if every finite direct Ω-decomposition $\mathcal{H}$ induces direct $(\Omega \cup G)$-decompositions $\mathcal{H} \cap N$ of N and $\mathcal{H}N/N$ of G/N. We call an exact sequence $1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} Q \to 1$ of Ω-groups Ω-graded and call the extension, of N by Q, Ω-graded, if $N\iota$ is Ω-graded. The universal quantifier in the definition of graded subgroups may seem difficult to satisfy; nevertheless, in Section 3.2 we show many well-known subgroups are graded, for example the commutator subgroup. We close this section with a proof of Theorem 1.

3.1. General properties.

We start with a simple test of a graded subgroup.

Lemma 3.1. *Let G be an Ω-group with a finite direct Ω-decomposition $\mathcal{H}$. If N is an $(\Omega \cup G)$-subgroup of G and $N = \langle \mathcal{H} \cap N \rangle$, then $\mathcal{H} \cap N$ is a direct $(\Omega \cup G)$-decomposition of N and $\mathcal{H}N/N$ is a direct Ω-decomposition of G/N. If $N = \langle \mathcal{H} \cap N \rangle$ for every direct Ω-decomposition $\mathcal{H}$ of G then N is Ω-graded.*

Proof. First we show $\mathcal{H} \cap N$, cf. (1.2), is a direct $(\Omega \cup G)$-decomposition of N. For $(H \cap N) \cap \langle \mathcal{H} \cap N - \{H \cap N\} \rangle = 1$ for all $H \cap N \in \mathcal{H} \cap N$.

Next we show $\mathcal{H}N/N$, cf. (1.3), is a direct $(\Omega \cup G)$-decomposition of G/N. Let $|\mathcal{H}| > 1$, take $H \in \mathcal{H}$, and set $K = \langle \mathcal{H} - \{H\} \rangle$. From the first part, $HN \cap KN = (H \times (K \cap N)) \cap ((H \cap N) \times K) = (H \cap N) \times (K \cap N) = N$. □

Along with the notations $\mathcal{H} \cap N$ and $\mathcal{H}N/N$ we have occasion to use

$$\mathcal{H}N = \{HN : H \in \mathcal{H}\} - \{N\}. \tag{3.2}$$

Lemma 3.3. *If N is Ω-graded in G and $\mathcal{H}$ a finite direct Ω-decomposition, then $H \mapsto HN \mapsto HN/N$ are bijections $\mathcal{H} - \{H \in \mathcal{H} : H \leq N\} \to \mathcal{H}N \to \mathcal{H}N/N$.*

Proof. $H \mapsto HN$ is surjective. We show it is also injective on $\mathcal{H} - \{H \in \mathcal{H} : H \leq N\}$. Choose $H, K \in \mathcal{H}$ with $HN = KN$. As N is $(\Omega \cup G)$-graded, $N = (H \cap N) \times (\langle \mathcal{H} - \{H\} \rangle \cap N)$ so that $HN = H \times (\langle \mathcal{H} - \{H\} \rangle \cap N)$. Yet $K \leq HN$ and $K \leq \langle \mathcal{H} - \{H\} \rangle$ so $K \leq HN \cap \langle \mathcal{H} - \{H\} \rangle = \langle \mathcal{H} - \{H\} \rangle \cap N$. So $K \leq N$. The bijective correspondence $HN \mapsto HN/N$ is immediate. □

Lemma 3.4. *If M and N are $(\Omega \cup G)$-graded subgroups of G then NM and $N \cap M$ are $(\Omega \cup G)$-graded. In particular, the set of Ω-graded subgroups of G is a modular sublattice of the lattice of $(\Omega \cup G)$-subgroups of G.*

Proof. Let $g \in N \cap M$. So there are unique $h \in H$ and $k \in K := \langle \mathcal{H} - \{H\} \rangle$ with $g = hk$. As N is graded, $N = (H \cap N) \times (K \cap N)$ and so $h \in H \cap N$. Likewise $h \in H \cap M$ so that $H \in H \cap (N \cap M)$. Also $k \in \langle \mathcal{H} - \{H\} \rangle \cap (N \cap M)$. Thus, $g \in \langle \{H \cap (N \cap M), \langle \mathcal{H} - \{H\} \rangle \cap (N \cap M)\} \rangle$. By induction on $|\mathcal{H}|$, $N \cap M \leq \langle \mathcal{H} \cap (N \cap M) \rangle \leq N \cap M$. The rest is argued similarly. □

The final general property is that grading is essentially a transitive relation.

Lemma 3.5. *Fix an Ω-group G and an Ω-grade subgroup N.*

(i) If M is an $(\Omega \cup G)$-graded subgroup of N, then M is an Ω-graded subgroup of G.

(ii) If $N \leq M \leq G$ such that M/N is an Ω-graded subgroup of G/N, then M is an Ω-graded subgroup of G.

Proof. Fix a finite direct Ω-decomposition $\mathcal{H}$ of G. For (i), $\mathcal{H}\cap N$ is a direct $(\Omega\cup G)$-decomposition of N and so $\mathcal{H}\cap M = (\mathcal{H}\cap N)\cap M$ is a direct $(\Omega\cup G)$-decomposition of M. By Lemma 3.1, M is Ω-graded in G. Next for (ii), $\mathcal{H}N/N$ is a direct Ω-decomposition of G/N and as M/N is Ω-graded it follows that $\mathcal{H}N/N \cap M/N$ is a direct Ω-decomposition of M/N and so $\langle \mathcal{H}N \cap M\rangle = M$. Taking $H \in \mathcal{H}$, applying the modular law we see $HN \cap M = (H \cap M)N$. So $\mathcal{H}N \cap M = (\mathcal{H} \cap M)N$. As $N = \langle \mathcal{H}\cap N\rangle \leq \langle \mathcal{H}\cap M\rangle$ it follows that $\langle \mathcal{H}\cap M\rangle = \langle(\mathcal{H}\cap M)N\rangle = \langle \mathcal{H}N\cap M\rangle = M$. By Lemma 3.1, M is Ω-graded. □

3.2. **Group classes and associated graded subgroups.** To explain the existence of graded subgroups we focus on classes of groups which are closed to direct products and direct decompositions. We use standard terms for classes of groups, compare [DH, p. 264]).

By a *class of Ω-groups* we mean a class which is closed to Ω-isomorphic images. If $\mathfrak{X}$ is a class of groups without operators, then $\mathfrak{X}^\Omega$ denotes the subclass of Ω-groups in $\mathfrak{X}$. As in Section 1.2, a class $\mathfrak{X}$ of Ω-groups is direct if it is closed to finite direct products (D_0*-closed*) and also to direct factors (DF*-closed*), i.e. if $G \in \mathfrak{X}$ and H is a direct Ω-factor of G then $H \in \mathfrak{X}$.

A D_0-closed class that is also closed to subgroups (S*-closed*) is a direct class. The converse is not true, e.g. the class of finite direct products of finite simple groups is direct but not S-closed. To specify the groups in a direct class it is sufficient to specify the directly Ω-indecomposable groups it contains. However, in practical terms there are few settings where the directly Ω-indecomposable groups are actually known.

3.3. **Verbal and marginal subgroups are graded.** Recall from Section 2.2 that a variety $\mathfrak{V}$ of groups is a class of groups that satisfy a set $\mathtt{W}$ of words in a free group $F(\mathtt{X})$. Along with these classes we associate verbal and marginal subgroups $\mathfrak{V}(G)$ and $\mathfrak{V}^*(G)$. We now demonstrate these groups are the prototypical instances of down and up graders.

Recall from Section 1.2 that a direct class $\mathfrak{X}$ and a function $G \mapsto \mathfrak{X}(G)$ is an up (resp. down) Ω-grading pair when

(a) $\mathfrak{X}(G) \in \mathfrak{X}$ (resp. $G/\mathfrak{X}(G) \in \mathfrak{X}$),
(b) If $G \in \mathfrak{X}$ then $\mathfrak{X}(G) = G$ (resp. $\mathfrak{X}(G) = 1$),
(c) $\mathfrak{X}(G)$ is an Ω-graded subgroup of G, and
(d) for each direct Ω-factor H of G, $\mathfrak{X}(H) = H \cap \mathfrak{X}(G)$.

Notice if $\langle \mathfrak{X}, G \mapsto \mathfrak{X}(G)\rangle$ is an Ω-grading pair then $\mathfrak{X}(H \times K) = \mathfrak{X}(H) \times \mathfrak{X}(K)$.

Proposition 3.6. *The marginal subgroup of a variety of Ω-groups is an up Ω-grader and the verbal subgroup is a down Ω-grader for the variety.*

Proof. Let $\mathfrak{V} = \mathfrak{V}^\Omega$ be a variety of Ω-groups with defining laws $\mathtt{W}$ and fix an Ω-group G. As the marginal function is idempotent, (2.10) implies that $\mathfrak{V}^*(G) \in \mathfrak{V}$ and that if $G \in \mathfrak{V}$ then $G = \mathfrak{V}^*(G)$. Similarly, verbal subgroups are radical so that by (2.9) we have $G/\mathfrak{V}(G) \in \mathfrak{V}$ and when $G \in \mathfrak{V}$ then $\mathfrak{V}(G) = 1$.

Fix a direct Ω-decomposition $\mathcal{H}$ of G, fix an $H \in \mathcal{H}$, and set $K = \langle \mathcal{H} - \{H\}\rangle$. For each $\bar{g} \in G^{\mathtt{X}} = (H \times K)^{\mathtt{X}}$ there are unique $\bar{g}_H \in H^{\mathtt{X}}$ and $\bar{g}_K \in K^{\mathtt{X}}$ such that $\bar{g} = \bar{g}_H\bar{g}_K$. Thus, for all $w \in \mathtt{W}$, $w(\bar{g}) = w(\bar{g}_H)w(\bar{g}_K)$ and so $w(H \times K) = w(H) \times w(K)$. Hence, $\mathfrak{V}(H \times K) = \mathfrak{V}(H) \times \mathfrak{V}(K)$. By induction on $|\mathcal{H}|$, $\mathcal{H} \cap \mathfrak{V}(G) = \{\mathfrak{V}(H) : H \in \mathcal{H}\}$ is a direct Ω-decomposition of $\mathfrak{V}(G)$. So $\mathfrak{V}(G)$ is a down Ω-grader.

