THE AUTOMORPHISM TOWER OF A GROUP WITH TRIVIAL CENTER

by

GEOFFREY ALLAN KANDALL

A.B., Princeton University
(1958)

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE
DEGREE OF MASTER OF
SCIENCE
at the
MASSACHUSETTS INSTITUTE OF
TECHNOLOGY
June, 1960

Signature of Author Signature redacted
Department of Mathematics, May 20, 1960

Certified by Signature redacted
Thesis Supervisor

ABSTRACT

THE AUTOMORPHISM TOWER OF A GROUP WITH TRIVIAL CENTER

GEOFFREY ALLAN KANDALL

Submitted to the Department of Mathematics on May 20, 1960 in partial fulfillment of the requirements for the degree of Master of Science

This thesis is a collection of results relating to the automorphism tower of a group with trivial center.

The exposition is divided into four parts. The first part deals with the construction of the automorphism tower of such a group. This tower is denoted by:

$$A^0 < A^1 < A^2 < \ldots .$$

It is also proved in this section that the centralizer of A^i in A^j is equal to 1 if $j \geq i$.

In the second part, the following general theorem on normally persistent group properties is proved: A group property is normally persistent if and only if it is subnormally persistent. This theorem is then applied to two special cases and the results are used in Part III.

Part III contains a proof of the most important theorem connected with the automorphism tower. This theorem, due to H. Wielandt, asserts that the automorphism tower of a finite group with center 1 is of finite height.

In Part IV, the main theorem is illustrated by means of a few specific examples. The object of the investigation is to determine the stage at which the automorphism tower stops. The groups discussed are the symmetric groups S_n $(n \geq 3,\ n \neq 6)$, the alternating groups A_n $(n \geq 5)$, and certain groups of 2x2-matrices of order $p(p-1)$, p an odd prime.

THESIS SUPERVISOR: PROFESSOR KENKICHI IWASAWA

TITLE: PROFESSOR OF MATHEMATICS

TABLE OF CONTENTS

0. INTRODUCTION

The object of this thesis is to present proofs of some of the interesting properties of the automorphism tower of a group with trivial center. The main theorem to be proved is the following:

The automorphism tower of a finite group with trivial center is of finite height.

The exposition is divided into four parts. In Part I, we start with an arbitrary group with center 1 and show how its automorphism tower is constructed. A property of the centralizers of the groups in this tower is also proved. In Part II, we prove a general result on normally persistent group properties. This theorem states that a group property is normally persistent if and only if it is subnormally persistent. The specialization of this theorem to two particular cases is necessary for the proof of the main theorem. Part III is devoted to a proof of the main theorem stated above. This theorem was originally proved by Wielandt [4], but the proof given here follows the exposition of Zassenhaus [5]. Some of the details have been relegated to a series of lemmas. In Part IV, the notion of a complete group is introduced and related to Wielandt's theorem. Some examples are then provided to show, in a few special cases, when the automorphism tower stops.

I would like to express my thanks to Professor Kenkichi Iwasawa, whose many helpful suggestions were of great

assistance to me in writing this paper.

I. THE AUTOMORPHISM TOWER

Notation: Suppose G is any group. We denote the group of automorphisms of G by A(G) or by $A^1(G)$. The group $A^n(G)$ is defined inductively by $A^n(G) = A(A^{n-1}(G))$ for $n \geq 2$. The group of inner automorphisms of G will be denoted by I(G). The symbols $A^n(G)$, I(G) may be abbreviated to A^n, I if it is clear that no confusion will result.

If $X, Y \subset G$, we denote the centralizer of X in Y by Z(X,Y), that is, Z(X,Y) is the set of all $y \in Y$ which permute elementwise with X. The center of X, Z(X,X), will be written simply as Z(X). The normalizer of X in Y will be denoted by N(X,Y).

If X is a normal subgroup of G, we write $X \lhd G$.

Let G be any group, x a fixed element of G. Let δ_x denote the inner automorphism of G determined by x:

$$\delta_x(g) = xgx^{-1} = g^x \text{ for all } g \in G.$$

Since $\delta_{xy}(g) = \delta_x\delta_y(g)$, the mapping $x \dashrightarrow \delta_x$ is a homomorphism of G onto I. The kernel of this mapping is clearly Z(G) = Z, hence $G/Z \cong I$.

Choose arbitrary elements $a \in A$, $\delta_x \in I$. For any $g \in G$: $a\delta_x a^{-1}(g) = a(xa^{-1}(g)x^{-1}) = a(x)ga(x)^{-1} = \delta_{a(x)}(g)$. Hence we have the useful rule: $a\delta_x a^{-1} = \delta_{a(x)}$. This rule shows,

in particular, that $I < A$.

For the remainder of this section, we make the assumption that $Z(G) = 1$. Then $G \cong I$ under the one-to-one correspondence $x \longleftrightarrow \delta_x$.

Theorem 1.1: (i) $Z(I,A) = 1$ (ii) $Z(A) = 1$
(iii) Any automorphism of I is induced by an inner automorphism of A.

Proof: (i) Suppose $a \in Z(I,A)$. Then $\delta_x = a\delta_x a^{-1} = \delta_{a(x)}$ for all $x \in G$. This implies $x = a(x)$ or $a = 1$.

(ii) $Z(A) \subset Z(I,A) = 1$.

(iii) Let ϕ be any automorphism of I. Since $G \cong I$, there exists $a \in A$ such that $\phi(\delta_x) = \delta_{a(x)} = a\delta_x a^{-1}$.

