On O-Basis Groups and Generalizations

Except where reference is made to the work of others, the work described in this dissertation is my own or was done in collaboration with my advisory committee. This dissertation does not include proprietary or classified information.

_____

Jason Ervin

Certificate of Approval:

_____	_____
Gary Gruenhage Professor Mathematics and Statistics	Randall Holmes, Chair Professor Mathematics and Statistics
_____	_____
Huajun Huang Assistant Professor Mathematics and Statistics	Joe F. Pittman Interim Dean Graduate School

On O-Basis Groups and Generalizations

Jason Ervin

A Dissertation

Submitted to

the Graduate Faculty of

Auburn University

in Partial Fulfillment of the

Requirements for the

Degree of

Doctor of Philosophy

Auburn, Alabama
August 4, 2007

On O-Basis Groups and Generalizations

Jason Ervin

_____

Signature of Author

_____

Date of Graduation

Dissertation Abstract

On O-Basis Groups and Generalizations

Jason Ervin

Doctor of Philosophy, August 4, 2007
(M.S., Mississippi State University, 2002)
(B.S., Mississippi State University, 2000)
(B.S., Mississippi State University, 2000)
(A.A., Mississippi Delta Community College, 1998)

79 Typed Pages

Directed by Randall Holmes

A class of finite groups which we call o-basis groups is generalized and explored. One reason for interest in these groups lies with the concept's origins. The notion of o-basis group arose from the study of the existence, in the n-fold tensor product of a complex inner product space, of an orthogonal basis consisting entirely of "standard symmetrized tensors". We call such a basis an o-basis. The term "symmetrized" refers to the action on the tensor product of a subgroup of the symmetric group S_n. Given a subgroup of S_n, one may ask if the corresponding symmetrized tensor space has an o-basis. The answer will depend in part on the structure of the given group. Since any group can be homomorphically embedded onto a subgroup of the symmetric group, arbitrary finite groups may be considered. It has already been shown that if G is an o-basis group and $\varphi : G \to S_n$ is a homomorphism, then the symmetrized space corresponding to $\varphi(G)$ has an o-basis. The study of these groups therefore may well be of interest to those working with o-bases of symmetrized spaces. Our focus, however, is on the group structure and character theory of o-basis groups themselves with a view toward using the o-basis property as a means of distinguishing between abstract

finite groups. The tools come from finite group theory and the character theory of finite groups. Field theory appears very briefly. In previous work, some interesting classes of groups have been shown to be o-basis, and so far all groups identified as o-basis are nilpotent. Particularly compelling are the dihedral groups. It has been shown that the o-basis dihedral groups are precisely those that are 2-groups. These are also precisely the nilpotent dihedrals. With this in mind, we ask whether or not all o-basis groups are nilpotent. We consider this question for a restricted class of groups. Conversely, there are examples of nilpotent groups that are not o-basis leading us to explore conditions on a nilpotent group which will guarantee that the group is o-basis. The results obtained indicate a possible connection between the o-basis property and the nilpotence class of a group.

The second main division of the present work is an exploration of a generalization of o-basis groups. While the following definitions contain technicalities, the reader should be able, without preliminary preparation, to understand the nature of the generalization. A group is o-basis if for each subgroup $H \leq G$ and $\chi \in Irr(G)$ for which $(\chi, 1)_H \neq 0$, there are a certain number of "orthogonal cosets" of H in G. We generalize by relaxing the subgroup condition as follows. Let $K \leq G$. We say G is K-o-basis if for each $\chi \in Irr(G)$ and each subgroup H containing K where $(\chi, 1)_H \neq 0$, there are the required number of "orthogonal cosets" of H. The o-basis groups, therefore, are the $\langle e \rangle$-o-basis groups, where $\langle e \rangle$ denotes the identity subgroup. Note that to apply this notion to a given class of groups, K must be defined for all groups in that class. Some results are obtained for the case when K is a member of the lower central series and when it is a member of the upper central series. Finally, the still open question of whether a direct product of o-basis groups is o-basis is briefly discussed.

Acknowledgments

For the many and patient efforts on my behalf, I would like to express my most sincere gratitude to Dr. Randall Holmes. To Dr. Gary Gruenhage and Dr. Huajun Huang, I would also like to earnestly convey my thanks. To the professors of the Auburn Department of Mathematics who have given their time and energy toward making my program successful and to the Department itself for supplying the resources that have made it possible, I am truly grateful.

Style manual or journal used Journal of Approximation Theory (together with the style known as "aums"). Bibliograpy follows van Leunen's *A Handbook for Scholars*.

Computer software used The document preparation package TEX (specifically LATEX) together with the departmental style-file `aums.sty`.

Table of Contents

Chapter 1

Preliminaries

1.1 Introduction

In this dissertation we study the notion of o-basis group. We also define and explore generalizations of this notion. O-basis groups were defined by Holmes in [Hlms], but their origins go back to an earlier paper by Holmes and Tam, [Hlms,Tam]. In that former paper, the authors studied the problem of the existence, in the n-fold tensor product of a complex inner product space, of a basis consisting entirely of "standard symmetrized tensors". Holmes would later call such a basis an o-basis. The term "symmetrized" refers to the action of a subgroup G of the symmetric group S_n on the tensor product. The question arises as to the extent to which the existence of an o-basis depends upon the structure of the group G. In particular, one may seek conditions on G which will guarantee that the corresponding symmetrized space has an o-basis. Since any group can be homomorphically embedded into S_n, abstract finite groups can be considered. For example, the authors proved in [Hlms,Tam] that if G is the dihedral group of order $2n$ (the group of symmetries of the regular n-gon), then the corresponding symmetrized tensor space has an o-basis if and only if n is a power of 2. Motivated by this, Holmes defined, in [Hlms], the o-basis groups as a class of abstract finite groups satisfying certain, rather technical, conditions. He then proved that, given an o-basis group G, for any quotient of G, regardless of how it is embedded into S_n, the corresponding tensor space has an o-basis. Thus, o-basis groups may well be of interest to those working with the existence of o-bases in tensor spaces. That problem and its connection with o-basis groups are discussed in more detail in section 2.2 below.

The focus in the present work is on o-basis groups themselves. In defining o-basis groups, Holmes' aim was to use the concept as a tool for distinguishing between abstract groups. For example, we have noted that the o-basis property chooses, from among the dihedrals, exactly those of prime-power order. Following the example of the dihedrals, Holmes was able to produce a list of familiar groups that are o-basis according to the definition he gives in [Hlms].

Theorem 1.1.1 ***([Hlms], p. 142)*** *The following groups are o-basis groups (p, prime, $n \geq 1$):*

(i) *any finite abelian group,*

(ii) *the dihedral group D_{2^n},*

(iii) *the quaternion group Q_{2^n},*

(iv) *the semidehedral group S_{2^n},*

(v) *the group with presentation $\langle x, a | x^p = 1 = a^{p^{n-1}}, a^x = a^{1+p^{n-2}} \rangle$*

(vi) *any group of order p^3,*

(vii) *any extra-special p-group.*

Holmes also provides a list of groups that are not o-basis.

Theorem 1.1.2 ***([Hlms], p. 138)*** *The following groups are not o-basis groups:*

(i) *any dihedral group D_n (order $2n$) with n not a power of 2.*

(ii) *any 2-transitive subgroup of S_n with $n \geq 3$ (e.g., the alternating group A_n, $n \geq 4$ and the symmetric group S_n $n \geq 3$),*

(iii) *any finite simple group of Lie type.*

Let us state, for future reference, the dihedral group result noting that if follows from Theorems 1.1.1 and 1.1.2 taken together.

Theorem 1.1.3 *A dihedral group of order* $2n$ *is o-basis if and only if* n *is a power of* 2.

Noting that all of the above examples that are o-basis are also p-groups, Holmes asked if all p-groups are o-basis. He answered this in the negative by constructing a group of order 3^4 that is not.

It is at this point that the present study begins. The new work presented here can be divided into two parts. The first part deals with the relationship between the property of being o-basis and that of being nilpotent. Since all prime power groups are nilpotent, we see that, so far, every group that has been identified as o-basis is also nilpotent. Even more compelling is the fact, already mentioned, that the dihedral groups that are o-basis are precisely those that are 2-groups. These also happen to be precisely the nilpotent dihedrals. In summary, two questions arise.

- Which nilpotent groups are o-basis?

  (not all of them, as the example of order 3^4 shows)

- Are all o-basis groups nilpotent?

Concerning the first of these questions, we begin by proving that if $G' \subseteq Z(G)$ (a condition implying nilpotentcy), then G is o-basis. We use this fact as a tool to obtain some further results. It also raises an interesting question for possible future study. Any group with $G' \subseteq Z(G)$ has nilpotence class less than or equal to 3 (see the definition of $\gamma_n(G)$ in the notation section). Noting that the example of order 3^4 has class 4, one might ask whether or not an o-basis group must be of class 3. This question remains open.

The reader might recall that nilpotent groups are characterized as being direct products of their Sylow subgroups. We use this fact to show that a nilpotent group is o-basis if and

only if each of its Sylow subgroups is o-basis. The method of proof does not generalize to direct products in general, and we briefly discuss the dilemma that arises after proving the result. From this result on Sylow subgroups, we see that in some sense the question of which nilpotent groups are o-basis would be answered if one knew which p-groups are o-basis. In [Hlms], Holmes has given some sufficient conditions on a p-group for it to be o-basis. In the present study, we take the approach of considering groups of increasingly higher prime power order. As shall be seen, it follows quickly from the defintion of o-basis that all abelian groups, and therefore all groups of order p^2, are o-basis. Holmes has also shown that all groups of order p^3 are o-basis (Theorem 1.1.1). Arriving at p^4, Holmes' group of order 3^4 gives the first example of a prime power group this is not o-basis. In hopes of better understanding groups of order p^4, we derive some necessary conditions for such a group to fail to be o-basis. The groups that arise from this investigation begin to look very much like Holmes' example.

After these considerations, we turn to the second of our questions. Are all o-basis groups nilpotent? Again taking our cue from the dihedrals, we narrow the focus of the question by considering a class of "dihedral-like" groups. More precisely, let p be prime and let $A \lhd G$ be abelian with $|G : A| = p^n$ for some positive integer n. Is it true that, whenever G is o-basis, G is also nilpotent? We obtain some limited results for small values of n.

The second major division of this work begins in section 3.1 where we define a generalized notion of o-basis group. The reader should be able to understand the nature of the generalization without begin concerned with the technicalities of the definitions given

below. O-basis groups could be defined as follows (although, our working definition will include some additional conditions in order to eliminate trivialities).

A finite group G is called an ***o-basis group*** *if for all $H \leq G$, and all $\chi \in Irr(G)$, there exist at least $\chi(e)(\chi, 1)_H$ cosets of H in G which are mutually orthogonal relative to B_H^χ.*

This definition gives conditions to be satisfied by all pairs (H, χ), with $H \leq G$ and χ an irreducible character of G. To generalize this, we require these conditions to hold for only certain subgroups. We also make an attempt at more convenient notation.

*For $H \leq G$ and $\chi \in Irr(G)$, we say G is $\big(H, \chi\big)$-**o-basis** if there are at least $\chi(e)\big(\chi, 1\big)_H$ cosets of H in G which are mutually orthogonal relative to B_H^χ. Let $K \leq G$. If G is $\big(H, \chi\big)$-o-basis for all subgroups H with $K \subseteq H$ and all $\chi \in Irr(G)$, we say G is K-**o-basis**.*

Let us note that the new definition encompasses the old since an o-basis group is one that is $\langle e \rangle$-o-basis, where e denotes identity element. One might try to use the notion of K-o-basis to distinguish between groups in a given class. To do this, K must be chosen so that it is defined for all groups in the class. For example, it makes sense to ask for any finite group whether or not the group is $Z(G)$-o-basis, where $Z(G)$ denotes the center of G. In section 3.3, we explore the notion of K-o-basis, where K is an element of the lower central series and also where K is an element of the upper central series. For example, we show that all finite groups are γ_3-o-basis, where γ_3 is the third term of the lower central series (see the notation section for the definition of these series).

Our tools come from finite group theory and from the character theory of finite groups. Field theory also appears very briefly.

The remainder of this preliminary chapter is devoted to material that will be needed in the main body which the reader may need to be introduced to or at least reminded of. We discuss some general concepts and facts from Group Theory in section 1.2 and Character theory in sections 1.3.1 - 1.3.3. Sections 1.3.4 and 1.3.5 are devoted to the specialized topics of Semi-Direct Products and Frobenius Groups respectively.

In section 2.1, we state our working definition of o-basis groups and look in some detail at Holmes' original development of the concept. We also state some results obtained by Holmes in [Hlms] that we use directly in the main body of this work. In section 2.2, we take a closer look at the tensor space problem that gave rise to the notion of o-basis groups.

1.2 Group Theory

This seems a convenient place to collect several facts and definitions from group theory that we will need and that the reader may not immediately recall.

Theorem 1.2.1 ***([Hun] p. 93)*** *Let p be a prime and G be a group of order p^n for some integer $n \geq 0$. Suppose G acts on a finite set S and let S^G denote the set of fixed points under the action. Then $|S| \equiv |S^G| \pmod{p}$.*

Definition 1.2.2 ***([Suz], p. 50)*** *Let K be a subgroup of a group G. We say K **characteristic** is in G, written K char G, if every automorphism of G maps K into itself. That is, $K^\sigma \subseteq K$ for all $\sigma \in Aut(G)$.*

Theorem 1.2.3 ***([Suz], p. 51)*** *Suppose $K \subseteq N$ are subgroups of a group G and that K char N. If $N \lhd G$, then $K \lhd G$.*

Theorem 1.2.4 ***([Hun] p. 94)*** *Let p be prime. The center of a non-trivial finite p-group contains more than one element.*

Theorem 1.2.5 ***([Hun], p. 96)*** *Let p be a prime. If G is a finite p-group, $N \lhd G$ and $N \neq \langle e \rangle$, then $N \cap Z(G) \neq \langle e \rangle$.*

Theorem 1.2.6 ***([Suz], p. 88)*** *Let p be prime and suppose G is a p-group. Let M be a maximal subgroup of G. Then $M \lhd G$ and G/M has order p.*

Definition 1.2.7 ***([Karp] p. 811)*** *Let p be prime. A p-group is called an* ***extra-special p-group*** *if $G' = Z(G)$, $|G'| = p$ and G/G' is elementary abelian.*

All groups of order p^3 are extra-special. To prove this, we can use the lemma below.

Lemma 1.2.8 *Suppose that G/Z is cyclic. Then G is abelian.*

Proof: Suppose for the sake of contradiction that G is non-abelian. Using the assumption that G/Z is cyclic, let $g \in G - Z$ such that $G/Z = \langle gZ \rangle$. Observe that $C_G(g)$ contains g and $Z(G)$. Thus $C_g(G)/Z = G/Z$ so that $C_g(G) = G$. It follows that $g \in Z(G)$, a contradiction. Therefore, G is abelian as desired.

□

Proposition 1.2.9 *Let G be a non-abelian group of order p^3. Then G is extra-special.*

Proof: We verify the conditions of Definition 1.2.7. Since G is non-abelian, we have $|G'| > 1$ and $|Z| \leq p^2$, where $Z = Z(G)$. If $|Z| = p^2$, then G/Z is cyclic so that, contrary to our assumption, G is abelian by Lemma 1.2.8. Thus $|Z| = p$. By Theorem 1.2.5, Z is contained in every normal subgroup of G. In particular, $Z \subseteq G'$. Also, G/Z is abelian,

being a p-group with order p^2. If follows that $G' \subseteq Z$ so that $G' = Z$. Finally, note that if $G/G' = G/Z$ is cyclic then Lemma 1.2.8 again gives that G is abelian. It follows that $G/G' \cong Z_p \times Z_p$. That is, G/G' is elementary abelian and the proof is complete.

□

Definition 1.2.10 ***([Suz], p.159)*** *Let p be prime. An abelian group A is said to be* ***elementary abelian*** *if $a^p = 1$ for all $a \in A$.*

If A is an elementary abelian p-group, then A is isomorphic to a direct sum of cyclic groups of order p.

1.3 Character Theory

In this section, we introduce the basics of the character theory of finite groups and present a number of definitions and results which we will call upon throughout this work. It is hoped that this will be an informative and enjoyable introduction to character theory for those readers not familiar with it. Secondly, we aim to make the subsequent discussion of o-basis groups more accessible and meaningful.

1.3.1 Brief Introduction to Character Theory

Character Theory can be developed in two alternate contexts, that of linear representations and that of modules over the group algebra. The resulting theories are essentially equivalent. We begin with representations. Let G be a finite group, let K be a field, and let V be a finite-dimensional vector space over K. We denote by $\mathrm{GL}(V)$ the group of invertible linear transformations of V onto itself. A group homomorphism $\rho : G \to \mathrm{GL}(V)$ is called

a **linear K-representation** (or simply a representation) of G in V. In the main body of this work, we will always take K to be the field of complex numbers. This assumption, as will be briefly explained below, simplifies the theory. We state what we can in the more general context to make the reader aware of that theory.

We move from representations to characters as follows. Suppose $\dim_{\mathbb{C}}(V) = n$ and let $B = \{v_1, \ldots, v_n\}$ be an ordered basis of V. For $v \in V$, we have $v = \sum_i \beta_i v_i$ for uniquely determined $\beta_i \in K$. Put

$$[v]_B = \begin{bmatrix} \beta_1 \\ \cdot \\ \cdot \\ \cdot \\ \beta_n \end{bmatrix}$$

(the coordinate vector of v relative to B). If $f : V \to V$ is a linear transformation, the **matrix of f relative to** B is given by $[f]_B = [\alpha_{ij}]$, where $f(v_j) = \sum_i \alpha_{ij} v_i (1 \leq j \leq n)$. That is, the jth column of $[f]_B$ is the coordinate vector of $f(v_j)$. The matrix of f satisfies the equation $[f(v)]_B = [f]_B[v]_B$, for all $v \in V$. If a second basis, B', is chosen for V, then there is an invertible $n \times n$ matrix A such that $[f]_{B'} = A[f]_B A^{-1}$. Recall that the **trace** of a matrix is the sum of the diagonal elements. Since the trace in invariant under conjugation, we see that $Tr[f]_B = Tr[f]_{B'}$. This fact will be called upon shortly.

Now suppose $\rho : G \to \mathrm{GL}(V)$ is a representation of G. We define the **character afforded by** ρ to be the function $\varphi : G \to K$ given by $\varphi(g) = Tr[\rho(g)]_B$ $(g \in G)$, where B is some chosen ordered basis. We have noted that the trace of the matrix of $\rho(g)$ is independent of the basis used when forming that matrix. Therefore, the character φ is also independent of the choice of basis. Suppose W is a K-subspace of V such that $\rho(g)(W) \subseteq W$ for all $g \in G$. Then the map $\rho_W : G \to \mathrm{GL}(W)$ given by $\rho_W(g) = \rho(g)|_W$ is a well-defined representation of G. It is called the **sub-representation** of ρ afforded by W. If ρ has no

proper, non-trivial sub-representations, then ρ is said to be irreducible and the character it affords is called an **irreducible character**. We will see that the irreducible characters play a critical role in character theory. First, however, let us develop these ideas in the alternative context of KG-modules.

