AN ANALYSIS OF FINITE GROUPS WITH AUTOMORPHISMS INVERTING MOST GROUP ELEMENTS

by

Rodney L. Overturff II

A thesis submitted to the Graduate Council of
Texas State University in partial fulfillment
of the requirements for the degree of
Master of Science
with a Major in Mathematics
May 2015

Committee Members:

Thomas Keller, Chair

Yong Yang

Teodora Acosta

FAIR USE AND AUTHOR'S PERMISSION STATEMENT

Fair Use

Duplication Permission

ACKNOWLEDGMENTS

First and foremost I would like to thank my family and friends. I can honestly say that I would not be where I am today without their continued love and support. I owe my deepest gratitude to my professor and committee chair Dr. Thomas Keller. He inspired me to persue research in group theory and without his much needed guidance this thesis would not have been possible. I would also like to thank Dr. Yong Yang and Dr. Teodora Acosta for serving as members of my thesis committee. I would like to thank Christine Herrera for pushing me to write a thesis in the first place; and finally I would like to thank my friend and classmate Joseph Skelton for being so excited about algebra with me. Thank you all so very much.

TABLE OF CONTENTS

Page

ACKNOWLEDGMENTS....iv

CHAPTER

I. INTRODUCTION 1

II. NOTATION 2

III. PRELIMINARY THEOREMS 3

IV. THE STRUCTURE OF $> \frac{1}{2}$-GROUPS 14

V. GROUPS CONSISTING MOSTLY OF INVOLUTIONS 36

REFERENCES 48

CHAPTER I

INTRODUCTION

Throughout this paper I present an expansion of an article from the journal *Mathematische Zeitschrift* called "Groups with Automorphisms Inverting most Elements", by Hans Liebeck and Desmond MacHale. Although the structure of the groups under consideration in this article had previously been determined by C. T. C. Wall using character theory, Liebeck and MacHale demonstrate an alternative approach to determining the structure of finite nonabelian groups in which there exists some automorphism inverting more than half of the group elements. It is noteworthy however that this group structure need not apply to groups with automorphisms inverting exactly half of the group elements.

As will be shown, a group is abelian if and only if there exists some automorphism that inverts the group elementwise. It follows that the groups under consideration in this paper are *nearly* abelian. We will show that such groups have an abelian subgroup of index 2 or are nilpotent of class 2 of a specific type as will be outlined in Theorem (4.10). After developing the structure of these groups we will restrict the groups under consideration to finite nonabelian groups in which the identity automorphism inverts more than half of the group elements. We will show that these groups are precisely those groups in which at least half of the group elements are involutions and will close by outlining the structure of this smaller class of groups in Theorem (5.10).

CHAPTER II

NOTATION

Throughout this paper G will denote a finite nonabelian group. For any automorphism α of G, we let S_α denote the set of elements in G inverted by α and we define

$$I(\alpha) = \frac{|S_\alpha|}{|G|}.$$

Furthermore we define $I(G) = \max I(\gamma)$ as γ runs through all automorphisms of G. Thus the objective of this paper is to determine the possible structures of a finite nonabelian group G in which $I(G) > \frac{1}{2}$. Such a group will be referred to as a $>\frac{1}{2}$-group and any automorphism inverting over half of the group elements will be referred to as a $> \frac{1}{2}$-automorphism. Note that we use the convention of writing functions from from the right whenever function composition is relevant. Finally, for subgroups H and K of G we define $[H, K] = \{\langle [h, k] \rangle = \langle h^{-1}k^{-1}hk \rangle : h \in H, k \in K\}$ and we define $|G : H|$ to be the index of H in G.

CHAPTER III

PRELIMINARY THEOREMS

Liebeck and MacHale begin by developing results that relate the subgroup structure of an arbitrary $> \frac{1}{2}$-group to the elements that are inverted by $> \frac{1}{2}$-automorphisms of the group. We will do the same but will also develop additional results that will serve to simplify several of the proofs in the next chapter. We begin by proving a well known result regarding arbitrary abelian groups.

(3.1) **Lemma.** A group is abelian if and only if it has an automorphism inverting it elementwise.

Proof. ($\Rightarrow$) Let H be an abelian group. Define the function α by $(a)\alpha = a^{-1}$ for all $a \in H$. Let x, $y \in H$ and suppose that $(x)\alpha = (y)\alpha$. Then $x^{-1} = y^{-1}$. It follows easily that $x = y$ so α is injective. As $(x^{-1})\alpha = x$ we see that α is surjective. Thus all that remains is to verify that α is a homomorphism. Since H is abelian we have

$$(xy)\alpha = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = (x)\alpha(y)\alpha$$

as desired.

($\Leftarrow$) Now suppose that α is an automorphism that inverts the group H elementwise. Then for all x, $y \in H$ we have

$$xy = (y^{-1}x^{-1})\alpha = (y^{-1})\alpha(x^{-1})\alpha = yx.$$

Thus H is abelian and the proof is complete. ■

(3.2) **Lemma.** Let α be an automorphism of G and let $s \in S_\alpha$. Let I_s be the inner automorphism of G induced by s and define $\beta = I_s\alpha$. It follows that $S_\beta = S_\alpha s^{-1} = sS_\alpha$. In particular, $I(\beta) = I(\alpha)$.

Proof. Notice first that $(g)\beta = (g)I_s\alpha = g^{-1}$ if and only if$(s^{-1}gs)\alpha = g^{-1}$ if and only if $(s^{-1})\alpha(gs)\alpha = g^{-1}$ if and only if $(gs)\alpha = s^{-1}g^{-1} = (gs)^{-1}$ if and only if

$gs \in S_\alpha$ for any $g \in G$. Thus for $g \in G$, we have $g \in S_\beta$ if and only if $gs \in S_\alpha$ if and only if $g \in S_\alpha s^{-1}$. This demonstrates the first equality.

Similarly, for $g \in G$ we have

$$(g)\beta = (s^{-1}gs)\alpha = g^{-1}$$

if and only if

$$(s^{-1}g)\alpha(s)\alpha = g^{-1}$$

if and only if

$$(s^{-1}g)\alpha = g^{-1}s = (s^{-1}g)^{-1}.$$

So for $g \in G$, we have $g \in S_\beta$ if and only if $s^{-1}g \in S_\alpha$ if and only if $g \in sS_\alpha$. This demonstrates the second equality. Thus,

$$I(\alpha) = \frac{|S_\alpha|}{|G|} = \frac{|sS_\alpha|}{|G|} = \frac{|S_\beta|}{|G|} = I(\beta)$$

which completes the proof. ■

The following theorem leads to an important result concerning arbitrary abelian subgroups of $> \frac{1}{2}$-groups. Namely, any abelian subgroup of a $> \frac{1}{2}$-group G is inverted elementwise by some $> \frac{1}{2}$-automorphism of G.

(3.3) **Subgroup Theorem.** Let H be a subgroup of a $> \frac{1}{2}$-group G. Then there exists a $> \frac{1}{2}$-automorphism of G that inverts more than half of the elements of H and hence maps H onto itself. Moreover, $I(H) \geq I(G)$.

Proof. Let α be a $> \frac{1}{2}$-automorphism of G. Notice that $|S_\alpha| = I(\alpha)|G|$. Then as G may be written as the disjoint union of right cosets of H in G, there must be some coset of H in G, Hs say, such that at least $I(\alpha)|Hs|$ elements of Hs are in S_α. Thus we have $|Hs \cap S_\alpha| \geq I(\alpha)|Hs|$ and it follows that $|H \cap S_\alpha s^{-1}| \geq I(\alpha)|H|$.

Now define $\beta = I_s\alpha$. We may without loss of generality assume that $s \in S_\alpha$

since we know that there is some $hs \in Hs \cap S_\alpha$ and $Hhs = Hs$. Hence by Lemma (3.2) we have

$$|H \cap S_\beta| = |H \cap S_\alpha s^{-1}| \geq I(\alpha)|H| = I(\beta)|H|.$$

Thus,

$$\frac{|H \cap S_\beta|}{|H|} \geq I(\beta) = I(\alpha) > \frac{1}{2}$$

which tells us that β inverts over half of the elements in H. Hence $|(H)\beta \cap H|$ is greater than $|H|/2$; and as $(H)\beta \cap H \leq H$ we see that $|(H)\beta \cap H| = |H|$. Thus we have $(H)\beta = H$ and we see that β maps H onto itself as desired. Hence, $\beta|_H$ is an automorphism of H such that

$$I(\beta|_H) = \frac{|H \cap S_\beta|}{|H|} \geq I(\beta) = I(\alpha).$$

So if we choose α such that $I(\alpha) = I(G)$, then we have $I(\beta|_H) \geq I(G)$. Therefore, $I(H) \geq I(G)$. ■

Note that the proof of the following result in "Groups with Automorphisms Inverting most Elements" was omitted. We offer a proof to clarify.

(3.4) **Corollary.** Let $H \leq G$ be an abelian subgroup of the $> \frac{1}{2}$-group G. Then there is a $> \frac{1}{2}$-automorphism of G that inverts H elementwise.

Proof. By the Subgroup Theorem there exists a $> \frac{1}{2}$-automorphism of G that inverts over half of H, β say, and $\beta|_H$ defines an automorphism of H. By Lemma (3.1) there exists an automorphism that inverts H elementwise, γ say. Define $\delta = \beta|_H\gamma^{-1}$ and note that $\delta \in Aut(H)$. Notice that for all $x \in H$ such that x is inverted by $\beta|_H$, we have

$$(x)\delta = (x)\beta|_H\gamma^{-1} = (x^{-1})\gamma^{-1} = x.$$

Since $\beta|_H$ inverts over half of H we see that δ fixes over half of H. And as the set

of all elements that are fixed by δ, $Fix(\delta)$, forms a subgroup of H, we see that $Fix(\delta) = H$. Thus, δ is the identity map on H and $\beta|_H = \gamma$. Therefore, β is an automorphism of G that inverts H elementwise. ■

(3.5) **Lemma.** Let β be a $> \frac{1}{2}$-automorphism of G that inverts the abelian subgroup H elementwise. Suppose that the right coset Hg of H in G has nonempty intersection with S_β. Then the number of elements in Hg that are inverted by β is $|C_H(g)|$.

Proof. By hypothesis we can choose some $s \in Hg \cap S_\beta$; and as $s \in Hs$ we have $Hg = Hs$. Notice that for $h \in H$, we have $hs \in S_\beta$ if and only if

$$h^{-1}s^{-1} = (h)\beta(s)\beta = (hs)\beta = (hs)^{-1} = s^{-1}h^{-1}$$

if and only if $h \in C_H(s)$. Thus for $h \in H$, we have $hs \in S_\beta$ if and only if $hs \in C_H(s)s$. It follows that $Hg \cap S_\beta = C_H(s)s$. Now, $s = hg$ for some $h \in H$. So $x \in C_H(s)$ if and only if $x \in C_H(hg)$ if and only if $x(hg) = (hg)x$ if and only if $hxg = hgx$ if and only if $xg = gx$ if and only if $x \in C_H(g)$ since H is abelian. Hence, $C_H(s) = C_H(g)$. Thus $Hg \cap S_\beta = C_H(g)s$ and we see that $|Hg \cap S_\beta| = |C_H(g)s| = |C_H(g)|$ and we have our result. ■

(3.6) **Transversal Theorem.** Let β be a $> \frac{1}{2}$-automorphism of G that inverts the abelian subgroup H elementwise. Suppose that H is not contained properly in any subgroup of G that is contained in S_β. Then we may write G as the disjoint union of cosets $G = H \cup Hs_2 \cup \cdots \cup Hs_n$ where $s_i \in S_\beta$ for $i \in \{2, ..., n\}$.