From now on, when $Z(G) = 1$ we will identify G with I and write $G < A$. Since $Z(A) = 1$, we also have $A < A^2$. Continuing in this fashion, we obtain the automorphism tower of G:

$$G < A^1 < A^2 < \ldots < A^n < \ldots .$$

Putting $G = A^0$, we see that we have proved that for all $i \geq 0$: $Z(A^i, A^{i+1}) = 1$, $Z(A^i) = 1$.

Theorem 1.2: (i) If $Z(A^i, A^j) = 1$ and $j-i \geq 1$, then $N(A^i, A^j) = A^{i+1}$. (ii) $Z(A^i, A^j) = 1$ if $j \geq i$.

Proof: (i) $A^{i+1} \subset A^j$, so it is clear that $A^{i+1} \subset N(A^i, A^j)$. On the other hand, suppose that $x \in N(A^i, A^j)$. The mapping $u \longrightarrow u^x$ $(u \in A^i)$ is an automorphism of A^i. Hence there

exists $y \in A^{i+1}$ such that $u^x = u^y$ for all $u \in A^i$. This implies that $y^{-1}x \in Z(A^i, A^j) = 1$. Therefore $x = y \in A^{i+1}$.

(ii) We proceed by induction on $j-i$. The truth of the assertion (ii) for the cases $j-i = 0,1$ has already been established. Assume (ii) is true for $j-i = k \geq 1$ and now suppose that $j-i = k+1 \geq 2$. Note that (i) together with the induction hypothesis implies $N(A^i, A^{j-1}) = A^{i+1}$, $N(A^{i+1}, A^j) = A^{i+2}$.

Suppose that $a \in Z(A^i, A^j)$. Then we have $(A^{i+1})^a = N((A^i)^a, (A^{j-1})^a) = N(A^i, A^{j-1}) = A^{i+1}$. Hence $a \in N(A^{i+1}, A^j) = A^{i+2}$. Choose any $x \in A^{i+1}$, $y \in A^i$. Then $y(x^a) = ax(a^{-1}ya)x^{-1}a^{-1} = y^{ax} = (y^x)^a = y^x$. Therefore $x^{-1}x^a \in Z(A^i, A^{i+1}) = 1$. Hence $x = x^a$ for all $x \in A^{i+1}$, that is, $a \in Z(A^{i+1}, A^{i+2}) = 1$.

The only property of G which we needed in order to construct the automorphism tower was $Z(G) = 1$. We now assume that G is finite. With only this simple additional assumption, we are able to obtain the following remarkable result:

The automorphism tower of G is of finite height, that is, there exists N such that $A^n = A^N$ for all $n \geq N$.

Chapter III is devoted to a proof of this theorem. But first we derive some preliminary results, which are quite interesting in themselves.

II. NORMAL AND SUBNORMAL PERSISTENCE

Notation: Suppose G is any group. If G possesses a certain property Q, then we call G a Q-group.

Suppose $X, Y \subset G$. The set obtained from X by conjugating its elements by the elements of Y is denoted by $C(X,Y)$, that is, $C(X,Y)$ is the set of all elements of the form $x^y = yxy^{-1}$, where $x \in X$, $y \in Y$. The subgroup of G generated by X will be denoted by $[X]$.

A subgroup G of a group H is said to be a subnormal subgroup of H if there exists a finite normal chain from G to H:

$$G < G_1 < G_2 < \dots < G_r < H. \qquad (*)$$

We denote the least possible length of such a chain by $m(G,H)$. If G is subnormal in H, we write $G << H$. Trivially, $G < H$ implies $G << H$.

If (*) holds and $h \in H$, then we have:

$$G^h < G_1^h < \dots < G_r^h < H^h = H.$$

It follows that if $G << H$ and K is a conjugate subgroup of G, then $K << H$ and $m(K,H) = m(G,H)$.

Let Q be a property of groups. Q is called normally persistent (resp. subnormally persistent) if and only if Q satisfies the following two conditions:

(1) Any group isomorphic to a Q-group is a Q-group

(2) In a given group, the subgroup generated by a non-empty set of normal (resp. subnormal) Q-subgroups is a Q-group.

We will abbreviate the phrase normally persistent (resp. subnormally persistent) by NP (resp. SP).

Lemma 2.1: Let S be a non-empty set of subnormal Q-subgroups of a group G, where Q is a NP group property. Suppose that $m(X,G) \leq n$ for all $X \in S$. Then $S' = [\cup_{X \in S} X]$ is a Q- group.

Proof: The proof is by induction on n. If $n = 0$, $X = G = S'$ for all $X \in S$. Hence S' is a Q-group, because X is. If $n = 1$, each $X < G$. S' is a Q-group in this case because Q is NP. Now suppose $n > 1$ and assume that the theorem is true whenever the function values of m are at most n-1 as X ranges over the given set of subgroups.

Consider some $X \in S$. There exists a normal chain $X = X_0 < X_1 < \ldots < X_n = G$ of length n, possibly with repetitions. For any $g \in S'$:

$$X^g = X_0^g < X_1^g < \ldots < X_{n-1}^g = X_{n-1}.$$

$X^g \cong X$, hence each X^g is itself a Q-group. The set of all X^g ($g \in S'$) is therefore a set of subnormal Q-subgroups of X_{n-1} and $m(X^g, X_{n-1}) \leq n-1$ for all $g \in S'$. By induction: $X' = [\cup_{g \in S'} X^g] = [C(X,S')]$ is a Q-group. $X' < S'$. Then $S' = [\cup_{X \in S} X']$ and Q being NP imply S' is a Q-group.

Theorem 2.2: A group property Q is NP if and only if it is SP.

Proof: Trivially, if Q is SP, then it is certainly NP. To prove the converse, suppose Q is NP, T is a non-empty set of subnormal Q-subgroups of a group G, $T' = [\cup_{X\in T} X]$. We have to show that T' is a Q-group.