As mentioned, the notion of a group representation is interchangeable with a second notion which we now introduce, that of a KG-module. Denote by KG the free K-module with basis G (or more simply, the K-vector space having the elements of G as basis). That is, KG consists of all formal sums of the form $\sum_{g\in G} \alpha_g g$, where $\alpha_g \in K$ (Since G is finite, the sums are finite). Note that, as a vector space over K, KG has dimension $|G|$. The K-space KG can be made into a ring by defining multiplication as follows:

$$\Big(\sum_{x\in G} \alpha_x x\Big)\Big(\sum_{y\in G} \beta_y y\Big) = \sum_{x\in G}\Big[\alpha_x x \sum_{y\in G} \beta_y y\Big] = \sum_{x,y\in G} (\alpha_x\beta_y)xy.$$

As a ring, KG has a multiplicative identity: the formal sum $1e$, where e denotes the identity element of G. We may imbed G into KG via $g \mapsto 1g$ and identify G with its image. Note that $1a \cdot 1b = 1(ab)$, for $a, b \in G$.

The K-vector space structure on KG combines with the ring structure to make KG a K-algebra. A **K-algebra** is a ring A with identity that is also a vector space over K such that the "scalar multiplication" interacts with the ring multiplication as follows: $\alpha(ab) = (\alpha a)b = a(\alpha b)$ for all $\alpha \in K$ and all $a, b \in A$. It is not hard to verify that KG is indeed a K-algebra and we refer to KG with this structure as the **group algebra**. We are now ready to discuss modules over the group algebra and their connections with representations and characters.

Let A be a K-algebra and let V be a K-vector space. Suppose for every $v \in V$ and $x \in A$ that a unique $xv \in V$ is defined. Also assume for all $x, y \in A$, $v, w \in V$, and $k \in K$ that

(i) $x(v+w) = xv + xw$

(ii) $(x+y)v = xv + yv$

(iii) $x(yv) = (xy)v$

(iv) $x(kv) = k(xv) = (kx)v$

(v) $1v = v$

Then V is called an **A-module**. Some authors omit (v) and call an A-module with this additional property a unitary A-module. Also, an A-module is usually not assumed to be finite-dimensional as a K-space.

Suppose again that $\rho : G \to \mathrm{GL}(V)$ is a representation of a group G. One makes V into a KG-module by defining $gv = \rho(g)(v)(g \in G, v \in V)$, and extending linearly to KG.

Conversely, let V be a KG-module. Then V can be viewed as a (finite-dimensional) vector space over K. Here we use the fact that the map $K \to KG$ given by $\alpha \mapsto \alpha 1$, where $\alpha \in K$, is a ring monomorphism. We may therefore identify K with its image in KG under this map. Define $\rho : G \to \mathrm{GL}(V)$ by $\rho(g)(v) = gv$. One uses the above properties of a K-algebra to show that ρ is a well-defined homomorphism, and hence a representation of G. We call ρ the **representation of G afforded by** V. If φ is the character afforded by ρ, we say that φ is **afforded by the KG-module** V.

If $W \subseteq V$ is a KG-submodule of V (meaning that $sW \subseteq W$ for all $s \in KG$), then W affords a representation of G and this representation is a sub-representation of ρ (see our discussion of representations). A non-zero KG-module is **simple** if it has no non-zero, proper submodules. If V is a simple KG-module, then the representation it affords is

irreducible in the sense defined previously and the character it affords is an **irreducible character**. We may, in this way, pass from representations to KG-modules and back and develop the theory in either context. Let us take this opportunity to point out that sums of characters are characters. Indeed, let V_1 and V_2 be KG-modules affording the characters χ_1 and χ_2 respectively. The direct sum $V_1 \oplus V_2$ becomes a KG-module by defining $s(v_1, v_2) = (sv_1, sv_2)$ $(s \in KG, v_i \in V_i)$. In this case, $V_1 \oplus V_2$ affords the character $\chi_1 + \chi_2$ defined as usual by $(\chi_1 + \chi_2)(g) = \chi_1(g) + \chi_2(g)$. As will be seen, any character can be written as a sum of irreducible characters.

If one assumes that $K = \mathbb{C}$, the field of complex numbers, a simplified theory results. This is due to the fact that the complex numbers form an algebraically closed field of characteristic zero. In fact, the simplified theory continues to hold, with minor adjustments, for any algebraically closed field whose characteristic does not divide $|G|$. The utility of these properties for character theory lies in part with two results which we state below: Maschke's Theorem and Schur's Lemma. This theory is covered in detail (and in more generality) in Chapter 1 and in the beginning of Chapter 2 of [Is].

Definition 1.3.1 *Let R be a ring. If there is a least positive integer n such that $na = 0$ for all $a \in R$, then R is said to have* ***characteristic n****. If no such n exists, R is said to have* ***characteristic zero****.*

Note that the field of complex numbers has characteristic zero and is algebraically closed.

Theorem 1.3.1.1 ***(Maschke's Theorem)*** *Let K be a field and let G be a finite group. If char(K) does not divide $|G|$, then every KG-module is a direct sum of simple modules.*

Thus, given a group G, to know all simple KG-modules is to know all KG-modules. As an interesting aside, we mention that it is pointed out in Isaacs' book that a KG-module is external to KG. Therefore, it is not clear how one might determine from KG all simple KG-modules. One must produce a set of KG-modules large enough to contain copies of all simple KG-modules. Let us note that KG can be considered a module over itself by left multiplication. Denote this KG-module by KG°. It can be shown that every simple KG-module is a submodule of KG°.

Theorem 1.3.1.2 ***(Schur's Lemma)*** *Let V and W be simple KG-modules and let $f : V \to W$ be a KG-module homomorphism.*

(i) *If $V \ncong W$, then $f = 0$.*

(ii) *Assume that K is algebraically closed. If $V = W$, then $f = \alpha 1_V$ for some $\alpha \in K$.*

We assume henceforth that $K = \mathbb{C}$. As an illustration of how Maschke's Theorem and Schur's Lemma are used, we include a sketch of their role in a portion of the theory that will be of interest to us. We need to define the notion of a class function.

A function $f : G \to \mathbb{C}$ is said to be a **class function** on G if for each $g \in G$, $f(xgx^{-1}) = f(g)$ for all $x \in G$. That is, a class function is constant on conjugacy classes of G. The class functions of G form a complex vector space, $Cl(G)$. Let $\{H_i\}_{i=1}^{k}$ be the conjugacy classes of G and define, for each i, $\chi_i : G \to \mathbb{C}$ by $\chi_i(g) = \begin{cases} 1 & \text{if } g \in H_i \\ 0 & \text{if } g \notin H_i \end{cases}$. Then the set $\{\chi_i : 1 \leq i \leq k\}$ forms an obvious basis of $Cl(G)$ so that the dimension of $Cl(G)$ over $\mathbb{C}$ is equal to the number of conjugacy classes of G.

Characters are class functions and this fact will be used directly at least once in this work. We have already mentioned the fact that, if K is taken to be $\mathbb{C}$, the irreducible characters of G play a particularly important role in character theory. It turns out, in this

case, that $Irr(G)$ forms a basis for $Cl(G)$ that is orthonormal relative to a certain "inner product". The proof involves both Maschke's Theorem and Schur's Lemma.

Definition 1.3.1.3 *Let φ, ϑ be class functions on a finite group G. Define the* ***inner product of φ and ϑ*** *by*

$$(\varphi, \vartheta) = (\varphi, \vartheta)_G = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\overline{\vartheta(g)}.$$

Our "inner product" has the following properties for all $x, y, z \in V$ and every $\alpha, \beta \in \mathbb{C}$:

(i) $(\alpha x + \beta y, z) = \alpha(x, z) + \beta(y, z)$

(ii) $(y, x) = \overline{(x, y)}$

(iii) $(x, x) \geq 0$

(iv) $(x, x) = 0$ iff $x = 0$.

From this definition, it follows that the inner product is conjugate linear in the second variable. That is $(x, \alpha y + \beta z) = \overline{\alpha}(x, y) + \overline{\beta}(x, z)$, where the notation is as in the definition. We have the following.

Theorem 1.3.1.4 ***Orthogonality Relation ([Is], p.20)*** *Let $\chi, \varphi \in Irr(G)$.*
Then $(\chi, \varphi)_G = \frac{1}{|G|} \sum_{g \in G} \chi(g)\varphi(g^{-1}) = \delta_{\chi\varphi}$, where $\delta_{\chi\varphi}$ is the Kronecker delta.

The orthogonality relation says that the irreducible characters of G form an orthonormal set with respect to the inner product defined above. We note that there is, in fact, a "first" and "second" orthogonality relation. What we have stated is the "first". Let us now turn to the proof that $Irr(G)$ forms a basis for $Cl(G)$. We need one further lemma.

Lemma 1.3.1.5 *Let S be a simple $\mathbb{C}G$-module affording the character χ. Let $f \in Cl(G)$ and define $h = \sum_{g \in G} f(g)g : V \to V$. Then $h = \frac{|G|}{n}(f, \overline{\chi})1_V$, where $n = \dim_{\mathbb{C}} V$.*

Sketch of proof for Lemma 1.3.1.5: One shows that h is a $\mathbb{C}G$-module homomorphism. By Theorem 1.3.1.2, we have $h = \alpha 1_V$ for some $\alpha \in \mathbb{C}$. Thus,

$$\alpha n = Tr(h) = Tr\left(\sum_{g\in G} f(g)g\right) = \sum_{g\in G} Tr(f(g)g) = \sum_{g\in G} f(g)Tr(g) = \sum_{g\in G} f(g)\chi(g) = |G|(f,\overline{\chi}),$$

where the last equality follows immediately from Definition 1.3.1.3. The result follows.

□

Theorem 1.3.1.6 *Let G be a finite group. Then $Irr(G)$ is a basis for $Cl(G)$.*

Sketch of proof: We have seen that $Irr(G)$ forms an orthonormal set in $Cl(G)$. Thus it suffices to show that $Irr(G)$ spans $Cl(G)$. For this, it is enough to show that the orthogonal complement of the subspace generated by $Irr(G)$ is zero (relative to the inner product defined in 1.3.1.3). Let $f \in Cl(G)$ such that $(\chi, f) = 0$ for all $\chi \in Irr(G)$. Let $V = \mathbb{C}G$ and set $h = \sum_{g\in G} \overline{f(g)}g : V \to V$. (That is, $h(v) = \left(\sum_{g\in G} \overline{f(g)}g\right)v$ for all $v \in \mathbb{C}G$.) If S is a simple submodule of V affording the character χ, then Lemma 1.3.1.5 gives that the restriction of h to S equals $\frac{|G|}{n}(\overline{f},\overline{\chi})1_S$, where $n = \dim_{\mathbb{C}} S$. Note that $(\overline{f},\overline{\chi}) = (\chi, f)$ (easily verified from Definition 1.3.1.3). Since the quantity on the right is zero by assumption, we see that h_S is zero. By Theorem 1.3.1.1, V is a direct sum of simple modules. It follows that $h : V \to V$ is the zero map. Hence $\sum_{g\in G} \overline{f(g)}g = h(e) = 0$. This last quantity is a linear combination in the vector space $\mathbb{C}G$ and the elements of G are a basis for that space. Thus the elements of G form a linearly independent set. This implies that $\overline{f}(g) = 0$ for all $g \in G$. That is, $\overline{f} = 0$. It follows that $f = 0$, as desired.

□

By Theorem 1.3.1.6, $Irr(G)$ forms a basis over $\mathbb{C}$ for $Cl(G)$. The first part of the theorem below follows immediately.

Theorem 1.3.1.7 ***([Is], p.16)*** *Every class function φ of G can be uniquely expressed in the form $\varphi = \sum_{\chi \in Irr(G)} a_\chi \chi$, where $a_\chi \in \mathbb{C}$. Furthermore, φ is a character if and only if all of the a_χ are nonnegative integers and $\varphi \neq 0$.*

The module viewpoint can be used to give an easy proof of the second statement of the theorem. Let V be a KG-module affording the character φ. According to Maschke's Theorem, V is a direct sum of simple modules. Therefore, φ is the sum of the irreducible characters that these simple modules afford.

More can be said of the α_χ. These quantities will play an important role in several of our arguments. They can be described in terms of the inner product.

Proposition 1.3.1.8 ***([Is], p.20)*** *Let χ be a character of G. Then*

(i) $|\chi(g)| \leq \chi(e)$, *and*

(ii) $\chi(g^{-1}) = \overline{\chi(g)}$.

Proposition 1.3.1.9 *Let $\varphi \in Cl(G)$. Then $\varphi = \sum_{\sigma \in Irr(G)} (\varphi, \sigma)\sigma$.*

Proof: By Theorem 1.3.1.7, $\varphi = \sum_{\sigma \in Irr(G)} \alpha_\sigma \sigma$, for uniquely determined $\alpha_\sigma \in \mathbb{C}$. Fix $\chi \in Irr(G)$ and observe that

$$(\varphi, \chi) = \left(\sum_{\sigma \in Irr(G)} \alpha_\sigma \sigma, \chi \right) = \sum_{\sigma \in Irr(G)} \alpha_\sigma (\sigma, \chi) = \alpha_\chi,$$

where the last equality follows from Theorem 1.3.1.4. The result follows.

□

Suppose φ is a character of G. For any $\chi \in Irr(G)$ for which $(\varphi, \chi) \neq 0$, we say that χ is an **irreducible constituent** of φ. In this case, we see from Proposition 1.3.1.9 that (φ, χ) is the multiplicity of χ as an irreducible constituent. Note also that $\varphi(e) = \sum(\varphi, \chi)\chi(e)$.

Proposition 1.3.1.10 ***([Is], p.21)*** *Let φ and ψ be (not necessarily irreducible) characters of a group G. Then $(\varphi, \psi) = (\psi, \varphi)$ is a non-negative integer. Also, $\chi \in Irr(G)$ if and only if $(\chi, \chi) = 1$.*

1.3.2 Basic Concepts and Related Theorems

In this section, we introduce some basic concepts in and collect a number of results from character theory that we will need.

Definition 1.3.2.1 *For a character χ of G, the positive integer $\chi(e)$ is called the **degree** of χ. We say χ is **linear** if $\chi(e) = 1$.*

Let $\chi \in Irr(G)$ and let $\rho : G \to \mathrm{GL}(V)$ be the representation affording χ. Since ρ is a homomorphism, the matrix of $\rho(e)$ is the identity matrix. Thus $\chi(e)$, the trace of this matrix, is the dimension over $\mathbb{C}$ of V. In particular, it is a positive integer. As noted in the remarks before Proposition 1.3.1.10, the degree of χ is the sum of the degrees of its irreducible constituents (counting multiplicities).

Note that the linear characters are precisely those that are afforded by representations into 1-dimensional spaces. This means that linear characters are irreducible.

Proposition 1.3.2.2 *Let χ be a linear character of G. Then χ is irreducible.*

Proof: Let $\rho : G \to GL(V)$ be a representation affording χ. We have $\dim_{\mathbb{C}} V = \chi(e) = 1$. Thus V has no proper, non-trivial subspaces so that ρ has no proper, non-trivial sub-representations. That is ρ, and thus χ is irreducible.

□

Theorem 1.3.2.3 ***([Is], p.16)*** *A group G is abelian if and only if every irreducible character of G is linear.*

Definition 1.3.2.4 *Let χ be a character of G. The* ***kernel*** *of χ is the subgroup of G defined by:* $\ker \chi = \{g \in G : \chi(g) = \chi(e)\}$. *We say that χ is* ***faithful*** *if* $\ker \chi = \{e\}$.

Suppose that $N \lhd G$. There is a one-to-one correspondence between the irreducible characters of G/N and those irreducible characters of G whose kernels contain N. More precisely, we have the following result taken from Isaacs.

Proposition 1.3.2.5 ***([Is], p.24)*** *Let $N \lhd G$.*

(i) *If χ is a character of G and $N \subseteq \ker \chi$, then χ is constant on cosets of N in G and the function $\widehat{\chi}$ on G/N defined by $\widehat{\chi}(gN) = \chi(g)$ is a character of G/N.*

(ii) *If $\widehat{\chi}$ is a character of G/N, then the function χ defined by $\chi(g) = \widehat{\chi}(gN)$ is a character of G.*

(iii) *In both (a) and (b), $\chi \in Irr(G)$ iff $\widehat{\chi} \in Irr(G/N)$.*

Suppose $\chi \in Irr(G)$ and $\ker\chi \supseteq G'$. Then $\widehat{\chi} \in Irr(G/G')$. Since G/G' is abelian, Proposition 1.3.2.3 gives that $\chi(e) = \widehat{\chi}(e) = 1$. That is, χ is linear. The converse is true in fact, as the proposition below states.

Propositon 1.3.2.6 $G' = \bigcap\{\ker(\lambda) : \lambda \in Irr(G), \lambda(1) = 1\}$

Definition 1.3.2.7 *Let χ be a character of G. The* ***center*** *of χ is the subgroup of G given by:* $Z(\chi) = \{g \in G : |\chi(g)| = \chi(e)\}$.

Note that $\ker\chi \subseteq Z(\chi)$ for all characters χ.

Corollary 1.3.2.8 ***([Is], p.27)*** *Let $\chi \in Irr(G)$. Then $Z(G) = \bigcap\{Z(\chi) : \chi \in Irr(G)\}$.*

Lemma 1.3.2.9 ***([Is], p.27)*** *Let $\chi \in Irr(G)$. Then $Z(\chi)/\ker\chi = Z(G/\ker\chi)$.*

This follows from Proposition 1.3.2.5 and Theorem 1.3.2.3.

Proposition 1.3.2.10 ***([Is], p.28)*** *Let $\chi \in Irr(G)$. Then $\chi^2(e) \leq |G : Z(\chi)|$. Equality occurs if and only if $\chi \equiv 0$ on $G - Z(\chi)$.*

Theorem 1.3.2.11 ***([Is], p.28)*** *Suppose that $\chi \in Irr(G)$ and that $G/Z(\chi)$ is abelian. Then $|G : Z(\chi)| = \chi^2(e)$.*

The following result follows from remarks accompanying exercise 2.12, [Is], p.31.

Proposition 1.3.2.12 *Let φ be a character of G and let $n = |G|$. Let $g \in G$ with $\varphi(g) = 0$. Then $\chi(g^m) = 0$ for all $m \in \mathbb{Z}$ with $(m, n) = 1$.*

Proof: Let ϵ be a primitive nth root of unity in $\mathbb{C}$. Let $m \in \mathbb{Z}$ with $(m, n) = 1$. Referring to exercise 2.12 ([Is], p. 31), there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}[\epsilon], \mathbb{Q})$ such that $\varphi(g^m) = \sigma(\varphi(g))$. By assumption, we have $\sigma(\varphi(g)) = \sigma(0) = 0$, where the last equality follows since σ is a field automorphism. The result is established.