For the marginal case, for all $\bar{g}' \in \langle (h,k) \rangle^{\mathtt{X}} \leq (H \times K)^{\mathtt{X}} = G^{\mathtt{X}}$ and all $\bar{g} \in G^{\mathtt{X}}$, again there exist unique $\bar{g}_H, \bar{g}'_H \in H^{\mathtt{X}}$ and $\bar{g}_K, \bar{g}'_K \in K^{\mathtt{X}}$ such that $\bar{g} = \bar{g}_H \bar{g}_K$ and $\bar{g}' = \bar{g}'_H \bar{g}'_K$. Also, $w(\bar{g}\bar{g}') = w(\bar{g})$ if, and only if, $w(\bar{g}_H \bar{g}'_H) = w(\bar{g}_H)$ and $w(\bar{g}_K \bar{g}'_K) = w(\bar{g}_K)$. Thus, for all $w \in \mathtt{W}$, $w^*(H \times K) = w^*(H) \times w^*(K)$. Hence, $\mathfrak{V}^*(H \times K) = \mathfrak{V}^*(H) \times \mathfrak{V}^*(K)$ and by induction $\mathcal{H} \cap \mathfrak{V}^*(G)$ is a direct Ω-decomposition of $\mathfrak{V}^*(G)$. Thus, $\mathfrak{V}^*(G)$ is an up Ω-grader. □

Remark 3.7. There are examples of infinite direct decompositions $\mathcal{H}$ of infinite groups G and varieties $\mathfrak{V}$, where $\mathfrak{V}(G) \neq \langle \mathcal{H} \cap \mathfrak{V}(G) \rangle$ [A]. However, our definition of grading purposefully avoids infinite direct decompositions.

With Proposition 3.6 we get a simultaneous proof of some individually evident examples of up and down grading pairs.

Corollary 3.8. *Following the notation of Example 2.8 we have the following.*

(i) The class $\mathfrak{N}_c$ of nilpotent groups of class at most c is a direct class with up grader $G \mapsto \zeta_c(G)$ and down grader $G \mapsto \gamma_c(G)$.

(ii) The class $\mathfrak{S}_d$ of solvable groups of derived length at most d is a direct class with up grader $G \mapsto (\delta_d)^*(G)$ and down grader $G \mapsto G^{(d)}$.

(iii) For each prime p the class $\mathfrak{V}([x,y]z^p)$ of elementary abelian p-groups is a direct class with up grader $G \mapsto \Omega_1(\zeta_1(G))$ and down grader $G \mapsto [G,G]\mathfrak{V}_1(G)$.[5]

3.4. **Completed classes, cores, and residues.** We also wish to include direct classes $\mathfrak{N} := \bigcup_{c \in \mathbb{N}} \mathfrak{N}_c$ and $\mathfrak{S} := \bigcup_{d \in \mathbb{N}} \mathfrak{S}_d$. These classes are not varieties (they are not closed to infinite direct products as required by Theorem 2.4). Therefore, we must consider alternatives to verbal and marginal groups for appropriate graders.

We say an Ω-group class $\mathfrak{X}$ is R_0-closed, writing $\mathfrak{X} = R_0\mathfrak{X}$, if for every Ω-group G having normal Ω-subgroups $N_1, \ldots, N_r$ with $G/N_i \in \mathfrak{X}$ then $G/\cap_{i=1}^r N_i \in \mathfrak{X}$ [DH, p. 264]. For example, such is the case for the class of solvable groups.

Definition 3.9. Fix an Ω-class $\mathfrak{X}$ containing 1, and fix a finite Ω-group G.

(a) The $\mathfrak{X}$-*core* $O_{\mathfrak{X}}(G)$ is the intersection of all maximal $(\Omega \cup G)$-subgroups contained in $\mathfrak{X}$. Dually, the $\mathfrak{X}$-*cocore* $O^{\mathfrak{X}}(G)$ is the join of the kernels of all maximal $(\Omega \cup G)$-quotients that lie in $\mathfrak{X}$.

(b) If $\mathfrak{X}$ is R_0-closed then define the $\mathfrak{X}$-residue $G^{\mathfrak{X}}$ as the smallest normal Ω-subgroup with $G/G^{\mathfrak{X}} \in \mathfrak{X}$. This is well-defined; cf. [DH, Lemma II.2.4].

We assume $1 \in \mathfrak{X}$ so that $O_{\mathfrak{X}}(G)$ and $O^{\mathfrak{X}}(G)$ are defined. If $\mathfrak{X}$ is S-closed (closed to subgroups) then $O_{\mathfrak{X}}(G) \in \mathfrak{X}$ and if $\mathfrak{X}$ is closed to quotients then $O^{\mathfrak{X}}(G) \in \mathfrak{X}$. Finally, if $\mathfrak{X}$ is R_0-closed and G is finite then there is a unique maximal quotient that lies in $\mathfrak{X}$, $G/G^{\mathfrak{X}}$, and so $O^{\mathfrak{X}}(G) = G^{\mathfrak{X}}$.

Example 3.10. (i) $O_{\mathfrak{A}}(G)$ is the intersection of all maximal normal abelian subgroups of G which is generally a non-trivial intersection. On the other hand, $O^{\mathfrak{A}}(G) = G^{\mathfrak{A}}$ is the commutator subgroup since a group has a unique maximal abelian quotient.

(ii) $O_{\mathfrak{N}_c}(G)$ is the intersection of all maximal normal nilpotent subgroups of G with class at most c. As in (i), this need not be a trivial intersection. However, if $c > \log|G|$ then all nilpotent subgroups of G have class at most c and

[5]Here $\Omega_1(X) = \langle x \in X : x^p = 1 \rangle$ and $\mathfrak{V}_1(X) = \langle x^p : x \in G \rangle$, which are traditional notations having nothing to do with our use of Ω for operators elsewhere.

therefore $O_{\mathfrak{N}}(G) = O_{\mathfrak{N}_c}(G)$ is the Fitting subgroup of G: the unique maximal normal nilpotent subgroup of G.

(iii) $O_{\mathfrak{S}_d}(G)$, $d > \log|G|$, is the unique maximal normal solvable subgroup of G, i.e.: the solvable radical $O_{\mathfrak{S}}(G)$ of G. Since solvable groups are closed to extensions, $O^{\mathfrak{S}}(G)$ is the solvable residue, i.e. the largest solvable quotient of G.

Proposition 3.11. *If $\mathfrak{V}$ is a group variety of Ω-groups and G an Ω-group, then*

(i) $\mathfrak{V}^*(G) \leq O_{\mathfrak{V}}(G)$,

(ii) $\mathfrak{V}(G) = O^{\mathfrak{V}}(G)$, *and*

(iii) if M is an $(\Omega \cup G)$-subgroup then $O_{\mathfrak{V}}(G)O_{\mathfrak{V}}(M)$ is an $(\Omega \cup G)$-subgroup contained in $\mathfrak{V}$.

Proof. Let $\mathtt{W}$ be a set of defining laws for $\mathfrak{V}$.

For (i), let $\bar{g} = (g_x : x \in \mathtt{X}) \in G^{\mathtt{X}}$ where for every $x \in \mathtt{X}$, $g_x \in \mathfrak{V}^*(G)H$. Thus, for all $w \in \mathtt{W}$, and all $x \in \mathtt{X}$, $g_x = g'_x g''_x$ where $g'_x \in w^*(G)$ and $g''_x \in H$. As $w^*(G)$ is marginal to G it is marginal to H and so $w(\bar{g}) = w(\bar{g}'')$. As $H \in \mathfrak{V}$, $w(\bar{g}'') = 1$. Thus, $w(\bar{g}) = 1$ and so $w(w^*(G)H) = 1$. It follows that $\mathfrak{V}^*(G)H \in \mathfrak{V}$. Therefore, $\mathfrak{V}^*(G)H \leq O_{\mathfrak{V}}(G)$.

For (ii), as $G/H \in \mathfrak{V}$, for all $w \in \mathtt{W}$ and all $\bar{g} \in G^{\mathtt{X}}$, $w(\bar{g}) \equiv 1 \pmod{H}$ so $w(\bar{g}) \in H$. Thus, $w(G) \leq H$ and so $\mathfrak{V}(G) \leq H$. Consequently $\mathfrak{V}(G)$ is the unique maximal Ω-quotient in $\mathfrak{V}$.

Finally we prove (iii). 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 $\mathfrak{V}$. □

Example 3.12. It is possible to have $\mathfrak{V}^*(G) < O_{\mathfrak{V}}(G)$. For instance, with $G = S_3 \times C_2$ and the class $\mathfrak{A}$ of abelian groups, the $\mathfrak{A}$-marginal subgroup is the center $1 \times C_2$, whereas the $\mathfrak{A}$-core is $C_3 \times C_2$.

Proposition 3.13. *Let G be a finite Ω-group with a direct Ω-decomposition $\mathcal{H}$. If $\mathfrak{V}$ is a variety of Ω-groups then*

$$\mathcal{H} \cap O_{\mathfrak{V}}(G) = \{O_{\mathfrak{V}}(H) : H \in \mathcal{H}\}$$

and this is a direct Ω-decomposition of $O_{\mathfrak{V}}(G)$. In particular, $G \mapsto O_{\mathfrak{V}}(G)$ is an up Ω-grader. Furthermore, if $\mathfrak{V}$ is a union of a chain $\mathfrak{V}_0 \subseteq \mathfrak{V}_1 \subseteq \cdots$ of varieties of Ω-groups then $O_{\mathfrak{V}}(G)$ is an up Ω-grader and $O^{\mathfrak{V}}(G)$ is a down Ω-grader.

Proof. 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 $\mathfrak{V} = \mathfrak{V}(w)$. For each $\bar{g} \in (MN)^{\mathtt{X}}$, write $\bar{g} = \bar{g}_N \times \bar{g}_K$ where $\bar{g}_N \in N^{\mathtt{X}}$ and $\bar{g}_K \in M_K^{\mathtt{X}}$. Hence, $w(\bar{g}) = w(\bar{g}_N \times \bar{g}_K) = w(\bar{g}_N) \times w(\bar{g}_K)$. However, $w(N) = 1$ and $w(M_K) = 1$ as $N, M_K \in \mathfrak{V}$. Thus, $w(\bar{g}) = 1$, 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 Lemma 3.1, $O_{\mathfrak{V}}(G)$ is Ω-graded.