If $X \in T$, put $X' = [\cup_{g\in T'} X^g] = [C(X,T')]$. Then $X' < T'$ and $T' = [\cup_{X\in T} X']$. Take S to be the set of all X^g $(g \in T')$. $m(X^g,G)$ is a finite constant for all $g \in T'$. The conditions of Lemma 2.1 are satisfied and so X' is a Q-group. Hence T' is a Q-group, since Q is NP.

A group G is said to be a p-group if the order of every element of G is a power of the prime p. If G is finite, this is equivalent to saying that the order of G is a power of p. The property of being a p-group is NP.

A group G is said to be semi-simple if it may be decomposed into a direct product of non-abelian simple groups. The property of being a semi-simple group is NP.

From Theorem 2.2 and the above remarks, we have:

Theorem 2.3: Any non-empty set of subnormal p-subgroups (resp. subnormal semi-simple subgroups) of a group generate a p-subgroup (resp. semi-simple subgroup). In particular, the normal subgroup generated by all the conjugates of a subnormal p-subgroup (resp. subnormal semi-simple subgroup) is a p-subgroup (resp. semi-simple subgroup).

III. WIELANDT'S THEOREM

Notation: Suppose G and H are groups. The direct product of G and H will be denoted by $G + H$. If $H \subset G$, we will denote the index of H in G by $G:H$. If $x,y \in G$, we will write $(x,y) = xyx^{-1}y^{-1}$. If G and H are both subgroups of some larger group, then (G,H) will denote the subgroup generated by all elements of the form (g,h), where $g \in G$, $h \in H$.

Lemma 3.1: Suppose $G \neq 1$ is a finite group, N a minimal normal subgroup of G. Then N is a direct product of isomorphic simple groups.

Proof: If N is simple, there is nothing to prove. If N is not simple, let H_1 be a minimal normal subgroup of N. Let $H_1, H_2, \ldots, H_m$ $(m > 1)$ be the subgroups conjugate to H_1 in G. Each $H_i < N$ and $H_i \cong H_j$ for all i,j. $[H_1, \ldots, H_m]$ is normal in G and is contained in N, hence $[H_1, \ldots, H_m]$ is equal to N. Choose the smallest number of these H_i which generate N. Suppose that these are $H_1, \ldots, H_n$ $(n > 1)$, renumbering if necessary. Clearly $H_i \cap [H_1, \ldots, H_{i-1}] = 1$ for each i, $1 \leq i \leq n$, because of the minimal nature of the H_i. Hence $N = H_1 + H_2 + \ldots + H_n$. Furthermore, H_i is simple. For if it is not, there exists $K_i < H_i$ such that $K_i \neq 1, H_i$. Then $K_i < N$, contradicting the minimal property of H_i.

Lemma 3.2: Suppose A, B are subnormal in a finite group G,

A is semi-simple, $H = [A,B]$. Then $B < H$.

Proof: Let $A' = [C(A,H)]$. Then $A' < H$ and Theorem 2.3 shows that A' is semi-simple. $B \ll H$ (Zassenhaus [5]). Consider a normal chain of minimal length s from B to H:

$$B = B_0 < B_1 < \ldots < B_s = H.$$

Clearly $B_{s-1} \cap A' < A'$. We now use the fact that in any semi-simple group, any normal subgroup has one and only one complementary normal subgroup. There exists $A_1 < A'$ such that $A' = A_1 + (B_{s-1} \cap A')$. If $h \in H$, we obtain $A' = A_1^h + (B_{s-1} \cap A')$. Hence $A_1^h = A_1$, or $A_1 < H$. Now $x \in A_1 \cap B_{s-1}$ implies that $x \in A_1 \cap (B_{s-1} \cap A') = 1$. Also $A' = [A_1, B_{s-1} \cap A'] \subset [A_1, B_{s-1}]$ and clearly we also have $B \subset [A_1, B_{s-1}]$. Therefore $H = [A', B] \subset [A_1, B_{s-1}]$. It follows that $H = A_1 + B_{s-1}$. If $s > 1$, the same argument shows that there exists a subgroup A_2 such that $B_{s-1} = A_2 + B_{s-2}$. Thus $H = A_1 + A_2 + B_{s-2}$. So $B_{s-2} < H$ and $B = B_0 < B_1 < \ldots < B_{s-2} < B_s = H$ is a normal chain from B to H of length s-1, a contradiction. Hence $s \leq 1$, that is, $B < H$.

Lemma 3.3: Let x,y be elements of a group G, $(x,y) = z$, $n \geq 1$. Then $(x^n,y) = z^{x^{n-1}} \ldots z^x z$.

Proof: It is easy to check the following general commutator identity: $(ab,c) = (b,c)^a(a,c)$. Our lemma is trivially true for $n = 1$. Assume that it is true for some $n \geq 1$. Then $(x^{n+1},y) = (x^n x,y) = (x,y)^{x^n}(x^n,y) = z^{x^n} z^{x^{n-1}} \ldots z^x z$, hence it is true for n+1. This completes the proof.

Lemma 3.4: Suppose G is a group, $H < G$, $G:H = n$. Then $x^n \in H$ for all $x \in G$.

Proof: The order of G/H is n. Therefore for any $x \in G$: $(xH)^n = x^nH = H$. This implies $x^n \in H$.

Lemma 3.5: Suppose P is a Sylow p-subgroup of G, $N < G$. Then (i) $N \cap P$ is a Sylow p-subgroup of N (ii) PN/N is a Sylow p-subgroup of G/N.