Proof. Suppose for the moment that some coset of H in G, Hg say, contains some $s \in S_\beta$. Then $Hg = Hs$. Now, if $Hs \neq H$, then $C_H(s)$ must be a proper subgroup of H. For otherwise, $H_1 = \langle s, H \rangle \subseteq S_\beta$ is an abelian subgroup that properly contains H contradicting our hypothesis. Thus, as $C_H(g) = C_H(s)$, we have

$$|C_H(g)| = |C_H(s)| \leq \frac{|H|}{2} = \frac{|Hg|}{2}$$

whenever $Hs \neq H$. It follows by Lemma (3.5) that if $Hg \neq H$, then at most half of the elements of Hg are inverted by β. This tells us that each coset of H in G necessarily contains some element of S_β for otherwise β is not a $> \frac{1}{2}$-automorphism. This completes the proof. ■

(3.7) **Centralizer Theorem.** Let β be a $> \frac{1}{2}$-automorphism of G that inverts the abelian subgroup H elementwise. Suppose that H is not contained properly in any subgroup of G that is contained in S_β and write $G = H \cup Hg_2 \cup \cdots \cup Hg_n$ where $g_i \in S_\beta$ for $i \in \{2, ..., n\}$. Put $q_i = |H : C_H(g_i)|$. Then $|S_\beta| = |H| + \sum_{i=2}^{n} |C_H(g_i)|$, where $q_i \geq 2$ (i = 2, ..., n) and $\sum_{i=2}^{n} (\frac{1}{2} - \frac{1}{q_i}) < \frac{1}{2}$.

Proof. The equation regarding the cardinality of S_β is an immediate consequence of Lemma (3.5); and by arguments in the Transversal Theorem we see that $q_i \geq 2$ (i = 2, ..., n). Thus, it remains to prove the last inequality.

Notice,

$$\begin{aligned}
\sum_{i=2}^{n} (\frac{1}{2} - \frac{1}{q_i}) &= \frac{n-1}{2} - \sum_{i=2}^{n} \frac{1}{|H : C_H(g_i)|} \\
&= \frac{n-1}{2} - \sum_{i=2}^{n} \frac{|C_H(g_i)|}{|H|} \\
&= \frac{n-1}{2} - \frac{|S_\beta| - |H|}{|H|} \\
&= \frac{n+1}{2} - \frac{|S_\beta|}{|H|} \\
&< \frac{n+1}{2} - \frac{n|H|}{2|H|} = \frac{1}{2},
\end{aligned}$$

where the last inequality comes from the fact that $|S_\beta| > \frac{n|H|}{2}$. Hence result. ■

(3.8) **Corollary.** An automorphism of a $> \frac{1}{2}$-group G either inverts $I(G)|G|$ elements of G or it inverts at most half of the elements of G.

Proof. Let α be a $> \frac{1}{2}$-automorphism of G and let H be an arbitrary maximal abelian subgroup of G. Then by Lemma (3.2) and Corollary (3.4) there exists an

automorphism of G, β say, that inverts H elementwise such that $I(\alpha) = I(\beta)$. Now, by Lemma (3.1), we know that any subgroup of G contained in S_β is necessarily abelian. As H is a maximal abelian subgroup of G, H is not properly contained in any subgroup of G contained entirely in S_β. Thus, by the Centralizer Theorem, $|S_\alpha| = |S_\beta| = |H| + \sum_{i=2}^{n} |C_H(g_i)|$ where G admits the coset decomposition given in the Centralizer Theorem. It follows that $|S_\alpha|$ is independent of α and that any $> \frac{1}{2}$-automorphism of G inverts $I(G)|G|$ elements of G. This gives us our result. ■

(3.9) **Remark.** The previous result provides us with a general formula relating the maximal abelian subgroups of a $> \frac{1}{2}$-group G to $I(G)$. It tells us that if H is an arbitrary maximal abelian subgroup of a $> \frac{1}{2}$-group G, then $I(G)|G| = |H| + \sum_{i=2}^{n} |C_H(g_i)|$ where G admits the coset decomposition given in the Centralizer Theorem. Furthermore, the Centralizer Theorem, or more specifically the inequality regarding the indices q_i, forces certain restrictions on H. Simple algebra techniques demonstrate that one of the following conditions must be satisfied relative to a suitable ordering of the cosets of H in G:

I $n = 2$;

II $n \geq 3$, $q_i = 2$ $(i = 2, ..., n)$;

III $n \geq 3$, $q_2 \geq 3$, $q_i = 2$ $(i = 3, ..., n)$;

IV $n \geq 3$, $q_2 = 3$, $q_3 = 4$ or 5, $q_i = 2$ $(i = 4, ..., n)$;

V $n \geq 3$, $q_2 = q_3 = 3$, $q_i = 2$ $(i = 4, ..., n)$;

As we will see, some of these cases do not occur in the groups under consideration. We obtain more results regarding the abelian subgroup structure of $> \frac{1}{2}$-groups before demonstrating this.

(3.10) **Squares Theorem.** Let H be a subgroup of G that has maximum order among subgroups of G contained in S_β where β is a $> \frac{1}{2}$-automorphism of G. Then

the square of every element inverted by β is in H.

Proof. First note that H is an abelian subgroup as subgroups contained in S_β are necessarily abelian. Let $s \in S_\beta$. We may assume that $s \notin H$ as the result is trivial otherwise. If $|G : H| = 2$, then $H \triangleleft G$ and the factor group $G/H = \{H, Hs\}$. In this case, $Hs^2 = (Hs)^2 = H$ so $s^2 \in H$. Thus we may assume that $|G : H| \geq 3$. Recall that $C_H(s)$ is a proper subgroup of H. Consider two cases.

Case (i) $|H : C_H(s)| = 2$. Define $H_1 = \langle s, C_H(s)\rangle$. As s commutes elementwise with $C_H(s)$ and $\{s\} \cup C_H(s) \subseteq S_\beta$, we have $H_1 \subseteq S_\beta$. We claim that $s^2 \in C_H(s) \leq H$ and the result follows in this case. To verify our claim, suppose $s^2 \notin C_H(s)$. Then since $s \notin C_H(s)$, we see that $s^2 \notin C_H(s)s$; and since $s^2 \in H_1$, it follows that $|H_1 : C_H(s)| \geq 3$. Thus,

$$|H_1| \geq 3|C_H(s)| > 2|C_H(s)| = |H|$$

contradicting the definition of H. This verifies our claim.

Case (ii) $q = |H : C_H(s)| \geq 3$. By way of contradiction suppose that $s^2 \notin H$. Then $s \notin Hs^{-1}$ so $Hs \neq Hs^{-1}$. But $C_H(s) = C_H(s^{-1})$ so

$$|H : C_H(s)| = |H : C_H(s^{-1})| \geq 3.$$

It follows that the structure of G is subject to condition (3.9)V. So

$$q = |H : C_H(s)| = |H : C_H(s^{-1})| = 3.$$

We claim that $s^3 \in C_H(s)$. To verify, suppose that $s^3 \notin C_H(s)$. Notice that $s^2 \notin C_H(s)$ so $s^3 \notin C_H(s)s$; and $s \notin C_H(s)$ so $s^3 \notin C_H(s)s^2$ either. As $C_H(s)$, $C_H(s)s$,

and $C_H(s)s^2$ are distinct cosets it follows that $|H_1 : C_H(s)| \geq 4$. Thus,

$$|H_1| \geq 4|C_H(s)| > 3|C_H(s)| = |H|.$$

This contradicts the definition of H since we know that $H_1 \subseteq S_\beta$. Thus our claim is verified and we have $s^3 \in C_H(s)$.

Now, define $G_1 = \langle s, H \rangle$. For the moment, assume that $H \triangleleft G_1$. Then $s^{-1}hs \in H$ for all $h \in H$ and so β inverts $s^{-1}hs$ for all $h \in H$. Thus,

$$s^{-1}h^{-1}s = (s^{-1}hs)\beta = sh^{-1}s^{-1} \iff s^2h^{-1} = h^{-1}s^2 \iff hs^2 = s^2h$$

for all $h \in H$. It follows that $C_H(s^{-1}) = H$ contradicting that $q = 3$. To see this, notice that since s^3 and hence $s^{-3} \in H$, we have

$$hs^{-1} = hs^2s^{-3} = s^2hs^{-3} = s^2s^{-3}h = s^{-1}h$$

for all $h \in H$.

Thus we may assume that $H \not\triangleleft G_1$. It follows that $s^{-1}Hs \neq H$. Now, choose an arbitrary $h \in H - C_H(s)$. As H is abelian, $C_H(s) \triangleleft H$ and we have $|H/C_H(s)| = 3$. Thus $H/C_H(s)$ is cyclic and generated by either of its nonidentity elements. So we may write $H/C_H(s) = \langle hC_H(s) \rangle$. This tells us that we may write $H = \langle h, C_H(s) \rangle$ and that $h^3 \in C_H(s)$.

As $h \in H$ we see that $C_H(s) = C_H(sh) = C_H(sh^2)$ and that each of these centralizers has index 3 in H. Since G must satisfy condition (3.9)V it follows that two of the cosets Hs, Hsh, and Hsh^2 must be equal. If $Hs = Hsh$ then $shs^{-1} \in H$ and we get the contradiction that $H \triangleleft G_1$. If $Hsh = Hsh^2$ then $Hs = Hsh$ and we

obtain the same contradiction. If $Hs = Hsh^2$ then

$$Hsh = Hsh^3 = Hh^3s = Hs,$$

since $h^3 \in C_H(s)$. Again we get the same contradiction. Thus $s^2 \in H$. ■

(3.11) **Index 2 Theorem.** Let A be an abelian subgroup of maximum order in G. Let β be a $> \frac{1}{2}$-automorphism of G inverting A elementwise. Then for every $s \in S_\beta - A$ we have $|\langle s, A\rangle : A| = 2$.

Proof. Define $G_1 = \langle s, A\rangle$ where $s \in S_\beta - A$ and write $|G_1 : A| = n$. We consider two cases.

Case (i) $|A : C_A(s)| = 2$. Notice that if there exists some $g \in G - A$ such that $g \in C_G(G_1)$, then $g \in C_G(A)$ and $\langle g, A\rangle$ is an abelian subgroup of G of order greater than $|A|$. Thus, $C_G(G_1) = C_A(G_1) = C_A(s) = Z$ say. Clearly $Z \triangleleft G_1$ so we may consider the factor group G_1/Z. If G_1/Z contains a coset, bZ, of order $m > 2$, then the subgroup $B = \langle b, Z\rangle$ is abelian and $|B| = m|Z| > 2|Z| = |A|$ which contradicts the definition of A. Hence, all nonidentity elements of G_1/Z are of order 2 or equivalently, G_1/Z is an elementary abelian 2-group. Thus, $A/Z \triangleleft G_1/Z$ and by correspondence, $A \triangleleft G_1$. Recall that any subgroup of G contained in S_β is abelian. Then as A is abelian of maximum order in G, A certainly has maximum order among subgroups contained in S_β. Thus, by the square's theorem, $s^2 \in A$. Since G_1/A is also an elementary abelian 2-group, it follows that $G_1/A = \{A, As\}$ and $|G_1 : A| = 2$ as desired.

Case (ii) $|A : C_A(s)| \geq 3$. By way of contradiction suppose that $n > 2$. Then besides A and As, there exists a third coset of A in G_1. Since $s^2 \in A$, we may write this third coset as Asa for some $a \in A - C_A(s)$. Note that we could possibly write this third coset as $Asas$ for some $a \in A - C_A(s)$. But in this case it follows easily that Asa is distinct from A and As as well. Similarly, if we write this third coset as

$Asasa_2$ for some a, $a_2 \in A - C_A(s)$, it follows easily that $Asas$ or Asa_2 is distinct from A and As as well. (To verify, simply assume that $Asas$ is equal to A or As.) Thus, we choose to write this third coset in simplest from as Asa.

Now, since A is abelian, $C_A(s) = C_A(sa) = C_A(sa^2)$. Thus,

$$|A : C_A(s)| = |A : C_A(sa)| = |A : C_A(sa^2)|.$$

Since As and Asa are distinct cosets of A in G_1, we see that G_1 is subject to condition (3.9)V and that $|A/C_A(s)| = 3$. It follows that $A/C_A(s)$ is cyclic and is generated by $C_A(s)a$. Thus we may write $A = \langle a, C_A(s)\rangle$ and we see that $a^3 \in C_A(s)$. Again, as

$$|A : C_A(s)| = |A : C_A(sa)| = |A : C_A(sa^2)|,$$

we see that two of the cosets, As, Asa, and Asa^2 must be equal. Since $A = \langle a, C_A(s)\rangle$, in any case we may use an argument similar to that in the proof of the Squares Theorem to determine that $A \lhd G_1$. It follows that

$$Asa = Aa^3sa = Asa^4 = AsAa^4 = As.$$

This contradiction completes the proof. ■

We prove two final results before proceeding to the next section. Note that these results are not included in "Groups with Automorphisms Inverting most Elements" and were simply added for convenience.

(3.12) **Lemma.** If H is a finite elementary abelian 2-group of order 2^n, then H contains exactly $2^n - 1$ distinct subgroups of index 2.