Finally suppose $\mathfrak{V}$ is the union of varieties $\mathfrak{V}_1 \subseteq \mathfrak{V}_2 \subseteq \cdots$. Now for every $H \in \mathcal{H}$, $O_{\mathfrak{V}}(H) \in \mathfrak{V}$ which means that for some i, $O_{\mathfrak{V}}(H) = O_{\mathfrak{V}_n}(H)$ for all $n \geq i$. As $\mathcal{H}$ is finite, there is a maximum integer n such that for all $H \in \mathcal{H}$, $O_{\mathfrak{V}}(H) = O_{\mathfrak{V}_n}(H)$ and $O_{\mathfrak{V}}(G) = O_{\mathfrak{V}_n}(G)$. Hence,

$$H \cap O_{\mathfrak{V}}(G) = H \cap O_{\mathfrak{V}_n}(G) = \{O_{\mathfrak{V}_n}(H) : H \in \mathcal{H}\} = \{O_{\mathfrak{V}}(H) : H \in \mathcal{H}\}.$$

Thus $O_{\mathfrak{V}}(G)$ is an up Ω-grader. Similarly, $O^{\mathfrak{V}}(G)$ is a down Ω-grader. □

Corollary 3.14. *(i) The class $\mathfrak{N}$ of nilpotent groups is a direct class and $G \mapsto O_{\mathfrak{N}}(G)$ (the Fitting subgroup) is an up grader.*

(ii) The class $\mathfrak{S}$ of solvable groups is a direct class and $G \mapsto O_{\mathfrak{S}}(G)$ (the solvable radical) is an up grader.

Proof. For a finite group G, the Fitting subgroup is the $\mathfrak{N}_c$-core where $c > |G|$. Likewise, the solvable radical is the $\mathfrak{S}_c$-core for $d > |G|$. The rest follows from Proposition 3.13. □

Recall from Section 1.2 we announced in Theorem 1 that every finite Ω-group has an Ω-graded chief series.

Lemma 3.15. *Let M be a finite-dimensional faithful module of a finite-dimensional $(\mathbb{Z}/p\mathbb{Z})$-algebra R. It follows that M has an R-graded chief series.*

Proof. If M is irreducible the result holds trivially. Otherwise, by Lemma 3.5 it suffices to identify a proper nontrivial R-graded submodule. Let $J = J(R)$ be the Jacobson radical of R.

If $J = 0$ then R is semisimple Artinian and M is direct sum of its simple submodules. In particular, every simple submodule is R-graded. So assume $J > 0$. We claim MJ is R-graded. Let $\mathcal{M}$ be a direct R-decomposition of M. Fix $X \in M$ and set $Y = \langle \mathcal{M} - \{X\} \rangle$. So $M = X \oplus Y$ and so $MJ = XJ \oplus YJ$. By induction on Y and Lemma 3.1, it follows that MJ is R-graded. □

3.5. **Proof of Theorem 1.** Let G be a finite Ω-group. We may assume G is not a characteristically simple Ω-group.

By Lemma 3.5 it is sufficient to show that G has a proper nontrivial $(\Omega \cup G)$-graded subgroup. In our induction we re-purpose G but we cannot forget to use the original operators $\Gamma = \Omega \cup G$, where the G is the original group.

First, suppose that G is solvable. Then the derived subgroup G' is Γ-graded series because it is a verbal subgroup. If $\gamma_2(G) > 1$ we are done so suppose that $\gamma_2(G) = 1$. Pick a prime p dividing $|G|$ and observe that G^p is also a verbal subgroup, therefore an Γ-graded subgroup. So finally assume G is an elementary abelian p-group; hence, G is a finite-dimensional $(\mathbb{Z}/p\mathbb{Z})[\Gamma]$-module. By Lemma 3.15, G has an Γ-graded chief series.

Otherwise G is non-solvable. The solvable radical $O_{\mathfrak{S}}(G)$ is a proper Γ-graded subgroup (Corollary 3.14(ii)) and so we are left to assume $O_{\mathfrak{S}}(G) = 1$. Now the socle $\operatorname{soc}(G/O_{\mathfrak{S}}(G))$ is a direct product of the minimal Γ-normal subgroups of G,

so for any direct Γ-factor H of G, $H \cap \mathrm{soc}(G)$ is the direct product of the minimal Γ-subgroups of H. Thus, $\mathrm{soc}(G)$ is Γ-graded. The socle of a group with trivial solvable radical is non-trivial. So finally we are left only with the case that $G = \mathrm{soc}(G)$ and $O_{\mathfrak{S}}(G) = 1$. So every nontrivial Γ-subgroup of G is Γ-graded. □

4. Lifting, extending, and matching

Having created sufficient instances of graded subgroups and graded pairs we now focus on how these groups lead to instances where direct decompositions of quotients or subgroups lift or extend to Remak decompositions. In particular we prove Theorems 2 & 3.

Recall from Section 1.2 that we consider three types of problems we called lifting, extending and matching. In general terms we fix an Ω-graded short exact sequence of Ω-groups:

$$1 \longrightarrow N \xrightarrow{\ i\ } G \xrightarrow{\ q\ } Q \longrightarrow 1. \tag{4.1}$$

With respect to (4.1) the three problems we consider are as follows. For fixed direct $(\Omega \cup G)$-decompositions $\mathcal{N}$, $\mathcal{H}$, and $\mathcal{Q}$ of N, G, and Q respectively

- $\mathcal{H}$ *extends* (or is an extension of) $\mathcal{N}$ if $\mathcal{N}\iota$ refines $\mathcal{H} \cap N$.
- $\mathcal{H}$ *lifts* (or is a lift of) $\mathcal{Q}$ if $\mathcal{Q}$ refines $\mathcal{H}q$.
- $\mathcal{H}$ is *matches* (or is a match for) $(\mathcal{N}, \mathcal{Q})$ if $\mathcal{H}$ both extends $\mathcal{N}$ and lifts $\mathcal{Q}$.

4.1. **Proof of Theorem 2.** Remak decompositions of finite groups need not be unique as a set, e.g. the Remak decompositions of a finite vector space of order p^d has $p^{O(d^2)}$ distinct Remak decompositions. However, Remak's proof of the "Krull-Schmidt" theorem shows that $\mathrm{Aut}_{\Omega \cup G} G$ acts transitively on the Remak Ω-decompositions of G. Thus, in the case of a nonabelian Ω-group G we have a simple means to merge all Remak Ω-decompositions $\mathcal{R}$ into one set $\mathcal{R}\zeta_1(G)$, or dually $\mathcal{R} \cap \gamma_2(G)$. These two sets suggest a unique place to look for direct decompositions that lift and extend and this the main idea in Theorem 2.

Lemma 4.2. *For all Remak Ω-decompositions $\mathcal{R}$ and all direct Ω-decompositions $\mathcal{K}$ of G,*

(i) for all $(\Omega \cup G)$-subgroups $M \geq \zeta_1(G)$, $\mathcal{R}M$ refines $\mathcal{K}M$,
(ii) for all $(\Omega \cup G)$-subgroups $M \leq \gamma_2(G)$, $\mathcal{R} \cap M$ refines $\mathcal{K} \cap M$.

Proof. Let $\mathcal{T}$ be a Remak Ω-decomposition of G which refines $\mathcal{K}$. By Theorem 1.1, there is a $\varphi \in \mathrm{Aut}_{\Omega \cup G} G$ such that $\mathcal{R}\varphi = \mathcal{T}$. Form (2.1) it follows that $\mathcal{R}\zeta_1(G) = \mathcal{R}\zeta_1(G)\varphi = \mathcal{T}\zeta_1(G)$ and $\mathcal{R} \cap \gamma_2(G) = (\mathcal{R} \cap \gamma_2(G))\varphi = \mathcal{T} \cap \gamma_2(G)$. □

We now prove the following slight generalization (needed for algorithmic purposes) of Theorem 2.

Theorem 4.3. *Given the commutative diagram in Figure 1 which is exact and Ω-graded in all rows and all columns, the following hold.*

(i) If $\zeta_1(\hat{Q})r = 1$ then for every Remak Ω-decomposition $\hat{\mathcal{Q}}$ of $\hat{Q}$ and every Remak Ω-decomposition $\mathcal{R}$ of G, $\hat{\mathcal{Q}}r$ refines $\mathcal{R}q$.
(ii) If $\hat{N}j \leq \gamma_2(N)$ then for every Remak $(\Omega \cup G)$-decomposition $\mathcal{N}$ of N and every Remak Ω-decomposition $\mathcal{R}$ of G, $\mathcal{N}i \cap \hat{N}\hat{i}$ refines $\mathcal{R} \cap \left(\hat{N}\hat{i}\right)$.

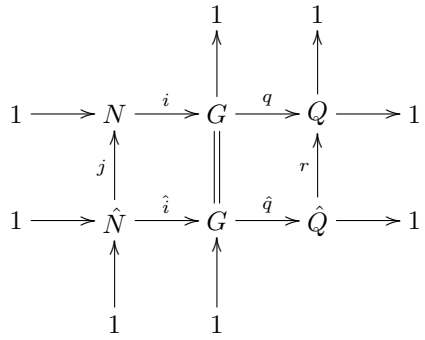

FIGURE 1. A commutative diagram of Ω-groups which is exact and Ω-graded in all rows and all columns.

Proof. Fix a Remak Ω-decomposition $\mathcal{R}$ of G.

As $\hat{N}$ and N are Ω-graded, $\mathcal{R}\hat{q}$ is a direct Ω-decompositions of $\hat{Q}$. Let $\hat{\mathcal{T}}$ be a Remak Ω-decomposition of $\hat{Q}$ which refines $\mathcal{R}\hat{q}$. By Lemma 4.2(i), $\hat{\mathcal{Q}}\zeta_1(\hat{Q}) = \hat{\mathcal{T}}\zeta_1(\hat{Q})$ and so $\hat{\mathcal{Q}}r = \mathcal{T}r$. Therefore, $\hat{\mathcal{Q}}r$ refines $\mathcal{R}\hat{q}r = \mathcal{R}q$. That proves (i).