Proof: It is clear that a subgroup H of G is a Sylow p-subgroup of G if and only if $H:1$ is a power of p and $G:H$ is relatively prime to p.

$NP:P$, $G:NP$ are prime to p, $P:N\cap P$, $N\cap P:1$ are powers of p. Then $NP:N = P:N\cap P$ is a power of p. Also since $(NP:P)(P:N\cap P) = NP:N\cap P = (NP:N)(N:N\cap P)$, we have that $NP:P = N:N\cap P$ is prime to p.

Statements (i), (ii) now follow easily.

Lemma 3.6: Let G be a p-group, $N < G$, $N \neq 1$. Then $N \cap Z(G) \neq 1$.

Proof: Since $N < G$, N is a union of complete conjugate classes of G. Let $N \cap Z(G):1 = k$. This means that N contains exactly k conjugate classes which consist of only one element. The number of elements in each of the other conjugate classes contained in N is divisible by p. Since $N:1$ is also divisible by p, p divides k. Hence $k \geq 1$. This proves the lemma.

Theorem 3.7: Suppose G, H are finite groups, $G \ll H$, and $Z(G,H) = 1$. Then there exists a constant M, depending only on G, such that $H:1 \leq M$.

Proof: If $G = 1$, it follows that $H = 1$, hence we may take $M = 1$. Suppose that $G \neq 1$. Consider a minimal normal subgroup of G. By Lemma 3.1, this subgroup is either a p_1-group for some prime p_1 or semi-simple. Depending on which case occurs, let V_1 be either the maximal normal p_1-subgroup of G or the maximal normal semi-simple subgroup of G. If $V_1 \neq G$, we repeat this construction in the group G/V_1, thus obtaining $V_2/V_1 < G/V_1$. Continuing in this way, we eventually obtain a finite normal chain:

$$1 = V_0 < V_1 < V_2 < \ldots < V_r = G,$$

where $V_i < G$ and V_{i+1}/V_i is either a p_{i+1}-group or semi-simple.

Define $H_i = [C(V_i,H)]$. $H_i < H$, hence we have a normal chain:

$$1 = H_0 < H_1 < H_2 < \ldots < H_r < H.$$

Clearly $H_{i+1}/H_i = [C(V_{i+1}H_i/H_i, H/H_i)]$. Notice that $V_{i+1}H_i/H_i \cong V_{i+1}/V_{i+1}\cap H_i \cong (V_{i+1}/V_i)/(V_{i+1}\cap H_i/V_i)$. Hence if V_{i+1}/V_i is a p_{i+1}-group (resp. semi-simple), so is $V_{i+1}H_i/H_i$, and therefore H_{i+1}/H_i is a p_{i+1}-group (resp. semi-simple), by Theorem 2.3.

We will now show by induction on i that $H_i \cap G = V_i$. For $i = 0$, this statement reduces to $1 \cap G = 1$. Suppose that $H_i \cap G = V_i$ $(i < r)$. $V_i < H_{i+1} \cap G$. Then since $H_{i+1}\cap G/V_i = H_{i+1}\cap G/H_i \cap G$, we deduce that if H_{i+1}/H_i is a

p_{i+1}-group (resp. semi-simple), then so is $H_{i+1} \cap G/V_i$. But $V_{i+1} \subset H_{i+1} \cap G$. By the maximal property of V_{i+1}, we have $V_{i+1} = H_{i+1} \cap G$. This completes the induction.

Now the following problem faces us. We want to show the existence of subgroups $X(i+1)$ of G $(i = 0, \ldots, r-1)$ which depend only on G and which also satisfy:

$$(X(i+1), H_{i+1}) \subset H_i V_{i+1} \qquad (*)$$

$$Z(X(i+1), H_{i+1}) \subset H_i \qquad (**).$$

If V_{i+1}/V_i is semi-simple, the problem is easily solved. For then H_{i+1}/H_i is semi-simple and also we know that $GH_i/H_i \ll H/H_i$. By Lemma 3.2, we obtain that $GH_i/H_i < [GH_i/H_i, H_{i+1}/H_i] = GH_{i+1}/H_i$, that is, $GH_i < GH_{i+1}$. This easily implies that $(G, H_{i+1}) \subset H_{i+1} \cap GH_i$. Since $H_{i+1} \cap GH_i = H_i(G \cap H_{i+1}) = H_i V_{i+1}$, we have the result $(G, H_{i+1}) \subset H_i V_{i+1}$. Furthermore, we have:

$$Z(G, H_{i+1}) \subset Z(G, H) = 1 \subset H_i.$$

Hence in this case we may take $X(i+1) = G$.

If, however, V_{i+1}/V_i is a p_{i+1}-group, we must work a little harder. Let U_{i+1} be the intersection of all normal subgroups of G whose index in G is a power of p_{i+1}. Then $U_{i+1} < G$ and $G:U_{i+1}$ is a power of p_{i+1}. It is known that if the exponent of G/U_{i+1} divides p_{i+1}^n, then U_{i+1} is the subgroup generated by all p_{i+1}^n-powers of elements of G. We will show that U_{i+1} has the properties we require of $X(i+1)$.

Since $G \ll H$, there exists a normal chain:

$$G = G_0 < G_1 < G_2 < \ldots < G_s = H.$$

Let $G(i,j) = H_i(G_j \cap H_{i+1}) = H_iG_j \cap H_{i+1}$. By the Zassenhaus Lemma, $G(i,0) < G(i,1) < \ldots < G(i,s) = H_{i+1}$. Let $G'(i,j)$ be the set of all $x \in G$ such that $(x,H_{i+1}) \subset G(i,j)$.