Proof. Let H be an elementary abelian 2-group of order 2^n. Then we may view H as an n-dimensional vector space, V say, over the field of two elements. Thus, maximal subgroups of H, or equivalently subgroups of index 2, may be viewed as

subspaces of V of dimension n-1; and subgroups of H of order 2 may be viewed as subspaces of V of dimension 1. In this proof I use the following well known linear algebra result that I will not prove: If V is an n-dimensional vector space, then V has the same number of k-dimensional subspaces as $(n-k)$-dimensional subspaces.

Using this result, we see that that the number of subgroups of index 2 in H is equal to the number of subgroups of H of order 2. Thus, it suffices to count the number of subgroups of order 2. Each nonidentity element of H generates such a subgroup and these are clearly the only subgroups of order 2 in H. As there are $2^n - 1$ nonidentity elements of H the result follows. ■

(3.13) **Lemma.** Let H, $K \leq G$ be arbitrary subgroups of G with indices p and q in G respectively. Then $|G : H \cap K| \leq pq$. Moreover, if p and q are relatively prime, then $|G : H \cap K| = pq$.

Proof. Notice first that

$$|G| \geq |HK| = \frac{|H||K|}{|H \cap K|} \iff |G||H \cap K| \geq |H||K| \iff \frac{|G|}{|H|} \geq \frac{|K|}{|H \cap K|}.$$

Thus we have,

$$|K : H \cap K| \leq |G : H|.$$

Hence,

$$|G : H \cap K| = |G : K||K : H \cap K| \leq |G : K||G : H| = pq,$$

as desired. Now, since $|H \cap K|$ divides $|H|$ and $|K|$, it follows that p and q divide $|G : H \cap K|$. Thus, if p and q are relatively prime, pq divides $|G : H \cap K|$ and equality follows. This completes the proof. ■

CHAPTER IV

THE STRUCTURE OF $> \frac{1}{2}$-GROUPS

In this section we use abelian subgroups of maximum order and results obtained in the last section to develop the structure of finite nonabelian $> \frac{1}{2}$-groups. Throughout this section, let G denote a finite nonabelian $> \frac{1}{2}$-group such that $A \leq G$ is an abelian subgroup of maximum order in G.

(4.1) **Theorem.** The subgroup A is normal and G/A is an elementary abelian 2-group. Furthermore, if A, Ax, and Ay are distinct cosets of A in G, then Axy is distinct as well.

Proof. By Corollary (3.4), there exists a $> \frac{1}{2}$-automorphism of G, β say, that inverts A elementwise. As A is an abelian subgroup of maximum order in G and subgroups contained in S_β are necessarily abelian, A is a subgroup of maximum order contained in S_β. Let $g \in G$. Then by the Transversal Theorem, $g = as$ for some $a \in A$ and $s \in S_\beta$. Notice that $g^{-1}Ag = s^{-1}a^{-1}Aas = s^{-1}As$. Define $G_1 = \langle s, A \rangle$. If $s \in A$ then clearly $g^{-1}Ag = A$ so we may assume without loss that $s \notin A$. By the Index 2 Theorem, $[G_1 : A] = 2$. Thus, $A \lhd G_1$. So $g^{-1}Ag = s^{-1}As = A$. As g was chosen arbitrarily, it follows that $A \lhd G$. Moreover, $g^2 = asas = as^2(s^{-1}as) \in A$ since we know $s^2 \in A$ by the Squares Theorem. Thus G/A is an elementary abelian 2-group.

Now, suppose that A, Ax, and Ay are distinct cosets of A in G. If $A = Axy$, then $Ax = Ay^{-1} = A(y^{-2})y = Ay$ which is a contradiction. If $Ax = Axy$, then $Ax = AxAy = AyAx = Ayx$. In this case it follows that $yx \in Ax$ which tells us that $y \in A$. We obtain a similar contradiction whenever $Ay = Axy$. Thus, Axy is distinct from A, Ax, and Ay as desired. This completes the proof. ■

In Remark (3.9) we saw that if a maximal abelian subgroup $H \leq G$ has index n in G (with $I(G) > \frac{1}{2}$), then the structure of G is subject to one of five conditions. The following theorem demonstrates that only three of those conditons actually

occur in the groups under consideration in this paper.

(4.2) **Centralizer Structure Theorem** Let β be a $> \frac{1}{2}$-automorphism of G that inverts A elementwise. Let $G = A \cup Ag_2 \cup \cdots \cup Ag_n$ be a decomposition of G into disjoint cosets of A in G such that $g_i \in S_\beta$ for $i \in \{2, ..., n\}$ and define $q_i = |A : C_A(g_i)|$. Then one of the following conditions must hold relative to a suitable ordering of the cosets of A in G:

I $\mathrm{n} = 2$;

II $\mathrm{n} = 2^k$ ($\mathrm{k} \geq 2$), $\mathrm{q_i} = 2$ ($\mathrm{i} = 2, ..., 2^k$);

III $\mathrm{n} = 4$, $\mathrm{q_2} = 4$, $\mathrm{q_3} = \mathrm{q_4} = 2$.

Furthermore, if the first condition is met, then $I(G) = \frac{q_2+1}{2q_2}$. If the second condition is met, then $I(G) = \frac{2^k+1}{2^{k+1}}$. And if the third condition is met, then $I(G) = \frac{9}{16}$.

Proof. First notice that $n = |G/A|$ must be a power of 2 for otherwise there would exist a prime $p \neq 2$ dividing $|G/A|$. In this case it follows that G/A has an element of order p and is not a 2-group. Next, we rule out conditions (3.9)IV and V. By way of contradiction, suppose that $q_2 = 3$ and that $q_3 = 3$, 4, or 5. By Theorem (4.1) we know that Ag_2, Ag_3, and Ag_2g_3 are distinct cosets of A in G. Assuming that condition (3.9)IV or V holds, we see that $|A : C_A(g_2g_3)| = 2$. Now, as A is abelian and $(g_2)^2 \in A$, we see that $C_A(g_3) = C_A((g_2)^2g_3)$. Thus,

$$C_A(g_3) = C_A((g_2)^2g_3) \geq C_A(g_2) \cap C_A(g_2g_3) = B$$

say. By Lemma (3.13), $|A : B| = 6$ as 2 and 3 are relatively prime. It follows that $q_3 \neq 4$ and $q_3 \neq 5$ since q_3 must divide 6. Thus, we have ruled out condition (3.9)IV and may assume that $q_2 = q_3 = 3$. Next, notice that

$$C_A(g_2g_3) \geq C_A(g_2) \cap C_A(g_3) = C$$

say. We claim that $|A : C| = 3$ or 9. In this case, as $|A : C_A(g_2g_3)| = 2$ must divide $|A : C|$ we have reached a contradiction that rules out condition (3.9)V. To verify our claim, notice that by Lemma (3.13), we have $|A : C| \leq 9$. And as $q_2 = 3$ must divide $|A : C|$, we see that $|A : C| = 3$, 6, or 9. Thus it suffices to show that $|A : C| \neq 6$. Notice,

$$\begin{aligned}
|A : C| &= |A : C_A(g_2)||C_A(g_2) : C| \\
&= 3|C_A(g_2) : C| \\
&= 3\frac{|C_A(g_2)|}{|C_A(g_2) \cap C_A(g_3)|} \\
&= 3\frac{|C_A(g_2)||C_A(g_2)C_A(g_3)|}{|C_A(g_2)||C_A(g_3)|} \\
&= 3\frac{|C_A(g_2)C_A(g_3)|}{|C_A(g_3)|} \\
&= 9\frac{|C_A(g_2)C_A(g_3)|}{|A|}.
\end{aligned}$$

Now, since A is abelian we have $C_A(g_2)C_A(g_3) = C_A(g_3)C_A(g_2)$. Thus, $C_A(g_2)C_A(g_3) \leq A$ and so $|C_A(g_2)C_A(g_3)|$ divides $|A|$. It follows that $|A : C| \neq 6$ and our claim is verified.

Next we consider condition (3.9)III. Suppose that $q_i = 2$ $(i \geq 3)$. Since $(g_3)^2 \in A$, we have

$$C_A(g_2) = C_A(g_2g_3^2) \geq C_A(g_2g_3) \cap C_A(g_3) = D$$

say. Since $q_3 = 2$ must divide $|A : D|$ and by Lemma (3.13) we have $|A : D| = 2$ or 4. Thus $q_2 = |A : C_A(g_2)| = 2$ or 4. As it turns out, the case where $n = 4$, $q_2 = 4$, and $q_3 = q_4 = 2$ arises in $> \frac{1}{2}$-groups but the case $n = 2^k$ $(k > 2)$, $q_2 = 4$, and $q_i = 2$ $(i = 3, ..., 2^k)$ does not occur as we will now show.

Suppose that $|G/A| = 2^k$ $(k > 2)$. As G/A is an elementary abelian 2-group we may suppose that G/A is generated by x_1A, ..., x_kA where we select x_1 such that $|A : C_A(x_1)| = 4$ where $|A : C_A(x)| = 2$ for all $x \notin A \cup x_1A$. We claim that if Ax and

Ay are distinct cosets of A in G such that $C_A(x)$ and $C_A(y)$ have index 2 in A, then

$$C_A(x) = C_A(y) \Rightarrow C_A(x) = C_A(xy). \tag{1}$$

To see this, assume that the necessary hypotheses are satisfied and that $C_A(x) = C_A(y)$. Then

$$C_A(xy) \geq C_A(x) \cap C_A(y) = C_A(x)$$

and so $|A : C_A(xy)| = 1$ or 2. But by Theorem (4.1), $A \neq Axy$ so $xy \notin A$. Thus $|A : C_A(xy)| = 2$ since A is an abelian subgroup of maximum order in G. It follows that $C_A(xy) = C_A(x)$ and (1) is verified.

Now, each of x_2, x_3, x_2x_3, x_1x_2, x_1x_3, and $x_1x_2x_3$ belong to disinct cosets of A in G and each of their centralizers has index 2 in A. Moreover, since $(x_2)^2 \in A$,

$$C_A(x_1) = C_A(x_1x_2^2) \geq C_A(x_1x_2) \cap C_A(x_2).$$

As $|A : C_A(x_1x_2) \cap C_A(x_2)| \leq 4$ by Lemma (3.13) and $|A : C_A(x_1)| = 4$, it follows that $C_A(x_1) = C_A(x_1x_2) \cap C_A(x_2)$. Using similar methods we see that

$$\begin{aligned} C_A(x_1) &= C_A(x_1x_2) \cap C_A(x_2) \\ &= C_A(x_1x_3) \cap C_A(x_3) \\ &= C_A(x_1x_2x_3) \cap C_A(x_2x_3). \end{aligned} \tag{2}$$

Thus, $C_A(x_1)$ is contained in each of these six centralizers. Notice also that since

$|A : C_A(x_1)| = 4$ we have

$$C_A(x_1x_2) \neq C_A(x_2), \tag{3}$$

$$C_A(x_1x_3) \neq C_A(x_3), \tag{4}$$

$$C_A(x_1x_2x_3) \neq C_A(x_2x_3). \tag{5}$$

Now, since $C_A(x_1x_2)$ and $C_A(x_2)$ are of index 2 in A and intersect to form $C_A(x_1)$, it follows that for all $x \in A - C_A(x_1)$, we have $x^2 \in C_A(x_1)$. Thus, $A/C_A(x_1)$ is an elementary abelian 2-group of order 4. Hence, by Lemma (3.12), $A/C_A(x_1)$ has 3 distinct subgroups of index 2. It follows by correspondence that there are exactly 3 subgroups of index 2 in A which contain $C_A(x_1)$. Thus, the centralizers of x_2, x_3, x_2x_3, x_1x_2, x_1x_3, and $x_1x_2x_3$ are distributed over 3 subgroups of index 2 in A. It is routine to verify by application of (1) that either $C_A(x_2)$, $C_A(x_3)$, and $C_A(x_2x_3)$ are either all distinct or they are all equal. We will demonstrate that in either case we obtain a contradiction.