□

Theorem 1.3.2.13 ***Ito's Theorem ([Is], p.84)*** *Let $A \lhd G$ be abelian. Then $\chi(e)$ divides $|G : A|$ for all $\chi \in Irr(G)$.*

1.3.3 New Characters from Old: Products, Induction, Restriction and Conjugation

Definition 1.3.3.1 *Let φ and ψ be class functions on a group G. The* ***product*** *$\varphi\psi$ of φ and ψ is defined by $\varphi\psi(g) = \varphi(g)\psi(g)$. If φ and ψ are characters, then $\varphi\psi$ (see immediately below).*

Let V_1 and V_2 be $\mathbb{C}G$-modules affording the characters φ_1 and φ_2 respectively. The tensor product $V_1 \otimes V_2$ becomes a $\mathbb{C}G$-module by defining $g(v_1 \otimes v_2) = gv_1 \otimes gv_2$ ($g \in G$, $v_i \in V_i$) and extending linearly in both $\mathbb{C}G$ and in $V_1 \otimes V_2$. As a $\mathbb{C}G$-module, $V_1 \otimes V_2$ affords the product character $\varphi_1\varphi_2$.

Theorem 1.3.3.2 ***([Is], p.59)*** *Let G be the direct product of subgroups H and K. Let φ be a character of H and ψ be a character of K. Extend φ, ψ to G by putting $\varphi(h, k) = \varphi(h)$ and $\psi(h, k) = \psi(k)$. These functions are characters of G so that the product $\varphi\psi$ is a character of G. Moreover, the irreducible characters of G are exactly the products of the extended irreducible characters of H and K: $Irr(G) = \{\varphi\psi : \varphi \in Irr(H), \psi \in Irr(K)\}$.*

Theorem 1.3.3.2 generalizes in the natural way to a direct product with any finite number of factors.

Theorem 1.3.3.3 *Suppose $H \leq G$ and let $\chi \in Irr(G)$. The restriction, χ_H, of χ to H is a character of H.*

Keeping the above notation, we see that $\chi_H(e) = \chi(e)$. Thus the restriction of a linear character is linear and so irreducible by Proposition 1.3.2.2. Let $\chi \in Irr(G)$ and $\varphi \in Irr(H)$. When referring to the inner product in H we will suppress the subscript on the restricted character and write $(\chi, \varphi)_H$ rather than $(\chi_H, \varphi)_H$ (see Definition 1.3.1.3).

Theorem 1.3.3.4 ***([Is], p.81)*** *Let $N \lhd G$ and suppose that $\chi \in Irr(G)$ with $\big(\chi, 1\big)_N \neq 0$. Then $N \subseteq \ker \chi$.*

Definition 1.3.3.5 *Let $H \leq G$ and let $\varphi \in Cl(H)$. The **induced class function** φ^G on G is defined by*

$$\varphi^G(g) = \frac{1}{|H|} \sum_{x \in G} \varphi^\circ\big(xgx^{-1}\big)$$

where $\varphi^\circ(y) = \varphi(y)$ if $y \in H$ and $\varphi^\circ(y) = 0$ if $y \notin H$.

It follows immediately from the definition that $\varphi^G(e) = |G : H| \cdot \varphi(e)$. Also, if $N \lhd G$ and $\varphi \in Cl(N)$, then $\varphi^G \equiv 0$ on $G - N$.

Lemma 1.3.3.6 ***([Is], p.67)*** *Let φ be a character of a subgroup of G. Then $\ker(\varphi^G) = \bigcap_{x \in G} (\ker \varphi)^x$.*

Definition 1.3.3.7 *Let $H \leq G$, let χ be a character of H and let $g \in G$. The **conjugate character,** ${}^g\chi$, of χ is the character of ${}^gH$ defined by the equation ${}^g\chi({}^gh) := \chi(h)$.*

Definition 1.3.3.8 *Let $H \lhd G$ and let $\varphi \in Irr(H)$. The set $I_G(\varphi) = \{g \in G : {}^g\varphi = \varphi\}$ is called the **inertial subgroup** of φ.*

Conjugate characters play a central role in two important theorems concerning characters of subgroups: Clifford's Theorem and Mackey's Theorem. Clifford's Theorem deals with restriction to a normal subgroup.

Theorem 1.3.3.9 ***(Clifford's Theorem for Characters)*** *Let $H \lhd G$, let $\chi \in Irr(G)$, let $\lambda \in Irr(H)$ and assume $(\chi, \lambda)_H \neq 0$. Then $\chi_H = (\chi, \lambda)_H \sum_{s \in \Omega} {}^s\lambda$, where $\{{}^s\lambda\}_{s \in \Omega}$ is a complete set of distinct conjugates of λ.*

We will also be interested in inducing up to G a character of some subgroup H of G and then restricting this induced character to a subgroup K of G to obtain a character of K. Mackey's Theorem provides a description of the restricted character. The theorem involves the notion of conjugate characters and that of double cosets.

Definition 1.3.3.10 *Let H, K be subgroups of a group G and let $g \in G$. The* ***(H,K)-double coset*** *containing g is the set $HgK := \{hgk : h \in H, k \in K\}$.*

Theorem 1.3.3.11 ***Mackey's Theorem*** *Let H, K be subgroups of a group G and let φ be a character of H. Then $(\varphi^G)_K = \sum_{s \in \Omega} \left({}^s\varphi)_{{}^sH \cap K}\right)^K$, where Ω is a complete set of (H, K)-double coset representatives in G.*

Theorem 1.3.3.12 ***Frobenius Reciprocity([Is], p.62)*** *Let H be a subgroup of a group G. Suppose $\varphi \in Cl(H)$ and $\psi \in Cl(G)$. Then $\left(\varphi, \psi_H\right)_H = \left(\varphi^G, \psi\right)_G$.*

Definition 1.3.3.13 *Let φ be a character of G. We say φ is* ***mononial*** *if $\varphi = \lambda^G$, where λ is a linear character of some (not necessarily proper) subgroup of G. The group G is an* ***M-group*** *if every irreducible character of G is monomial.*

Let $H \leq G$, let $\lambda \in Irr(H)$ be linear, and let $\chi = \lambda^G$. If χ is non-linear, then $|G : H| = |G : H|\lambda(e) = \chi(e) > 1$ (see the comments after Definition 1.3.3.5). That is, H is a proper subgroup in this case.

Theorem 1.3.3.14 ***([Is], p.83)*** *Every nilpotent group is an M-group.*

1.3.4 Semi-Direct Products

In this section we discuss a generalization of the notion of direct product.

Definition 1.3.4.1 *Let A, T be subgroups of G. We say G is the* ***internal semi-direct product*** *of A and T (written $A \rtimes T$) if the following hold:*

(i) $G = AT$,

(ii) $A \cap T = \langle e \rangle$.

Our interest in the semi-direct product structure stems in large part from the following discussion taken from [Ser], p.62. We refer the reader to that passage for a full discussion and proofs. Consider a semi-direct product, $G = A \rtimes T$, where A is abelian. The irreducible characters of G shall be described in terms of those for A and T. The group T acts on $Irr(A)$ as follows: $\lambda^t(a) = \lambda(t^{-1}at)$, where $\lambda \in Irr(A)$, $t \in T$, and $a \in A$. Choose a representative λ of an orbit in $Irr(A)$ under the action of T and let T_λ denote the stabilizer of λ in T. Put $H = AT_\lambda$. The character λ is extended to an irreducible character of H by putting $\lambda(at) = \lambda(a)$ for $a \in A$ and $t \in T_\lambda$. Choose $\rho \in Irr(T_\lambda)$. Putting $\tilde{\rho} = \rho\pi$, where $\pi : H \to H/A \cong T_\lambda$ is the canonical map, one obtains a second irreducible character of H. Now set $\theta_{\lambda,\rho} = (\lambda\tilde{\rho})^G$ to obtain an irreducible character of G. That $\theta_{\lambda,\rho}$ is indeed an irreducible character of G and that the above construction gives all irreducible characters of G is the substance of the next theorem.

Theorem 1.3.4.2 *Suppose that $G = A \rtimes T$, where A is abelian. Referring to the above discussion, let $\{\lambda_i\}$ be a complete set of orbit representatives in $Irr(A)$ under the action of T and put $\theta_{\lambda_i,\rho} = (\lambda_i\tilde{\rho})^G$ for each orbit representative λ_i and character $\rho \in Irr(T_{\lambda_i})$. Then the following statements hold:*

(i) $\theta_{\lambda_i,\rho} \in Irr(G)$,

(ii) If $\theta_{\lambda_i,\rho} = \theta_{\lambda_i',\rho'}$, *then* $i = i'$ *and* $\rho = \rho'$,

(iii) For every $\chi \in Irr(G)$, $\chi = \theta_{\lambda_i,\rho}$ *for some* i *and* $\rho \in Irr(T_{\lambda_i})$.

The following Theorem will be used to verify that certain groups of interest are semi-direct products.

Theorem 1.3.4.3 ***(Schur-Zassenhaus)*** *Let* $A \lhd G$. *If* $|G : A|$ *is relatively prime to* $|A|$, *then* G *is the internal semi-direct product* $A \rtimes T$, *where* T *is a subgroup of* G *with* $T \cong G/A$.

1.3.5 Frobenius Groups

We will have occasion to work with a special class of groups known as Frobenius Groups. We will, when there is need, refer the reader to this section for the definition of these groups and pertinent results.

Definition 1.3.5.1 *Let* $H \subseteq G$, *with* $\langle e \rangle \neq H \neq G$. *Assume that* $H \cap H^g = \langle e \rangle$ *whenever* $g \in G - H$. *Then* H *is a* ***Frobenius complement*** *in* G. *A group that contains a Frobenius complement is called a* ***Frobenius group***.

Theorem 1.3.5.2 ***(Frobenius, [Is], p.99-100)*** *Let* G *be a Frobenius group with complement* H. *Then there exists* $N \lhd G$ *with* $HN = G$ *and* $H \cap N = \langle e \rangle$. *In this case,* $C_G(x) \subseteq N$ *for all* $\langle e \rangle \neq x \in N$.

The normal subgroup N above is called the **Frobenius kernel** of G. It is uniquely determined by H. (see [Is], p.101).

Theorem 1.3.5.3 ***([Is], p.94)*** *Let $N \lhd G$ and assume that $C_G(x) \subseteq N$ for every $e \neq x \in N$. Then*

(i) For $\varphi \in Irr(N)$, with $\varphi \neq 1_N$, we have $I_G(\varphi) = N$ and $\varphi^G \in Irr(G)$.

(ii) For $\chi \in Irr(G)$ with $N \nsubseteq \ker \chi$, we have $\chi = \varphi^G$ for some $\varphi \in Irr(N)$.

Lemma 1.3.5.4 ***([Is], p.199)*** *Let G be solvable and assume that G' is the unique minimal normal subgroup of G. Then all non-linear irreducible characters of G have equal degree f and for some prime p one of the following holds:*

(i) G is a p-group, $Z(G)$ is cyclic and $G/Z(G)$ is elementary abelian of order f^2.

(ii) G is a Frobenius group with an abelian Frobenius complement of order f.

Also, G' is the Frobenius kernel and is an elementary abelian p-group.

Chapter 2

O-Basis Groups

In this chapter, we define o-basis groups, make some preliminary observations and discuss connections to a problem in multi-linear algebra.

2.1 Construction and Definition

The o-basis groups were defined by Holmes in [Hlms]. We give here a brief account of his construction which will serve to motivate our working definition. We also state some results from [Hlms] which we will use later.

Let G be a finite group and let H be a subgroup of G. Denote by G/H the set of left cosets of H in G. The natural left action of G on the set G/H extends linearly to the complex vector space having this set as basis. Denote this vector space by $\mathbb{C}(G/H)$. Let $\chi \in Irr(G)$. Define a form B_H^χ on $\mathbb{C}(G/H)$ by putting

$$B_H^\chi(aH, bH) \quad = \quad \frac{\chi(e)}{|H|} \sum_{h \in H} \chi(a^{-1}bh), \tag{2.1}$$

and extending linearly in the first component and anti-linearly in the second component. This can be shown to be a well-defined G-invariant Hermitian form. The term G-invariant means that $B_H^\chi(gaH, gbH) = B_H^\chi(aH, bH)$ for all $g, a, b \in G$. Put $C_H^\chi := \mathbb{C}(G/H)/\ker B_H^\chi$, where $\ker B_H^\chi := \{x \in \mathbb{C}(G/H) : B_H^\chi(x, y) = 0 \text{ for all } y \in \mathbb{C}(G/H)\}$. Then B_H^χ induces

a well-defined form $\overline{B}_H^\chi$ on C_H^χ given by $\overline{B}_H^\chi(\overline{x},\overline{y}) = B_H^\chi(x,y)$ $(x,y \in \mathbb{C}(G/H))$, where $\overline{x}$ denotes the coset $x + \ker B_H^\chi$. We have the following.

Theorem 2.1.1 ***([Hlms] p.135)***

(i) $\dim_{\mathbb{C}} C_H^\chi = \chi(e)(\chi,1)_H$, *where* $(\chi,1)_H = \dfrac{1}{|H|}\sum_{h\in H}\chi(h)$.

(ii) *The form* $\overline{B}_H^\chi$ *is positive definite.*

Holmes defines a group G to be an **o-basis group** if for every $H \leq G$ and $\chi \in Irr(G)$ the vector space C_H^χ has a basis that is orthogonal relative to $\overline{B}_H^\chi$ and consists entirely of elements of the form $\overline{aH}$. Such a basis he calls an **o-basis** of C_H^χ. He then gives a characterization of o-basis groups entirely in terms of subgroups and characters without reference to the linear algebra. This result is given below after one further definition.

Theorem 2.1.2 ***([Hlms], p.139)*** *The following are equivalent.*

(i) *G is an o-basis group.*

(ii) *For each $H \leq G$ and each $\chi \in Irr(G)$, there exists at least $\chi(e)\big(\chi,1\big)_H$ cosets of H in G that are mutually orthogonal relative to B_H^χ.*

(iii) *For each $H \leq G$ and each non-linear $\chi \in Irr(G)$ with $\big(\chi,1\big)_H \neq 0$, there exist at least $\chi(e)\big(\chi,1\big)_H$ cosets of H in G that are mutually orthogonal relative to B_H^χ.*

We will take (iii) of Theorem 2.1.2 as our definition of o-basis group. It is obvious in the theorem that (ii) implies (iii). It seems desirable to provide a brief sketch of the proof for the remainder of the theorem since the reader will likely be curious about this and some of the details are not difficult.

Sketch of proof of Theorem 2.1.2: Let $H \leq G$, let $\chi \in Irr(G)$ and assume that (iii) holds. We prove (i). By assumption, we may assume either $(\chi, 1)_H = 0$ or that χ is linear. Suppose that $(\chi, 1)_H = 0$. Then by Theorem 2.1.1 part(i), $\dim_{\mathbb{C}} C_H^\chi = 0$. In this case, the basis of C_H^χ is empty and satisfies Holmes' original definition vacuously. We assume therefore that $(\chi, 1)_H \neq 0$. Let us suppose that χ is linear. Then the restriction of χ_H is linear (since $1 = \chi(e) = \chi_H(e)$) and, by Proposition 1.3.2.2, $\chi_H \in Irr(H)$. By Proposition 1.3.1.9, $\chi_H = 1_H$ and $(\chi, 1)_H = 1$. Theorem 2.1.1 now gives that $\dim_{\mathbb{C}} C_H^\chi = 1$. Thus, C_H^χ has as basis the set $\{\overline{H}\}$, where $\overline{H} := H + \ker(B_H^\chi)$. This single set serves as an o-basis, the orthogonality condition again being satisfied vacuously. This shows that (iii) implies (i).

For (i) implies (ii), observe first that for every $a, b \in G$, $\overline{B}_H^\chi(\overline{aH}, \overline{bH}) = B_H^\chi(aH, bH)$ so that $\overline{aH}$ and $\overline{bH}$ are orthogonal relative to $\overline{B}_H^\chi$ if and only if aH and bH are orthogonal relative to B_H^χ. Assume that G is an o-basis group, let $H \leq G$ and $\chi \in Irr(G)$. There exists an o-basis $\{\overline{a_1 H}, \ldots, \overline{a_t H}\}$ of C_H^χ, (possibly empty with $t = 0$). By Theorem 2.1.1, $t = \chi(e)(\chi, 1)_H$ and, by the above observations, $a_1 H, \ldots, a_t H$ are mutually orthogonal relative to B_H^χ. This shows that (i) implies (ii) and the proof is complete.

□

As we have said, we take Theorem 2.1.2 part (iii) for our definition of o-basis group.

Definition 2.1.3 *A finite group G is called an **o-basis group** if for all $H \leq G$ and all non-linear $\chi \in Irr(G)$ with $(\chi, 1)_H \neq 0$, there exist at least $\chi(e)(\chi, 1)_H$ cosets of H in G which are mutually orthogonal relative to B_H^χ.*

The next result follows almost immediately from the definition.

Theorem 2.1.4 *Let G be abelian. Then G is o-basis.*

Proof: By Theorem 1.3.2.3, every irreducible character of G is linear. Therefore, G satisfies Definition 2.1.3 vacuously and is o-basis.

□

Throughout this work, we will often shift focus from a given group to a quotient of the group. The success of this technique depends on the discussion below and the two subsequent results. For the proofs, the reader is referred to [Hlms].

Let $N \lhd G$, let $\chi \in Irr(G)$ and assume that $N \subseteq \ker \chi$. For a subgroup $H \leq G$, denote by $\widehat{H}$ the image of H under the canonical map $G \to G/N$. The function $\widehat{\chi} : \widehat{G} \to \mathbb{C}$ given by $\widehat{\chi}(gN) = \chi(g)$ is a well-defined irreducible character of $\widehat{G}$ (see Theorem 1.3.2.5, (i) and (iii)). Let $H \leq G$.

Proposition 2.1.5 ***([Hlms], p.137)*** *Let the notation be as in the above paragraph. The linear map $\phi : C_H^{\chi} \to C_{\widehat{H}}^{\widehat{\chi}}$ given by $\phi(\overline{gH}) = \overline{(gN)\widehat{H}}$ is a well-defined linear isometry. In particular, C_H^{χ} has an o-basis if and only if $C_{\widehat{H}}^{\widehat{\chi}}$ has an o-basis.*

Theorem 2.1.6 ***([Hlms], p.137)*** *The class of o-basis groups is closed under taking homomorphic images.*

The following theorem, also found in [Hlms], has proven useful for inspiration and as a direct tool in this study.

Theorem 2.1.7 ***([Hlms], p.139)*** *Let G be a finite p-group (p, prime) and assume that G has an abelian normal subgroup A and a cyclic normal subgroup C with $C \subseteq A$ satisfying $|G : A| \leq p$ and $|A : C| \leq p$. Then G is an o-basis group.*

2.2 Connections with Linear Algebra

O-basis groups arose in connection with a problem from multi-linear algebra. We give a brief description below. For a more in-depth discussion including proofs see [Hlms] and [Hlms,Tam].