Now suppose $x \in G'(i,j)$, $h \in H_{i+1}$. By definition of $G'(i,j)$, $(x,h) \in G(i,j)$. Put $(x,h) = w$ and consider $(x^n,w) = x^nwx^{-n}w^{-1} = wx^nw^{-1}$ $(n \geq 1)$. Clearly $(x^n,w) \in H_{i+1}$. Since $G(i,j) \subset H_iG_j$, we may put $w = ab$, where $a \in H_i$, $b \in G_j$. Then $(x^n,w) = x^na(bx^{-n}b^{-1})a^{-1}$. We know that $x \in G \subset G_{j-1} < G_j$, hence $(x^n,w) = (x^na)(ca^{-1})$, where $c \in G_{j-1}$. $(x^n,w) \in G_{j-1}H_i$, hence $(x^n,w) \in H_iG_{j-1} \cap H_{i+1} = G(i,j-1)$. It follows that w, $w^{x^n} \in G(i,j)$ and are congruent modulo $G(i,j-1) < G(i,j)$. Now by Lemma 3.3, $(x^n,h) = w^{x^{n-1}} \ldots w^xw$. Therefore $(x^n,h) \in G(i,j)$ and is congruent to w^n modulo $G(i,j-1)$. This shows that if $x \in G'(i,j)$, then so is x^n $(n \geq 1)$. Now by Lemma 3.4, $(x^{G(i,j):G(i,j-1)},h) \in G(i,j-1)$, that is, $x^{G(i,j):G(i,j-1)} \in G'(i,j-1)$. Now since $G(i,j):G(i,j-2)$ is the product of $G(i,j):G(i,j-1)$ and $G(i,j-1):G(i,j-2)$, we have that $x^{G(i,j):G(i,j-2)} \in G'(i,j-2)$. Continuing in this manner, we obtain $x^{G(i,j):G(i,0)} \in G'(i,0)$. Notice that $H_{i+1}:H_i = (H_{i+1}:G(i,j))(G(i,j):G(i,0))(G(i,0):H_i)$. This implies that $x^{Hi+1:Hi} \in G'(i,0)$ for all $x \in G'(i,j)$. Since this holds for any j: $x^{Hi+1:Hi} \in G'(i,0)$ for all $x \in G'(i,s) = G$. $H_{i+1}:H_i$ is a power of p_{i+1}. Since U_{i+1} is generated by all the p_{i+1}^n-powers of G for large n, we deduce that $U_{i+1} \subset G'(i,0)$. Therefore $(U_{i+1}, H_{i+1}) \subset G(i,0) = H_i(G \cap H_{i+1})$

$= H_iV_{i+1}$, so (*) holds with $X(i+1) = U_{i+1}$.

For convenience, put $W = Z(U_{i+1},H_{i+1}) = Z(U_{i+1},H) \cap H_{i+1}$. If $x \in G$, then $W^x = Z(U_{i+1}^x,H) \cap H_{i+1}^x = Z(U_{i+1},H) \cap H_{i+1} = W$. Therefore $W < WG$. Let P be a Sylow p_{i+1}-subgroup of G. P is contained in some Sylow p_{i+1}-subgroup P' of WG. Clearly $Z(P') \cap W \subset Z(U_{i+1},H) \cap Z(P,H) = Z(U_{i+1}P,H)$. By Lemma 3.5 (ii), $U_{i+1}P/U_{i+1}$ is a Sylow p_{i+1}-subgroup of G/U_{i+1}, a p_{i+1}-group. Therefore, we have $U_{i+1}P = G$. Hence $Z(P') \cap W \subset Z(G,H) = 1$. Now $W < WG$ implies that $W \cap P' < P'$. We deduce that $W \cap P' = 1$, for if it were greater than 1, we would have $P' \cap W \cap Z(P') = W \cap Z(P') \neq 1$ by Lemma 3.6, a contradiction. Since $W < WG$, P' a Sylow p_{i+1}-subgroup of WG, it follows from Lemma 3.5 (i) that $W \cap P'$ is a Sylow p_{i+1}-subgroup of W. But $W \cap P' = 1$. Hence p_{i+1} does not divide $W:1 = Z(U_{i+1},H) \cap H_{i+1}$. Hence p_{i+1} does not divide $Z(U_{i+1},H)\cap H_{i+1} : Z(U_{i+1},H)\cap H_i = (Z(U_{i+1},H)\cap H_{i+1})H_i : H_i$. But $(Z(U_{i+1},H)\cap H_{i+1})H_i : H_i$ divides $H_{i+1}:H_i$, a power of p_{i+1}. It follows that we have $(Z(U_{i+1},H)\cap H_{i+1})H_i : H_i = 1$, hence $Z(U_{i+1},H)\cap H_{i+1} = Z(U_{i+1},H_{i+1}) \subset H_i$. Thus we see that (**) holds with $X(i+1) = U_{i+1}$.

We will now use these subgroups $X(i+1)$ to obtain the bound on $H:1$. Because of the property (*), each $x \in H_{i+1}$ determines a function $\phi_x: X(i+1) \longrightarrow H_iV_{i+1}$ given by $\phi_x(z) = (z,x)$ for all $z \in X(i+1)$. There are at most $(H_iV_{i+1}:1)^{X(i+1):1}$ such functions. But clearly $\phi_x = \phi_y$ if and only if $y^{-1}x \in Z(X(i+1),H_{i+1})$, that is, if and only if

x and y lie in the same left coset of $Z(X(i+1),H_{i+1})$. The number of distinct ϕ's is therefore equal to $H_{i+1}:Z(X(i+1),H_{i+1})$. Hence:

$$H_{i+1}:Z(X(i+1),H_{i+1}) \leq (H_iV_{i+1}:1)^{X(i+1):1}.$$

From (**) : $Z(X(i+1),H_{i+1}) \subset H_i \subset H_{i+1}$, therefore $H_{i+1}:H_i \leq H_{i+1}:Z(X(i+1),H_{i+1}) \leq (H_iV_{i+1}:1)^{X(i+1):1}$. Hence $H_{i+1}:H_i \leq (H_iV_{i+1}:H_i)^{X(i+1):1}(H_i:1)^{X(i+1):1}$. Now use the following: $H_iV_{i+1}:H_i = V_{i+1}:H_i\cap V_{i+1} \leq V_{i+1}:V_i$, which easily follows from $V_i \subset H_i\cap V_{i+1} \subset V_{i+1}$. This yields the estimate: $H_{i+1}:H_i \leq (V_{i+1}:V_i)^{X(i+1):1}(H_i:1)^{X(i+1):1}$. Since $H_{i+1}:1 = (H_{i+1}:H_i)(H_i:1)$, we obtain:

$$H_{i+1}:1 \leq (V_{i+1}:V_i)^{X(i+1):1}(H_i:1)^{X(i+1):1} + 1$$

Since $V_r = G$, we have $G \subset H_r$. $Z(H_r,H) \subset Z(G,H) = 1$. Every $h \in H$ gives rise to an inner automorphism of H which induces an automorphism of H_r. Since $Z(H_r,H) = 1$, each of these automorphisms of H_r is distinct from the others. Therefore $(H:1) \leq A(H_r):1 \leq (H_r:1)!$

Define the numbers M_i $(i = 0, 1, \ldots, r)$ by: $M_0 = 1$, $M_{i+1} = (V_{i+1}:V_i)^{X(i+1):1}M_i^{X(i+1):1} + 1$, for $i = 0, 1, \ldots, r-1$. Furthermore, define $M = M_r!$.

A simple induction argument shows that $H_i:1 \leq M_i$ for each i. In particular, $H_r:1 \leq M_r$. Hence:

$$H:1 \leq M_r! = M.$$

We need only observe that all the V_i's and $X(i)$'s depend only on G. Hence M depends only on G. This completes the proof.

Theorem 3.8 (Wielandt's Theorem): Suppose G is a finite group such that $Z(G) = 1$. Then its automorphism tower is of finite height.

Proof: Let $G = A^0 < A^1 < \ldots < A^n < \ldots$ be the automorphism tower of G. $G \ll A^n$ and by Theorem 1.2 (ii), we have $Z(G,A^n) = 1$. Then there exists a constant M, which depends only on G, such that $A^n:1 \leq M$. Hence the tower must be of finite height.

IV. COMPLETE GROUPS

A group G is said to be complete if $Z(G) = 1$ and every automorphism of G is an inner automorphism.

Clearly if G is complete, then $G \cong A$. Hence its automorphism tower collapses to only one term.

Theorem 4.1: Suppose G is a finite group with $Z(G) = 1$. Then G can be imbedded subnormally in a finite complete group which also has center 1.

Proof: Consider the automorphism tower of G:

$$G = A^0 < A^1 < A^2 < \ldots \quad .$$

By Wielandt's Theorem, there exists an integer N such that $A^N = A^{N+1} = A^{N+2} = \ldots$. Clearly A^N is a complete group with center 1, and $G \ll A^N$.

We will now consider some examples of finite groups

with center 1. Our object will be to determine at what stage the automorphism tower stops. In other words, we want to find the first complete group which occurs in the tower.

Theorem 4.2: S_n, the symmetric group of degree n, is complete when $n \geq 3$, $n \neq 6$.

Proof: We first note that $n \geq 3$ implies $Z(S_n) = 1$. For suppose $x \in S_n$ and $x \neq (1)$, say $x(1) = 2$. If $y = (23)$, then $yxy^{-1}(1) = yx(1) = y(2) = 3$. Hence $yxy^{-1} \neq x$, that is, $x \notin Z(S_n)$.

We now assume in addition that $n \neq 6$ and show that every automorphism of S_n is an inner automorphism.

An element of S_n is of order 2 if and only if its decomposition into independent cycles has the following form: $(a_1a_2)....(a_{2k-1}a_{2k})$, $2 \leq 2k \leq n$. Let C_k denote the conjugate class of S_n which consists of all the elements of S_n which are products of k independent transpositions. Denote the number of elements in C_k by $o(C_k)$.

Now consider any automorphism ϕ of S_n. Since any automorphism preserves the order of an element and permutes conjugate classes, ϕ maps C_1 onto C_k, for some $k \geq 1$. We will now prove that $k = 1$.

If $n = 3$, we have $2 \leq 2k \leq 3$, hence $k = 1$. So we may assume that $n \geq 4$. Suppose that $k \geq 2$. We know that $o(C_1) = n(n-1)/2$, $o(C_k) = n(n-1)...(n-2k+1)/k!2^k$. Since

$o(C_1) = o(C_k)$, we obtain after simplification:

$$(n-2)(n-3)\ldots(n-2k+1) = k!2^{k-1}. \qquad (*)$$

If $k = 2$, (*) becomes $(n-2)(n-3) = 4$, a contradiction, since no integer n satisfies this equation. If $k = 3$, (*) becomes $(n-2)(n-3)(n-4)(n-5) = 24$. The only possible solution of this equation for $n \geq 4$ is $n = 6$, but our hypothesis excludes this case. Hence $k \neq 3$. Now since $n \geq 2k$, $(n-2)(n-3)\ldots(n-2k+1) \geq (2k-2)!$ But a straightforward induction argument shows that $(2k-2)! > k!2^{k-1}$ for $k \geq 4$. Therefore $k \geq 4$ would imply that $(n-2)(n-3)\ldots(n-2k+1) > k!2^{k-1}$, a contradiction of (*). We conclude that $k = 1$. In other words, ϕ maps every transposition onto a transposition.