Case (i) $C_A(x_2) = C_A(x_3) = C_A(x_2x_3)$. As there are only 3 distinct subgroups of index 2 in A, by (3), (4), and (5), two of $C_A(x_1x_2)$, $C_A(x_1x_3)$ and $C_A(x_1x_2x_3)$ must be the same. If $C_A(x_1x_2) = C_A(x_1x_2x_3)$, then since $(x_1x_2)^2 \in A$ and by (1),

$$C_A(x_1x_2) = C_A(x_1x_2x_1x_2x_3) = C_A(x_3) = C_A(x_2)$$

contradicting (3). If $C_A((x_1x_2)^{-1}) = C_A(x_1x_2) = C_A(x_1x_3)$, then since $Ax_2^{-1}x_1^{-1}$ and Ax_1x_3 are distinct cosets of A in G, by (1) we have

$$C_A(x_2^{-1}x_1^{-1}) = C_A(x_2^{-1}x_1^{-1}x_1x_3) = C_A(x_2^{-1}x_3) \geq C_A(x_2^{-1}) \cap C_A(x_3) = C_A(x_2).$$

This contradicts (3) since $C_A(x_1x_2)$ and $C_A(x_2)$ are both of index 2 in A. If $C_A(x_3^{-1}x_1^{-1}) =$

$C_A(x_1x_3) = C_A(x_1x_2x_3)$, then by a similar argument we have

$$C_A(x_3^{-1}x_1^{-1}) = C_A(x_3^{-1}x_2x_3) \geq C_A(x_3^{-1}) \cap C_A(x_2x_3) = C_A(x_3).$$

This contradicts (4) since $C_A(x_1x_3)$ and $C_A(x_3)$ are both of index 2 in A. Thus this case does not occur in the groups under consideration.

Case (ii) $C_A(x_2)$, $C_A(x_3)$, and $C_A(x_2x_3)$ are all distinct. In this case, as there are only 3 distinct subgroups of index 2 in A, each of $C_A(x_1x_2)$, $C_A(x_1x_3)$, and $C_A(x_1x_2x_3)$ must be equal to one of $C_A(x_2)$, $C_A(x_3)$, or $C_A(x_2x_3)$; and by equation (3) we have either $C_A(x_1x_2) = C_A(x_3)$ or $C_A(x_2x_3)$.

For the moment we assume that $C_A(x_1x_2) = C_A(x_3)$. Then by (1) we have $C_A(x_1x_2) = C_A(x_3) = C_A(x_1x_2x_3)$. Now, by (4) we have either $C_A(x_1x_3) = C_A(x_2)$ or $C_A(x_2x_3)$. If $C_A(x_1x_3) = C_A(x_2)$, then since $Ax_1x_2 = Ax_2x_1$ and by (1), for some $a \in A$ we have

$$C_A(x_1x_3) = C_A(x_2) = C_A(x_2x_1x_3) = C_A(ax_1x_2x_3) = C_A(x_1x_2x_3) = C_A(x_3)$$

contradicting (4). Similarly, if $C_A(x_1x_3) = C_A(x_2x_3)$, then we have

$$\begin{aligned} C_A(x_1x_3) &= C_A(x_2x_3) \\ &= C_A(x_1x_3x_2x_3) \\ &= C_A(x_1a_1x_2(x_3)^2) \\ &= C_A(x_1a_1x_2) \\ &= C_A(a_2x_1x_2) \\ &= C_A(x_1x_2) \\ &= C_A(x_3) \end{aligned}$$

for some a_1, $a_2 \in A$. Again, this contradicts (4).

Thus $C_A(x_1x_2) \neq C_A(x_3)$ and we may assume that $C_A(x_1x_2) = C_A(x_2x_3)$. Then by (1) and similar arguments from the previous paragraph we have

$$C_A(x_1x_2) = C_A(x_2x_3) = C_A(x_1(x_2)^2x_3) = C_A(x_1x_3).$$

Now, by (5) we have either $C_A(x_1x_2x_3) = C_A(x_3)$ or $C_A(x_2)$. If $C_A(x_1x_2x_3) = C_A(x_3)$, then by (1),

$$C_A(x_1x_2x_3) = C_A(x_1x_2(x_3)^2) = C_A(x_1x_2) = C_A(x_2x_3)$$

which contradicts (5). And if $C_A(x_1x_2x_3) = C_A(x_2)$, by similar arguments we have

$$\begin{aligned} C_A(x_1x_2x_3) &= C_A(x_1x_2x_3x_2) \\ &= C_A(x_1a_1x_3(x_2)^2) \\ &= C_A(x_1a_1x_3) \\ &= C_A(x_1x_3a_2) \\ &= C_A(x_1x_3) \\ &= C_A(x_2x_3) \end{aligned}$$

for some $a_1, a_2 \in A$ contradicting (5). Thus this case doesn't occur in the groups under consideration either. Since we obtain a contradiction in either case, we see that G must satisfy one of the three conditions as stated in this theorem.

Throughout the rest of this paper, whenever a group G satisfies condition I, II, or III of the Centralizer Structure Theorem, we will say that G is of Type I, II, or III respectively. Now, to complete the proof, recall that $I(G) = I(\beta)$. First, consider G of Type I. In this case $G = A \cup Ag_2$. Thus, by Lemma (3.5), the number of

elements in Ag_2 that are inverted by β is equal to $|C_A(g_2)|$. It follows that

$$\begin{aligned} I(\beta) &= I(G) \\ &= \frac{|A| + |C_A(g_2)|}{|G|} \\ &= \frac{|A| + \frac{|A|}{q_2}}{|G|} \\ &= \frac{1}{2} + \frac{1}{2q_2} \\ &= \frac{q_2 + 1}{2q_2}, \end{aligned}$$

as desired.

Next, consider G of Type II. In this case $G = A \cup Ag_2 \cup \cdots \cup Ag_{2^k}$. Thus by Lemma (3.5) we have

$$\begin{aligned} |G|I(\alpha) &= |G|I(G) \\ &= |A| + \sum_{i=2}^{2^k} |C_A(g_i)| \\ &= |A| + \sum_{i=2}^{2^k} \frac{|A|}{2} \\ &= |A| + (2^k - 1)\frac{|A|}{2} \\ &= |A|(\frac{2^k + 1}{2}) \\ &= \frac{|G|}{2^k}(\frac{2^k + 1}{2}) \\ &= |G|(\frac{2^k + 1}{2^{k+1}}). \end{aligned}$$

Hence, $I(G) = \frac{2^k+1}{2^{k+1}}$.

Finally, consider G of Type III. In this case $G = A \cup Ag_2 \cup Ag_3 \cup Ag_4$. Thus by

Lemma (3.5) we have

$$\begin{aligned} |G|I(G) &= |A| + \sum_{i=2}^{4} |C_A(g_i)| \\ &= |A| + \frac{|A|}{2} + \frac{|A|}{2} + \frac{|A|}{4} \\ &= |A|(\frac{9}{4}) \\ &= |G|(\frac{9}{16}). \end{aligned}$$

Hence $I(G) = \frac{9}{16}$. This completes the proof. ■

We now focus our attention on $> \frac{1}{2}$-groups of Type II and III. Note that in the proof of the next theorem we will use two well known commutator identities. Namely, if x, y, and z are elements of G, then

$$[xy, z] = [x, z]^y[y, z]$$

and

$$[x, yz] = [x, z][x, y]^z.$$

The proofs of these identities are completely routine and will hence be omitted.

(4.3) **Theorem.** Suppose that G is of Type II or III. Then if x and y are elements of different cosets of A in G, then $C_A(x) \neq C_A(y)$.

Proof. By way of contradiction, suppose $Ax \neq Ay$ and that $C_A(x) = C_A(y)$. We claim that x, $y \notin A$. It follows by Theorem (4.1) that $xy \notin A$ either. To verify, suppose without loss of generality that $x \in A$. Then $C_A(y) = C_A(x) = A$ which implies that $|A : C_A(y)| = 1$. As $y \notin A$ we obtain the contradiction that A is not a maximal abelian subgroup of G. Thus our claim is verified. Moreover since $|A : C_A(x)| = |A : C_A(y)|$, it follows by the Centralizer Structure Theorem that $|A : C_A(x)| = 2$.

Now, define $G_1 = \langle x, y, A\rangle$. By the Subgroup Theorem, G_1 is a $> \frac{1}{2}$-group and

since $|G_1 : A| > 2$ we see that G_1 is of Type II or III. Notice that

$$C_A(xy) \geq C_A(x) \cap C_A(y) = C_A(x).$$

As $xy \notin A$ we see that $|A : C_A(xy)| \neq 1$. Thus $|A : C_A(xy)| = 2$ and we have $C_A(xy) = C_A(x) = C_A(y) = Z$ say. Furthermore, since A, Ax, Ay, and Axy are all distinct cosets of A in G, we see that G_1 cannot be of Type III. It follows that G is not of Type III either for otherwise we have $G = A \cup Ax \cup Ay \cup Axy = G_1$. Hence we may assume that both G and G_1 are of Type II.

Notice that since A is an abelian subgroup of maximum order in G, it follows that $C_G(A) = A$. Thus Z is the center of G_1. As $|A : Z| = 2$ we may write $A = \langle a_1, Z \rangle = Z \cup a_1 Z$ for some $a_1 \in A - Z$. Note that $C_{G_1}(a_1) = A$ since any element of G_1 that commutes with a_1 certainly centralizes Z and is hence an element of $C_G(A) = A$. We claim that

$$x^{-1} a_1 x = a_1 z_1, \tag{6}$$

$$y^{-1} a_1 y = a_1 z_2, \tag{7}$$

for distinct elements of order 2, z_1 and $z_2 \in Z$.

To see this, first notice that $A \lhd G_1$ so $x^{-1} a_1 x \in A$. If $x^{-1} a_1 x = z_0$ for some $z_0 \in Z$, then it follows that $a_1 = (z_0)^{x^{-1}} = z_0 \in Z$ which is a contradiction. A similar argument can be made for $y^{-1} a_1 y$. To see that $z_1 \neq z_2$, suppose otherwise. Then $x^{-1} a_1 x = y^{-1} a_1 y$ which implies that $y x^{-1} a_1 = a_1 y x^{-1}$. In this case we have $y x^{-1} \in C_{G_1}(a_1) = A$ and it follows easily that $Ax = Ay$ which is a contradiction. Finally to see that z_1 is of order 2, write $(a_1)^2 = z_0$ for some $z_0 \in Z$. Then

$$z_0 = (z_0)^x = (a_1^2)^x = (a_1^x)^2 = (a_1 z_1)^2 = z_0 (z_1)^2.$$

It follows that $(z_1)^2 = 1$. A similar argument shows that z_2 is also of order 2. Thus our claim is verified.

Next note that x and y do not commute. For otherwise $\langle x, y, Z\rangle$ is an abelian subgroup of G such that $|\langle x, y, Z\rangle| \geq 4|Z| = 2|A| > |A|$ which contradicts the definition of A.

Now, let α be a $> \frac{1}{2}$-automorphism of G_1 that inverts A elementwise. We may assume that α inverts x and y by the Transversal Theorem. Thus, $(axy)\alpha = a^{-1}x^{-1}y^{-1}$ for all $a \in A$. We know by Lemma (3.5) that α inverts $|C_A(xy)|$ elements or equivalently half of the elements of Axy. Furthermore, α doesn't invert any elements in Zxy for if some $zxy \in Zxy$ is inverted by α, then $z^{-1}x^{-1}y^{-1} = (zxy)\alpha = y^{-1}x^{-1}z^{-1}$. This leads to the contradiction that $xy = yx$. It follows that $(axy)\alpha = (axy)^{-1}$ for all $a \in A - Z$. In particular, we have $y^{-1}x^{-1}a_1^{-1} = (a_1xy)^{-1} = (a_1xy)\alpha = a_1^{-1}x^{-1}y^{-1}$.