To prove (ii), $\mathcal{R} \cap (Ni)$ is a direct $(\Omega \cup G)$-decompositions of Ni. Let $\mathcal{T}$ be a Remak $(\Omega \cup G)$-decomposition of Ni which refines $\mathcal{R} \cap (Ni)$. By Lemma 4.2(ii), $\mathcal{N} \cap (\hat{N}j) = (\mathcal{T}i^{-1}) \cap (\hat{N}j)$ so $(\mathcal{N}i) \cap (\hat{N}\hat{i}) = (\mathcal{N}i) \cap (\hat{N}ji) = \mathcal{T} \cap (\hat{N}ji) = \mathcal{T} \cap (\hat{N}\hat{i})$ which by choice of $\mathcal{T}$ also refines $\mathcal{R} \cap \left(\hat{N}\hat{i}\right)$. □

4.2. **Separated and refined decompositions.** In this section we begin our work to consider the extension, lifting, and matching problems in a constructive fashion. Throughout we fix a direct class $\mathfrak{X}$ (closed to isomorphisms, finite direct products and direct factors).

We will have several occasions to partition direct Ω-decompositions based on group classes. So if $\mathcal{H}$ is a direct Ω-decomposition of an Ω-group G then set

$$\mathcal{H} \cap \mathfrak{X} = \{H \in \mathcal{H} : H \in \mathfrak{X}\}, \text{ and} \tag{4.4}$$

$$\mathcal{H} - \mathfrak{X} = \mathcal{H} - (\mathcal{H} \cap \mathfrak{X}). \tag{4.5}$$

Definition 4.6. A direct Ω-decomposition $\mathcal{H}$ is $\mathfrak{X}$-*separated* if for each $H \in \mathcal{H} - \mathfrak{X}$, if H has a direct Ω-factor K, then $K \notin \mathfrak{X}$. If additionally every member of $\mathcal{H} \cap \mathfrak{X}$ is directly Ω-indecomposable, then $\mathcal{H}$ is $\mathfrak{X}$-*refined*.

Proposition 4.7. *Suppose that $\mathfrak{X}$ is a direct class of Ω-groups, that G is an Ω-group, and that $\mathcal{H}$ is a direct Ω-decomposition of G. The following hold.*

(i) $\langle \mathcal{H} \cap \mathfrak{X} \rangle \in \mathfrak{X}$.
(ii) If $\mathcal{H}$ is $\mathfrak{X}$-separated and $\mathcal{K}$ is a direct Ω-decomposition of G which refines $\mathcal{H}$, then $\mathcal{K}$ is $\mathfrak{X}$-separated.
(iii) $\mathcal{H}$ is a $\mathfrak{X}$-separated if, and only if, $\{\langle \mathcal{H} - \mathfrak{X} \rangle, \langle \mathcal{H} \cap \mathfrak{X} \rangle\}$ is $\mathfrak{X}$-separated.
(iv) Every Remak Ω-decomposition is $\mathfrak{X}$-refined.
(v) If $\mathcal{H}$ and $\mathcal{K}$ are $\mathfrak{X}$-separated direct Ω-decompositions of G then $(\mathcal{H} - \mathfrak{X}) \sqcup (\mathcal{K} \cap \mathfrak{X})$ is an $\mathfrak{X}$-separated direct Ω-decomposition of G.

Proof. First, (i) follows as $\mathfrak{X}$ is closed to direct Ω-products.

For (ii), notice that a direct Ω-factor of a $K \in \mathcal{K}$ is also a direct Ω-factor of the unique $H \in \mathcal{H}$ where $K \leq H$.

For (iii), the reverse direction follows from (ii). For the forward direction, let K be a direct Ω-factor of $\langle \mathcal{H} - \mathfrak{X} \rangle$. Because $\mathfrak{X}$ is closed to direct Ω-factors, if $K \in \mathfrak{X}$ then so is every directly Ω-indecomposable direct Ω-factor of K, and so we insist that K is directly Ω-indecomposable. Therefore K lies in a Remak Ω-decomposition of $\langle \mathcal{H} - \mathfrak{X} \rangle$. Let $\mathcal{R}$ be a Remak Ω-decomposition of $\langle \mathcal{H} - \mathfrak{X} \rangle$ which refines $\mathcal{H} - \mathfrak{X}$. By Theorem 1.1 there is a $\varphi \in \mathrm{Aut}_{\Omega \cup G} \langle \mathcal{H} - \mathfrak{X} \rangle$ such that $K\varphi \in \mathcal{R}$ and so $K\varphi$ is a direct Ω-factor of the unique $H \in \mathcal{H}$ where $K\varphi \leq H$. As $\mathcal{H}$ is $\mathfrak{X}$-separated and $K\varphi$ is a direct Ω-factor of $H \in \mathcal{H}$, it follows that $K\varphi \notin \mathfrak{X}$. Thus, $K \notin \mathfrak{X}$ and $\{\langle \mathcal{H} - \mathfrak{X} \rangle, \langle \mathcal{H} \cap \mathfrak{X} \rangle\}$ is $\mathfrak{X}$-separated.

For (iv), note that elements of a Remak Ω-decomposition have no proper direct Ω-factors.

Finally for (v), let $\mathcal{R}$ and $\mathcal{T}$ be a Remak Ω-decompositions of G which refine $\mathcal{H}$ and $\mathcal{K}$ respectively. Set $\mathcal{U} = \{R \in \mathcal{R} : R \leq \langle \mathcal{H} \cap \mathfrak{X} \rangle\}$. By Theorem 1.1 there is a $\varphi \in \mathrm{Aut}_{\Omega \cup G} G$ such that $\mathcal{U}\varphi \subseteq \mathcal{T}$ and $\mathcal{R}\varphi = (\mathcal{R} - \mathcal{U}) \sqcup \mathcal{U}\varphi$. As $\mathfrak{X}$ is closed to isomorphisms, it follows that $\mathcal{U}\varphi \subseteq \mathcal{T} \cap \mathfrak{X}$. As $\mathcal{H}$ is $\mathfrak{X}$-separated, $\mathcal{U} = \mathcal{R} \cap \mathfrak{X}$. As $\mathrm{Aut}_{\Omega \cup G} G$ is transitive on the set of all Remak Ω-decompositions of G (Theorem 1.1), we have that $|\mathcal{T} \cap \mathfrak{X}| = |\mathcal{R} \cap \mathfrak{X}| = |\mathcal{U}\varphi|$. In particular, $\mathcal{U}\varphi = \mathcal{T} \cap \mathfrak{X} = \{T \in \mathcal{T} : T \leq \langle \mathcal{K} \cap \mathfrak{X} \rangle\}$. Hence, $\mathcal{R}\varphi$ refines $(\mathcal{H} - \mathfrak{X}) \sqcup (\mathcal{K} \cap \mathfrak{X})$ and so the latter is a direct Ω-decomposition. □

4.3. **Proof of Theorem 3.** Recall we are to prove the following "local-global" property. Let $G \mapsto \mathfrak{X}(G)$ be an up Ω-grader for a direct class $\mathfrak{X}$ of Ω-groups and let G be an Ω-group. If H is an $(\Omega \cup G)$-subgroup of G and the following hold:

(a) for some direct Ω-factor R of G, $H\mathfrak{X}(G) = R\mathfrak{X}(G) > \mathfrak{X}(G)$, and
(b) H lies in an $\mathfrak{X}$-separated direct $(\Omega \cup G)$-decomposition (Definition 4.6) of $H\mathfrak{X}(G)$;

then H is a direct Ω-factor of G.

By (a) there is a direct $(\Omega \cup G)$-complement C in G to R. Also $\mathfrak{X}(G) = \mathfrak{X}(R) \times \mathfrak{X}(C)$, as $\mathfrak{X}(G)$ is Ω-graded. Hence, $R\mathfrak{X}(G) = R \times \mathfrak{X}(C)$. By (b), there is an $\mathfrak{X}$-separated direct Ω-decomposition $\mathcal{H}$ of $H\mathfrak{X}(G)$ such that $H \in \mathcal{H}$. As $H\mathfrak{X}(G) > \mathfrak{X}(G)$ it follows that $H \notin \mathfrak{X}$ and so by Lemma 3.3, $\mathcal{H} - \mathfrak{X} = \{H\}$ and $X = \langle \mathcal{H} \cap \mathfrak{X} \rangle \in \mathfrak{X}$. So

$$R \times \mathfrak{X}(C) = R\mathfrak{X}(G) = H\mathfrak{X}(G) = H \times X.$$

Let $\mathcal{K}$ be Remak $(\Omega \cup G)$-decomposition of R. Since $\mathfrak{X}(C) \in \mathfrak{X}$, $\mathcal{K} \sqcup \{\mathfrak{X}(C)\}$ is an $\mathfrak{X}$-separated direct $(\Omega \cup G)$-decomposition of $R\mathfrak{X}(G)$. By Proposition 4.7(v),

$$\mathcal{C} = \{H\} \sqcup \{\mathfrak{X}(C)\} \sqcup (\mathcal{K} \cap \mathfrak{X})$$

is an $\mathfrak{X}$-separated direct $(\Omega \cup G)$-decomposition of $R\mathfrak{X}(G)$, and we note that $\{H\} = \mathcal{C} - \mathfrak{X}$. We claim that $\{H, C\} \sqcup (\mathcal{K} \cup \mathfrak{X})$ is a direct Ω-decomposition of G. Indeed, $H \cap \langle C, \mathcal{K} \cap \mathfrak{X} \rangle \leq R\mathfrak{X}(G) \cap C\mathfrak{X}(G) = \mathfrak{X}(G)$ and so $H \cap \langle C, \mathcal{K} \cap \mathfrak{X} \rangle = H \cap \langle \mathfrak{X}(C), \mathcal{K} \cap \mathfrak{X} \rangle = 1$. Also, $\mathfrak{X}(C) \leq \langle H, C, \mathcal{K} \cap \mathfrak{X} \rangle$ thus $\langle H, C, \mathcal{K} \cap \mathfrak{X} \rangle = G$. As the members of $\{H, C\} \sqcup (\mathcal{K} \cap \mathfrak{X})$ are $(\Omega \cup G)$-subgroups we have proved the claim. In particular, H is a direct Ω-factor of G. □

5. Local-global properties of direct factors

This section explains how the property of being a direct factor is more local than it may seem. Initially we define a direct factor of a group G as a subgroup H which lies in a direct decomposition $\mathcal{H}$ of G. However, this definition is not of any immediate value since having a direct decomposition is more powerful than having a direct factor. However, we have seen in Section 4 that direct decompositions of quotients and subgroups can be used to constrain the possible location of direct factors. Thus, to find a direct factor we no longer need to think globally. The key results of this section are Theorems 4 and 5.