We next prove the following statement: If a is one of the permuted symbols, then the images under ϕ of all transpositions (ax) contain a common symbol a'.

Suppose $\phi((ab)) = (b'b")$, $\phi((ac)) = (c'c")$, where b',b",c',c" are all distinct. Then $\phi((abc)) = \phi((ac)(ab)) = (c'c")(b'b")$, a contradiction, since an element of order 3 cannot be equal to an element of order 2. Therefore (b'b") and (c'c") have a common symbol, say a'. Suppose, then, that $\phi((ab)) = (a'b')$, $\phi((ac)) = (a'c')$. This symbol a' must appear in every $\phi((ax))$. For suppose that $\phi((ad)) = (d'd")$, where neither d' nor d" is equal to a'. From the above argument, it is clear that $(d'd") = \phi((ad)) = (b'c')$. Then $\phi((abdc)) = \phi((ac)(ad)(ab)) = (a'c')(b'c')(a'b') = (b'c')$. But this is a contradiction,

since an element of order 4 cannot be equal to an element of order 2. This proves the assertion.

Clearly, a' is uniquely determined by a. The function π defined on the permuted symbols by $\pi(a) = a'$ is easily seen to be an element of S_n. Note that $\pi(ab)\pi^{-1} = (a'b') = \phi((ab))$. Now if w is an arbitrary element of S_n, it follows that $\pi w \pi^{-1} = \phi(w)$, since w can be expressed as a product of transpositions. This proves the theorem.

Theorem 4.3: Let G be a group with $Z(G) = 1$. If G is a characteristic subgroup of A, then A is a complete group.

Proof: By Theorem 1.1 (ii), $Z(A) = 1$, so we need only show that every automorphism of A is an inner automorphism.

Let ϕ be any automorphism of A. ϕ is induced by an inner automorphism of A^2, that is, there exists $s \in A^2$ such that $\phi(x) = x^s$ for all $x \in A$. Since G is a characteristic subgroup of A, ϕ induces an automorphism of G. There exists $a \in A$ such that $\phi(y) = y^a$ for all $y \in G$. Hence $y^s = y^a$ for all $y \in G$, that is, $a^{-1}s \in Z(G, A^2) = 1$. $s = a \in A$. ϕ is an inner automorphism of A.

Theorem 4.4: Let G be a non-abelian simple group. Then A is a complete group.

Proof: $Z(G) < G$, hence we must have either $Z(G) = 1$ or $Z(G) = G$. Then since G is non-abelian, $Z(G) = 1$. By Theorem 4.3, we need only show that G is a characteristic

subgroup of A.

Let ϕ be any automorphism of A. $G < A$ implies that $\phi(G) < A$. Hence $G \cap \phi(G) < \phi(G)$. However $\phi(G)$ is simple, since $\phi(G) \cong G$. Hence $G \cap \phi(G)$ is equal either to 1 or to $\phi(G)$. If $G \cap \phi(G) = 1$, then it is easy to see that G and $\phi(G)$ commute elementwise. This implies that $\phi(G) \subset Z(G,A) = 1$, a contradiction, since a simple group is by definition $\neq 1$. The only other possibility is that $G \cap \phi(G) = \phi(G)$, that is, $\phi(G) \subset G$. G is a characteristic subgroup of A.

Theorem 4.5: Let A_n denote the alternating group of degree n. Then $A(A_n)$ is complete if $n \geq 5$.

Proof: Assuming $n \geq 5$, we will show that A_n is a simple group. It will follow that A_n is non-abelian, because $A_n:1 = n!/2$, which is not a prime number. The proof will then be complete, in view of Theorem 4.4.

(1) A_n is generated by the 3-cycles.

Any 3-cycle $(abc) = (ac)(ab) \in A_n$. On the other hand, any permutation $\pi \in A_n$ can be written as a product of an even number of transpositions, hence as a product of pairs of transpositions. From the equations: $(ab)(ab) = 1$, $(ab)(ac) = (acb)$, $(ab)(cd) = (adc)(abc)$, it follows that π can be written as a product of 3-cycles. (1) is proved.

(2) If $N < A_n$ and N contains a 3-cycle, then $N = A_n$.

Suppose $(123) \in N$, (ijk) any 3-cycle. Since we have at least two additional symbols at our disposal, we can extend the mapping $1 \dashrightarrow i$, $2 \dashrightarrow j$, $3 \dashrightarrow k$ to a permutation:

$$\pi = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & \dots \\ i & j & k & x & y & \dots \end{bmatrix}.$$

We may assume that $\pi \in A_n$, for if it turns out to be an odd permutation, we simply consider $(xy)\pi$ instead. Then since $N \lhd A_n$: $\pi(123)\pi^{-1} = (ijk) \in N$. So N contains all 3-cycles, therefore $N = A_n$ by (1).

(3) A_n is simple.

Suppose $N \lhd A_n$, $N \neq 1$. Choose $\pi \in N$ such that $\pi \neq 1$ and leaves fixed as many symbols as any other permutation $\neq 1$ in N. π must displace at least three symbols. The claim is that π displaces exactly three symbols. For suppose it displaced more than three, that is, suppose at least four symbols appear in the cycle decomposition of π. Either (i) π contains a cycle of length ≥ 3, so $\pi = (123\dots)\dots$, or else (ii) π consists only of 2-cycles, $\pi = (12)(34)\dots$. Note that if (i) holds, π must displace at least two other symbols, say 4, 5, since $(123x) = (1x)(13)(12) \notin A_n$.