Thus, by (5) and (6) we have

$$a_1xy = yxa_1 = y(xa_1z_1)z_1 = y(a_1x)z_1(z_2)^2 = (ya_1z_2)xz_1z_2 = (a_1y)xz_1z_2.$$

It follows that $xy = yxz_1z_2$ and that $x^{-1}y^{-1}xy = [x, y] = z_1z_2$. Furthermore (5) and (6) also tell us that,

$$[x, a_1][a_1, y] = (a_1x)^{-1}(xa_1)(ya_1)^{-1}(a_1y) = (xa_1z_1)^{-1}(a_1xz_1)(a_1yz_2)^{-1}(ya_1z_2),$$

so we have

$$[x, a_1][a_1, y] = a_1^{-1}(x^{-1}a_1x)y^{-1}a_1^{-1}(ya_1) = a_1^{-1}(a_1z_1)y^{-1}a_1^{-1}(a_1yz_2) = z_1z_2.$$

Now, by the commutator identities introduced prior to the start of this theorem, we

see that

$$[xa_1, ya_1] = [x, ya_1]^{a_1}[a_1, ya_1] = ([x, a_1][x, y]^{a_1})^{a_1}[a_1, a_1][a_1, y]^{a_1}.$$

Since $[x, y] = z_1 z_2 \in Z$ we have

$$[xa_1, ya_1] = ([x, a_1][x, y])^{a_1}[a_1, y]^{a_1} = a_1^{-1}[x, y][x, a_1][a_1, y]a_1 = (z_1 z_2)^2 = 1.$$

Hence xa_1 and ya_1 commute and $\langle xa_1, ya_1, Z\rangle$ is an abelian subgroup of G. As $xa_1, ya_1 \notin Z$ and $Zxa_1 \neq Zya_1$, we obtain the contradiction that $\langle xa_1, ya_1, Z\rangle$ is an abelian subgroup of G of order greater than A. This contradiction completes the proof. ■

(4.4) **Corollary.** Suppose that G is of Type II or III and that G/A is an elementary abelian 2-group of order 2^k $(k \geq 2)$ generated by $Ax_1, Ax_2, ..., Ax_k$. Put

$$Z = C_A(x_1) \cap C_A(x_2) \cap \cdots \cap C_A(x_k).$$

Then Z is the center of G and $|A : Z| = 2^k$. Moreover, A/Z is an elementary abelian 2-group.

Proof. First write $G = \langle x_1, ..., x_k, A\rangle$. Notice that the center of G must be contained in A for if there exists some $x \in C_G(G) - A$ then $\langle x, A\rangle$ is an abelian subgroup of G of order greater than $|A|$. Thus the center of G is the set of all elements in A that commute with each of $x_1, ..., x_k$. It follows that the center of G is Z as claimed. Consider two cases.

Case (i) G is of Type II. Then $|A : C_A(x_i)| = 2$ for $i \in \{1, ..., k\}$. It follows immediately that A/Z is an elementary abelian 2-group. By Lemma (3.13) we have $|A : Z| \leq 2^k$. As G/A has $2^k - 1$ nonidentity elements, by Theorem (4.3) there are at least $2^k - 1$ distinct subgroups of index 2 in A, each containing Z. Hence by

correspondence, A/Z has at least $2^k - 1$ distinct subgroups of index 2. Thus, by Lemma (3.12) we have $|A : Z| = |A/Z| = 2^k$.

Case (ii) G is of Type III. Then two of $C_A(x_1)$, $C_A(x_2)$, and $C_A(x_1x_2)$ have index 2 in A and the other has index 4 in A. We will prove the result in the case that $C_A(x_1)$ and $C_A(x_2)$ are of index 2 in A. The other two cases are similar. Again, it follows immediately that A/Z is an elementary abelian 2-group. By Lemma (3.13) we see that $|A : Z| \leq 4$. Since $C_A(x_1x_2) \geq C_A(x_1) \cap C_A(x_2)$ and $|A : C_A(x_1x_2)| = 4$, we see that $|A : Z| = 4$. This completes the proof. ■

(4.5) **Lemma.** Let G, G/A, and Z be defined as in Corollary (4.4) and suppose that if G is of Type III, the generators x_1 and x_2 are chosen so that $C_A(x_1)$ and $C_A(x_2)$ are of index 2 in A. Then for each $i \in \{1, ..., k\}$ there exists an $a_i \in A$ and a $z_i \in Z$ such that $[a_i, x_i] = z_i$, $[a_i, x_j] = 1$ $(j \neq i)$ where $z_i \neq 1$ is of order 2. Furthermore, if G is of Type II then $z_1 = z_2 = \cdots = z_k$; and if G is of Type III then $z_1 \neq z_2$.

Proof. We begin by defining

$$D_i = C_A(x_1) \cap \cdots \cap C_A(x_{i-1}) \cap C_A(x_{i+1}) \cap \cdots \cap C_A(x_k).$$

Note that by Lemma (3.13) we have $|A : D_i| \leq 2^{k-1}$; and by Corollary (4.4) we have $|A : Z| = 2^k$. As A/Z is an elementary abelian 2-group, for any $x \in D_i$ we have $x^2 \in Z$. It follows that $|D_i : Z| = 2$.

Thus we may choose some $a_i \in D_i - Z = D_i - C_A(x_i)$. Then $[a_i, x_j] = 1$ $(j \neq i)$, and $[a_i, x_i] \neq 1$. We will now show that $[a_i, x_i] \in Z$. First note that by a well known commutator identity that can be found in the text "Algebra: A Graduate Course" by Martin Isaacs ([II], p. 110-111), we have

$$[x_i^{-1}, x_j^{-1}, a_i]^{x_j}[x_j, a_i^{-1}, x_i^{-1}]^{a_i}[a_i, x_i, x_j]^{x_i^{-1}} = 1. \tag{8}$$

Now, since G/A is elementary abelian,

$$[x_i^{-1}, x_j^{-1}] = x_i x_j x_i^{-1} x_j^{-1} = a x_j x_i x_i^{-1} x_j^{-1} = a$$

for some $a \in A$. It follows that $[x_i^{-1}, x_j^{-1}, a_i]^{x_j} = 1$ as A is abelian. Also since $[a_i, x_j] = 1$ $(j \neq i)$, it follows that $[x_j, a_i^{-1}] = 1$. Thus we have $[x_j, a_i^{-1}, x_i^{-1}]^{a_i} = 1$. Hence, by (8) we have $[a_i, x_i, x_j]^{x_i^{-1}} = 1$ $(j \neq i)$. Thus $[a_i, x_i, x_j] = 1^{x_i} = 1$ $(j \neq i)$ and it follows that $[a_i, x_i] \in C_A(x_j)$ $(j \neq i)$. So we have $[a_i, x_i] \in D_i$.

We claim that $[a_i, x_i] \in C_A(x_i)$ as well. In this case we have that $[a_i, x_i] \in Z$ as desired. To verify our claim, notice that since $A \triangleleft G$ and A/Z is an elementary abelian 2-group, we have

$$\begin{aligned}
[[a_i, x_i], x_i] &= [a_i^{-1} x_i^{-1} a_i x_i, x_i] \\
&= (x_i^{-1} a_i^{-1} x_i) a_i x_i^{-1} a_i^{-1} x_i^{-1} a_i x_i x_i \\
&= a_i (x_i^{-1} a_i^{-1} x_i) x_i^{-1} a_i^{-1} x_i^{-1} a_i x_i^2 \\
&= a_i x_i^{-1} (a_i^{-1})^2 x_i^{-1} a_i x_i^2 \\
&= a_i x_i^{-1} (a_i^{-1})^2 x_i^{-1} x_i^2 a_i \\
&= a_i (a_i^{-1})^2 x_i^{-1} x_i^{-1} x_i^2 a_i \\
&= 1.
\end{aligned}$$

Hence, $[a_i, x_i]$ commutes with x_i and our claim is verified. Therefore, we may write

$[a_i, x_i] = z_i$ for some $1 \neq z_i \in Z$. To see that z_i is of order 2, notice

$$\begin{aligned}(z_i)^2 &= [a_i, x_i]^2 \\ &= a_i^{-1}(x_i^{-1}a_i x_i)a_i^{-1}x_i^{-1}a_i x_i \\ &= (a_i^{-1})^2(x_i^{-1}a_i x_i)x_i^{-1}a_i x_i \\ &= (a_i^{-1})^2 x_i^{-1}a_i a_i x_i \\ &= x_i^{-1}(a_i^{-1})^2 a_i^2 x_i \\ &= 1.\end{aligned}$$

Thus, the first statement is proven. To complete the proof we must consider two cases.

Case (i) G is of Type II. Consider $C_A(x_i x_j)$ $(j \neq i)$. We claim that $a_i a_j \in C_A(x_i x_j)$. To see this, first notice that since $a_i x_i \neq x_i a_i$ we have $a_i x_i x_j \neq x_i a_i x_j = x_i x_j a_i$. So $a_i \notin C_A(x_i x_j)$. Similarly, $a_j \notin C_A(x_i x_j)$. As $|A : C_A(x_i x_j)| = 2$ we may write $A/C_A(x_i x_j) = \{C_A(x_i x_j), C_A(x_i x_j)a_i\} = \{C_A(x_i x_j), C_A(x_i x_j)a_j\}$. It follows that $C_A(x_i x_j)a_i = C_A(x_i x_j)a_j$. Thus, $C_A(x_i x_j) = C_A(x_i x_j)a_i^2 = C_A(x_i x_j)a_i a_j$ and our claim is verified. Again, by the commutator identities introduced prior to Theorem (4.3) we have

$$\begin{aligned}1 &= [x_i x_j, a_i a_j] \\ &= [x_i, a_i a_j]^{x_j}[x_j, a_i a_j] \\ &= ([x_i, a_j][x_i, a_i]^{a_j})^{x_j}[x_j, a_j][x_j, a_i]^{a_j} \\ &= (z_i)^{a_j x_j} z_j \\ &= z_i z_j.\end{aligned}$$

Thus, we have $z_i z_j = 1 = z_i^2$. It follows that $z_i = z_j$ as desired.

Case (ii) G is of Type III. Then $|A : C_A(x_1 x_2)| = 4$ as the centralizers of x_1 and x_2 were chosen to be of index 2 in A. Notice that $C_A(x_1 x_2) \geq C_A(x_1) \cap C_A(x_2)$

and that $|A : C_A(x_1) \cap C_A(x_2)| \leq 4$. It follows that $C_A(x_1x_2) = C_A(x_1) \cap C_A(x_2)$. Assume that $a_1a_2 \in C_A(x_1x_2)$. Then $a_1a_2 \in C_A(x_1)$. As $a_2 \in C_A(x_1)$ we obtain the contradiction that $a_1a_2(a_2)^{-1} = a_1 \in C_A(x_1)$. It follows that $a_1a_2 \notin C_A(x_1x_2)$. Thus $1 \neq [x_1x_2, a_1a_2] = z_1z_2$ by arguments in the previous case. Finally, we see that $z_1 \neq (z_2)^{-1} = z_2$ which completes the proof. ■

Note that the proof of the following corollary was omitted in the article that we are analyzing. We offer a proof to clarify the result.

(4.6) **Corollary.** If G is of Type II or III, then $[G, A]$ is in the center of G. Moreover, if G is of Type II, $[G, A]$ has order 2; and if G is of Type III, $[G, A]$ is noncyclic of order 4.

Proof. Continue to use the notation of Corollary (4.4) and Lemma (4.5). We claim that we can write $A = \langle a_1, ..., a_k, Z\rangle$. To see this, let $\bar{a_i}$ denote the coset a_iZ of Z in A and suppose that

$$\prod_{j=1}^{k}(\bar{a_j})^{f_j} = Z \tag{9}$$

where $f_j \in \{0, 1\}$ for all $j \in \{1, ..., k\}$. Suppose further that $f_i \neq 0$ for some $i \in \{1, ..., k\}$. The following notation seems a little unnatural as we proceed by conjugating elements of G by cosets of Z in A. Technically, conjugation by a coset yields another set. But in this case, since we are conjugating by cosets of the center of G in A, we see that x^{aZ} is just the set containing x^a for all $x \in G$ and $a \in A$. For this reason, we identify the set $x^{aZ} = \{x^a\}$ with the element x^a.

Notice that $[a_i, x_i] = z_i$ if and only if $(a_i)^{-1}x_i a_i = x_i z_i$. Thus, by (9) we see that

$$\begin{aligned} x_i^{\prod_{j=1}^{k}(\bar{a_j})^{f_j}} &= (a_k)^{-f_k} \cdots (a_1)^{-f_1} x_i (a_1)^{f_1} \cdots (a_k)^{f_k} \\ &= (a_k)^{-f_k} \cdots (a_i)^{-f_i} x_i (a_i)^{f_i} \cdots (a_k)^{f_k} \\ &= (a_k)^{-f_k} \cdots (a_{i+1})^{-f_{i+1}} x_i z_i (a_{i+1})^{f_{i+1}} \cdots (a_k)^{f_k} \\ &= x_i z_i \\ &\neq x_i. \end{aligned}$$

But as $(x_i)^Z = x_i$, we have obtained a contradiction. Thus, $\prod_{j=1}^{k}(\bar{a_j})^{f_j} = Z$ if and only if $f_j = 0$ for all $j \in \{1, ..., k\}$. It follows that

$$|\{\prod_{j=1}^{k}(\bar{a_j})^{f_j} : f_j \in \{0, 1\}\}| = 2^k = |A/Z|.$$

Thus, $\{\prod_{j=1}^{k}(\bar{a_j})^{f_j} : f_j \in \{0, 1\}\} = A/Z$ and we may write $A/Z = \langle a_1 Z, ..., a_k Z\rangle$. So $A = \langle a_1, ..., a_k, Z\rangle$ and our claim is verified.