Throughout this section we assume that $(\mathfrak{X}, G \mapsto \mathfrak{X}(G))$ is an up Ω-grading pair in which $\zeta_1(G) \leq \mathfrak{X}(G)$.

5.1. **Direct chains.** In Theorem 2 (and more specifically Theorem 4.3) we specified conditions under which any direct decomposition of an appropriate subgroup, resp. quotient, led to a solution of the extension (resp. lifting) problem. However, within that theorem we see that it is not the direct decomposition of the subgroup (resp. quotient group) which can be extended (resp. lifted). Instead it a some unique refinement of the direct decomposition. Finding the correct refinement by trial and error is an exponentially sized problem. To avoid this we outline how an incremental greedy-type construction is sufficient. The algorithm itself is given in the subsequent paper.

Throughout this section we suppose that $G \mapsto \mathfrak{X}(G)$ is an (up) Ω-grader for a direct class $\mathfrak{X}$. Recall from Definition 1.7 that a *direct chain* is a proper chain

$$\mathfrak{X}(G) = C_0 < C_1 < \cdots < C_\ell = G$$

of $(\Omega \cup G)$-subgroups with *directions* a direct Ω-decomposition $\mathcal{R}$ of G with:

(i) for all $0 \leq i \leq \ell$, $C_i = \langle \mathcal{R} \cap C_i \rangle$, and
(ii) for each $0 \leq i < \ell$, there is a unique *direction* $R \in \mathcal{R}$ such that

$$R\mathfrak{X}(G) \cap C_i < R\mathfrak{X}(G) \cap C_{i+1}.$$

Notice, if $\{C_i : 0 \leq i \leq \ell\}$ is a direct chain with directions $\mathcal{R}$, then for all $0 \leq i \leq \ell$, $\mathcal{R} \cap C_i$ is a direct Ω-decomposition of C_i (Lemma 3.1). Also notice for all $R \in \mathcal{R}$, and any group $C \geq \mathfrak{X}(G)$, by the modular law

$$(R \cap C)\mathfrak{X}(G) = R\mathfrak{X}(G) \cap C.$$

Therefore if $\mathfrak{X}(G) \leq C < D \leq G$, $C = \langle \mathcal{R} \cap C \rangle$, $D = \langle \mathcal{R} \cap D \rangle$, and

$$(\forall R \in \mathcal{R} - \mathfrak{X}) \qquad R\mathfrak{X}(G) \cap C = R\mathfrak{X}(G) \cap D \tag{5.1}$$

then $C = \langle \mathcal{R} \cap C \rangle = \langle \mathcal{R} \cap C, \mathfrak{X}(G) \rangle = \langle \mathcal{R} \cap D, \mathfrak{X}(G) \rangle = \langle \mathcal{R} \cap D \rangle = D$. Therefore, it suffices to show there is at most one $R \in \mathcal{R} - \mathfrak{X}$ such that $R\mathfrak{X}(G) \cap C \neq R\mathfrak{X}(G) \cap D$.

Lemma 5.2. *Suppose that $\mathcal{H} = \mathcal{H}\mathfrak{X}(G)$ is an $(\Omega \cup G)$-decomposition of G such that $\mathcal{H}$ refines $\mathcal{R}\mathfrak{X}(G)$, for a direct Ω-decomposition $\mathcal{R}$. It follows that, if $L = \langle \mathcal{J}, \mathfrak{X}(G) \rangle$, for some $\mathcal{J} \subseteq \mathcal{H}$, then $L = \langle \mathcal{R} \cap L \rangle$.*

Proof. As $\mathfrak{X}(G) \leq L$, for each $R \in \mathcal{R}$, $R \cap \mathfrak{X}(G) \leq R \cap L$. As $\mathfrak{X}(G)$ is $(\Omega \cup G)$-graded, $\mathfrak{X}(G) = \langle \mathcal{R} \cap \mathfrak{X}(G) \rangle$. Thus, $\mathfrak{X}(G) \leq \langle \mathcal{R} \cap L \rangle$. Also, $\mathcal{H}$ refines $\mathcal{R}\mathfrak{X}(G)$. Thus, for each $J \in \mathcal{J} \subseteq \mathcal{H}$ there is a unique $R \in \mathcal{R} - \{R \in \mathcal{R} : R \leq \mathfrak{X}(G)\}$ such that $J \leq R\mathfrak{X}(G)$. As $L = \langle \mathcal{J}, \mathfrak{X}(G) \rangle$, $J \leq L$ and so $J \leq R\mathfrak{X}(G) \cap L = (R \cap L)\mathfrak{X}(G)$. Now $R \cap L, \mathfrak{X}(G) \leq \langle \mathcal{R} \cap L \rangle$ thus $J \leq \langle \mathcal{R} \cap L \rangle$. Hence $L = \langle \mathcal{J}, \mathfrak{X}(G) \rangle \leq \langle \mathcal{R} \cap L \rangle \leq L$. □

5.2. **Proof of Theorem 4.** Recall we must prove that if $\mathcal{H} = \mathcal{H}\mathfrak{X}(G)$ is an $(\Omega \cup G)$-decomposition of G and $\mathcal{R}$ is a direct Ω-decomposition of G such that $\mathcal{H}$ refines $\mathcal{R}\mathfrak{X}(G)$, then every maximal proper chain $\mathscr{C}$ of subsets of $\mathcal{H}$ induces a direct chain $\{\langle \mathcal{C}, \mathfrak{X}(G)\rangle : \mathcal{C} \in \mathscr{C}\}$.

Let $\mathscr{C} = \{\emptyset = \mathcal{J}_0 \subset \cdots \subset \mathcal{J}_\ell = \mathcal{H}\}$. Then $C_i = \langle \mathcal{J}_i, \mathfrak{X}(G)\rangle$ is a chain $\mathfrak{X}(G) < C_1 < \cdots < C_\ell = G$. By Lemma 5.2, $C_i = \langle \mathcal{R} \cap C_i\rangle$.

Next we show each C_i has a most one direction. Fix $0 \le i < \ell$ and let $H \in \mathcal{H}$ such that $C_{i+1} = HC_i$. By the definition of refinement there is a unique $R \in \mathcal{R}$ such that $H \le R\mathfrak{X}(G)$. Set $S = \langle \mathcal{R} - \{R\}\rangle$. By Lemma 5.2, $\mathcal{R} \cap C_{i+1}$ and $\mathcal{R} \cap C_i$ are direct $(\Omega \cup G)$-decompositions of C_{i+1} and C_i respectively. So $C_i = (R \cap C_i) \times (S \cap C_i)$ and as $\mathfrak{X}(G) \le C_i$, $C_i = (R\mathfrak{X}(G) \cap C_i)(S\mathfrak{X}(G) \cap C_i)$. Also, $\mathfrak{X}(G)$ is $(\Omega \cup G)$-graded; hence, $G/\mathfrak{X}(G) = R\mathfrak{X}(G)/\mathfrak{X}(G) \times S\mathfrak{X}(G)/\mathfrak{X}(G)$ in particular $S\mathfrak{X}(G) \cap R\mathfrak{X}(G) = \mathfrak{X}(G)$. From these equations and applying the modular law twice we find:

$$\begin{aligned} S\mathfrak{X}(G) \cap C_{i+1} = S\mathfrak{X}(G) \cap HC_i &= S\mathfrak{X}(G) \cap \Big(H(R\mathfrak{X}(G) \cap C_i) \cdot (S\mathfrak{X}(G) \cap C_i)\Big) \\ &= \Big(S\mathfrak{X}(G) \cap H(R\mathfrak{X}(G) \cap C_i)\Big)(S\mathfrak{X}(G) \cap C_i) \\ &= (S\mathfrak{X}(G) \cap R\mathfrak{X}(G) \cap HC_i)(S\mathfrak{X}(G) \cap C_i) \\ &= \mathfrak{X}(G)(S\mathfrak{X}(G) \cap C_i) = S\mathfrak{X}(G) \cap C_i. \end{aligned}$$

Thus, $\langle \mathcal{R} - \{R\}\rangle\mathfrak{X}(G) \cap C_{i+1} = S\mathfrak{X}(G) \cap C_i$. Hence, the direction of C_i cannot lie in $\mathcal{R} - \{R\}$ and so C_i has at most one direction and so by (5.1) C_i has a unique direction and so $\mathscr{C}$ is a direct chain. □

5.3. **Proof of Theorem 5.** Recall we must prove that if $\mathfrak{X}(G) = C_0 < \cdots < C_\ell = G$ is a direct chain with directions $\mathcal{R}$, then for $0 \le i < \ell$, and $R \in \mathcal{R}$ the direction of C_i, then for every $\mathfrak{X}$-separated direct $(\Omega \cup G)$-decomposition $\mathcal{K}$ of C_i such that $\mathcal{K}\mathfrak{X}(G)$ refines $\mathcal{R}\mathfrak{X}(G) \cap C_i$, it follows that

$$\big\{K \in \mathcal{K} - \mathfrak{X} : K \le \langle \mathcal{R} - \{R\}\rangle\mathfrak{X}(G)\big\}$$

lies in an $\mathfrak{X}$-separated direct $(\Omega \cup G)$-decomposition of C_{i+1}.