Fix positive integers m and n and put $\Gamma_{m,n} = \{\gamma \in \mathbb{Z}^n : 1 \leq \gamma_i \leq m\}$. Let G be a subgroup of the symmetric group S_n. There is a right action of G on $\Gamma_{m,n}$ given by $\gamma\sigma = (\gamma_{\sigma(1)} \ldots, \gamma_{\sigma(n)})$ $(\gamma \in \Gamma_{m,n}, \sigma \in G)$.

Let V be a complex inner product space of dimension m and let $\{e_1, \ldots e_m\}$ be an orthonormal basis of V. To avoid trivialities, one assumes that $m \geq 2$. Denote by $V^{\otimes n}$ the n-fold tensor power of V. For $\gamma \in \Gamma_{m,n}$, put $e_\gamma := e_{\gamma_1} \otimes \cdots \otimes e_{\gamma_n} \in V^{\otimes n}$. Then $\{e_\gamma : \gamma \in \Gamma_{m,n}\}$ is a basis for $V^{\otimes n}$.

Let $\chi \in Irr(G)$. The **symmetrizer** relative to χ is the element of the group algebra $\mathbb{C}G$ of G (see the discussion on KG in section 1.3.1) given by $s^\chi := (\chi(e)/|G|) \sum_{\sigma \in G} \chi(\sigma)\sigma$. For $\gamma \in \Gamma_{m,n}$, put $e^\chi_\gamma := s^\chi e_\gamma$, where we view $V^{\otimes n}$ as a left $\mathbb{C}G$-module via $\sigma e_\gamma = e_{\gamma\sigma^{-1}}$ $(\sigma \in G)$. The quantity e^χ_γ is referred to as a **standard symmetrized tensor**.

The inner product on V induces an inner product on $V^{\otimes n}$. If W is a subspace of $V^{\otimes n}$, then we call an orthogonal basis of W consisting entirely of standard symmetrized tensors an **o-basis** of W relative to G and χ. One may ask about conditions on G which will guarantee the existence of an o-basis for $V^{\otimes n}$ relative to G and χ for all $\chi \in Irr(G)$. When discussing this situation, we will suppress reference to χ and talk about the existence on o-basis relative to G.

Now let G be an arbitrary group. One may ask if there are homomorphisms $\varphi : G \to S_n$ such that $V^{\otimes n}$ has an o-basis relative to $\varphi(G)$. Having fixed G, one might also wonder if

some embeddings work while other do not. In [Hlms], Holmes has shown that, for G an o-basis group, $V^{\otimes n}$ has an o-basis regardless of the homomorphism.

Theorem 2.2.1 ***([Hlms], p.138)*** *If G is an o-basis group and $\varphi : G \to S_n (n \in \mathbb{N})$ is a homomorphism, then $V^{\otimes n}$ has an o-basis relative to $\varphi(G)$.*

The reader may recall Cayley's Theorem which states that for any group G there is a homomorphic injection of G onto a subgroup of S_n. For each $g \in G$, one defines $\varphi(g)$ to be the permutation of G given by $\varphi(g)(h) = gh$ $(h \in G)$. In this case, $\varphi(G)$ can be viewed as a subgroup of S_n where $n = |G|$. This map is called the **Cayley embedding**. With the next result, Holmes provides, as he says, a characterization of o-basis groups in terms of symmertized tensors.

Theorem 2.2.2 ***([Hlms], p.139)*** *Let G be a finite group, let $n = |G|$, and let $\varphi : G \to S_n$ be the Cayley embedding. Then G is an o-basis group if and only if $V^{\otimes n}$ has an o-basis relative to $\varphi(G)$.*

In this work, we are interested in studying the o-basis property as a tool for distinguishing between abstract groups. However, as the above discussion indicates, those working with symmetrized tensor spaces may find the class of o-basis groups interesting as well.

Chapter 3

New Work

3.1 A Generalized Definition and Some Preliminary Results

In this section, we define a generalization of o-basis group and make some elementary observations. We will begin to use the terminology immediately. Later, in section 3.3, we will further explore the generalized notion. Also in this section, we obtain several preliminary results that will be key to some of the techniques used in later sections. Let us fix, for the remainder of this work, a finite group G.

Definition 3.1.1 *For $H \leq G$ and $\chi \in Irr(G)$, say that G is $\big(H, \chi\big)$-**o-basis** if there are at least $\chi(e)\big(\chi, 1\big)_H$ cosets of H in G which are mutually orthogonal relative to B_H^χ. Fix $K \leq G$. If G is $\big(H, \chi\big)$-o-basis for all subgroups H with $K \subseteq H$ and all non-linear $\chi \in Irr(G)$ for which $(\chi, 1)_H \neq 0$, we say G is K-**o-basis**.*

Note that G is o-basis (see Definition 2.1.3) precisely when G is $\langle e \rangle$-o-basis so that the generalized definition includes the original. Also, for any two subgroups H, K of G with $H \subseteq K$, whenever G is H-o-basis, G is also K-o-basis.

Since we do not want to refer to the linear algebra involved in Holmes' original definition of o-basis, we have introduced notation in the above definition which avoids reference to that material. Let us restate, for use later, the last part of Theorem 2.1.5 with our new notation.

Let $N \lhd G$, let $\chi \in Irr(G)$ and assume that $N \subseteq \ker \chi$. For a subgroup $H \leq G$, denote by $\widehat{H}$ the image of H under the canonical map $G \to G/N$. The function $\widehat{\chi} : \widehat{G} \to \mathbb{C}$ given

by $\widehat{\chi}(gN) = \chi(g)$ is a well-defined irreducible character of $\widehat{G}$ (see Theorem 1.3.2.5, (i) and (iii)).

Theorem 3.1.2 *Keeping the above notation, let $N \lhd G$ and let $\chi \in Irr(G)$ such that $N \subseteq ker(\chi)$. Let $H \leq G$. Then G is (H, χ)-o-basis if and only if $\widehat{G}$ is $(\widehat{H}, \widehat{\chi})$-o-basis.*

In the following lemma and its corollary, we obtain an upper bound on the number of orthogonal cosets. This will be critical in proving that certain groups are not o-basis.

Lemma 3.1.3 *Let $\chi \in Irr(G)$. Suppose that $H, K \leq G$ with $H \subseteq K$. Assume that no two cosets of H in K are orthogonal relative to B_H^χ. Then the number of cosets of H in G which are mutually orthogonal relative to B_H^χ is no greater than $|G : K|$.*

Proof: By assumtion, for $a, b \in K$ we have $0 \neq B_H^\chi\big(aH, bH\big) = \dfrac{\chi(e)}{|H|} \displaystyle\sum_{h \in H} \chi\big(a^{-1}bh\big)$. Suppose there are more than $|G : K|$ cosets of H in G which are orthogonal relative to B_H^χ. Then at least one coset of K in G contains two cosets of H which are orthogonal. More precisely, there exists $g \in G$ and $a, b \in K$ such that
$0 = B_H^\chi\big(gaH, gbH\big) = \dfrac{\chi(e)}{|H|} \displaystyle\sum_{h \in H} \chi\big(a^{-1}g^{-1}gbh\big) = \dfrac{\chi(e)}{|H|} \displaystyle\sum_{h \in H} \chi\big(a^{-1}bh\big)$, a contradiction.

□

Keeping the above notation, let aH and bH be two (not necessarily distinct) cosets of H in K which are orthogonal relative to B_H^χ. Then $0 = B_H^\chi(aH, bH) = \frac{\chi(e)}{|H|} \sum_{h \in H} \chi(a^{-1}bh)$ so that $\sum_{h \in H} \chi(kh) = 0$ for some $k \in K$. Conversely, let $k \in K$ such that $\sum_{h \in H} \chi(kh) = 0$. There exist $a, b \in K$ (a, b not necessarily distinct) such that $a^{-1}b = k$. Note that aH and bH are orthogonal relative to B_H^χ. In short, there are two (not necessarily distinct) cosets of H in K which are orthogonal relative to B_H^χ if and only if for some $k \in K$

(possibly $k = e$), $\sum_{h \in H} \chi(kh) = 0$. Now suppose $H = \langle e \rangle$. The cosets of H are the singleton sets $\{g\}$ ($g \in G$). In this case, the above statement becomes: there are two (not necessarily distinct) "orthogonal elements" in K relative to B_H^χ if and only if $\chi(k) = 0$ for some $k \in K$. We restate the special case of Lemma 3.1.3 when $H = \langle e \rangle$ as a corollary.

Corollary 3.1.4 *Let $\chi \in Irr(G)$ and $K \leq G$. Suppose $\chi(k) \neq 0$ for all $k \in K$. Then the number of cosets of $\langle e \rangle$ which are mutually orthogonal relative to $B_{\langle e \rangle}^\chi$ is no greater than $|G : K|$.*

We will often find it helpful to deal with quotients of G. The utility of this derives from the result below which follows from Proposition 1.3.2.5 and Theorem 3.1.2.

Theorem 3.1.5 *Let $N \lhd G$. Then G is N-o-basis if and only if G/N is o-basis.*

Proof: For $L \leq G$, let $\widehat{L}$ denote the image of L under the canonical map $G \to G/N$, and, for $\chi \in Irr(G)$ define $\widehat{\chi} : \widehat{G} \to \mathbb{C}$ by $\widehat{\chi}(gN) = \chi(g)$.

Assume that G is N-o-basis. Let $K \leq G/N$ and $\varphi \in Irr(G/N)$. By the Correspondance Theorem, $K = \widehat{H}$ for some $H \leq G$ with $N \subseteq H$. By Proposition 1.3.2.5 (ii) and (iii), $\varphi = \widehat{\chi}$ for some $\chi \in Irr(G)$. As G is N-o-basis, G is (H, χ)-o-basis. By Theorem 3.1.2, G/N is (K, φ)-o-basis. Since K, χ were chosen arbitrarily, this shows that G/N is o-basis.

Conversely, assume that G/N is o-basis. Let $H \leq G$ with $N \subseteq H$ and let $\chi \in Irr(G)$ such that $(\chi, 1)_H \neq 0$. Then $(\chi, 1)_N \neq 0$. Since $N \lhd G$, Theorem 1.3.3.4 gives that $N \subseteq \ker(\chi)$. Since G/N is o-basis, G/N is $(\widehat{H}, \widehat{\chi})$-o-basis. By Theorem 3.1.2, G is (H, χ)-o-basis and it follows that G is N-o-basis.

□

3.2 O-basis Groups and Nilpotency

In this section, we address two questions.

1) Which nilpotent groups are o-basis?

2) Are all o-basis groups nilpotent?

The possibility of a special connection between o-basis groups and nilpotentcy is implied by two facts. First, every group that has been identified as o-basis is also nilpotent (see Theorem 1.1.1). Second, the o-basis property picks out from the dihedrals exactly the nilpotent groups (see Theorem 1.1.3). Not all nilpotent groups are o-basis however. In [Hlms] (p.143), Holmes constructs an example of order 3^4 that is not o-basis. What conditions, then, on a nilpotent group are sufficient for the group to be o-basis? Our first result gives such a condition: that $G' \subseteq Z(G)$. Note that this condition implies nilpotentcy.

Theorem 3.2.1 *Suppose that $G' \subseteq Z(G)$. Then G is o-basis.*

Proof: Let $H \leq G$ and let $\chi \in Irr(G)$. For any subgroup $K \leq G$, let $\widehat{K}$ denote the image of K under the canonical map $G \to G/\ker\chi$. Define $\widehat{\chi} : \widehat{G} \to \mathbb{C}$ by $\widehat{\chi}(g\ker\chi) = \chi(g)$ for all $g \in G$. By Lemma 1.3.2.5, $\widehat{\chi} \in Irr(\widehat{G})$ and, by Theorem 3.1.2, G is (H, χ)-o-basis if and only if $\widehat{G}$ is $(\widehat{H}, \widehat{\chi})$-o-basis. It suffices, therefore, to show that $\widehat{G}$ is $(\widehat{H}, \widehat{\chi})$-o-basis. Note that $\ker(\widehat{\chi}) = \{e\}$

We first show that $\widehat{G}/Z(\widehat{\chi})$ is abelian. Note that $(\widehat{G})' \subseteq Z(\widehat{G})$. For since $G' \subseteq Z(G)$, we have $(\widehat{G})' = \widehat{G'} \subseteq \widehat{Z(G)} \subseteq \widehat{Z(\chi)} = Z(\widehat{G})$, where the last containment and equality follow respectively from Corollary 1.3.2.8 and Lemma 1.3.2.9. Also, $Z(\widehat{G}) = Z(\widehat{\chi})$. Indeed, Corollary 1.3.2.8 gives that $Z(\widehat{G}) \subseteq Z(\widehat{\chi})$. Conversely, suppose that $g\ker\chi \in Z(\widehat{\chi})$. Then $|\chi(g)| = |\widehat{\chi}(g\ker\chi)| = \widehat{\chi}(e\ker\chi) = \chi(e)$ so that $g\ker\chi \in \widehat{Z(\chi)} = Z(\widehat{G})$. This shows that $(\widehat{G})' \subseteq Z(\widehat{\chi})$ so that $\widehat{G}/Z(\widehat{\chi})$ is abelian as claimed. By Theorem 1.3.2.11, $\widehat{\chi}(e)^2 = |\widehat{G} : Z(\widehat{\chi})|$

and so, by Proposition 1.3.2.10, $\widehat{\chi} \equiv 0$ on $\widehat{G} - Z(\widehat{\chi})$. Since $Z(\widehat{\chi}) = Z(\widehat{G})$, we have $\widehat{\chi} \equiv 0$ on $\widehat{G} - Z(\widehat{G})$.

Assume that $(\widehat{\chi}, 1)_{\widehat{H}} \neq 0$. In this case, $(\widehat{\chi}, 1)_{\widehat{H} \cap Z(\widehat{G})} \neq 0$. As $\widehat{H} \cap Z(\widehat{G}) \lhd \widehat{G}$, Proposition 1.3.3.4 gives that $\widehat{H} \cap Z(\widehat{G}) \subseteq \ker(\widehat{\chi}) = \{e\}$. Since $\widehat{\chi} \equiv 0$ on $\widehat{G} - Z(\widehat{G})$ we have

$$(\widehat{\chi}, 1)_{\widehat{H}} = \frac{1}{|\widehat{H}|} \sum_{h \in \widehat{H}} \widehat{\chi}(h) = \frac{\widehat{\chi}(e)}{|\widehat{H}|}.$$

Therefore, $\widehat{\chi}(e)(\widehat{\chi}, 1)_{\widehat{H}} = \dfrac{\widehat{\chi}(e)^2}{|\widehat{H}|} = \dfrac{|\widehat{G} : Z(\widehat{G})|}{|\widehat{H}|} = \dfrac{|\widehat{G}|}{|Z(\widehat{G})| \cdot |\widehat{H}|} = |\widehat{G} : \widehat{H}Z(\widehat{G})|$, where the last equality holds since $\widehat{H} \cap Z(\widehat{G}) = \{e\}$. Let $\{a_i \widehat{H} Z(\widehat{G}) : 1 \leq i \leq t\}$ be a complete set of coset representatives of $\widehat{H}Z(\widehat{G})$ in $\widehat{G}$. Suppose $i \neq j$. Then, for all $h \in \widehat{H}$, $a_i^{-1} a_j h \notin Z(\widehat{G})$. Since $\widehat{\chi} \equiv 0$ on $\widehat{G} - Z(\widehat{G})$, $\widehat{\chi}(a_i^{-1} a_j h) = 0$ for each $h \in \widehat{H}$. Therefore,

$$B_{\widehat{H}}^{\widehat{\chi}}(a_i \widehat{H}, a_j \widehat{H}) = \frac{\widehat{\chi}(e)}{|\widehat{H}|} \sum_{h \in \widehat{H}} \widehat{\chi}(a_i^{-1} a_j h) = 0.$$

The $\widehat{\chi}(e)(\widehat{\chi}, 1)_{\widehat{H}}$ cosets $\{a_i \widehat{H} : 1 \leq i \leq t\}$ form a mutually orthogonal collection of cosets of $\widehat{H}$ in $\widehat{G}$. This shows that G is $(\widehat{H}, \widehat{\chi})$-o-basis and the proof is complete.

□

To obtain the following corollary to Theorem 3.2.1, we will use two lemmas.

Lemma 3.2.2 ***([Is], p.75, ex. 5.14(a))*** *Let G be non-abelian and let $f = min\{\chi(e) : \chi \in Irr(G), \chi(e) > 1\}$. If $|G'| \leq f$, then $G' \subseteq Z(G)$.*

Lemma 3.2.3 ***([Is], p.38)*** *Let $\chi \in Irr(G)$. Then $\chi(e)$ divides $|G|$.*

Corollary 3.2.4 *Suppose G is a p-group with $|G'| = p$. Then G is o-basis.*

Proof: Since $G' \neq \langle e \rangle$, G is non-abelian. By Theorem 1.3.2.3, G has non-linear irreducible characters. Let χ be an arbitrary non-linear irreducible character of G. By Theorem 3.2.3, $\chi(e)$ divides $|G|$ so that $\chi(e) \geq p$. Since χ was chosen arbitrarily and $|G'| = p \leq \chi(e)$, Lemma 3.2.2 gives that $G' \subseteq Z(G)$. By Theorem 3.2.1, G is o-basis.

□

We note that, in Corollary 3.2.4, one can easily show that $G' \subseteq Z(G)$ without using characters. However, our approach has the advantage of giving the reader further exposure to elementary character theory.

We will have occasion to call upon Theorem 3.2.1 in several results. We will also give a slight generalization the theorem (Theorem 3.3.5). In addition to this, Theorem 3.2.1 raises an interesting question for possible future study. Any group with $G' \subseteq Z(G)$ has nilpotence class no greater than 3 (see the definition of the lower central series in the notation). Holmes' example of order 3^4 that is not o-basis is easily seen to have nilpotence class 4. We ask if nilpotence class less than or equal to 3 is a necessary condition for a nilpotent group to be o-basis. This is an open question, and one the author looks forward to considering in the future.

In studying nilpotent groups one might wish to narrow the focus by concentrating on p-groups. In our next result, we find that there is some valid grounds for doing so. More precisely, we show that a nilpotent group is o-basis precisely when each of its Sylow subgroups is o-basis. Before proving this, we remind the reader of some basic information about Sylow subgroups.

Definition 3.2.5 *Let p be a prime and let G be a group. A* ***p-subgroup*** *of G is a subgroup whose order (cardinality as a set) is a power of p. A* ***Sylow p-subgroup*** *is a p-subgroup that is not properly contained in any other p-subgroup.*

Thus a Sylow p-subgroup is a maximal p-subgroup. The reader may recall that, given a prime p, if a Sylow p-subgroup is normal in G, then it is the unique Sylow p-subgroup of G for that prime. Our result for nilpotent groups depends heavily on Lemma 3.2.6 below.