Now, we may write $G = \langle x_1, ..., x_k, A\rangle$. To prove that $[G, A] \leq Z$, it suffices to show that $[x_i, A] \leq Z$ for an arbitrary $i \in \{1, ..., k\}$. Let $a \in A$. Then we may write $a = (\prod_{j=1}^{k}(a_j)^{f_j})z$ for suitable $f_j \in \{0, 1\}$ and some $z \in Z$. Thus,

$$\begin{aligned} [x_i, a] &= (x_i)^{-1}a^{-1}x_i a \\ &= (x_i)^{-1}z^{-1}(a_k)^{-f_k} \cdots (a_1)^{-f_1} x_i (a_1)^{f_1} \cdots (a_k)^{f_k} z \\ &= (x_i)^{-1}(a_k)^{-f_k} \cdots (a_i)^{-f_i} x_i (a_i)^{f_i} \cdots (a_k)^{f_k} \qquad (10) \\ &= (x_i)^{-1}(a_k)^{-f_k} \cdots (a_{i+1})^{-f_{i+1}} x_i z_i (a_{i+1})^{f_{i+1}} \cdots (a_k)^{f_k} \\ &= z_i \end{aligned}$$

whenever $f_i = 1$ and $[x_i, a] = 1$ whenever $f_i = 0$. Hence, $[x_i, A] \leq Z$ for all $i \in \{1, ..., k\}$ and we see that $[G, A] \leq Z$. By (10) we also see that if G is of Type II,

then $[G, A] = \langle z_i \rangle$ for any $i \in \{1, ..., k\}$; and if G is of Type III, then $[G, A] = \{1, z_1, z_2, z_1 z_2\}$. This completes the proof. ■

(4.7) **Lemma.** Continuing with the notation of Corollary (4.4) and Lemma (4.5), the elements x_1, x_2, ..., x_k can be chosen to commute pairwise.

Proof. Consider first G of Type II. By Corollary (4.6), $[G, A] \leq Z$ and has order 2. Furthermore we may write $[G, A] = \langle [a_i, x_i] \rangle = \langle z \rangle$ for any $i \in \{1, ..., k\}$. We first show that for $i, j \in \{1, ..., k\}$ we have $[x_i, x_j] = z$ or 1. Consider the abelian subgroup $A_j = \langle x_j, C_A(x_j) \rangle$. Since $(x_j)^2 \in A$ and commutes with x_j we see that $x_j^2 \in C_A(x_j)$. Thus $|A_j : C_A(x_j)| = 2$ and $|A_j| = |A|$. So A_j is an abelian subgroup of maximum order in G. It follows by Corollary (4.6) that $[G, A_j]$ is of order 2; and as $1 \neq z = [a_j, x_j] \in [G, A_j]$, we may write $[G, A_j] = \langle z \rangle$. It follows that $[x_i, x_j] = z$ or 1.

We now prove by induction that the coset representatives x_1, ..., x_k may be chosen to commute pairwise. Consider x_1. For any $j \in \{2, ..., k\}$ such that $[x_1, x_j] = z$, we replace the coset representative x_j by $a_1 x_j$. Notice that for each such j, we have

$$[x_1, a_1 x_j] = [x_1, x_j][x_1, a_1]^{x_j} = z^2 = 1$$

since z is in the center of G. Also note that for each x_j that we replace, the replacement coset representative $a_1 x_j$ satisfies the same commutator relations with each of the a_i that we constructed in Lemma (4.5) as x_j. In other words, $[a_i, a_1 x_j] = 1$ $(j \neq i)$ and $[a_j, a_1 x_j] = z$. This completes the base case.

Now suppose that we have already chosen x_1, ..., x_k such that x_1, ..., x_{i-1} commute with x_j for all $j \in \{1, ..., k\}$. Then in particular, x_i commutes with x_1, ..., x_{i-1}. For any j > i such that $[x_i, x_j] = z$, we replace the coset representative x_j by $a_i x_j$. Notice that for each such j, we have

$$[x_i, a_i x_j] = [x_i, x_j][x_i, a_i]^{x_j} = z^2 = 1$$

since z is in the center of G. Thus we've constructed new coset representatives that commute with x_1, ..., x_i and our proof by induction is complete. Again notice that these replacement coset representatives satisfy the same commutator relations with each of the a_i constructed in Lemma (4.5).

Now consider G of Type III. By Corollary (4.6), $[G, A] \leq Z$ and is non-cyclic of order 4. Moreover, $[G, A] = \{1, z_1, z_2, z_1z_2\}$. I claim that $[x_1, x_2] \in [G, A]$. In this case, it follows easily that either $[x_1, x_2] = 1$, $[x_1, a_1x_2] = 1$, $[a_2x_1, x_2] = 1$, or $[a_2x_1, a_1x_2] = 1$. Thus we may choose coset representatives that commute. All that remains is to verify my claim. Consider the abelian subgroup $A_1 = \langle x_1, C_A(x_1)\rangle$. Since $(x_1)^2 \in A$ and commutes with x_1, we see that $(x_1)^2 \in C_A(x_1)$. Thus $|A_1 : C_A(x_1)| = 2$ and $|A_1| = |A|$. So A_1 is an abelian subgroup of maximum order in G. It follows by Corollary (4.6) that $[G, A_1]$ is non-cyclic of order 4. Clearly $[a_1, x_1] = z_1 \in [G, A_1]$; and since $a_2 \in A$ commutes with x_1 we see that $[x_2, a_2] = (z_2)^{-1} = z_2 \in [G, A_1]$. It follows that $[G, A_1] = \{1, z_1, z_2, z_1z_2\}$. As $[x_1, x_2] = [x_2, x_1]^{-1} \in [G, A_1]$, we see that $[x_1, x_2] \in \{1, z_1, z_2, z_1z_2\} = [G, A]$ as claimed. Notice once again that these replacement coset representatives satisfy the same commutator relations with each of the a_i constructed in Lemma (4.5). ■

(4.8) **Corollary.** If G is of Type II or III, then $[G, G] = [G, A]$. Moreover, G is nilpotent of class 2.

Proof. We first consider G of Type II. Continuing with the notation used in Corollary (4.4) and Lemma (4.5) we may write

$$G = \langle x_1, ..., x_k, A\rangle = \langle x_1, ..., x_k, a_1, ..., a_k, Z\rangle$$

and we may assume without loss that x_1, ..., x_k commute pairwise. By the commutator relations obtained in Lemma (4.5) it follows that for all g, $h \in G$ we have $[g, h] = z$ or 1 where $z = z_1 = \cdots = z_k$. Thus $[G, G] \leq [G, A]$. Equality fol-

lows immediately. Thus by Corollary (4.6) we have $[G, G] \leq Z$. As Z is a normal subgroup of G that contains $G' = [G, G]$ we see that G/Z is abelian. Hence, G is nilpotent of class 2. The result follows by an analogous argument for G of Type III. This completes the proof. ■

(4.9) **Lemma.** Continuing with the notation of Corollary (4.4) and Lemma (4.5), if G is of Type II, then G/Z is an elementary abelian 2-group of order 2^{2k} and is generated by the cosets x_1Z, ..., x_kZ, a_1Z, ..., a_kZ of Z in G. Similarly, if G is of Type III, then G/Z is an elementary abelian 2-group of order 2^4 and is generated by the cosets x_1Z, x_2Z, a_1Z, a_2Z of Z in G.

Proof. First consider G of Type II. By the proof of Corollary (4.6) and by Lemma (4.7) we may write

$$G = \langle x_1, ..., x_k, A\rangle = \langle x_1, ..., x_k, a_1, ..., a_k, Z\rangle$$

where $[x_i, x_j] = 1$ $(i \neq j)$. It follows immediately that

$$G/Z = \langle x_1Z, ..., x_kZ, a_1Z, ..., a_kZ\rangle.$$

Notice that

$$|G : Z| = |G : A||A : Z| = 2^k 2^k = 2^{2k},$$

by Corollary (4.4). Thus, G/Z is of order 2^{2k} as claimed.

Now, consider x_i for some $i \in \{1, ..., k\}$. As $(x_i)^2 \in A$ and commutes with x_j for each $j \in \{1, ..., k\}$, we see that $(x_i)^2 \in Z$. Also by Corollary (4.4), $(a_i)^2 \in Z$. Hence, since G/Z is abelian and each generator of G/Z is of order 2, we see that G/Z is an elementary abelian 2-group. An analogous argument for G of Type III completes the proof. ■

The following theorem summarizes the results regarding nonabelian $> \frac{1}{2}$-groups

obtained thus far. We continue with the notation developed in Corollary (4.4) and Lemma (4.5).

(4.10) **Structure Theorem.** If G is a nonabelian $> \frac{1}{2}$-group, then G is one of the following types.

Type I G has a maximal abelian subgroup A of index 2 in G. For any $> \frac{1}{2}$-automorphism α of G,

$$I(\alpha) = I(G) = \frac{q+1}{2q}$$

where $q = |A : C_A(x)|$ for any $x \notin A$.

Type II G is nilpotent of class 2 with commutator subgroup $\langle z \rangle$ of order 2. The center Z of G has index 2^{2k} (k ≥ 2) in G and G/Z is an elementary abelian 2-group. Moreover, G/Z is generated by the cosets $x_1Z, ..., x_kZ, a_1Z, ..., a_kZ$, of Z in G where

$$[x_i, x_j] = [a_i, a_j] = 1,$$

for all $i, j \in \{1, ..., k\}$,

$$[a_i, x_j] = 1,$$

for all $i, j \in \{1, ..., k\}$ such that $i \neq j$, and

$$[a_i, x_i] = z,$$

for all $i \in \{1, ..., k\}$. Furthermore, for any $> \frac{1}{2}$-automorphism α of G,

$$I(\alpha) = I(G) = \frac{2^k + 1}{2^{k+1}}.$$

Type III G is nilpotent of class 2 with noncyclic and hence elementary abelian commutator subgroup $\langle z_1, z_2 \rangle$ of order 4. The center Z of G has index 2^4 in G and G/Z is an elementary abelian 2-group. Moreover, G/Z is generated by the cosets

x_1Z, x_2Z, a_1Z, and a_2Z of Z in G where

$$[x_1, x_2] = [a_1, a_2] = [a_1, x_2] = [a_2, x_1] = 1,$$

$$[a_1, x_1] = z_1,$$

and

$$[a_2, x_2] = z_2.$$

Furthermore, for any $> \frac{1}{2}$-automorphism α of G we have

$$I(\alpha) = I(G) = \frac{9}{16}.$$

CHAPTER V

GROUPS CONSISTING MOSTLY OF INVOLUTIONS

In this chapter we explore $> \frac{1}{2}$-groups in which the identity automorphism inverts more than half of the group elements. Using arguments from Corollary (3.4) we see that if an automorphism α inverts over half of the elements of an abelian group H, then α inverts H elementwise. For this reason we see that the groups under consideration in this chapter are necessarily nonabelian, except for in the case where the group is inverted elementwise by the identity automorphism. Notice that such abelian groups are elementary abelian 2-groups or equivalently groups in which all nonidentity elements are involutions.

Throughout this chapter, let G denote a finite nonabelian group in which the identity automorphism, α say, inverts over half of the elements of G. Let A denote an abelian subgroup of maximum order in G and let Z denote the center of G. Finally, let G' denote the commutator subgroup of G. Notice that by the Structure Theorem of $> \frac{1}{2}$-groups presented in the previous chapter, G must be of even order. It follows that G has exactly $I(G)|G| - 1 \geq \frac{1}{2}|G|$ involutions.

(5.1) **Lemma.** Suppose that G is of Type I as defined in the Structure Theorem of the previous chapter. Then the center Z of G is an elementary abelian 2-group. Furthermore if A is an elementary abelian 2-group, then there exists an involution in $G - A$ that induces by conjugation an automorphism of G of order 2 in A. Otherwise, there exists an involution in $G - A$ that induces by conjugation an automorphism of G that inverts A elementwise.