Put $w = (345)$, $\pi_1 = w\pi w^{-1}$. In (i), $\pi_1 = (124\dots)\dots$ and in (ii), $\pi_1 = (12)(45)\dots$. In either case $\pi_1 \neq \pi$, that is, $\pi^{-1}\pi_1 \neq 1$. If a symbol $x > 5$ is left fixed by π, then it is also left fixed by π_1, hence by $\pi^{-1}\pi_1$. But in (i), $\pi^{-1}\pi_1(1) = \pi^{-1}(2) = 1$, and in (ii), similarly,

$\pi^{-1}\pi_1(1) = 1$, $\pi^{-1}\pi_1(2) = 2$. In either case, we observe that $\pi^{-1}\pi_1$ leaves fixed more symbols than π, contradicting the choice of π.

Therefore π displaces exactly three symbols, that is, π is a 3-cycle. By (2), $N = A_n$, hence A_n is simple.

Theorem 4.6: Let G be the group of all 2x2-matrices of the form

$$R(x,y) = \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix}, \quad x \neq 0,$$

with entries being elements of the field GF(p), p an odd prime. G is a complete group.

Proof: Note the following rule of multiplication:

$$R(x_1,y_1)R(x_2,y_2) = R(x_1x_2, x_1y_2+y_1).$$

We first show $Z(G) = 1$. Suppose $R(x,y) \in Z(G)$. $R(x,x+y) = R(x,y)R(1,1) = R(1,1)R(x,y) = R(x,y+1)$. Hence $x = 1$. Also $R(2x,y) = R(x,y)R(2,0) = R(2,0)R(x,y) = R(2x,2y)$. Hence $y = 2y$, or $y = 0$. $R(x,y) = R(1,0) = 1$. Note that we had to exclude the case $p = 2$ in order to get $R(2,0) \in G$.

Observe that $G:1 = p(p-1)$. Hence the Sylow p-subgroups of G are of order p. The number of these subgroups is congruent to 1 modulo p and also divides p-1. Therefore there is only one Sylow p-subgroup of G. Let us denote this subgroup by P. Obviously, P is a characteristic subgroup of G. It is easy to check that the p elements $R(1,y)$ form a subgroup of G, hence this subgroup must be P.

Next we show that $Z(P,G) = P$. Since P is abelian, $P \subset Z(P,G)$. On the other hand, suppose $R(x,y) \in Z(P,G)$. Then $R(x,y)$ commutes with $R(1,1)$. As we have already seen, this implies $x = 1$, that is, $R(x,y) \in P$.

Let δ_x denote the inner automorphism of G determined by $x \in G$. Since P is a characteristic subgroup of G, δ_x induces an automorphism, $\delta_x|P$, of P. Consider the homomorphism $f: G \longrightarrow A(P)$ given by $f(x) = \delta_x|P$. The kernel of f is clearly $Z(P,G) = P$. Then $f(G) \cong G/P$, hence we have $f(G):1 = p-1$. But $A(P) \cong A(Z_p) \cong Z_{p-1}$. Hence the mapping f is onto. This shows (i) any automorphism of P is induced by an inner automorphism of G, and (ii) $\delta_x|P = \delta_y|P$ if and only if x and y lie in the same coset of P.

P and $G/P \cong Z_{p-1}$ are both cyclic. Let $a \in P$ be a generator of P and let $b \in G$ be such that bP generates G/P. Note that $b \notin P$. Clearly $G = [a,b]$.

Now let ϕ be any automorphism of G. ϕ induces an automorphism of P. Hence there exists an element $x \in G$ such that $\phi|P = \delta_x|P$. Then $\phi_1 = \phi\delta_x^{-1}$ is an automorphism of G which leaves the elements of P fixed.

Now $bab^{-1} \in P$, so there exists an integer r such that $bab^{-1} = a^r$. Note that $r \neq 1$, for if it were, we would have $b \in Z(P,G) = P$. The above relation between a and b gives us $\phi_1(b)a\phi_1(b)^{-1} = a^r$. Therefore $\delta_b|P = \delta_{\phi_1(b)}|P$, that is, b and $\phi_1(b)$ lie in the same coset of P. There exists an integer k such that $\phi_1(b) = ba^k$.

Since $r \neq 1$, we can find an integer n such that

$n(1-r) = rk$. Then $a^n a^{-nr} = a^{rk}$. Using the fact that $bab^{-1} = a^r$, we have $a^n b a^{-n} b^{-1} = b a^k b^{-1}$. Hence $a^n b a^{-n} = b a^k$, or $\delta_{a^n}(b) = \phi_1(b)$. But we also have $\delta_{a^n}(a) = a^n a a^{-n} = a = \phi_1(a)$. Thus ϕ_1 coincides with δ_{a^n} on the generators of G. We conclude that $\phi_1 = \delta_{a^n}$. Hence $\phi = \delta_{a^n}\delta_x = \delta_{a^n x}$, an inner automorphism of G. This completes the proof.

BIBLIOGRAPHY

[1] Burnside, W. , Theory of Groups of Finite Order, New York, 1955 (Reprint of 2nd Edition, 1911)

[2] Kurosh, A. G. , Theory of Groups, New York, 1955 (Translated from the Russian and edited by K. A. Hirsch)

[3] Ledermann, W. , Introduction to the Theory of Finite Groups, New York, 1957 (3rd Edition)

[4] Wielandt, H. , Eine Verallgemeinerung der invarianten Untergruppe, Math. Zeit., vol. 45 (1939), pp. 209-244

[5] Zassenhaus, H. J. , The Theory of Groups, New York, 1958 (2nd Edition)