Lemma 3.2.6 ***([Rob], p.134 ex. 12)*** *For $1 \leq i \leq n$, let p_i denote a prime such that $p_i \neq p_j$ whenever $i \neq j$ and let G_i denote a p_i-group . Let $G = \prod_{i=1}^{n} G_i$, the direct product of the G_i. Let $H \leq G$. Then $H = \prod_{i=1}^{n} H_i$, where $H_i = H \cap G_i$.*

Theorem 3.2.7 ***([Rob], p.126)****Let G be a finite group. Then G is nilpotent if and only if G is the direct product of its Sylow subgroups.*

Theorem 3.2.8 *Assume that G is nilpotent. Then G is o-basis if and only if every Sylow subgroup of G is o-basis.*

Proof: Let $\{P_i\}_{i=1}^{m}$ be the distinct Sylow subgroups of G. By Theorem 3.2.7, $G = \prod_{i=1}^{m} P_i$. Suppose that G is o-basis and fix $1 \leq j \leq m$. Put $D = \prod_{i=1, i\neq j}^{m} P_i$. Note that $D \lhd G$ and let $\pi : G \to G/D$ denote the canonical map. Then $\pi(G) = P_j$. Theorem 2.1.6 gives that P_j is o-basis. As j was chosen arbitrarily, the forward direction is proved.

Suppose now that P_i is o-basis for each $1 \leq i \leq m$. Let $H \leq G$ and let $\chi \in Irr(G)$ be non-linear such that $(\chi, 1)_H \neq 0$ (see Definition 2.1.3). For each i, put $p_i = |P_i|$ (so p_i is a prime). Since $P_i \lhd G$, P_i is the unique p_i-subgroup of G. It follows that $p_i \neq p_j$ whenever $i \neq j$. Therefore, Lemma 3.2.6 gives that $H = \prod_{i=1}^{m} H_i$, where $H_i = H \cap P_i$. Also,

Theorem 1.3.3.2 gives that $\chi = \chi_1 \cdots \chi_m$, where $\chi_i \in Irr(P_i)$ is extended to G by putting $\chi_i(\prod_{j=1}^m g_j) = \chi_i(g_i)$.

For convenience, let $g_1 \cdots g_m$ denote the element $(g_1, \ldots, g_m) \in G$. Let $a = a_1 \cdots a_m$ and $b = b_1 \cdots b_m$ be elements of G. We claim that

$$B_H^{\chi}(aH, bH) = B_{H_1}^{\chi_1}(a_1H_1, b_1H_1) \cdots B_{H_m}^{\chi_m}(a_mH_m, b_mH_m). \tag{3.1}$$

Proceed by induction on m. The formula is obvious for the case $m = 1$. Therefore, fix $m > 1$. Put $\hat{H} = \prod_{i=1}^{m-1} H_i$, $\hat{G} = \prod_{i=1}^{m-1} P_i$, $\hat{\chi} = \chi_1 \cdots \chi_{m-1}$, $\hat{a} = a_1 \cdots a_{m-1}$, and $\hat{b} = b_1 \cdots b_{m-1}$. Note that $\hat{\chi} \in Irr(\hat{G})$ and assume

$B_{\hat{H}}^{\hat{\chi}}(\hat{a}\hat{H}, \hat{b}\hat{H}) = B_{H_1}^{\chi_1}(a_1H_1, b_1, H_1) \cdots B_{H_{m-1}}^{\chi_{m-1}}(a_{m-1}H_{m-1}, b_{m-1}H_{m-1})$.

We have,

$$\begin{aligned}
& B_H^{\chi}(aH, bH) = \frac{\chi(e)}{|H|} \sum_{h \in H} \chi(a^{-1}bh) \\
= \; & \frac{\chi_1(e) \cdots \chi_m(e)}{|H_1| \cdots |H_m|} \sum_{h_1 \cdots h_m \in H} \chi(a_1^{-1}b_1h_1 \cdots a_m^{-1}b_mh_m) \\
= \; & \frac{\chi_1(e) \cdots \chi_m(e)}{|H_1| \cdots |H_m|} \sum_{h_1 \cdots h_m \in H} \chi_1(a_1^{-1}b_1h_1) \cdots \chi_m(a_m^{-1}b_mh_m) \\
= \; & \frac{\chi_m(e)}{|H_m|} \sum_{h_m \in H_m} \left[\chi_m(a_m^{-1}b_mh_m) \frac{\hat{\chi}(e)}{|\hat{H}|} \sum_{h \in \hat{H}} \hat{\chi}(\hat{a}^{-1}\hat{b}h) \right] \\
= \; & \frac{\chi_m(e)}{|H_m|} \sum_{h_m \in H_m} \chi_m(a_m^{-1}b_mh_m) B_{H_1}^{\chi_1}(a_1H_1, b_1H_1) \cdots B_{H_{m-1}}^{\chi_{m-1}}(a_{m-1}H_{m-1}, b_{m-1}H_{m-1}) \\
= \; & B_{H_1}^{\chi_1}(a_1H_1, b_1H_1) \cdots B_{H_m}^{\chi_m}(a_mH_m, b_mH_m),
\end{aligned}$$

where the next to last equality follows from by the induction hypothesis. The claim follows.

Also observe that

$$\begin{aligned}\chi(e)(\chi,1)_H = \frac{\chi(e)}{|H|}\sum_{h\in H}\chi(h) &= \frac{\chi(e)}{|H|}\sum_{h\in H}\chi(a^{-1}ah)\\ &= B_H^{\chi}(aH,aH)\\ &= B_{H_1}^{\chi_1}(a_1H_1,a_1H_1)\cdots B_{H_m}^{\chi_m}(a_mH_m,a_mH_m)\\ &= \chi_1(e)(\chi_1,1)_{H_1}\cdots\chi_m(e)(\chi_m,1)_{H_m},\end{aligned}$$

where the next to last equality follows from equation 3.1. Thus, we have

$$\chi(e)(\chi,1)_H = \chi_1(e)(\chi_1,1)_{H_1}\cdots\chi_m(e)(\chi_m,1)_{H_m}. \tag{3.2}$$

For each $1 \leq i \leq m$, let A_i denote a set (non-empty, as will be shown) of distinct cosets representatives of H_i in P_i such that $B_{H_i}^{\chi_i}(aH_i,bH_i) = 0$ whenever $a,b \in A_i$ with $a \neq b$. Since $(\chi,1)_H \neq 0$, equation 3.2 gives that $(\chi_i,1)_{H_i} \neq 0$ for all i. Since P_i is o-basis, we may assume that A_i contains at least $\chi_i(e)(\chi_i,1)_{H_i}$ elements.

Now let $a = a_1\cdots a_m$ and $b = b_1\cdots b_m$ be elements of G with $a \neq b$ such that $a_i, b_i \in A_i$ for each i. As $a \neq b$, there is at least one i such that $a_i \neq b_i$. Then, by definition of A_i, $B_{H_i}^{\chi_i}(a_iH,b_iH) = 0$. It follows from equation 3.1 that $B_H^{\chi}(aH,bH) = 0$. We see that the set cartesian product $A_1 \times \cdots \times A_m$ forms a collection of coset representatives of H in G that are mutually orthogonal relative to B_H^{χ}. The cardinality of this collection is $\chi_1(e)(\chi_1,1)_{H_1}\cdots\chi_m(e)(\chi_m,1)_{H_m}$, and we have already noted that this last quantity is equal to $\chi(e)(\chi,1)_H$. Thus G has an (H,χ)-o-basis. It follows that G is o-basis as desired.

□

Suppose G is a direct product of a finite number of groups. It follows immediately from Theorem 2.1.6 that whenever G is o-basis, each of the direct factors is o-basis as well. The truth or falsity of the converse however remains an open question. Critical to the converse

in the above argument is the fact that the primes of the distinct Sylow subgroups are all distinct. Lemma 3.2.6 then gives that any subgroup is the direct product of its intersection with the factors. The absence of this property for subgroups of general direct products has been the primary obstacle to the analogous result for that case. For example, it is suspected (but not proven) that the "diagonal" subgroup could fail for some non-linear character.

In light of the above result, we see that the question of which o-basis groups are nilpotent can be "reduced" in some sense to that of which prime power groups are o-basis. Let us briefly consider this. Suppose p is a prime. Since any group of order p^2 is abelian, Theorem 2.1.4 gives that any such group is o-basis. Holmes' has shown that any group of order p^3 is o-basis (see Theorem 1.1.1). However, in [Hlms], Holmes also provided an example of order 3^4 that is not o-basis. We take a closer look at groups of order p^4 beginning with the fact that any such group G is $Z(G)$-o-basis (see Definition 3.1.1).

Theorem 3.2.9 *Suppose that $|G| = p^4$. Then G is $Z(G)$-o-basis. That is, every group of order p^4 is Z-o-basis.*

Proof: Since G is a p-group, we have by Theorem 1.2.4 that $Z(G)$ is non-trivial. Thus $|G/Z| \leq p^3$. If $|G/Z| \leq p^2$, then G/Z is abelian and so o-basis by Theorem 1.1.1 (i). Suppose that $|G/Z| = p^3$. Then G/Z is o-basis by Theorem 1.1.1 (iv). By Theorem 3.1.5, G is Z-o-basis if and only if G/Z is o-basis, and the result follows.

□

Which groups of order p^4 are o-basis? We explore this question as follows. Suppose G is a group of p^4 that is not o-basis. Then there exists a subgroup $H \leq G$ and $\chi \in Irr(G)$ such that G is not (H, χ)-o-basis. We derive some necessary conditions on H, χ and G. We will have need of the following two lemmas.

Lemma 3.2.10 ***([Is] p.204)*** *Let $A \lhd G$ with A abelian and G/A cyclic. Then $|A| = |G'| \cdot |A \cap Z(G)|$.*

Theorem 3.2.11 *([Karp], p.803) Let χ be an irreducible character of a nilpotent group G. Then $\chi(e)^2$ divides $|G : Z(\chi)|$.*

Theorem 3.2.12 *Let p be prime and suppose $|G| = p^4$. Let $\chi \in Irr(G)$ and let $H \leq G$ such that G is not (H, χ)-o-basis. Then the following hold.*

(i) $|Z(G)| = p$,

(ii) χ *is faithful and* $\chi(e) = p$,

(iii) *There exist $A \lhd G$ with A abelian and $|G : A| = p$.*

Also, $\chi \equiv 0$ on $G - A$.

(iv) $Z(G) \leq G' \leq A$ *and* $|A : G'| = |G' : Z(G)| = p$,

(v) *If $\chi(a) = 0$ for some $a \in G'$, then $\chi \equiv 0$ on $G' - Z(G)$. In this case,*

$H \not\lhd G$.

Proof: Throughout, let Z denote the center of G and K the kernel of χ. Suppose first that $|Z| \geq p^2$. Then G/Z is a p-group with order no greater than p^2. It follows that G/Z is abelian so that $G' \subseteq Z$. By Theorem 3.2.1, G is o-basis, a contradiction. By Theorem 1.2.4, $|Z| > 1$. Thus, $|Z| = p$ and (i) is established.

For the first condition of (ii), suppose, in view of a contradiction, that $K \neq \{e\}$. As $K \lhd G$, we have by Theorem 1.2.5 that $K \cap Z \neq \{e\}$. Since $|Z| = p$, it follows that $Z \subseteq K$. Define $\widehat{\chi} : G/Z \to \mathbb{C}$ by putting $\widehat{\chi}(gZ) = \chi(g)$ for all $g \in G$. Since $Z \subseteq K$, Proposition 1.3.2.5 gives that $\widehat{\chi} \in Irr(G/Z)$. By Theorem 3.2.9, G is Z-o-basis. Thus G/Z is o-basis by Theorem 3.1.5 so that G/Z has a $(\pi(H), \widehat{\chi})$-o-basis, where $\pi : G \to G/Z$ is

the canonical map. It follows from Theorem 3.1.2 that G is (H, χ)-o-basis, contrary to our assumption. This shows that χ is faithful.

Recalling that all p-groups are nilpotent, we see from Theorem 3.2.11 that $\chi(e)^2$ divides $|G : Z(\chi)|$. By Corollary 1.3.2.8, $Z(\chi) \supseteq Z(G) \neq \{e\}$ so that $|G : Z(\chi)| \leq p^3$. Since χ is non-linear, $\chi(e) = p$, and (ii) is fully established. By Theorem 1.3.3.14, G is an M-group. Choose a subgroup A of G and linear character $\varphi \in Irr(A)$ such that $\chi = \varphi^G$. We have $p = \chi(e) = \varphi^G(e) = |G : A|\varphi(e) = |G : A|$ (see remark after Definition 1.3.3.5). Note that A is a maximal subgroup of G. For suppose $L \leq G$ with $A \leq L \leq G$. Then $p = |G : A| = |G : L| \cdot |L : A|$. Either $|G : L| = 1$ so that $L = G$ or $|L : A| = 1$ so that $L = A$. By Theorem 1.2.6, $A \lhd G$. Thus, $\chi \equiv 0$ on $G \setminus A$. (see comments after Definition 1.3.3.5) For (iii), it remains to show that A is abelian. Note that $|\chi(z)| = \chi(e) \neq 0$ for all $z \in Z(\chi)$. Since $\chi \equiv 0$ on $G - A$, $Z(\chi) \subseteq A$ so that, by Corollary 1.3.2.8, $Z(G) \subseteq A$. Suppose that A is not abelian. As $|A| = p^3$, A is extra-special (see Definition 1.2.7 and remarks). We have that $Z(A) = A'$ and $|Z(A)| = p$. Since $Z(G) \subseteq A$, if follows that $Z(G) \subseteq Z(A)$. Thus, as $|Z(G)| = p$, we have that $Z(A) = Z(G)$. Since φ is linear, $Z(A) = A' \subseteq \ker \varphi$, the last containment being given by Proposition 1.3.2.6. By Lemma 1.3.3.6, $\ker \chi = \bigcap_{x \in G} (\ker \varphi)^x$. If follows that $Z \subseteq \ker \chi$, a contradiction since χ is faithful. As claimed therefore, A is abelian and the proof of (iii) is complete.

By Lemma 3.2.10, $p^3 = |A| = |Z(G)| \cdot |G'| = p|G'|$ so that $|G'| = p^2$. By Theorem 1.2.5, $Z(G) \subseteq G'$. Also, since $A \lhd G$ and G/A is abelian, we have that $G' \subseteq A$. This establishes (iv).

Suppose that G' is cyclic. Then putting $C = G'$ in Theorem 2.1.2, we see that G is o-basis, a contradiction. Thus G' cannot be cyclic. It follows that $G' \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Thus,

every proper, non-trivial subgroup of G' has order p. Since no two of these subgroups can intersect non-trivially, there are $p+1$ such subgroups and G' is their union. Since G is a p-group, every non-trivial, normal subgroup must intersect the center non-trivially. If follows that $Z(G)$ is the only normal subgroup of G having order p. Therefore, $Z(G)$ is the only subgroup of G' that is normal in G. Since $G' \subseteq A$ and A is abelian, G/A acts on the subgroups of G' by conjugation. For any given subgroup, the order of the orbit under this action is either 1 or p. Moreover, any subgroup having orbit of size 1 is normal in G. It follows that G/A acts transitively on the p non-central subgroups of G'.

For (v), suppose that $\chi(a) = 0$ for some $a \in G'$. Then $a \notin Z(G)$ since $Z(G) \subseteq Z(\chi)$ (Theorem 1.3.2.8). Put $K = \langle a \rangle$. Then χ_K is a character of K. Putting $\chi_K = \varphi$ in Proposition 1.3.2.12, it follows, since $|K| = p$, that $\chi \equiv 0$ on $K - \langle e \rangle$. Since G acts transitively on the p non-central subgroups of G', we see that $G - Z(G)$ is the union of the conjugates of K. Recalling that character values are invariant under conjugation (see the discussion on class functions in section 1.3.1) we have that $\chi \equiv 0$ on $G' - Z(G)$, as claimed in (v). Since G is not (H, χ)-o-basis, it follows from the definition that $(\chi, 1)_H \neq 0$. Suppose, to obtain a contradiction, that $H \lhd G$. Then $H \subseteq \ker \chi$ by Theorem 1.3.3.4 so that $H = \langle e \rangle$. Let $\{a_i : 1 \leq i \leq p\}$ and $\{g_i : 1 \leq i \leq p\}$ be complete sets of coset representatives of Z in G' and of A in G respectively. Put $S = \{g_j a_i : 1 \leq i, j \leq p\}$. Choose $g_{j_1} a_{i_i}, g_{j_2} a_{i_2} \in S$ and put $y = a_{i_1}^{-1} g_{j_1}^{-1} g_{j_2} a_{i_2}$. We have $B_H^\chi(g_{j_1} a_{i_i} H, g_{j_2} a_{i_2} H) = \chi(e)\chi(y)$. If $j_1 \neq j_2$, then $y \in G - A$ and $\chi(y) = 0$. If $j_1 = j_2$, then $y = a_{i_1}^{-1} a_{i_2} \in G' - Z$ and $\chi(y) = 0$. This gives $|S| = p^2$ cosets of H which are mutually orthogonal relative to B_H^χ. Finally, note that $\chi(e)(\chi, 1)_H = \chi(e)^2 = p^2$. This shows that G is (H, χ)-o-basis, a contradiction. It follows that $H \not\lhd G$ and the proof is complete.

□

All of the results so far in this section have dealt with the first of two questions posed at its beginning. Namely, which nilpotent groups are o-basis. Let us now turn to the second question. Are all o-basis groups nilpotent? With the dihedrals in mind, we will consider our second question for a particular class of "dihedral-like" groups. Every dihedral group has a cyclic normal subgroup of index 2. We consider those groups G having an abelian normal subgroup A of index p^n, where p is a prime and $n \geq 1$. Let us state our question as a conjecture.

Conjecture 3.2.13 *Let p be prime and $A \lhd G$ be abelian such that $|G : A| = p^n$ for some positive integer n. Suppose that G is o-basis. Then G is nilpotent.*

We are able to prove the conjecture in the case that G/A is abelian (Theorem 3.2.17). When G/A is non-abelian, we show the answer is still affirmative when $n = 3$ in Theorem 3.2.20. In Theorem 3.2.21, we obtain the conjecture for the case $n = 4$, but only after adding some additional conditions. Finally, we show that nilpotency is a necessary and sufficient condition for o-basisness when A is cyclic and $n = 1$. The following three lemmas set the stage.

Lemma 3.2.14 *Let p be prime and $A \lhd G$ be abelian with $|G : A| = p^n$ for some $n \geq 1$. Assume that G is not nilpotent. Then there is an integer $m \geq 1$ such that the following hold:*

(i) G/Z_m *is not abelian,*

(ii) $AZ_m/Z_m \lhd G/Z_m$ *is abelian,*

(iii) $|G/Z_m : AZ_m/Z_m| = p^k$ *for some* $k \geq 1$,

(iv) $\big(|G/Z_m : AZ_m/Z_m|, |AZ_m/Z_m|\big) = 1$.