Proof. First, consider the case in which A is an elementary abelian 2-group. It follows immediately that Z is as well. As at least half of the elements in G are involutions, we are guaranteed the existence of an involution $x \in G - A$. Thus, for all $a \in A$, we have $(a^x)^x = a^{x^2} = a$. Thus, x induces by conjugation the desired automorphism of G of order 2 in A.

Next, consider the case in which A is not an elementary abelian 2-group. Since A is an abelian subgroup of G, no more than half of A is inverted by α. Thus, less than $I(\alpha)|A|$ elements of A are in S_α. Now, choose some involution $x \in G - A$. As α is a $> \frac{1}{2}$-automorphism of G, it follows that at least $I(\alpha)|Ax|$ elements of Ax are in S_α. Thus, by the proof of the Subgroup Theorem and by Corollary (3.4), the inner automorphism, $I_x\alpha = I_x$, inverts A elementwise. It follows that for all $a \in A$, we have $x^{-1}ax = a^{-1}$. As x is an involution, we see that $(xa)^2 = 1$ for all $a \in A$. Thus, for all $z \in Z$ we have $(xz)^2 = x^2z^2 = z^2 = 1$. Hence Z is an elementary abelian 2-group as claimed. ■

Notice that in the latter case, G may be chosen to have arbitrary even order greater than or equal to 6. To see this, let $n = 2k$ for some $k \geq 3$ and consider the dihedral group, D_{2k}, of order $2k$. D_{2k} has a cyclic and hence abelian subgroup of index 2 that is inverted elementwise by the inner automorphism induced by any involution outside of the cyclic subgroup.

It is important to note that in the article under consideration, Liebeck and MacHale claim that in groups of Type I, abelian subgroups of maximum order are either elementary abelian 2-groups that are inverted elementwise by the identity automorphism, or are not elementary abelian. However, this claim is false. To verify this we consider the symmetric group on 3 elements, S_3. Since S_3 is a finite nonabelian group with an abelian subgroup of index 2, $\langle(123)\rangle$, such that the identity automorphism is a $> \frac{1}{2}$-automorphism, S_3 is of Type I. However, $\langle(123)\rangle$ is an abelian subgroup of maximum order that is an elementary abelian 3-group. Thus we altered the wording of the previous theorem to account for this mistake.

We now consider G of Type II or III as defined in the Structure Theorem of the previous chapter. Note that as we found the justification of the following results in "Groups with Automorphisms Inverting most Elements" to be difficult to follow or omitted entirely, we present alternative methods of determining the structure of

these groups.

(5.2) **Lemma.** If G is of Type II or III, then the elements of odd order form a subgroup Z_0 of the center Z of G.

Proof. Let x and y be elements of odd order in G. Then $x^m = y^n = 1$ for some odd integers m and n. We may assume that m and n are the smallest integers such that this happens. As G/Z is an elementary abelian 2-group, we see that $x^{-2} \in Z$. As $x^m \in Z$, we also see that $x^{m-2} \in Z$. Since m is odd, we may continue this process to show that $x \in Z$. Thus, elements of odd order are in fact contained in the center of G.

Now, notice that $(x^{-1})^m = (x^m)^{-1} = 1$ so the order of x^{-1} divides m and is hence odd. Furthermore,

$$(xy)^{mn} = x^{mn}y^{mn} = (x^m)^n(y^n)^m = 1,$$

so the order of xy divides mn and is hence odd. Thus, the elements of odd order in G form a subgroup Z_0 of Z and the proof is complete. ■

(5.3) **Lemma.** Let G be of Type II or III. Then G is a 2-group. Moreover, the center Z of G is an elementary abelian 2-group.

Proof. By way of contradiction, suppose that there exists some $x \in G$ of order $2j + 1$ for some $j \in \mathbb{N}$. Consider the subgroup $H = \langle x \rangle$. Let $G = H \cup Hg_2 \cup \cdots \cup Hg_n$ be a decomposition of G into distinct right cosets of H in G. Notice that as H is cyclic of odd order, there are no involutions in H. Consider the coset Hg_i for some $i \in \{2, ..., n\}$ and suppose that there exists some involution in Hg_i. We may without loss of generality assume that g_i is that involution for otherwise we simply exchange coset representatives. Note that by Lemma (5.2), $x \in Z$. Thus for any $x^b g_i \in Hg_i$ we have

$$(x^b g_i)^2 = x^{2b}(g_i)^2 = x^{2b} \neq 1.$$

Hence there is at most one involution in the coset Hg_i and we have obtained the contradiction that less than half of the elements in G are involutions. It follows immediately that G is a 2-group as claimed.

To see that Z is an elementary abelian 2-group, suppose by way of contradiction that there exists some $x \in Z$ of order 4. Again, consider the subgroup $H = \langle x \rangle$ and let $G = H \cup Hg_2 \cup \cdots \cup Hg_n$ be a decomposition of G into distinct right cosets of H in G. Notice that x^2 is the only involution in H. Consider the coset Hg_i for some $i \in \{2, ..., n\}$ and assume that some element of Hg_i is an involution. We may without loss of generality assume that g_i is that involtution for otherwise we exchange coset representatives. Notice that

$$(xg_i)^2 = x^2(g_i)^2 = x^2 \neq 1$$

as $x \in Z$. Similarly,

$$(x^3g_i)^2 = x^6(g_i)^2 = x^2 \neq 1.$$

It follows that exactly half of the elements of Hg_i are involutions. Again we obtain the contradiction that less than half of the elements of G are involutions. Thus, there are no elements of order 4 in Z and Z is an elementary abelian 2-group as claimed. This completes the proof. ■

(5.4) **Corollary** If G is of Type II, the center Z of G is isomorphic to the direct product $\langle z \rangle \times E$ where z generates the commutator subgroup of G and E is an elementary abelian 2-group. Similarly, if G is of Type III, Z is isomorphic to the direct product $\langle z_1, z_2 \rangle \times E$ where z_1 and z_2 generate the commutator subgroup of G and E is an elementary abelian 2-group.

Proof. The proof of this result is based on a well known fact from linear algebra that I will not prove: Any subspace of a vector space necessarily has a complement in that vector space. By the previous theorem we know that Z is an ele-

mentary abelian 2-group. Thus, we may view Z as a vector space over the field of 2-elements. Consider first G of Type II. Since $\langle z \rangle \leq Z$, we may view $\langle z \rangle$ as a subspace of Z. It follows that $\langle z \rangle$ has a complement E in Z. Such a complement is clearly also an elementary abelian 2-group. Since $\langle z \rangle$ and E are both normal subgroups of Z, we have $Z \cong \langle z \rangle \times E$ as desired. An analogous argument for G of Type III completes the proof. ■

For the moment we focus our attention on the case where G of Type II.

(5.5) **Lemma.** Let G be of Type II. Then the elementary abelian 2-group E obtained in Corollary (5.4) splits from G. Moreover, G is isomorphic to the direct product $G_0 \times E$ where $G_0 \leq G$ is of Type II with center $Z(G_0) = \langle z \rangle$ where z generates the commutator subgroup of G.

Proof. Take G_0 to be the largest subgroup of G with the property that the commutator subgroup $\langle z \rangle$ of G is contained in G_0 and $G_0 \cap E = 1$. Note that we are guaranteed the existence of such a G_0 since $\langle z \rangle$ satisfies the conditions. We see that $G_0 \trianglelefteq G$ since for all $u \in G_0$ and for all $g \in G$ we have $u^g = u[u, g] \in G_0$. As $E \leq Z$ we see that $E \trianglelefteq G$. We claim that $G_0 E = G$. It follows that $G \cong G_0 \times E$ as desired.

To verify our claim, by way of contradiction suppose that $G_0 E < G$ is a proper subgroup of G and choose some $g \in G - G_0 E$. Define $H = G_0 \langle g \rangle$. Then $G_0 < H$ is a proper subgroup of H. By the definition of G_0 there exists some nonidentity element $x \in H \cap E$. We may write $x = ag^i$ for some $a \in G_0$ and some $i \in \{0, 1, 2, 3\}$ since G/Z and Z are elementary abelian 2-groups. We consider four cases.

Case (i) $i = 0$. In this case $x = a \in G_0$. As $1 \neq x \in E$ this contradicts that $G_0 \cap E = 1$.

Case (ii) $i = 1$. Thus $x = ag$. It follows that $g = a^{-1}x \in G_0 E$. As we chose g to be outside of $G_0 E$, this is a contradiction.

Case (iii) $i = 2$. Thus $x = ag^2$. Now, $g^2 \notin G_0$ for otherwise we obtain the same contradiction as in the first case. In particular we see that $g^2 \neq 1$. Hence the

order of g is greater than 2. As $|G - G_0E| \geq \frac{|G|}{2}$, it follows that at least half of the elements in G have order greater than 2 which is a contradiction.

Case (iv) $i = 3$. Thus $x = ag^3$. As $g^{-2} \in Z \cong \langle z \rangle \times E$ which can be viewed as a subgroup of G_0E, we have $g = g^{-2}a^{-1}x = a^{-1}g^{-2}x \in G_0E$. which is a contradiction.

Thus our claim is verified and we may have $G \cong G_0 \times E$. It follows that $A \cong A_0 \times E$ for some abelian subgroup $A_0 \leq A$ of maximum order in G_0. Notice that since $G/E \cong G_0$ and $A/E \cong A_0$, we have

$$G/A \cong (G/E)/(A/E) \cong G_0/A_0.$$

It follows that G_0 is of Type II. Now, as $\langle z \rangle \leq G_0 \cap Z$, we have $\langle z \rangle \leq Z(G_0)$. To see the reverse containment, let $x \in Z(G_0)$. As G_0 and E are both normal subgroups of G that intersect trivially, we see that $[x, E] = 1$. It follows that $x \in Z \cap G_0 = \langle z \rangle$. Thus the center $Z(G_0)$ of G_0 is equal to $\langle z \rangle$ and the proof is complete. ■

Before proceeding to the next result we define what is known as the central product of extraspecial p-groups.

(5.6) **Definition.** Let P_1, ..., P_k be extraspecial p-groups. The finite group H is the *central product* of P_1, ..., P_k if the center of H is of order p and there exist subgroups H_1, ..., H_k of H such that $H_i \cong P_i$ for $i \in \{1, ..., k\}$ where $H = H_1 \cdots H_k$ and $[H_i, H_j] = 1$ for $i, j \in \{1, ..., k\}$ such that $i \neq j$. In this case we write $H = P_1 \circ \cdots \circ P_k$.

For the remainder of this paper we let D_8 denote the dihedral group of order 8 and Q_8 denote the quaternion group of order 8.

(5.7) **Corollary.** Let G be of Type II with commutator subgroup $G' = \langle z \rangle$. The subgroup $G_0 \leq G$ as defined in Lemma (5.5) is an extraspecial 2-group of order 2^{2k+1} where $|G : A| = |G_0 : A_0| = 2^k$ $(k \geq 2)$ and A_0 is as defined in the proof of Lemma (5.5). Moreover, G_0 is isomorphic to the central product of k copies of D_8.

Proof. Let G_0' denote the commutator subgroup of G_0 and $Z(G_0)$ denote the center of G_0. To prove that G_0 is an extraspecial 2-group we must show that G_0 is a 2-group such that $G_0' = Z(G_0)$, $|Z(G_0)| = 2$, and that $G_0/Z(G_0)$ is an elementary abelian 2-group. As G_0 is of Type II we know that G_0 is a 2-group and that $G_0/Z(G_0)$ is an elementary abelian 2-group. By Lemma (5.5) we see that $Z(G_0) = G'$ is of order 2. Now, G_0 is nonabelian so G_0' is nontrivial; and since $G_0' \leq G' = \langle z \rangle$ we see that $G_0' = G'$. Thus $G_0' = Z(G_0)$ as desired and G_0 is an extraspecial 2-group. By the Structure Theorem, $Z(G_0) = \langle z \rangle$ has index 2^{2k} in G_0. It follows that $|G_0| = 2^{2k}|Z(G_0)| = 2^{2k+1}$.

