Automorphisms of Finite Groups*

CHIH-HAN SAH

Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138

Communicated by Richard Brauer
Accepted October 24, 1967

Let $G$ be an arbitrary group. The automorphism group $A(G)$ of $G$ has the following sequence of normal subgroups:

$$1 < A_1(G) < A_3(G) < A_4(G) < A(G)$$

where,

$A_1(G) =$ group of all inner automorphisms of $G$;

$A_3(G) =$ group of all class-preserving automorphisms of $G$

$= \{ \sigma \in A(G) \mid \text{for each } g \in G, \sigma(g) \text{ and } g \text{ are conjugate in } G \};$

$A_4(G) =$ group of all family-preserving automorphisms of $G$

$= \{ \sigma \in A(G) \mid \text{for each } g \in G, \sigma(g) \text{ and } g \text{ generate conjugate subgroups of } G \}.$

These groups were introduced by Burnside [2], p. 463. Our notations are slightly different from his; however, the present definition works for infinite groups as well as for finite groups. When $G$ is a finite group, $A(G)$ acts on the set of all irreducible (complex) characters of $G$. $A_4(G)$ is the subgroup of $A(G)$ consisting of automorphisms that carry each irreducible character onto an algebraic conjugate (over the rationals). $A_5(G)$ is then the subgroup of all automorphisms that keep all irreducible characters fixed. Burnside remarked that $A_4(G)/A_3(G)$ is obviously Abelian. This depends on the fact that $A(C)$ is Abelian whenever $C$ is a cyclic group. For, if $\sigma$ and $\tau$ are in $A_4(G)$ and if $C$ is the cyclic group in $G$ generated by $g \in G$, then we can find inner automorphisms $i_\alpha$ and $i_\beta$ such that $i_\alpha \sigma(C) = C = i_\beta \tau(C).$ Since $A_4(G)$ is a normal subgroup of $A(G)$ contained in $A_3(G)$ we know that $i_\alpha [\sigma, \tau] = [i_\alpha \sigma, i_\beta \tau]$ for a suitable $i_\gamma \in A_5(G)$, where $[a, b]$ denotes the commutator $aba^{-1}b^{-1}$. From the

* This work was partially supported by a grant from the NSF.

fact that $A(C)$ is Abelian we can conclude that $i_a[\sigma, \tau]$ is the identity map on $C$. It follows that $[\sigma, \tau]$ carries $g$ onto a conjugate of $g$ in $G$. Since $g$ is arbitrary, we conclude that $[\sigma, \tau] \in A(C)$ and that $A(G)/A(G)$ is Abelian.

Burnside then continued (in our notation) "... and it may be shown by an extension of the method of §249 that $A(G)/A(G)$ is an Abelian group." In an oral communication, Gallagher informed us that Passman furnished an example of an infinite group $G$ for which $A(G)/A(G)$ is a non-Abelian simple group. Namely, let $G$ be the restricted symmetric group on a countable set. $G$ is then a normal subgroup of the unrestricted symmetric group $S$. Since the center of $G$ is trivial we can identify $G$ with $A(G)$. $S$ is then identified with a subgroup of $A(G)$. Adapting the proof that an automorphism of a finite symmetric group preserving the conjugacy class of a transposition must be inner, one sees that $S$ is all of $A(G)$. It is well known that $S/G$ is a non-Abelian simple group (cf. [1] and [9]).

In the present investigation, we first attempt to recover what Burnside might have had in mind when he made his "assertion". This is followed by the development of a number of reduction techniques which are of independent interest. Using these results we verify the following substitute conjecture to Burnside's assertion under the Schreier hypothesis:

**CONJECTURE.** Let $G$ be a finite group. Then $A(G)/A(G)$ is a solvable group.

Let us note that the example of Passman shows that finiteness is an essential feature of the conjecture.

Finally, we justify the substitution by presenting a family of finite prime power groups $G$ for which $A(G)/A(G)$ are not Abelian. Our examples are generalizations of those constructed by Wall [11]. However, Wall's examples possess the properties asserted by Burnside while ours do not.