Proof: Assume G is not nilpotent. Then there is an integer $m \geq 1$ such that $Z_m = Z_{m+i}$, for all $i \geq 0$ and $G \neq Z_m$. Fix such an m and note that $G/Z_m \neq \langle e \rangle$ and $Z(G/Z_m) = \langle e \rangle$. Since $AZ_m \lhd G$, the Correspondance Theorem gives that $AZ_m/Z_m \lhd G/Z_m$. Also, $AZ_m/Z_m \cong A/(A \cap Z_m)$. The latter is abelian, being the homomorphic image of an abelian group. This verifies (i). Observe that $Z_m \not\supseteq A$. Indeed, suppose that $Z_m \supseteq A$. Then $G/Z_m \cong (G/A)/(Z_m/A)$. The latter is a p-group since we have assumed G/A is a p-group. Therefore, $Z(G/Z_m) \neq \langle e \rangle$, a contradiction. It follows that AZ_m/Z_m is a non-trivial subgroup of G/Z_m with $|G/Z_m : AZ_m/Z_m| = |G : AZ_m|$. Now note that this last quantity divides $|G : A|$ and is therefore equal to p^k for some $k \geq 0$. If $k = 0$, then $G/Z_m = AZ_m/Z_m$. In this case, G/Z_m is abelian by (i). This again contradicts the fact that $Z(G/Z_m) = \langle e \rangle$. Therefore, $k > 0$ and (ii) is established.

Let T denote the quotient group G/AZ_m. There is a well-defined action of T on $(AZ_m)/Z_m$ given by conjugation and $Z(G/Z_m)$ is precisely the set, $(AZ_m/Z_m)^T$, of fixed points of AZ_m/Z_m under this action. Theorem 1.2.1 gives that

$1 = |Z(G/Z_m)| = |(AZ_m/Z_m)^T| \equiv |AZ_m/Z_m| \pmod{p}$.

Thus $(|AZ_m|, |G/Z_m : AZ_m/Z_m|) = 1$ and (iii) is established.

□

Lemma 3.2.15 *Let p be prime and $A \lhd G$ be abelian such that $|G : A| = p^n$ for some integer $n \geq 1$. Assume that G is not nilpotent. Then there exists $K \lhd G$ such that the following hold:*

(i) G/K *is a non-abelian internal semidirect product of* $AK/K \rtimes T$, *where* $T \cong (G/K)/\big(AK/K\big)$,

(ii) $|G/K : AK/K| = p^n$ *for some* $n \geq 1$, *and*

(iii) AK/K *is a non-trivial elementary abelian* q*-group for some prime* q *distinct from* p.

Proof: Since G is not nilpotent, Lemma 3.2.14 applies. Choose an integer m satisfying the conclusions of Lemma 3.2.14. Suppose we are able to construct a normal subgroup K of G/Z_m with $K \subseteq AZ_m/Z_m$ such that K satisfies (i) - (iii) above for G/Z_m. Then the Correspondance Theorem gives a normal subgroup $\overline{K}$ of G which also satisfies properties (i) - (iii). If, in addition, G/Z_m possessed the properties assumed of G, there would be no loss of generality in working with G/Z_m rather G. Since G/Z_m also possesses property (iii) of Lemma 3.2.14, this would be to our advantage. Let us note that, by (i) and (ii) of Lemma 3.2.14, G/Z_m does indeed possess the properties assumed here of G. Thus, we may, with loss generality, identify G with G/Z_m, A with AZ_m/Z_m and assume, by 3.2.14 (iii), that $(|A|, p) = 1$.

Denote by Q the set of prime divisors of $|A|$. Since A is abelian, every subgroup of A is normal in A. In particular, any Sylow subgroup of A is normal in A and is therefore unique. For $q \in Q$, denote by A_q the unique S_q subgroup of A and put $D_q = \prod_{\substack{r \in Q \\ r \neq q}} A_r$ if $|Q| > 1$. If $|Q| = 1$, put $D_q = \langle e \rangle$. Note that $A_q \lhd G$ for all $q \in Q$. Indeed, choose $g \in G$. Since $A \lhd G$, $(A_q)^g \subseteq A$. Also, $|(A_q)^g| = |A_q|$ so that $(A_q)^g$ is also a Sylow q-subgroup of A. By uniqueness, $(A_q)^g = A_q$. Now fix $q \in Q$. Since A is nilpotent, it is the direct product of

its Sylow subgroups so that $D_q \leq A$. It follows from the above discussion that each direct summand of $D_q \lhd G$ so that $D_q \lhd G$. Note that, since $(|A|, p) = 1$, $q \neq p$.

For each subset $S \subseteq G$, denote by $\widehat{S}$ the image of S under the canonical map $G \to G/D_q$. Note that $\widehat{A}$ is a non-trivial abelian q-group. We are ready to establish (iii). The Fundamental Theorem of Finitely Generated Abelian Groups gives that $\widehat{A} = \prod_{i=1}^{k} A_i$, where $A_i \cong \mathbb{Z}_{q^{m_i}}$ and $m_i \geq 1$ for all i. Put $\overline{m} = \max\{m_i\}_{1 \leq i \leq k}$. Define subgroups B_i of $\widehat{A}$ as follows: let $B_i = A_i$ whenever $m_i < \overline{m}$, let B_i be the unique subgroup of A_i of order $q^{m_i - 1}$ whenever $m_i = \overline{m}$. Put $B = \prod_{i=1}^{k} B_i$. Observe that B char $\widehat{A}$. To see this, fix $1 \leq i \leq k$ and choose b_i such that $B_i = \langle b_i \rangle$. Let $\sigma \in \mathrm{Aut}(\widehat{A})$. It suffices to show that $b_i^{\sigma} \in B$. We write $b_i^{\sigma} = \prod_{i=1}^{k} a_i$, where $a_i \in A_i$ and calculate

$$q^{\overline{m}} > |b_i| = |b_i^{\sigma}| = \left| \prod_{i=1}^{k} a_i \right| = \mathrm{lcm}\{|a_i| : 1 \leq i \leq k\}.$$

Therefore, $|a_i| < q^{\overline{m}}$ so that $a_i \in B_i$ and $b_i^{\sigma} \in B$, as desired. By Theorem 1.2.3, $B \lhd G$. It follows that there is a subgroup $K \lhd G$, such that $G/K \cong \big(G/D_q\big)/B$. Since $B \subsetneq \widehat{A}$, we have $|G/K : A/K| = |G : A|$ so that (ii) holds. Also $A/K \cong \widehat{A}/B$ and $\widehat{A}/B$ is an elementary abelian q-group so that (iii) holds. Finally, since $(|A/K|, p) = 1$, conclusion (i) follows from Theorem 1.3.4.3. The proof is complete.

□

Theorem 3.2.16 *Let p, q be distinct primes. Let $A \lhd G$ be an elementary abelian q-group with $|G : A| = p^n$ for some integer $n \geq 1$. Suppose $\chi \in Irr(G)$ is non-linear. Then $\chi(a) \neq 0$ for all $a \in A$.*

Proof: Let $a \in A$ and assume that $\chi(a) = 0$. Put $L = \langle a \rangle$. Note that χ_L is a character of L (see Definition 1.3.3.3). Since A is elementary abelian, $L \cong \mathbb{Z}_q$ (see Defintion 1.2.10). Therefore, for each $b \in L$ with $b \neq e$, we have that $b = a^i$, where $(i, q) = 1$. Putting $\chi_L = \varphi$ in Proposition 1.3.2.12, gives that χ vanishes on $L - \{e\}$.

We have $(\chi_L, \chi_L)_L = \dfrac{1}{|L|} \sum_{l \in L} |\chi(l)|^2 = \dfrac{\chi(e)^2}{|L|} = \dfrac{\chi(e)^2}{q}$. By Proposition 1.3.1.10, this last quantity should be an integer. However, by Theorem 1.3.2.13, $\chi(e)$ divides $|G : A|$, a power of p. This is a contradiction. It follows that $\chi(a) \neq 0$ for all $a \in A$.

□

Case 1: G/A **is abelian.**

Theorem 3.2.17 *Let p be prime and $A \lhd G$ be abelian such that $|G : A| = p^n$ for some integer $n \geq 1$. Assume also that G/A is abelian. If G is o-basis then G is nilpotent.*

Proof: We prove the contrapositive. Assume that G is not nilpotent. We show that G is not o-basis. Note that Theorem 3.2.14 applies and choose an integer m such that the conclusions of that theorem hold. By Theorem 2.1.6, it suffices to show that G/Z_m is not o-basis. By the Third Isomorphism Theorem, $(G/Z_m)/(AZ_m/Z_m) \cong G/(AZ_m)$. The latter is a quotient of G/A and so abelian. It follows that $G' \subseteq AZ_m$ so that $(G/Z_m)' \subseteq AZ_m/Z_m$.

Note that $\big(G/Z_m\big)' \subseteq AZ_m/Z_m$. This, along with 3.2.14 (ii) and (iii), shows that G/Z_m has all the properties we have assumed of G. Without loss of generality, we replace G with G/Z_m, A with AZ_m/Z_m and assume, citing 3.2.14 (iii), that $(|A|, p) = 1$.

Because G is non-abelian (see 3.2.14 (i)), there are normal subgroups of G with non-abelian quotient, the identity comprising one such subgroup. Since G is finite, we may choose from among the set of such subgroups one that is maximal with respect to containment. Let us make such a choice and call the subgroup K. Observe that every non-trivial,

normal subgroup of G/K contains $\big(G/K\big)'$. For suppose H is a non-trivial, normal subgroup of G/K that does not contain $(G/K)'$. Then $H = \overline{H}/K$ for some normal subgroup $\overline{H}$ of G, where $\overline{H} \supsetneq K$. Recalling that $(G/K)' = G'K/K$, we have $\overline{H} \not\supseteq G'$. It follows that $G/\overline{H}$ is non-abelian, contradicting the maximality of K. Therefore, $(G/K)'$ is the unique minimal (non-trivial) normal subgroup of G/K. In addition, since $G' \subseteq A$, G' is abelian. It follows that G is solvable so that G/K is solvable. These arguments show that G/K satisfies the hypotheses of Lemma 1.3.5.4. Since G/K is non-abelian and $G' \subseteq A$, we have that $K \not\supseteq A$. Thus AK/K is a nontrivial subgroup of G/K. Since $(|A|, p) = 1$, G/K is not a p-group. Conclusion (b) of Lemma 1.3.5.4 therefore applies. We have that G/K is a Frobenius group having Frobenius kernel $(G/K)' \subseteq AK/K$ and that $(G/K)'$ is an elementary abelian q-group for some prime q. Since $(|A|, p) = 1$, $q \neq p$.

By Theorem 2.1.6, it is enough to show that G/K is not o-basis. Recalling that G/K is non-abelian, fix a non-linear $\chi \in Irr(G/K)$.

Note that $\ker \chi \not\supseteq (G/K)'$ (see remarks after Proposition 1.3.2.5). Theorem 1.3.5.3 (b) gives that $\chi = \phi^{G/K}$ for some $\phi \in Irr((G/K)')$. Now $\chi(e) = \phi^{G/K}(e) = |G/K : (G/K)'| \cdot \phi(e) = |G/K : (G/K)'|$, where the last equality holds since ϕ is linear ($(G/K)'$ being abelian).

By Theorem 1.3.2.13, $|G/K : (G/K)'|$ divides $|G/K : AK/K|$. But $|G/K : AK/K|$ divides $|G/K : (G/K)'|$ since $(G/K)' \subseteq AK/K$. Thus the indices are equal, $AK/K = (G/K)'$ and $\chi(e) = |G/K : AK/K|$. Since AK/K is proper and elementary abelian, Theorem 3.2.16 gives that χ never vanishes on AK/K. Put $H = \langle e \rangle$. For G/K to be (H, χ)-o-basis, there must be as least $\chi(e)^2 = |G/K : AK/K|^2$ orthogonal cosets of H in G/K relative to B_H^χ. However, since χ never vanishes on AK/K, Corollary 3.1.4 gives that there are at most $|G/K : AK/K|$ such cosets. This shows that G/K is not o-basis and completes the proof.

□

Case II: G/A is not abelian.

We now turn to the situation where G/A is not abelian. Note that, in this case, $|G : A| \geq p^3$. In Lemma 3.2.18 and Theorem 3.2.19 below, we will assume that G is a semi-direct product. We refer the reader to section 1.3.4 for a discussion of semi-direct products and we adopt here the notation of that section.

Lemma 3.2.18 *Let p, q be distinct primes. Let $G = A \rtimes T$ be an internal semi-direct product. Assume that A is an elementary abelian q-group and that $|T| = p^n$ for some $n \geq 1$. Suppose that, for some $\lambda \in Irr(A)$, $|T_\lambda| = p^k$, where $0 \leq k < \frac{n}{2}$. Then G is not o-basis.*

Proof: Let $\rho \in Irr(T_\lambda)$, put $H = AT_\lambda$ and $\chi = \theta_{\lambda,\rho}$. We show that G is not $\big(\langle e \rangle, \chi\big)$-o-basis. We have $\chi(e) = |G : H| \cdot \theta_{\lambda,\rho}(e) \geq |G : H| = p^{n-k}$. Since $n > k$, χ is non-linear. By Theorem 3.2.16, χ never vanishes on A. Applying Corollary 3.1.4 with $K = A$ gives that the number of cosets of $\langle e \rangle$ which are orthogonal relative to $B^{\chi}_{\langle e \rangle}$ is no greater than $|G : A|$. However, the required number of cosets is $\chi(e)(\chi, 1)_{\langle e \rangle} = \chi(e)^2 \geq p^{2n-2k} > p^n = |G : A|$.

□

Theorem 3.2.19 *Let p, q be distinct primes. Let $G = A \rtimes T$ be an internal semi-direct product. Assume that A is an elementary abelian q-group and that $|T| = p^n$ for some $n \geq 1$. Suppose there exists $\lambda \in Irr(A)$ such that T_λ is a proper, normal subgroup of T. Then G is not o-basis.*

Proof: Choose $\lambda \in Irr(A)$ satisfying the hypotheses. Let $\rho = 1_{T_\lambda}$, put $H = AT_\lambda$ and $\chi = \theta_{\lambda,\rho} := (\lambda\tilde{\rho})^G$ (for convenience, we will suppress the subscript and write simply θ).

Note that $\chi(e) = |G : H| \cdot (\lambda\tilde{\rho})(e) \geq |G : H|$. We show that $\chi(h) \neq 0$ for all $h \in H$. Since $T_\lambda \lhd T$, the Correspondance Theorem gives that $H \lhd G$. We may therefore apply Clifford's Theorem (Theorem 1.3.3.9) to χ_H. By Frobenius Reciprocity (Theorem 1.3.3.12), $(\chi_H, \lambda\tilde{\rho})_H = (\chi, \theta)_G = (\chi, \chi)_G = 1$. Let $at \in H$, where $a \in A$ and $t \in T_\lambda$. Observe that

$$\chi_H(at) = (\chi, \theta)_H \sum_{s \in \Omega} {}^s\theta(at) = \sum_{s \in \Omega} \theta(sats^{-1}) = \sum_{s \in \Omega} \theta((sas^{-1})(sts^{-1}))$$

where Ω is a complete set of coset representatives of H in G. Since we are free to choose any such set, we choose Ω to be a complete set of representatives for T_λ in T. Since $s \in T$, we have $sts^{-1} \in T$ so that $\theta((sas^{-1})(sts^{-1})) = \lambda(sas^{-1})\tilde{\rho}(sts^{-1})$. Now recalling that $T_\lambda \lhd T$, we have $sts^{-1} \in T_\lambda$ for each $s \in \Omega$ so that $\tilde{\rho}(sts^{-1}) = \rho(sts^{-1}) = 1$, where the last equality holds since $\rho = 1_{T_\lambda}$. The above sum then becomes $\sum_{s \in \Omega} \lambda^s(a)$. Putting $t = e$ in the above computation shows that this last sum is actually $\chi(a)$. By Theorem 3.2.16, $\chi(a) \neq 0$. We have, therefore, shown that χ never vanishes on H. By Theorem 3.1.4, there are at most $|G : H|$ cosets of $\langle e \rangle$ which are orthogonal relative to $B^\chi_{\langle e \rangle}$. But the required number of orthogonal cosets is $\chi(e)(\chi, 1)_{\langle e \rangle} = \chi^2(e) \geq |G : H|^2$. Therefore, G is not o-basis.

□

Theorem 3.2.20 *Let $A \lhd G$ be abelian with $|G : A| = p^3$. If G is o-basis, then G is nilpotent.*

Proof: We prove the contrapositive. Assume that G is not nilpotent. Then Lemma 3.2.15 applies. Choose a normal subgroup K of G satisfying the conclusions of that lemma. By Theorem 2.1.6, it suffices to show that G/K is not o-basis.

By 3.2.15 (i) and (ii), G/K is a non-abelian semi-direct product of $AK/K \rtimes T$,where

$|T| = p^n$ for some $n \geq 1$. Therefore, Theorem 1.3.4.2 (concerning semi-direct products) applies to G/K and we adopt the notation established there. Observe that if $\lambda \in Irr(AK/K)$ and $T_\lambda = T$, then $(AK/K)T_\lambda = (AK/K)T = G/K$ so that $\theta_{\lambda,\rho}(e) = (\lambda\tilde{\rho})^G(e) = 1$. As we shall show, it follows that, for some character $\lambda \in Irr(AK/K)$, $T_\lambda \neq T$. For suppose that $T_\lambda = T$ for all $\lambda \in Irr(AK/K)$. Since, by Theorem 1.3.4.2 (iii), every character of G has the form $\theta_{\lambda,\rho}$ for some $\lambda \in Irr(AK/K)$ and $\rho \in Irr(T_\lambda)$, we have that $\chi(e) = 1$ for all $\chi \in Irr(G/K)$. Theorem 1.3.2.3 then gives that G/K is abelian, contrary to 3.2.15 (i). Therefore, choose $\lambda \in Irr(AK/K)$ such that $T_\lambda \neq T$. By Lemma 3.2.15 (iii), AK/K is an elementary abelian q-group for prime $q \neq p$. Applying Lemma 3.2.18 to G/K, we may assume that $|T_\lambda| = p^2$. Since $|T : T_\lambda| = p$, it follows that $T_\lambda \lhd T$. By Theorem 3.2.19, G is not o-basis.

□

In the next result, we will again take of advantage of semi-direct product structure. As before, we refer the reader to section 1.3.4 for a discussion of semi-direct products and the associated notation.

Theorem 3.2.21 *Let p be prime and let $A \lhd G$ be abelian with $|G : A| = p^4$. Suppose that G is o-basis. Then exactly one of the following holds:*

(i) *G is nilpotent.*

(ii) *There exists $K \lhd G$ with $K \subseteq A$ such that G/K is the internal semidirect product of A/K and T, where $T \cong G/A$. Moreover, there exists $\lambda \in Irr(A/K)$ such that $T_\lambda \neq G/A$. Finally, $T_\lambda \cap Z(G/A) = \langle e \rangle$ for all such characters λ.*

Proof: As in previous results, we prove the contrapositive. Suppose that G is not nilpotent. By Lemma 3.2.15 (i), there is a normal subgroup K of G with $K \subseteq A$ such that G/K is a non-abelian semidirect product $(A/K) \rtimes T$ for some subgroup $T \leq G/K$, where $T \cong (G/K)/(A/K) \cong G/A$, where the last isomorphism is given by the Third Isomorphism Theorem. Let us choose such a K. By Lemma 3.2.15 (ii), $|G/K : A/K| = p^4$, and, by 3.2.15 (iii), A/K is a non-trivial elementary abelian q-group for some prime $q \neq p$ (see Definition 1.2.10). If we can show that G/K is not o-basis, it will follow by Theorem 3.1.5 that G is not o-basis. By Theorem 3.2.17, G/K is not o-basis if T is abelian. We may assume, therefore, that T is non-abelian.