The remainder of the proof follows from results obtained from the text "Group Representation Theory" by Larry Dornhoff ([I], p. 181-193). We see that any extraspecial 2-group of order 2^{2k+1} is isomorphic to the central product of k extraspecial groups of order 2^3 and that $D_8 \circ D_8 \cong Q_8 \circ Q_8$. Since extraspecial groups are nonabelian and the only two nonabelian groups of order 8 up to isomorphism are D_8 and Q_8, it follows that either $G_0 \cong D_8 \circ D_8 \circ \cdots \circ D_8$ (k copies of D_8) or $G_0 \cong Q_8 \circ D_8 \circ \cdots \circ D_8$ ($k-1$ copies of D_8). We see that as the number of involutions in $Q_8 \circ D_8 \circ \cdots \circ D_8$ ($k-1$ copies of D_8) is only $2^{2k} - 2^k - 1 < \frac{|G_0|}{2}$, the latter case is impossible. This completes the proof. ■

We now focus on the case in which G is of Type III.

(5.8) **Lemma.** Let G be of Type III. Then the elementary abelian 2-group E obtained in Corollary (5.4) splits from G. Moreover, G is isomorphic to the direct product $G_0 \times E$ where G_0 is of Type III with center $Z(G_0) = \langle z_1, z_2 \rangle$ where z_1 and z_2 generate the commutator subgroup of G.

Proof. The proof of this result is analogous to the proof of Lemma (5.5). ■

(5.9) **Lemma.** Let G be of Type III and let G_0 be defined as in the previous lemma. Then G_0 is isomorphic to the direct product of two copies of D_8.

Proof. As G is of Type III, we may write $G/Z = \langle x_1Z, x_2Z, a_1Z, a_2Z \rangle$ where x_1,

x_2, a_1, and a_2 satisfy the commutator relations established in the Structure Theorem of the previous chapter. Let the subgroup $E \leq G$ be defined as in Corollary (5.4). Then since $G/E \cong G_0$ and $Z/E \cong Z(G_0)$ where $Z(G_0)$ is the center of G_0, we have

$$G/Z \cong (G/E)/(Z/E) \cong G_0/Z(G_0) = G_0/\langle z_1, z_2\rangle$$

where z_1 and z_2 generate the commutator subgroup of G. It follows that

$$G_0/Z(G_0) = \langle x_1Z(G_0), x_2Z(G_0), a_1Z(G_0), a_2Z(G_0)\rangle$$

and that

$$G_0 = \langle x_1, x_2, a_1, a_2, Z(G_0)\rangle = \langle x_1, x_2, a_1, a_2\rangle.$$

Consider the subgroup $P_1 = \langle x_1, a_1\rangle \leq G_0$ and recall that $G_0/Z(G_0)$ is an elementary abelian 2-group. Thus $\{x_1^2, a_1^2\} \subseteq \{1, z_1, z_2, z_1z_2\}$. We consider two cases.

Case (i) $x_1^2 = 1$ or z_1 and $a_1^2 = 1$ or z_1. In this case, since $[a_1, x_1] = z_1$ we have $P_1 = \{1, a_1, x_1, a_1x_1, z_1, a_1z_1, x_1z_1, a_1x_1z_1\}$. As P_1 is nonabelian of order 8 we have either $P_1 \cong D_8$ or Q_8.

Case (ii) Otherwise. There are 12 subcases to consider. We claim that in any subcase we obtain the contradiction that less than half of the elements in G_0 are involutions. To verify this claim, first notice that since $[a_1, x_1] = z_1$ and $[a_2, x_2] = z_2$, we see that

$$\begin{aligned} P_1 = \{&1, a_1, x_1, a_1x_1, z_1, a_1z_1, x_1z_1, a_1x_1z_1, z_2, a_1z_2,\\ &x_1z_2, a_1x_1z_2, z_1z_2, a_1z_1z_2, x_1z_1z_2, a_1x_1z_1z_2\} \end{aligned}$$

is of order 16. Now, since G_0 is of Type III, $|G_0 : Z(G_0)| = 2^4$. Thus $|G_0| = 64$ and

$|G_0 : P_1| = 4$. So we may write G_0 as the disjoint union of cosets

$$G_0 = P_1 \cup P_1a_2 \cup P_1x_2 \cup P_1a_2x_2. \tag{11}$$

Recall that $[a_2, P_1] = [x_2, P_1] = [a_2x_2, P_1] = 1$ and $\{(a_2)^2, (x_2)^2, (a_2x_2)^2\} \subseteq \langle z_1, z_2 \rangle$. In each subcase we simply count the number of involutions in G_0 by considering each coset in (11) separately.

We first consider the subcase in which $x_1^2 = 1$ and $a_1^2 = z_2$. In this subcase we have $(a_1x_1)^2 = a_1^2x_1^2z_1 = z_1z_2$. Note that P_1 has 7 involutions and consider the coset P_1a_2. The number of involutions in P_1a_2 is equal to the number of solutions to the equation

$$(ba_2)^2 = b^2a_2^2 = 1 \tag{12}$$

where $b \in P_1$. Thus if $a_2^2 = 1$ then P_1a_2 has 8 involutions. If $a_2^2 = z_1$ then P_1a_2 has no involutions. If $a_2^2 = z_2$ then P_1a_2 has 4 involutions. And if $a_2^2 = z_1z_2$ then P_1a_2 has 4 involutions. Hence the coset P_1a_2 has at most 8 involutions. Similar reasoning tells us that the cosets P_1x_2 and $P_1a_2x_2$ have at most 8 involutions as well. Thus G_0 has at most $7 + 8 + 8 + 8 = 31 < \frac{|G_0|}{2}$ involutions which is our desired contradiction. Note that the subcase in which $x_1^2 = z_2$ and $a_1^2 = 1$ results in the same contradiction by an analogous argument.

Next we consider the subcase in which $x_1^2 = 1$ and $a_1^2 = z_1z_2$. In this subcase we have $(a_1x_1)^2 = a_1^2x_1^2z_1 = z_2$. By arguments in the previous paragraph we obtain the contradiction that G_0 has at most 31 involutions. Note that the subcase in which $x_1^2 = z_1z_2$ and $a_1^2 = 1$ is similar.

Next we consider the subcase in which $x_1^2 = z_2$ and $a_1^2 = z_1z_2$. In this subcase we have $(a_1x_1)^2 = a_1^2x_1^2z_1 = 1$. Again by arguments in the first subcase we obtain the contradiction that G_0 has at most 31 involutions. The subcase in which $x_1^2 = z_1z_2$ and $a_1^2 = z_2$ is similar.

Next we consider the subcase in which $x_1^2 = z_1$ and $a_1^2 = z_2$. In this subcase we have $(a_1x_1)^2 = a_1^2x_1^2z_1 = z_2$. Note that P_1 has 3 involutions and consider the coset P_1a_2. Again to count the involutions in P_1a_2 it suffices to count the number of solutions to (12) where $b \in P_1$. Thus if $a_2^2 = 1$ then P_1a_2 has 4 involutions. If $a_2^2 = z_1$ then P_1a_2 has 4 involutions. If $a_2^2 = z_2$ then P_1a_2 has 8 involutions. And if $a_2^2 = z_1z_2$ then P_1a_2 has no involutions. Hence the coset P_1a_2 has at most 8 involutions. Similar reasoning tells us that the cosets P_1x_2 and $P_1a_2x_2$ have at most 8 involutions as well. Thus G_0 has at most $3 + 8 + 8 + 8 = 27$ involutions which is our desired contradiction. Note that the subcase in which $x_1^2 = z_2$ and $a_1^2 = z_1$ results in the same contradiction by an analogous argument.

Next we consider the subcase in which $x_1^2 = a_1^2 = z_2$. In this subcase we have $(a_1x_1)^2 = a_1^2x_1^2z_1 = z_1$. By arguments in the previous paragraph we obtain the contradiction that G_0 has at most 27 involutions.

Next we consider the subcase in which $x_1^2 = z_1$ and $a_1^2 = z_1z_2$. In this subcase we have $(a_1x_1)^2 = a_1^2x_1^2z_1 = z_1z_2$. Note that P_1 has 3 involutions and consider the coset P_1a_2. Again to count the involutions in P_1a_2 it suffices to count the number of solutions to (12) where $b \in P_1$. Thus if $a_2^2 = 1$ then P_1a_2 has 4 involutions. If $a_2^2 = z_1$ then P_1a_2 has 4 involutions. If $a_2^2 = z_2$ then P_1a_2 has no involutions. And if $a_2^2 = z_1z_2$ then P_1a_2 has 8 involutions. Hence the coset P_1a_2 has at most 8 involutions. Similar reasoning tells us that the cosets P_1x_2 and $P_1a_2x_2$ have at most 8 involutions as well. Thus G_0 has at most $3 + 8 + 8 + 8 = 27$ involutions which is our desired ccontradiction. Note that the subcase in which $x_1^2 = z_1z_2$ and $a_1^2 = z_1$ results in the same contradiction by an analogous argument.

Finally, we consider the subcase in which $x_1^2 = a_1^2 = z_1z_2$. In this subcase we have $(a_1x_1)^2 = a_1^2x_1^2z_1 = z_1$. By arguments in the previous paragraph we obtain the contradiction that G_0 has at most 27 involutions. This completes the verification of our claim and tells us that *case* (ii) does not occur in the groups under considera-

tion in this paper.

Hence $P_1 \cong D_8$ or Q_8. Similarly we see that the subgroup $P_2 = \langle x_2, a_2 \rangle \cong D_8$ or Q_8 as well. Notice that $P_1 \cap P_2 = 1$ and that since $[P_1, P_2] = 1$ we have

$$G_0 = \langle x_1, x_2, a_1, a_2 \rangle = \langle x_1, a_1 \rangle \langle x_2, a_2 \rangle = P_1 P_2.$$

Since P_1 and P_2 are normal subgroups of G_0 we see that $G_0 \cong P_1 \times P_2$. To see that $P_1 \cong P_2 \cong D_8$ we simply count involutions. Since Q_8 has a single involution, $Q_8 \times Q_8$ has only 3 involutions. And since D_8 has only 5 involutions $D_8 \times Q_8 \cong Q_8 \times D_8$ has only 11 involutions. Both cases yield a group that contradicts the definition of G_0. Hence result. ■

The following theorem summarizes the structure of nonabelian $> \frac{1}{2}$-groups in which at least half of the group elements are involutions.

(5.10) **Theorem.** If G is a $> \frac{1}{2}$-group in which at least half of the elements of G are involutions then G is one of the following types.

Type I G has a maximal abelian subgroup A of index 2 in G. The center Z of G is an elementary abelian 2-group. If A is inverted elementwise by the identity automorphism then there exists an involution outside of A that induces by conjugation an automorphism of G of order 2 in A. Otherwise, there exists an involution outside of A that induces by conjugation an automorphism of G that inverts A elementwise. Finally, G has $\frac{q+1}{2q}|G| - 1$ involutions where $q = |A : C_A(x)|$ for any $x \notin A$.

Type II G is a 2-group with maximal abelian subgroup A of index 2^k in G for some $k \geq 2$. The center Z of G is an elementary abelian 2-group isomorphic to the direct product $\langle z \rangle \times E$ where z generates the commutator subgroup of G and E is an elementary abelian 2-group. Moreover we have

$$G \cong G_0 \times E \cong (D_8 \circ D_8 \circ \cdots \circ D_8) \times E$$

(k copies of D_8) where G_0 is an extraspecial 2-group of order 2^{2k+1}. Finally, G has $\frac{2^k+1}{2^{k+1}}|G| - 1$ involutions.

Type III G is a 2-group with maximal abelian subgroup A of index 4 in G. The center Z of G is an elementary abelian 2-group isomorphic to the direct product $\langle z_1, z_2 \rangle \times E$ where z_1 and z_2 generate the commutator subgroup of G and E is an elementary abelian 2-group. Moreover we have

$$G \cong D_8 \times D_8 \times E.$$

Finally, G has $\frac{9}{16}|G| - 1$ involutions.

This completes our analysis of "Groups with Automorphisms Inverting most Elements", by Hans Liebeck and Desmond MacHale.

REFERENCES

I Dornhoff, Larry. *Group Representation Theory: Part A.* NY: Marcel Dekker Inc., 1971.

II Isaacs, I. Martin. *Algebra: A Graduate Course.* Providence, RI: American Mathematical Society, 2009.

III Liebeck, Hans, and Desmond MacHale. "Groups with Automorphisms Inverting most Elements." *Mathematische Zeitschrift* 124, no. 1 (January 1972): 51-63, accessed November 18, 2014, http://link.springer.com.libproxy.txstate.edu/article/10.1007/BF01142582.