Set $S = \langle \mathcal{R} - \{R\}\rangle$. As $\mathcal{K}\mathfrak{X}(G)$ refines $\mathcal{R}\mathfrak{X}(G) \cap C_i$, it also refines $\{R\mathfrak{X}(G) \cap C_i, S\mathfrak{X}(G) \cap C_i\}$ and so

$$S\mathfrak{X}(G) \cap C_i = \langle K \in \mathcal{K}, K \le S\mathfrak{X}(G)\rangle = \langle K \in \mathcal{K} - \mathfrak{X}, K \le S\mathfrak{X}(G)\rangle\mathfrak{X}(G).$$

Since $\mathcal{K}$ is $\mathfrak{X}$-separated $F = \langle K \in \mathcal{K} - \mathfrak{X}, K \le S\mathfrak{X}(G)\rangle$ has no direct $(\Omega \cup G)$-factor in $\mathfrak{X}$. Also, as the direction of C_i is R, $S\mathfrak{X}(G) \cap C_{i+1} = S\mathfrak{X}(G) \cap C_i$ and so

$$\begin{aligned} (S \cap C_{i+1})\mathfrak{X}(G) &= S\mathfrak{X}(G) \cap C_{i+1} \\ &= S\mathfrak{X}(G) \cap C_i \\ &= \langle K \in \mathcal{K} - \mathfrak{X}, K \le S\mathfrak{X}(G)\rangle\mathfrak{X}(G) \\ &= F \times \langle \mathcal{K} \cap \mathfrak{X}\rangle. \end{aligned}$$

Using $(C_{i+1}, F, S \cap C_{i+1})$ in the role of (G, H, R) in Theorem 3, it follows that F is a direct $(\Omega \cup G)$-factor of C_{i+1}. In particular, $\{K \in \mathcal{K} - \mathfrak{X}, K \le S\mathfrak{X}(G)\}$ lies in a direct $(\Omega \cup G)$-decomposition of C_{i+1}. □

6. Base cases

This section handles the bases cases left after recursively applying Theorem 2. This includes characteristically simple groups and groups with a 2-step graded chief series. Of these the challenging case is the class of p-groups of nilpotence class 2. For those groups we introduce bimaps, i.e. bilinear maps, and a commutative ring as a means to access direct decompositions of a p-group of class 2. As commutative rings have a unique Remak decomposition, and a decomposable p-group will have many Remak decompositions, we might expect such a method to have lost vital information. However, in view of results such as Theorem 2 we recognize that in fact what we will have constructed leads us to a matching for the extension $1 \to \zeta_1(G) \to G \to G/\zeta_1(G) \to 1$.

6.1. **Proof of Theorem 6.** Fix a finite characteristically simple Ω-group G. Then G is direct product of isomorphic simple groups [R3, (3.3.15)]. Hence, if G is abelian then G is an elementary abelian p-group for some prime p. Furthermore, the Remak Ω-decompositions of G correspond to sets $\mathcal{E} \subset \mathrm{End}_{(\mathbb{Z}/p\mathbb{Z})[\Omega]}(G)$ of pairwise orthogonal primitive idempotents that sum to 1 [R3, (3.3.3)]. So suppose instead that G is nonabelian. Then the set of minimal normal Ω-subgroups of G is the Remak Ω-decomposition of G [R3, (3.3.16)]. □

6.2. **Proof of Theorem 7.** For (i), assume $\zeta_1(G) = 1$. The set $\mathcal{M}$ of minimal $(\Omega \cup G)$-subgroups is a direct $(\Omega \cup G)$-decomposition of the socle of G and furthermore there is a unique partition of $\mathcal{M}$ which extends to the Remak Ω-decomposition of G.

For (ii), let $\gamma_2(G) = G$. It follows $\gamma_2(G/CR(G)) = G/CR(G)$. If $\mathcal{R}$ is a Remak Ω-decomposition of G then $\mathcal{R}CR(G)/CR(G)$ is a direct Ω-decomposition of $G/CR(G)$. Since $G/CR(G)$ is perfect it has a unique Remak Ω-decomposition $\mathcal{Q}$ and so $\mathcal{Q}$ refines $\mathcal{R}CR(G)/CR(G)$. In other words, $\mathcal{Q}$ lifts to $\mathcal{R}$. □

6.3. **Products of p-groups as products of bimaps.** We now consider the categorical direct product of bimaps up to homotopism. This is relevant because the functor $G \mapsto \mathsf{Bi}(G)$ embeds groups up to isomorphism into the isotopism category; cf. Section 2.5.

Definition 6.1. Let $\mathcal{B}$ be a family of Ω-bimaps $B : U_B \times V_B \to W_B$, $B \in \mathcal{B}$. Define $\oplus\mathcal{B} = \bigoplus_{B\in\mathcal{B}} B$ as the Ω-bimap $\bigoplus_{B\in\mathcal{B}} U_B \times \bigoplus_{B\in\mathcal{B}} V_B \to \bigoplus_{B\in\mathcal{B}} W_B$ where:

$$(u_B : B \in \mathcal{B})\,(\oplus\mathcal{B})\,(v_B : B \in \mathcal{B}) = (u_B B v_B : B \in \mathcal{B})$$

for all $(u_B : B \in \mathcal{B}) \in \bigoplus_{B\in\mathcal{B}} U_B$ and all $(v_B : B \in \mathcal{B}) \in \bigoplus_{B\in\mathcal{B}} V_B$.

Lemma 6.2. *If $B : U \times V \to W$ is an Ω-bimap, $\mathcal{C}$ a finite set of submaps of B such that*
(a) $\{X_C : C : X_C \times Y_C \to Z_C \in \mathcal{C}\}$ is a direct Ω-decomposition of U,
(b) $\{Y_C : C : X_C \times Y_C \to Z_C \in \mathcal{C}\}$ is a direct Ω-decomposition of V,
(c) $\{Z_C : C : X_C \times Y_C \to Z_C \in \mathcal{C}\}$ is a direct Ω-decomposition of W, and
(d) $X_C B Y_D = 0$ for distinct $C, D \in \mathcal{C}$;
then $B = \bigoplus \mathcal{C}$.

Proof. By (a), we may write each $u \in U$ as $u = (u_C)_{C\in\mathcal{C}}$ with $u_C \in X_C$, for all $C : X_C \times X_C \to Z_C \in \mathcal{C}$. Likewise with $v \in V$. By (d) followed by (c) we have that $uBv = \sum_{C,D\in\mathcal{C}} (u_C)B(v_D) = \sum_{C\in\mathcal{C}} (u_C)C(v_C) = (\oplus\mathcal{C})\,(u, v)$. □

Definition 6.3. A *direct Ω-decomposition* of an Ω-bimap $B : U \times V \to W$ is a set $\mathcal{B}$ of submaps of B satisfying the hypothesis of Lemma 6.2. Call B directly Ω-indecomposable if its only direct Ω-decomposition is $\{B\}$. A Remak Ω-decomposition of B is an Ω-decompositions whose members are directly Ω-indecomposable.

Recall from Section 2.5 that $\mathsf{Bi}(G)$ associates a bimap to a group. We now assign subgroups in a corresponding way. Given $H \leq G$ we define $U = H\zeta_1(G)/\zeta_1(G) \leq V$, $Z = H \cap \gamma_2(G) \leq W$, and $C := \mathsf{Bi}(H; G) : U \times U \to Z$ where

$$(\forall u, v \in U) \qquad uCv = uBv. \tag{6.4}$$

Proposition 6.5. *If G is a Ω-group and $\gamma_2(G) \leq \zeta_1(G)$, then every direct Ω-decomposition $\mathcal{H}$ of G induces a direct Ω-decomposition*

$$\mathsf{Bi}(\mathcal{H}) = \{\mathsf{Bi}(H; G) : H \in \mathcal{H}\}.$$

If $\mathsf{Bi}(G)$ is directly Ω-indecomposable and $\zeta_1(G) \leq \Phi(G)$, then G is directly Ω-indecomposable.

Proof. Set $B := \mathsf{Bi}(G)$. By Lemma 3.1 and Proposition 3.6, $\mathcal{H}\zeta_1(G)/\zeta_1(G)$ is a direct Ω-decomposition of $V = G/\zeta_1(G)$ and $\mathcal{H} \cap \gamma_2(G)$ is a direct Ω-decomposition of $W = \gamma_2(G)$. Furthermore, for each $H \in \mathcal{H}$,

$$(H\zeta_1(G)/\zeta_1(G))B(\langle \mathcal{H} - \{H\}\rangle\zeta_1(G)/\zeta_1(G)) = [H, \langle \mathcal{H} - \{H\}\rangle] = 0 \in W.$$

In particular, $\mathsf{Bi}(\mathcal{H})$ is a direct Ω-decomposition of B.

Finally, if $\mathsf{Bi}(P)$ is directly indecomposable then $|\mathsf{Bi}(\mathcal{H})| = 1$. Thus, $\mathcal{H}\zeta_1(G) = \{G\}$. Therefore $\mathcal{H}$ has exactly one non-abelian member. Take $Z \in \mathcal{H} \cap \mathfrak{A}$. As Z is abelian, $Z \leq \zeta_1(G)$. If $\zeta_1(G) \leq \Phi(G)$ then the elements of G are non-generators. In particular, $G = \langle \mathcal{H} \rangle = \langle \mathcal{H} - \{Z\}\rangle$. But by definition no proper subset of a decomposition generates the group. So $\mathcal{H} \cap \mathfrak{A} = \emptyset$. Thus, $\mathcal{H} = \{G\}$ and G is directly Ω-indecomposable. □

Corollary 6.6. *If G is a p-group with $G^p = 1$ and $\gamma_2(G) \leq \zeta_1(G)$ then G is directly Ω-indecomposable if, and only if, $\mathsf{Bi}(G)$ is directly Ω-indecomposable and $\zeta_1(G) \leq \Phi(G)$.*

Proof. The reverse directions is Proposition 6.5. We focus on the forward direction. As $G^p = 1$ it follows that $G \cong \mathsf{Grp}(\mathsf{Bi}(G)) =: \hat{G}$. Set $B := \mathsf{Bi}(G)$. Let $\mathcal{B}$ be a direct Ω-decomposition of B. For each $C : X_C \times X_C \to Z_C \in \mathcal{B}$, define $\mathsf{Grp}(C; B) = X_C \times Z_C \leq V \times W$. We claim that $\mathsf{Grp}(C; B)$ is an Ω-subgroup of $\mathsf{Grp}(B)$. In particular, $(0, 0) \in \mathsf{Grp}(C; B)$ and for all $(x, w), (y, w') \in \mathsf{Grp}(C; B)$,

$$\begin{aligned}(x, w) * (y, w')^{-1} &= (x, w) * (-y, -w') \\ &= \left(x - y, w - \frac{1}{2}xBy - w'\right) \in X_C \times Z_C = \mathsf{Grp}(C; B).\end{aligned}$$

Furthermore,

$$\left[\mathsf{Grp}(C; B), \mathsf{Grp}\left(\sum_{D \in \mathcal{C} - \{C\}} D; B\right)\right] = \left(0, X_C B\left(\sum_{D \in \mathcal{C} - \{C\}} X_D\right)\right) = (0, 0).$$

Combined with $\mathsf{Grp}(B) = \langle \mathsf{Grp}(C;B) : C \in \mathcal{C} \rangle$ it follows that $\mathsf{Grp}(C;B)$ is an $(\Omega \cup G)$-subgroup $\mathsf{Grp}(B)$ which commutes with $\mathsf{Grp}\left(\sum_{D\in\mathcal{C}-\{C\}} D; B\right)$. Finally,

$$\mathsf{Grp}(C;B) \cap \mathsf{Grp}\left(\sum_{D\in\mathcal{C}-\{C\}} D; B\right) = (X_C \times Z_C) \cap \left(\sum_{D\in\mathcal{C}-\{C\}} X_D\right) \times \left(\sum_{D\in\mathcal{C}-\{C\}} Z_D\right)$$
$$= 0 \times 0.$$

Thus, $\mathcal{H} = \{\mathsf{Grp}(C;B) : C \in \mathcal{C}\}$ is a direct Ω-decomposition of $\mathsf{Grp}(B)$. As G is directly Ω-indecomposable it follows that $\mathcal{H} = \{G\}$ and so $\mathcal{C} = \{B\}$. Thus, B is directly Ω-indecomposable. □

6.4. **Centroids of bimaps.** In this section we replicate the classic interplay of idempotents of a ring and direct decompositions of an algebraic object, but now for context of bimaps. This parallels the role of Jordan algebras in the study of central products; cf. [W4]. The relevant ring is the centroid, defined similar to centroid of a nonassociative ring [J, Section X.1]. As with nonassociative rings, the idempotents of the centroid of a bimap correspond to direct decompositions. Myasnikov [M2] may have been the first to generalize such methods to certain bimaps.