Let us suppose, to obtain a contradiction, that $T_\lambda = T$ for all $\lambda \in Irr(A/K)$. Then $(A/K)T_\lambda = (A/K)T = G/K$ and $\theta_{\lambda,\rho}(e) = 1$ for all pairs λ, ρ, where $\lambda \in Irr(A/K)$ and $\rho \in Irr(T_\lambda)$. In this case, every irreducible character of G/K is linear by Theorem 1.3.4.2 (iii). By Theorem 1.3.2.3, G/K is abelian. But we have noted that G/K is non-abelian. Assume that (ii) does not hold, and choose $\lambda \in Irr(A/K)$ with $T_\lambda \neq T$ such that $T_\lambda \cap Z(T) \neq \langle e \rangle$. Note that $|T_\lambda| > 1$. By Lemma 3.2.18, we may assume that $|T_\lambda| \geq p^2$. Suppose that $|T_\lambda| = p^3$. Then $T_\lambda \lhd T$ by Theorem 1.2.6. It follows from Lemma 3.2.19 that G is not o-basis. Assume, therefore, that $|T_\lambda| = p^2$.

Fix $\rho \in Irr(T_\lambda)$. Note that T_λ is abelian by reason of order and therefore ρ is linear by Theorem 1.3.2.3. Put $H = AT_\lambda$, $\overline{H} = A(T_\lambda \cap Z(T))$, and $\chi = \theta_{\lambda,\rho}$. Note that $\chi(a) \neq 0$ for all $a \in A/K$ by Theorem 3.2.16. We show that $\chi(h) \neq 0$ for all $h \in \overline{H}$.

Since $\overline{H}/(A/K) \subseteq Z(T)$, $\overline{H} \lhd G$ by the Correspondance Theorem. Let $az \in \overline{H}$, where $a \in A$ and $z \in T_\lambda \cap Z(T)$. Applying Mackey's Theorem, Theorem 1.3.3.11, we have

$$\chi_{\overline{H}}(az) = \left((\lambda\tilde{\rho})^G\right)_{\overline{H}}(az) = \sum_{s\in\Omega}\left[{}^s(\lambda\tilde{\rho})_{{}^sH\cap\overline{H}}\right]^{\overline{H}}(az),$$

where Ω is a complete set of $\overline{H} - H$ double coset representatives in G/K.

As $\overline{H} \lhd G$ and $\overline{H} \subseteq H$, we have ${}^sH \cap \overline{H} = \overline{H}$ so that the sum becomes

$$\sum_{s\in\Omega}\left[{}^s(\lambda\tilde{\rho})_{\overline{H}}\right]^{\overline{H}}(az) = \sum_{s\in\Omega}{}^s(\lambda\tilde{\rho})(az) = \sum_{s\in\Omega}(\lambda\tilde{\rho})(s^{-1}azs) = \sum_{s\in\Omega}\lambda(s^{-1}as)\tilde{\rho}(s^{-1}zs).$$

For $g \in G$, $\overline{H}gH = g\overline{H}H = gH$, where the next to last and last equalities hold since $\overline{H} \lhd G/K$ and $\overline{H} \subseteq H$ respectively. The elements of Ω can thus be chosen to be coset representatives of H in G and therefore we may assume these elements to be coset representatives of T_λ in T. Recall that $\tilde{\rho} = \rho\pi$, where $\pi : H \to H/(A/K) \cong T_\lambda$ is the canonical map. Since $z \in T_\lambda \cap Z(T)$, we have $s^{-1}zs = z$ for all $s \in \Omega$ and $\pi(s^{-1}zs) = \pi(z) = z$. Thus $\tilde{\rho}(s^{-1}zs) = \rho(z)$. We have

$$\sum_{s\in\Omega}\lambda(s^{-1}as)\rho(z) = \rho(z)\sum_{s\in\Omega}\lambda^s(a) = \rho(t)\chi(a),$$

where the last equality is obtained by carrying out the above computation with $t = e$. Since $\chi(a) \neq 0$, this shows that χ never vanishes on $\overline{H}$.

By Corollary 3.1.4 with $N = \overline{H}$, there are at most p^3 cosets of $\langle e\rangle$ in G/K which are orthogonal with respect to $B^{\chi}_{\langle e\rangle}$.

But $\chi(e) = |G : H|(\lambda\tilde{\rho})(1) = |G : H| = p^2$. Thus, in order for G/K to be $(\langle e\rangle, \chi)$-o-basis, it is required that there be at least $\chi(e)(\chi, 1)_{\langle e\rangle} = \chi(e)^2 = p^4$ mutually orthogonal cosets. It follows that G/K, and so G, is not o-basis and the proof is complete.

□

Lemma 3.2.22 *Let $K \leq G$ and let $N \lhd G$ with $K \subseteq N$. Let $\chi \in Irr(G)$ and assume that G is (K, χ)-o-basis. Then G is (N, χ)-o-basis.*

Proof: Let $H \leq G$ with $N \subseteq H$. Assume that $(\chi, 1)_H \neq 0$. Then $(\chi, 1)_N \neq 0$ and $N \subseteq \ker \chi$ by Lemma 1.3.3.4. Define $\widehat{\chi} : G/\ker\chi \to \mathbb{C}$ by $\widehat{\chi}(g\ker\chi) = \chi(g)$ for all $g \in G$. Since G is (K, χ)-o-basis, Theorem 3.1.2 gives that $G/\ker\chi$ is $(\langle e\rangle, \widehat{\chi})$-o-basis. A second application of Theorem 3.1.2, gives that G is (N, χ)-o-basis, as desired.

□

Theorem 3.2.23 *Suppose $A \lhd G$, that A is cylic and $|G : A| = p$. Then G is o-basis if and only if G is nilpotent.*

Proof: If G is o-basis, it follows immediately from Theorem 3.2.17 that G is nilpotent. Turning, therefore, to the other direction, let us assume that G is nilpotent. We may also assume that G is non-abelian (see Proposition 1.3.2.3). Note that A is a maximal subgroup. For suppose $K \leq G$ with $A \subseteq K$. We have $K/A \leq G/A \cong \mathbb{Z}_p$ so that either $K/A = A$ or $K/A = G/A$. Since $A \subseteq K$, it follows that either $K = A$ or $K = G$. Let $\chi \in Irr(G)$ be non-linear. Define $\hat{\chi} : G/\ker\chi \to \mathbb{C}$ by $\hat{\chi}(g\cdot\ker\chi) = \chi(g)$. By Lemma 1.3.2.5, $\hat{\chi} \in Irr(G/\ker\chi)$. Let us note that $\ker(\hat{\chi}) = \{e\}$. Moreover, since $|\hat{\chi}(g \cdot \ker\chi)| = |\chi(g)|$, we have $Z(\hat{\chi}) = Z(\chi)/\ker\chi = Z(G/\ker\chi)$, where the last equality is given by Lemma 1.3.2.9. Next observe that $\ker\chi$ is a proper subgroup of A. For suppose first, to obtain a contradiction, that $A \subseteq \ker\chi$. Then $G' \subseteq \ker\chi$ so that $G/\ker\chi$ is abelian. It follows from Lemma 1.3.2.3 that χ is linear, a contradiction. Assume then that neither of the groups A and $\ker\chi$ is contained in the other. In this case, $A \cdot \ker\chi$ properly contains A. Since A is maximal, $A \cdot \ker\chi = G$.

Thus $G/\ker\chi = (A\cdot\ker\chi)/\ker\chi \cong A/(A\cap\ker\chi)$. This last group is abelian, and we again have $G' \subseteq \ker\chi$, a contradiction. It follows then that $\ker\chi$ is properly contained in A. From this we deduce that $\{e\} \neq A/\ker\chi \lhd G/\ker\chi$, that $|G/\ker\chi : A/\ker\chi| = |G : A| = p$ and that $A/\ker\chi$ is cyclic since A is. Note also that $G/\ker\chi$ is nilpotent since G is. We have verified therefore that $G/\ker\chi$ has all of the properties assumed of G. Finally, by Proposition 2.1.5, G is χ-o-basis if and only if $G/\ker\chi$ is $\hat{\chi}$-o-basis. We lose no generality, then, in identifying G with $G/\ker\chi$, and χ with $\hat{\chi}$. With this identification, we may assume that χ is faithful, χ is non-linear and that $Z(\chi) = Z(G)$.

By Theorem 1.3.2.13, $\chi(e)$ divides $|G : A|$. Thus, $\chi(e) = p$. Let $\lambda \in Irr(A)$ such that $(\chi,\lambda)_A \neq 0$ (that this is possible follows from Proposition 1.3.1.9). Then $1 \leq (\chi,\lambda)_A = (\chi,\lambda^G)$, where the last equality is by Theorem 1.3.3.12. Now $\lambda^G(e) = |G : A|\lambda(e)$. Since $\lambda(e) = 1$ by Lemma 1.3.2.3, we have $\lambda^G(e) = p$ so that $(\chi,\lambda^G) \leq 1$. This shows that $(\chi,\lambda^G) = 1$ so that $\chi = \lambda^G$. Thus $\chi \equiv 0$ on $G - A$ (see note after Definition 1.3.3.5)and it follows that $\ker\chi \subseteq Z(\chi) \subseteq A$. We note here, for later use, that λ is faithful. Indeed, since A is cyclic, every subgroup of A is characteristic in A. Characteristic subgroups of normal subgroups are themselves normal. Therefore, every subgroup of A is normal in G. In particular, $\ker(\lambda) \lhd G$. Therefore, $\ker(\lambda) = \cap_{x\in G}[\ker(\lambda)]^x = \ker\chi = \{e\}$, where the next to last equality is given by Lemma 1.3.3.6 since $\chi = \lambda^G$.

Let $H \leq G$ and assume that $(\chi,1)_H \neq 0$. Note that $G' \subseteq A$. If $A \subseteq H$, then $G' \subseteq H$ and G is H-o-basis by Theorem 3.3.1. Let us now assume that $A \nsubseteq H$ and $H \nsubseteq A$. We will show that if G is $(H\cap A,\chi)$-o-basis, then G is (H,χ)-o-basis. From this, we will conclude that it suffices to assume $H \subseteq A$. Since A is maximal, we have $|G| = |AH| = \dfrac{|A|\cdot|H|}{|H\cap A|}$. Dividing by $|H|$, we have $|G : H| = |A : H\cap A|$. Also, dividing by $|A|$, we have that

$|H : H \cap A| = |G : A| = p$. Let S denote a complete set of coset representatives for $H \cap A$ in A. Let $a, b \in S$ with $a \neq b$ so that $a(A \cap H) \neq b(A \cap H)$. Suppose $aH = bH$. Then $a^{-1}b \in H$. However, $a^{-1}b \in A$ so that $a(H \cap A) = b(H \cap A)$, a contradiction. If follows that the set $\{aH : a \in S\}$ consists of distinct cosets of H in G. Since $|S| = |A : H \cap A| = |G : H|$, we see that S comprises a complete set of coset representatives for H in G. Now let $a \in S$. We claim that $a(H \cap A) = (aH) \cap A$. Indeed, let $g \in a(H \cap A)$. Then $g = ah$, $h \in H \cap A$. Since $h \in H$, $g \in aH$. Since $h \in A$, $g \in A$. Thus $g \in (aH) \cap A$. Conversely, suppose $g \in (aH) \cap A$. Then $g = ah$ and $g = \overline{a}$ for some $h \in H$ and $\overline{a} \in A$. We have $ah = \overline{a}$ so that $h = a^{-1}\overline{a} \in A$. Thus $g \in a(H \cap A)$ and the claim follows. Let $a, b \in S$. Then

$$\begin{aligned} B^{\chi}_{H\cap A}\big[a(H \cap A), b(H \cap A)\big] &= \frac{\chi(e)}{|H \cap A|} \sum_{h \in H \cap A} \chi\Big(a^{-1}bh\Big) \\ &= |H : H \cap A| \cdot \frac{\chi(e)}{|H \cap A| \cdot |H : H \cap A|} \sum_{h \in H \cap A} \chi\Big(a^{-1}bh\Big) \\ &= |H : H \cap A| \cdot \frac{\chi(e)}{|H|} \sum_{h \in H} \chi\Big(a^{-1}bh\Big) \\ &= |H : H \cap A| \cdot B^{\chi}_{H}\big(aH, bH\big) \end{aligned}$$

where, in obtaining the next to last equality, we have used the facts that $a^{-1}b(H \cap A) = (a^{-1}b)H \cap A$ and that $\chi \equiv 0$ on $G - A$. Thus, whenever $a, b \in S$ and $a(H \cap A)$ and $b(H \cap A)$ are orthogonal relative to $B^{\chi}_{H\cap A}$, aH and bH are orthogonal relative to B^{χ}_{H}.

Assume that G is $(\chi, H \cap A)$-o-basis. Then there are $\chi(e)(\chi, 1)_{H\cap A}$ cosets of $H \cap A$ which are mutually orthogonal relative to $B^{\chi}_{H\cap A}$. Since $|G : A| = \chi(e)$, some coset of A must contain $(\chi, 1)_{H\cap A}$ of these cosets. By G-invariance of $B^{\chi}_{H\cap A}$, every coset of A, and in particular A itself, must contain $(\chi, 1)_{H\cap A}$ such cosets. Choose $\overline{S} = \{a_i : 1 \leq i \leq (\chi, 1)_{H\cap A}\} \subseteq S$ such that $a_i(A \cap H)$ and $a_j(A \cap H)$ are orthogonal relative to $B^{\chi}_{H\cap A}$ whenever $i \neq j$. Then $\{a_iH : a_i \in \overline{S}\}$ consists of $(\chi, 1)_{H\cap A}$ mutually orthogonal cosets of H in G. We recall that $\chi \equiv 0$ on $G - A$ and calculate

$$
\begin{aligned}
(\chi,1)_{H\cap A} &= \frac{1}{|H\cap A|}\sum_{h\in H\cap A}\chi(h) &&= |H:H\cap A|\frac{1}{|H\cap A|\cdot|H:H\cap A|}\sum_{h\in H}\chi(h)\\
&&&= |H:H\cap A|\frac{1}{|H|}\sum_{h\in H}\chi(h)\\
&&&= p\cdot(\chi,1)_H\\
&&&= \chi(e)(\chi,1)_H
\end{aligned}
$$

It follows that G is (H,χ)-o-basis whenever G is $(H\cap A,\chi)$-o-basis. Therefore, we assume, without loss of generality, that $H\subseteq A$. Since A is cyclic, every subgroup of A is characteristic in A. Since $A\lhd G$, Lemma 1.2.3 gives that $H\lhd G$. By Lemma 3.2.22, it suffices to show that G is (E,χ)-o-basis, where E denotes the identity subgroup.

Recall that $Z(\chi)\subseteq A$. Since G is nilpotent, Theorem 3.2.11 gives that $\chi(e)^2$ divides $|G:Z(\chi)|$. It follows that p divides $|A:Z(\chi)|$. There is, therefore, a subgroup of $A/Z(\chi)$ of order p.This subgroup is of the form $D/Z(\chi)$, where $Z(\chi)\subseteq D\subseteq A$ and $|D:Z(\chi)|=p$. We claim that $\chi_D=\sum_{i=0}^{p-1}\eta_i$, where the η_i are distinct, irreducible characters of D. By Theorem 1.3.3.11, $\chi_D=(\lambda^G)_D=\sum_{\sigma\in\Omega}\left[{}^{\sigma}\lambda_{{}^{\sigma}A\cap D}\right]^D$, where Ω is a complete set of (D,A)-double coset representatives in G. We remind the reader that ${}^{\sigma}\lambda\in Irr({}^{\sigma}A)$, where ${}^{\sigma}A=\sigma A\sigma^{-1}$. Since $A\lhd G$ and $D\subseteq A$, we have that ${}^{\sigma}A=A$ and ${}^{\sigma}A\cap D=D$. Thus $\chi_D=\sum_{\sigma\in\Omega}\left[({}^{\sigma}\lambda)_D\right]^D=\sum_{\sigma\in\Omega}({}^{\sigma}\lambda)_D$. For each $\sigma\in\Omega$, we have $D\sigma A=\sigma DA=\sigma A$ since $D\lhd G$ and $D\subseteq A$. It follows that Ω may be taken to be the set $\{x^i:0\leq i\leq p-1\}$, where $x\in G-A$ is chosen so that $G/A=\langle xA\rangle$. That is, $\chi_D=\sum_{i=0}^{p-1}({}^{x^i}\lambda)_D$. Fix $0\leq i\leq p-1$ and let $\varphi\in Irr(D)$ such that $\left({}^{x^i}\lambda,\varphi\right)_D\geq 1$. Since λ is linear, we have $\left({}^{x^i}\lambda,\varphi\right)_D\leq 1$ so that ${}^{x^i}\lambda_D=\varphi$. That is, ${}^{x^i}\lambda_D$ is irreducible. It remains to show that the ${}^{x^i}\lambda$ are all distinct. Suppose that ${}^{x^i}\lambda={}^{x^j}\lambda$ for some $i\neq j$. Choose $d\in D-Z(G)$ such that $D/Z(G)=\langle d\cdot Z(G)\rangle$. Then $\lambda({}^{x^i}d)={}^{x^i}\lambda(d)={}^{x^j}\lambda(d)=\lambda({}^{x^j}d)$. Recalling that λ is a faithful homomorphism, we

have that ${}^{x^i}d = {}^{x^j}d$ so that ${}^{x^{j-i}}d = d$. Since $i \neq j$, $G = \langle x^{j-i}, A\rangle$. If follows that $d \in Z(G)$, a contradiction. We put $\eta_i = {}^{x^i}\lambda$ and the claim is established.

Put $Z = Z(G)$. We now show that $\chi \equiv 0$ on $D - Z$. By Theorem 1.3.3.9, $\chi_Z = (\chi, \mu)_Z \sum_g {}^g\mu$ for some $\mu \in Irr(Z)$, where $(\chi, \mu)_Z \neq 0$ and the ${}^g\mu$ are the distinct conjugates of μ under G. For all $g \in G$ and $z \in Z$, we have that ${}^g\mu \in Irr(Z)$ and ${}^g\mu(z) = \mu({}^g z) = \mu(z)$ so that ${}^g\mu = \mu$. Thus, $\chi_Z = (\chi, \mu)_Z \cdot \mu$ so that $p = \chi_Z(e) = (\chi, \mu)_Z \cdot \mu(e) = (\chi, \mu)_Z$ and we have $\chi_Z = p\mu$. Now observe that $p = (\chi, \mu)_Z = (\chi_D, \mu)_Z = \left(\sum_{i=0}^{p-1} \eta_i, \mu\right)_Z = \sum_{i=0}^{p-1} (\eta_i, \mu)_Z$. For each i, η_i is linear so that (η_i, μ) is either 1 or 0. It follows that $(\eta_i, \mu)_Z = 1$ for all i. By Theorem 1.3.3.12, $(\eta_i, \mu^D)_D = (\eta_i, \mu)_Z = 1$ for each i. Also, $\mu^D(e) = |D : Z|\mu(e) = p$. It follows that $\mu^D = \sum_{i=0}^{p-1} \eta_i = \chi_D$. Since $Z \lhd D$, it follows that $\chi_D \equiv 0$ on $D - Z$.