Definition 6.7. The *centroid* of an Ω-bimap $B : U \times V \to W$ is

$$C_\Omega(B) = \{(f,g;h) \in \mathrm{End}_\Omega U \times \mathrm{End}_\Omega V \times \mathrm{End}_\Omega W :$$
$$\forall u \in U, \forall v \in V,\ (uf)Bv = (uBv)h = uB(vg)\}.$$

If $\Omega = \emptyset$ then write $C(B)$.

Lemma 6.8. *Let $B : U \times V \to W$ be an Ω-bimap. Then the following hold.*

(i) $C_\Omega(B)$ is a subring of $\mathrm{End}_\Omega U \times \mathrm{End}_\Omega V \times \mathrm{End}_\Omega W$, and B is a $C_\Omega(B)$-bimap.
(ii) If B is K-bimap for a ring K, then there is a unique ring homomorphism $K \to C(B)$ such that the action of K on $U \times V \times W$ is that of $C(B)$.
(iii) If B is nondegenerate and $W = UBV$ then $C_\Omega(B) = C(B)$ and $C(B)$ is commutative. Furthermore, for each $X \in \{U, V, W\}$, the restriction of $C(B)$ to $End_K X$ is faithful.
(iv) If $U = V$, $W = VBV$, $B = \pm B^t$, and B is nondegenerate then for all $(f,g;h) \in C(B)$, $f = g$.

Proof. Part (i) is immediate. For (ii), for each $X \in \{U,V,W\}$ let $\rho_X : K \to \mathrm{End}\, X$ be the representation of the action of K on X. It follows that $\rho := (\rho_U, \rho_V; \rho_W) : K \to \mathrm{End}\, U \times \mathrm{End}\, V \times \mathrm{End}\, W$ and by the assumption that B is a K-bimap, $K\rho \subseteq C(B)$.

For part (iii), fix $s \in \Omega$ and $(f,g;h) \in C(B)$. It follows that for all $u, v \in V$,

$$(u(sf))Bv = (us)B(vf) = (uB(vf))s = ((uf)Bv)s = (u(fs))Bv.$$

Thus, $u(sf - fs) \in V^\top = 0$, so $f \in \mathrm{End}_\Omega U$. In a similar fashion, $g \in \mathrm{End}_\Omega V$ and $h \in \mathrm{End}_\Omega W$. Hence, $C(B) \subseteq C_\Omega(B) \subseteq C(B)$. Using a similar shuffling game, if $(f,g;h), (f',g';h') \in C(B)$ then $(u(ff'))Bv = uB(vff') = (u(f'f))Bv$. By the nondegenerate assumption we get that $ff' = f'f$ and likewise $gg' = g'g$. Finally, if $(f,g;h), (f',g;h) \in C(B)$ then for all $u \in U$ and all $v \in V$, $ufBv = uB(vg) = uf'Bv$ and so $f = f'$.

To prove (iv), suppose $B = \pm B^t$ is nondegenerate. For every $(f, g; h) \in C(B)$ and every $u, v \in V$,

$$(ug)Bv = \pm vB(ug) = \pm(vf)Bu = uB(vf).$$

Furthermore, $(ug)Bv = \pm vB(ug) = (\pm vBu)h = (uBv)h$. So $(g, f; h) \in C(B)$. As $W = VBV$, the restriction of $C(B)$ to $\mathrm{End}_\Omega W$ is faithful. So $(f, g; h) = (g, f; h)$. This proves (iv). □

We now extend the Fitting-type interplay of idempotents and direct decompositions to the context of bimaps and then to p-groups of class 2. This allows us to prove Theorem 8. This section follows the notation described in Subsection 2.3. Note if X is a direct factor in a direct decomposition of a module U then we write $e(X)$ for the projection idempotent.

Lemma 6.9. *Let $B : U \times V \times V \to W$ be an Ω-bimap.*

(i) A set $\mathcal{B}$ of Ω-submaps of B is a direct Ω-decomposition of B if, and only if,

$$\mathcal{E}(\mathcal{B}) = \{(e(U_C), e(V_C), e(W_C)) : C : U_C \times V_C \to W_C \in \mathcal{B}\}.$$

is a set of pairwise orthogonal idempotents of $C_\Omega(B)$ which sum to 1.

(ii) $\mathcal{B}$ is a Remak Ω-decomposition of B if, and only if, $\mathcal{E}(\mathcal{B})$ is a frame.

(iii) If B is nondegenerate and $W = VBV$, then B has a unique Remak Ω-decomposition of B.

Proof. For (i), by Definition 6.3, $\{U_B : B \in \mathcal{B}\}$, $\{V_B : B \in \mathcal{B}\}$, and $\{W_B : B \in \mathcal{B}\}$ are direct Ω-decompositions of U, V, and W respectively. Thus, $\mathcal{E}(\mathcal{B})$ is a set of pairwise orthogonal idempotents which sum to 1.

Let $(e, f; g) \in \mathcal{E}(\mathcal{X})$. As $1 - e = \sum_{(e', f; g'') \in \mathcal{E}(\mathcal{B}) - \{(e,f;g)\}} e'$ it follows that for all $u \in U$ and all $v \in V$ we have $(ue)B(v(1 - f)) \in (Ue)B(V(1 - f)) = 0$ by the assumptions on $\mathcal{B}$. Also, $(ue)B(vf) \in Wg$. Together we have:

$$\begin{aligned}
&(ue)Bv = (ue)B(vf) + (ue)B(v(1 - f)) = (ue)B(vf),\\
&uB(vf) = u(1 - e))B(vf) + (ue)B(vf) = (ue)B(vf), \text{ and}\\
&(uBv)g = \left(\sum_{(e', f'; g') \in \mathcal{E}(\mathcal{B})} (ue'Bvf')g' \right) g = ((ue)B(vf))g = (ue)B(vf).
\end{aligned}$$

Thus $(ue)Bv = (uBv)g = uB(vf)$ which proves $(e, f; g) \in C_\Omega(B)$; hence, $\mathcal{E}(\mathcal{B}) \subseteq C_\Omega(B)$.

Now suppose that $\mathcal{E}$ is a set of pairwise orthogonal idempotents of $C_\Omega(B)$ which sum to 1. It follows that $\{Ue : (e, f; g) \in \mathcal{E}\}$ is a direct Ω-decomposition of U, $\{Ve : (e, f; g) \in \mathcal{E}\}$ is a direct Ω-decomposition of V and $\{Wg : (e, f; g) \in \mathcal{E}\}$ is a direct Ω-decomposition of W. For distinct $(e, f; g), (e', f'; g') \in \mathcal{E}$, $(ue)B(vf') = (uee')Bv = 0$. Thus, $\{B|_{(e,f;g)} : Ue \times Ve \to Wg : (e, f; g) \in \mathcal{E}\}$ is a direct Ω-decomposition of $C(B)$.

Now (ii) follows. For (iii), we know by Lemma 6.8(ii) that $C(B) = C_\Omega(B)$ is commutative Artinian. The rest follows from Lemma 2.11(iv). □

6.5. **Proof of Theorem 8.** Suppose that G is a p-group and $\gamma_2(G) \leq \zeta_1(G)$. We must show there is a unique frame $\mathcal{E}$ in $C(\mathsf{Bi}(G))$, which follows from Lemma 6.9

and that if $\gamma_2(G) = \zeta_1(G)$ then every Remak Ω-decomposition $\mathcal{H}$ of G matches $(\mathcal{N}, \mathcal{Q})$ where

$$\mathcal{N} := \{W\hat{e} : (e, e; \hat{e}) \in \mathcal{E}\},$$
$$\mathcal{Q} := \{Ve : (e, e; \hat{e}) \in \mathcal{E}\}.$$

That is the content of Proposition 6.5, Lemma 6.9, and Corollary 6.6. Furthermore, if $G^p = 1$ and $\mathcal{R}$ is a Remak Ω-decomposition of G then $\mathcal{N} = \mathcal{R} \cap \gamma_2(G)$ and $\mathcal{R}\gamma_2(G)/\gamma_2(G) = \mathcal{Q}$. Therefore G is indecomposable if $\mathsf{Bi}(G)$ is indecomposable. □

7. Open problems

There are few open problems I wish to mention. To begin with, the "Krull-Schmidt" theorem reveals the presence of a matroid $\mathcal{D}(G)$ of a finite group G; cf. Section 1.1. This matroid is well-known for elementary abelian groups as it is a projective geometry [O2, Section 6.1]. For the general case of nonabelian groups some investigation can be found in [D1, Chapter 2]. Indeed, in that work it is remarked that the nonabelian case is likely to be difficult [D1, p. 85]. This is perhaps still true; however, we have demonstrated in Theorems 3–5 that the exchange and transitivity properties can be tamed considerably by moving through graded series were the lattices involved are isomorphic to power sets instead of the complicated modular lattices of all normal subgroups. We can only speculate that this will be useful to others. We would like to know what combinatorial structure is represented in the matroids $\mathcal{D}(G)$. So we ask:

Problem 1. *Characterize the matroids $\mathcal{D}(G)$.*

Next, we have examples of subgroups that are fully invariant graded subgroups such as $\gamma_2(G)$, and of characteristic but not fully invariant graded subgroups, e.g. $\zeta_1(G)$. It is possible to have a graded non-characteristic subgroup. E.g. if a group has no center or is perfect then the proper nontrivial direct factors are graded trivially (there is only one Remak decomposition of the group), but these direct factors need not be characteristic. We also know of normal subgroups that are not graded, e.g. noncyclic elementary abelian groups have no proper nontrivial graded subgroups. However, the reach the results in Section 3 has made it difficult to describe a characteristic subgroup that is not graded, so we ask:

Problem 2. *Describe a characteristic subgroup that is not graded.*

Thirdly we ask for an improved understanding of matches. Fix a group G and a proper nontrivial graded subgroup N. For a pair $(\mathcal{N}, \mathcal{Q})$ of direct decompositions of $(N, G/N)$, we say a direct decomposition $\mathcal{H}$ is a *perfect match* if $\mathcal{N} = \mathcal{H} \cap N$ and $\mathcal{Q} = \mathcal{H}N/N$. In our work we have demonstrated one case of perfect matchings, the case when G is a p-group with $G^p = 1$ and $\gamma_2(G) = \zeta_1(G)$. So whereas instances of lifts, extensions, and matches give sufficient conditions to prove indecomposability, perfect matches allow us to identify necessary conditions as well, and this would be very desirable.