Note that $B_E^\chi(aE, bE) = \chi(e)\chi(a^{-1}b)$ for all $a, b \in G$. If $aA \neq bA$, then $a^{-1}b \notin A$ and the above quantity is zero since $\chi \equiv 0$ on $G - A$. That is, any two elements of G in distinct cosets of A are orthogonal relative to B_E^χ. By the same reasoning, a is orthogonal to b relative to B_E^χ whenever $a, b \in D$ and $aZ \neq bZ$. Let $\{a_i : 1 \leq i \leq p\}$ be a complete set of distinct cosets of Z in D. Then the set $\bigcup_{j=0}^{p-1}\{x^j a_i : 1 \leq i \leq p\}$, where x^0 is chosen to be the identity of G, comprises a set of p^2 cosets of E which are mutually orthogonal relative to B_E^χ. Since $\chi(e)(\chi, 1)_E = p^2$, we have shown that G is (E, χ)-o-basis. As noted, it follows from this that G is (H, χ)-o-basis. As H and χ were chosen arbitrarily, G is o-basis and the proof is complete.

□

3.3 The Upper and Lower Central Series

In section 3.1, we defined the notion of K-o-basis. One reason for doing so is to use the generalized notion as a kind of filter for distinguishing between groups that is finer than that provided by the original notion of o-basis. To apply the generalized notion to all groups in a given class, the subgroup K must be chosen so that it is defined for all groups in that class. For example, the notion of Z-o-basis makes sense for all finite groups. In this section, we consider two series of "universal subgroups", the upper and lower central series. These series are defined in the notation section at the end of this work. It is expected that fewer groups G will be $\gamma_n(G)$-o-basis than γ_{n-1}-o-basis. One discovers quickly that every group is γ_2-o-basis (Theorem 3.3.1). Our main result in this section, Theorem 3.3.4, is that every group is in fact γ_3-o-basis. Finally, in Theorem 3.3.5, we also present a slight generalization of Theorem 3.2.1.

Theorem 3.3.1 *The group G is G'-o-basis. That is, every group is G'-o-basis.*

proof: By Theorem 3.1.5, G is G'-o-basis if and only if G/G' is o-basis. The latter holds by Theorem 2.1.4 since G/G' is abelian.

□

Lemma 3.3.2 *Let $N \lhd G$ and for $H \leq G$ let $\widehat{H}$ denote the image of H under the canonical map $G \to G/N$. Let $M \leq G$ with $N \subseteq M$. Then $\widehat{H} \subseteq \widehat{M} \Rightarrow H \subseteq M$ for all $H \leq G$.*

Proof: Let $H \leq G$, assume that $\widehat{H} \subseteq \widehat{M}$ and let $x \in H$. Then $xN = yN$ for some $y \in M$ so that $y^{-1}x = n$ for some $n \in N$. Thus $x = yn \in M$ by closure since $N \subseteq M$. It follows that $H \subseteq M$.

□

Lemma 3.3.3 *Let $m \geq 1$, $n \geq 0$ and put $\gamma_m = \gamma_m(G)$ and $Z_n = Z_n(G)$.*

Then $\gamma_m \subseteq Z_n \Leftrightarrow \gamma_{m+1} \subseteq Z_{n-1}$.

Proof: For a subset $S \subseteq G$, let $\widehat{S}$ denote the image of S under the canonical map $G \to G/Z_{n-1}$. Assume first that $\gamma_m \subseteq Z_n$. We recall that $\gamma_{m+1} = \big\langle \{[a,b] : a \in \gamma_m, b \in G\} \big\rangle$. Therefore, let $a \in \gamma_m$ and $b \in G$, and note that it is enough to show that $[a,b] \in Z_{n-1}$. We show $[a,b]Z_{n-1} = Z_{n-1}$. Indeed, $a \in Z_n$ by assumption and $\widehat{Z_n} = Z(\widehat{G})$. Thus $[a,b]Z_{n-1} = [aZ_{n-1}, bZ_{n-1}] = Z_{n-1}$. It follows that $[a,b] \in Z_{n-1}$, and thus $\gamma_{m+1} \subseteq Z_{n-1}$, as desired.

Assume now that $\gamma_{m+1} \subseteq Z_{n-1}$. Applying Lemma 3.3.2 with $N = Z_{n-1}$, we see that it suffices to show $\widehat{\gamma_m} \subseteq \widehat{Z}_n$. Now $\widehat{\gamma_m} = \big\langle \{[a,b]Z_{n-1} : a \in \gamma_{m-1}, b \in G\} \big\rangle$. Therefore, let $a \in \gamma_{m-1}$ and let $b, g \in G$. Then $[a,b] \in \gamma_m$ so that $\big[[a,b], g\big] \in \gamma_{m+1} \subseteq Z_{n-1}$, where this last containment is by assumption. We have

$$\big[[a,b]Z_{n-1}, gZ_{n-1}\big] = \big[[a,b], g\big]Z_{n-1} = Z_{n-1}.$$

It follows that $\widehat{\gamma}_m \subseteq Z(\widehat{G})$. Since $Z(\widehat{G}) = \widehat{Z}_n$, the desired containment is established.

□

Theorem 3.3.4 *The group G is γ_3-o-basis. That is, every group is γ_3-o-basis.*

Proof: For a subset $S \subseteq G$, let $\widehat{S}$ denote the image of S under the canonical map $G \to G/\gamma_2$. By Theorem 3.1.5, it suffices to show that $\widehat{G}$ is o-basis. Note that $\gamma_3(\widehat{G}) = \widehat{\gamma_3(G)} = \langle e \rangle = Z_0(\widehat{G})$. By Lemma 3.3.3, $(\widehat{G})' = \gamma_2(\widehat{G}) \subseteq Z_1(\widehat{G}) = Z(\widehat{G})$. Theorem 3.2.1 gives that $\widehat{G}$ is o-basis, as desired.

□

Our last result is a slight generalization of Theorem 3.2.1.

Theorem 3.3.5 *Let $m \geq 1$, $n \geq 0$ and assume that $\gamma_m \subseteq Z_n$. Then G is Z_{m+n-2}-o-basis.*

Proof: By Theorem 3.3.4, it suffices to show that $\gamma_3 \subseteq Z_{m+n-2}$. We proceed by induction on m. Assume first that $m = 0$. Then $G = \gamma_1 \subseteq Z_n$ so that $G = Z_n$. If $n = 0$, then $G = Z_0 = \langle e \rangle$ so that G is abelian and o-basis. The result holds since $Z_{m+n-2} = Z_{-1} = \langle e \rangle$. Assume that $n > 0$. Since $G = Z_n$, we have $G/Z_{n-1} = Z_n/Z_{n-1} = Z(G/Z_{n-1})$, where the last equality holds by definition of Z_n for $n > 0$. Thus G/Z_{n-1} is abelian and $\gamma_2 \subseteq Z_{n-1}$. It follows from Lemma 3.3.3 that $\gamma_3 \subseteq Z_{n-2}$, establishing the case $m = 0$.

Now let $m \geq 0$ and assume that $\gamma_m \subseteq Z_l \Rightarrow \gamma_3 \subseteq Z_{m+l-2}$ for all non-negative integers l. Suppose that $\gamma_{m+1} \subseteq Z_n$. We wish to show that $\gamma_3 \subseteq Z_{m+n-1}$. Applying the induction hypothesis with $l = n + 1$, it suffices to show that $\gamma_m \subseteq Z_{jn+1}$. We obtain this by applying the backwards implication in the conclusion of Lemma 3.3.3 to our assumption that $\gamma_{m+1} \subseteq Z_n$.

□

Chapter 4

Conclusions

Our work may be divided into main subdivisions. First, we have attempted to explore the connections between the o-basis property and nilpotency. We have posed two questions.

First, which nilpotent groups are o-basis? In [Hlms], Holmes has given an example of a group of order 3^4 that is not o-basis. Thus, it is known that not all nilpotent groups are o-basis. We have shown that whenever $G' \subseteq Z(G)$ (a condition implying nilpotency), G is o-basis. This result has been used in several subsequent arguments. In addition, it raises a question for possible future study. If $G' \subseteq Z(G)$, then G has nilpotence class no greater than 3 (see the notation section). Also, Holmes' example of order 3^4 has class 4. We ask, therefore, if nilpotence class 3 is a necessary condition for a (nilpotent) group to be o-basis, leaving this question, for the moment, open.

We have also shown that a nilpotent group is o-basis if and only if each of its Sylow subgroups are. Therefore, the question can be "reduced" in some sense to which p-groups are o-basis. Suppose G is a group of order p^n, where p is prime. We have taken the approach of considering the question for increasing values of n. Since all abelian groups are o-basis, we immediately find that G is o-basis if $n \leq 2$. That G is o-basis for $n = 3$ was established by Holmes in [Hlms] (see Theorem 1.1.1). We have attempted to better understand groups of order p^4 by working from the assumption that such a group is not o-basis. In this case, there exists a subgroup $H \leq G$ and $\chi \in Irr(G)$ such that G is not (H, χ)-o-basis. We derive from these assumptions some conditions on H, χ and G. We note that G begins to look very much like Holmes' example of order 3^4.

Our second question concerning the o-basis property and nilpotentcy is, "Are all o-basis groups nilpotent?". In this, there are two motivating facts. First, all examples so far of o-basis groups have been nilpotent. Second, the dihedral groups that are o-basis are precisely those that are nilpotent. With the dihedrals in mind, we have narrowed the question to those groups G having an abelian, normal subgroup A with non-trivial prime power index p^n. We have asked if nilpotentcy is a necessary condition for these groups to be o-basis. We have shown that if G/A is abelian, the answer is affirmative. When G/A is non-abelian, in which case $n \geq 3$, we have some limited results. In this case, nilpotentcy is necessary for o-basisness if $n = 3$. In the case $n = 4$, we obtain the result only after adding certain technical conditions. Finally, we have shown that nilpotentcy is a necessary and sufficient condition for o-basisness if A is cyclic and $n = 1$.

Our second major objective has been to explore the idea of generalizing the o-basis property. To this end, we defined the notion of a K-o-basis group, where K is a subgroup of G. In order for this notion to be used to distinguish between groups in a given class, the subgroup K must be chosen so that it makes sense for all of the groups in that class. For example, we may choose K to be the central subgroup. Since the center is defined for all groups, it makes sense to ask which groups are Z-o-basis. The upper and lower central series are two series of subgroups defined for all groups. In section 3.3, we have obtained some results with K coming from these series. One obtains quickly that every finite group is γ_2-o-basis. Our main result along these lines is that every group is in fact γ_3-o-basis. Theorem 3.2.1, mentioned above, was important to obtaining this result. In this same section, we also extend Theorem 3.2.1 somewhat.

Having summarized what has been done, we are positioned to look ahead. There seems to be quite a bit of room for further study with o-basis groups. Neither of our two questions concerning the o-basis property and nilpotentcy have been answered fully. The question of whether or not all o-basis groups are nilpotent is still open. As a more manageable goal, on may attempt to prove Conjecture 3.2.13. In our attempts at this conjecture, we only made it to $n = 4$. Even here, we were obliged in Theorem 3.2.21 to add certain technical conditions to make the argument work. It is not known whether these conditions are actually needed. One may therefore attempt to remove them. We have already mentioned the possibility that all o-basis groups are in fact not only nilpotent but of nilpotence class 3.

There are also open questions about how the o-basis property behaves with regard to basic group-theoretic operations. For example, it is unknown if a subgroup of an o-basis group o-basis. It is also unknown whether or not the direct product of a number of o-basis groups is o-basis (see the discussion following Theorem 3.2.8). Along these lines, it may be worth noting that, since the definition of o-basis involves characters, it may be that "o-basis" is not a purely group-theoretic property.

Room for further study also exists in experimenting with alternative means of generalizing the notion of o-basis group. There are at least two alternative generalizations. First, we have chosen, in the character theory, the complex numbers for the base field (or at least a field that is algebraically closed and whose characteristic does not divide $|G|$). However, theory exists for the case in which the field has prime characteristic (see [Is], Ch. 15). This involves the notion of Brauer characters. One might attempt to derive a notion of o-basis that in terms of Brauer characters rather than ordinary $\mathbb{C}$-characters.

Another possible generalization is to allow the group G to be infinite. In this case, one deals with arbitrary compact groups as opposed to finite groups. In this case, the group G is endowed with a certain topology, and a linear representation of G in V is a homomorphism $\rho : G \to \mathrm{GL}(V)$ which is continuous with respect to this topology. A portion of the theory of the $\mathbb{C}$-characters of finite groups has an analog in the setting of compact groups, and one might try to define the notion of o-basis in this setting.

Future researchers may do well to familiarize themselves with current research on p-groups, zeros of characters and number theory. The study of o-basis groups may well hold the potential for furthering progress in these on-going fields of research. Also, considering their connection with tensor spaces, the author feels he has reason to believe that the study of o-basis groups holds promise as a challenging and significant endeavor.

Bibliography

[Greub] Werner Greub, Linear Algebra, fourth edition, Sringer-Verlag, New-York Heidelberg Berlin, 1975.

[Hlms] R. Holmes, Orthogonality of Cosets Relative to Irreducible Characters of Finite Groups, Linear and Multilinear Algebra, March-April 2004 Vol.52, No.2, pp. 133-143.

[Hlms,Tam] R. Holmes and Tin-Yau Tam, Symmetry Classes of Tensors Associated with Certain Groups, Linear and Multilinear Algebra, 1992 Vol.32, pp. 21-31.

[Hun] T.W. Hungerford, Algebra, Springer New-York, 1974.

[Is] I.M. Isaacs, Character Theory of Finite Groups, Academic Press, New-York San Francisco London, 1976.

[Karp] G. Karpilovsky, Group Representations, volume 1, part B: Introduction to Group Representations and Characters, North-Holland, Amsterdam London New-York Tokyo, 1992.

[Rob] D.J.S. Robinson, A Course in the Theory of Groups, Springer-Verlag, New York Heidelberg Berlin, 1982.

[Ser] Jean-Pierre Serre, Linear Representations of Finite Groups, Springer-Verlag, New-York Heidelberg Berlin, 1977.

[Suz] M. Suzuki, Group Theory I, Springer-Verlag, New-York Heidelberg Berlin, 1982.

Notation

Let G denote a finite group. We use the following notational conventions. Entries are arranged according to category and, after that, roughly in the order that they appear in the text. References to relevant sections of the text are at the far right. Also, the reader will want to take note of comments that accompany some of the entries.

$\lvert A\rvert$,	the cardinality of the set A	
e,	the identity element of G	
$G - S$,	$\{g \in G : g \notin S\}$	
$H \leq G$,	H is a subgroup of G	
$\langle S \rangle$,	the subgroup generated by the subset $S \subseteq G$	
G/N,	the quotient group of left cosets of the normal subgroup N of G	
g^x,	$g^x = x^{-1}gx$, where $x, g \in G$	
${}^x g$,	${}^x g = xgx^{-1}$, where $x, g \in G$	
H^g,	$H^g = \{h^g : h \in H\}$, where $g \in G$ and $H \leq G$	
${}^g H$,	${}^g H = \{{}^g h : h \in H\}$, where $g \in G$ and $H \leq G$	
$C_G(x)$,	$C_G(x) := \{g \in G : g^{-1}xg = x\}$, where $x \in G$. This is called the **centralizer** of x in G. It is a subgroup of G.	
$\mathrm{Aut}(G)$,	the automorphism group of G	
K char G,	K is a characteristic subgroup of G	Def. 1.2.2 Th. 1.2.3
$\mathrm{lcm}(S)$,	the least common multiple of a finite set, S, of integers	

Y^X, the set of fixed points of a set Y under the action of a set X. That is $Y^X = \{y \in Y : y^x = y \text{ for all } x \in X\}$, where $y \mapsto y^x$ is the image of $y \in Y$ under the action of $x \in X$.

$[a, b]$, the commutator $aba^{-1}b^{-1}$, where $a, b \in G$

G', the **commutator subgroup** of G

$\gamma_n(G)$, the nth term of the lower central series of G (see below)

The **lower central series** of G is the series of subgroups defined recursively as follows: $\gamma_1(G) = G$ and, for $n > 1$, $\gamma_n(G) := \big\langle \{[a, b] : a \in \gamma_{n-1}(G), b \in G\} \big\rangle$.

Note that $\gamma_n(G) \lhd G$ for all $n \geq 1$ and that $G' = \gamma_2(G)$.

A group G is nilpotent $\Leftrightarrow \gamma_n(G) = \langle e \rangle$ for some n.

In this case, the smallest such n is called the **nilpotence class** of G. This can also be shown to be the smallest n such that $Z_n(G) = G$ (see below).

$Z(G)$, the center of the group G

$Z_n(G)$, the nth term of the upper central series of G

The **upper central series** is the series of subgroups of G defined recursively as follows. For $n \leq 0$, put $Z_n(G) = \langle e \rangle$ and let $Z_1(G)$, or simply $Z(G)$, denote the center of G.

For $n > 1$, $Z_n(G)$ is the unique subgroup of G containing Z_{n-1} such that $Z_n(G)/Z_{n-1}(G) = Z(G/Z_{n-1})$.

$\overline{z}$, the conjugate of the complex number z

$|z|$, the modulus of the complex number z

1_G,	the principal character of G, $1_G(g) = 1$ for all $g \in G$. Note that 1_G is linear and so irreducible. (see Def 1.3.2.1 and Propostion 1.3.2.2.)	
$\ker\chi$,	the kernel of the character χ, $\ker\chi := \{g \in G : \chi(g) = \chi(e)\}$	
$Z(\chi)$,	the center of the character χ, $Z(\chi) := \{g \in G : \lvert\chi(g)\rvert = \chi(e)\}$ For all characters χ, $\ker\chi \subseteq Z(\chi)$ and both subgroups are normal in G	
χ_K,	the restriction of the character χ to the subgroup K	sec. 1.3.3
φ^G,	the character of G **induced** from φ, where φ is a character of some subgroup of G	sec. 1.3.3
$I_G(\varphi)$,	the inertial subgroup of φ, where φ is a character of some subgroup of G	Def. 1.3.3.8
$Cl(G)$,	the set of class functions on G	Sec. 1.3.1
$(\chi,\psi)_G$	$(\chi,\psi)_G = \frac{1}{\lvert G\rvert}\sum_{g\in G}\chi(g)\overline{\psi(g)}$, where χ,ψ are class functions on G.	sec. 1.3.1
T_λ,	the stabilizer of λ in T	sec 1.3.4
$Gal(\mathbb{Q},\epsilon)$,	the galois group of $\mathbb{Q}[\epsilon]$ over $\mathbb{Q}$	
B_H^χ,		eqn. 2.1
$\prod_{i=1}^n G_i$,	the direct product of the groups G_i	