Problem 3. *Describe more general situations with perfect matchings.*

One possible approach to answer Problem 3 is to generalize Theorem 8. Specifically work with a variety $\mathfrak{V} = \mathfrak{V}(w)$ of groups and consider matchings of Ω-groups G where $w(G) \leq w^*(G)$. The role played by the bilinear maps of p-groups of class

2 is therefore replaced with the general word-map $w : (G/w^*(G))^{\mathtt{X}} \to w(G)$. If $w(G) \leq w^*(G)$ it may be possible to introduce a centroid-type object for w which also has a unique frame. As a consequence, the split stem groups in the isologism class (i.e. groups where $w(G) = w^*(G)$ splits in G) have perfect matches.

Finally we have a question concerning verbal and marginal subgroups which hints at our algorithmic goals of the next note. Word-maps are easy to evaluate and so they provide a mechanism by which we might begin to construct verbal and marginal subgroups. For example, to compute generators of the commutator subgroup we may use commutators of generators and then produce the normal closure. This works because of Hall's commutator collection formulas:

$$[xy, z] = [x, z]^y[y, z] \qquad\qquad [x, yz] = [x, z][x, y]^z.$$

This seems unlikely of most words. We suggests a notion of a "collectible word" to mean a word $w \in F(x_1, \ldots, x_\ell)$ such that for each i and each k, there is decomposition

$$w(x_1, \ldots, x_i x_k, \ldots, x_\ell) = \prod_f w(x_{f_1}, \ldots, x_{f_\ell})^{v_f} \qquad (v_f \in F(x_1, \ldots, x_\ell)).$$

We suspect collectible words are rare and related to commutators – this may even be well-known by different names. If not, then there are characteristic and fully invariant subgroups and isologism classes that might be more useful in decomposing groups and have no relationship to centers and commutators.

Problem 4. *Are the collectible words generalized commutators?*

Acknowledgments

I thank W. M. Kantor who offered a tireless sounding board and helpful critiques. Also thanks to E. M. Luks, C.R.B. Wright, and Á. Seress for encouragement and many helpful remarks. Thanks to A. Hulpke for help with translations and to P. M. Neumann for historical assistence. Finally I thank the referee whose attention to the material in earlier versions has been immensely useful, and thanks to Karie.

References

[A] S. A. Ašmanov, *Verbal subgroups of complete direct products of groups*, Uspehi Mat. Nauk **25** (1970), no. 3(153), 259–260 (Russian). MR 0294462 (45 #3532)

[B] Reinhold Baer, *Groups with abelian central quotient group*, Trans. Amer. Math. Soc. **44** (1938), no. 3, 357–386, DOI 10.2307/1989886. MR 1501972

[BNV] Simon R. Blackburn, Peter M. Neumann, and Geetha Venkataraman, *Enumeration of finite groups*, Cambridge Tracts in Mathematics, vol. 173, Cambridge University Press, Cambridge, 2007. MR **2382539 (2009c:**20041)

[B] W. Burnside, *Theory of groups of finite order*, Dover Publications Inc., New York, 1955. 2d ed. MR 0069818 (16,1086c)

[CR] Charles W. Curtis and Irving Reiner, *Methods of representation theory. Vol. I*, John Wiley & Sons Inc., New York, 1981. With applications to finite groups and orders; Pure and Applied Mathematics; A Wiley-Interscience Publication. MR **632548 (82i:**20001)

[DH] Klaus Doerk and Trevor Hawkes, *Finite soluble groups*, de Gruyter Expositions in Mathematics, vol. 4, Walter de Gruyter & Co., Berlin, 1992. MR **1169099 (93k:**20033)

[D1] Arne Dür, *Möbius functions, incidence algebras and power series representations*, Lecture Notes in Mathematics, vol. 1202, Springer-Verlag, Berlin, 1986. MR **857100 (88m:**05005)

[D2] Walther Dyck, *Gruppentheoretische Studien. II. Ueber die Zusammensetzung einer Gruppe discreter Operationen, über ihre Primitivität und Transitivität*, Math. Ann. **22** (1883), no. 1, 70–108, DOI 10.1007/BF01443244 (German). MR 1510217

[F] Hans Fitting, *Über die direkten Produktzerlegungen einer Gruppe in direkt unzerlegbare Faktoren*, Math. Z. **39** (1935), no. 1, 16–30, DOI 10.1007/BF01201342 (German). MR 1545486

[H1] P. Hall, *Verbal and marginal subgroups*, J. Reine Angew. Math. **182** (1940), 156–157. MR 0002876 (2,125i)

[H2] Otto Hölder, *Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4*, Math. Ann. **43** (1893), no. 2-3, 301–412, DOI 10.1007/BF01443651 (German). MR 1510814

[J] Nathan Jacobson, *Lie algebras*, Interscience Tracts in Pure and Applied Mathematics, No. 10, Interscience Publishers (a division of John Wiley & Sons), New York-London, 1962. MR 0143793 (26 #1345)

[K1] W. Krull, *Über verallgemeinerte endliche Abelsche Gruppen*, Math. Z. **23** (1925), no. 1, 161–196, DOI 10.1007/BF01506226 (German). MR 1544736

[K2] A. G. Kurosh, *The theory of groups*, Chelsea Publishing Co., New York, 1960. Translated from the Russian and edited by K. A. Hirsch. 2nd English ed. 2 volumes. MR 0109842 (22 #727)

[MW] J. H. Maclagan-Wedderburn, *On the direct product in the theory of finite groups*, Ann. of Math. (2) **10** (1909), no. 4, 173–176, DOI 10.2307/1967406. MR 1502387

[M1] G. A. Miller, *On the groups which are the direct products of two subgroups*, Trans. Amer. Math. Soc. **1** (1900), no. 1, 66–71, DOI 10.2307/1986404. MR 1500525

[M2] A. G. Myasnikov, *Definable invariants of bilinear mappings*, Sibirsk. Mat. Zh. **31** (1990), no. 1, 104–115, 220, DOI 10.1007/BF00971153 (Russian); English transl., Siberian Math. J. **31** (1990), no. 1, 89–99. MR **1046815 (91i:**03074)

[N] Hanna Neumann, *Varieties of groups*, Springer-Verlag New York, Inc., New York, 1967. MR 0215899 (35 #6734)

[O1] Oystein Ore, *On the foundation of abstract algebra. I*, Ann. of Math. (2) **36** (1935), no. 2, 406–437, DOI 10.2307/1968580. MR 1503232

[O2] James G. Oxley, *Matroid theory*, Oxford Science Publications, The Clarendon Press Oxford University Press, New York, 1992. MR **1207587 (94d:**05033)

[R1] R. Remark, *Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren.*, J. f ur Math. (1911), 293–308 (German).

[R2] Derek J. S. Robinson, *Recent results on finite complete groups*, Algebra, Carbondale 1980 (Proc. Conf., Southern Illinois Univ., Carbondale, Ill., 1980), Lecture Notes in Math., vol. 848, Springer, Berlin, 1981, pp. 178–185. MR **613185 (82j:**20045)

[R3] ———, *A course in the theory of groups*, Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1993. MR **1261639 (94m:**20001)

[R4] Joseph J. Rotman, *An introduction to the theory of groups*, 4th ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995. MR **1307623 (95m:**20001)

[S1] I. Schur. Jahrbuch database JFM 40.0192.02, available through Zentrallblat.

[S2] ———. Jahrbuch database JFM 42.0156.01, available through Zentrallblat.

[S3] O. Schmidt, *Sur les produits directs*, Bull. Soc. Math. France **41** (1913), 161–164 (French). MR 1504707

[W1] G. E. Wall, *Some applications of the Eulerian functions of a finite group*, J. Austral. Math. Soc. **2** (1961/1962), 35–59. MR 0125156 (23 #A2461)

[W2] Robert B. Warfield Jr., *Nilpotent groups*, Lecture Notes in Mathematics, Vol. 513, Springer-Verlag, Berlin, 1976. MR 0409661 (53 #13413)

[W3] James B. Wilson, *Group decompositions, Jordan algebras, and algorithms for p-groups*, ProQuest LLC, Ann Arbor, MI, 2008. Thesis (Ph.D.)–University of Oregon. MR 2712085

[W4] ———, *Decomposing p-groups via Jordan algebras*, J. Algebra **322** (2009), no. 8, 2642–2679, DOI 10.1016/j.jalgebra.2009.07.029. MR **2559855 (2010i:**20016)

[W5] ———, *Finding central decompositions of p-groups*, J. Group Theory **12** (2009), no. 6, 813–830, DOI 10.1515/JGT.2009.015. MR **2582050 (2011a:**20044)

[W6] ———, *Division, adjoints, and dualities of bilinear maps*, Comm. Alge. in press.

Department of Mathematics, Colorado State University, Fort Collins, CO 80523
E-mail address: jwilson@math.colostate.edu