1. **c-Closure and Strong c-Closure**

In an earlier work, [8], we introduced the notion of c-closure. Recall that a subgroup $H$ of the group $G$ is c-closed (in $G$) if elements of $H$ conjugate in $G$ are already conjugate in $H$. We now say that $H$ is strongly c-closed in $G$ if $M$ is c-closed in $G$ for every subgroup $M$ between $H$ and $G$. It is clear that $G$ and every subgroup $H$ of the center $Z(G)$ of $G$ are c-closed in $G$. It is also easy to see that $A(G)$ is c-closed in $A(G)$ for any group $G$. In many instances, it would be very convenient to embed $G$ as a normal subgroup of a suitable group $S$ such that conjugation by elements of $S/Z(G)$ faithfully reproduces the action of $A(G)$ on $G$. In theory, this can be carried out through the cohomological results of [4]. In practice, this is not very easy, because the calculations of [4] involve the knowledge of the position of $A(G)$ in $A(G)$.
However, when \( G \) has a trivial center, we can identify \( G \) with \( A_s(G) \). The action of \( A_s(G) \) on \( A_s(G) \) by conjugation then faithfully reflects the action of \( A_s(G) \) on \( G \). This remark will be used several times later. Our present task is to show that strong c-closure might be what Burnside had in mind.

The notations \( H \leq G \) and \( H \triangleleft G \) will respectively mean that \( H \) is a subgroup and a normal subgroup of \( G \).

**Proposition 1.1.** Let \( H \) be a c-closed normal subgroup of \( G \).

(a) If \( N \triangleleft G \), then \( HN/N \) is c-closed and normal in \( G/N \).

(b) If \( K \triangleleft G \), \( K \) is c-closed in \( G \), and \([H, K] = 1\), then \( HK \) is c-closed and normal in \( G \).

The proofs are straightforward and will be omitted.

**Proposition 1.2.** Let \( N \) be a strongly c-closed normal subgroup of the finite group \( G \). Then \( G/N \) is Abelian.

**Proof.** From the hypothesis and Proposition 1.1 we can assume that \( N = 1 \). From Theorem 3 of \([8]\) we can conclude that \( G \) is a nilpotent group. It is clear that an Abelian normal subgroup of \( G \) is c-closed in \( G \) if and only if it is part of the center of \( G \). Since \( G \) is a finite nilpotent group, we can find maximal Abelian normal subgroups of \( G \). These subgroups are characterized by the property that they are self-centralizing normal subgroups of \( G \). However, the centralizer of a subgroup of the center of \( G \) must be all of \( G \). Thus \( G \) must be an Abelian group. Q.E.D.

Let \( S \) be a subset of the group \( G \). \( C_G(S) = \{g \in G \mid gs = sg \text{ for all } s \in S\} \) is called the centralizer of \( S \) in \( G \). Let \( H \) be a subgroup of \( G \). \( S \) is called a \( H \)-orbit if there exists \( s \in S \) such that \( S = \{hsh^{-1} \mid h \in H\} \).

**Proposition 1.3.** Let \( N \) be a subgroup of the group \( G \). The following statements concerning \( g \in G \) are equivalent:

(a) \( G = NC_G(g) \).

(b) The \( G \)-orbit of \( g \) is equal to the \( N \)-orbit of \( g \).

We omit the trivial proof.

**Proposition 1.4.** Let \( N \) be a subgroup of the group \( G \). The following statements are equivalent:

(a) \( G = NC_G(x) \) holds for every \( x \in N \).

(b) Every \( N \)-orbit contained in \( N \) is a \( G \)-orbit.

(c) \( N \) is a c-closed normal subgroup of \( G \).
The proof of Proposition 1.4 becomes trivial as soon as we observe the facts that \( N \) is a union of \( N \)-orbits and that a subgroup is normal in \( G \) if and only if it is the union of \( G \)-orbits.

We now generalize Burnside's results [2], §249.

**Theorem 1.5.** Let \( N \) be a subgroup of the finite group \( G \). The following statements are all equivalent:

(a) \( N \) is a strongly \( c \)-closed normal subgroup of \( G \).

(b) \( G = NC_G(g) \) holds for every \( g \in G \).

(c) Every \( G \)-orbit in \( G \) is an \( N \)-orbit.

(d) Every irreducible character of \( N \) extends in at least (therefore exactly) \( |G:N| \) distinct ways to (necessarily irreducible) characters of \( G \).

(e) The character of \( G \) induced by an irreducible character of \( N \) is always the sum of at least (therefore exactly) \( |G:N| \) (suitably selected) distinct irreducible characters of \( G \) (each extending the given character of \( N \)).

(f) The restriction of each irreducible character of \( G \) to \( N \) is an irreducible character of \( N \).

Moreover, each of the preceding statements implies the following statement:

(g) \( N \) is a \( c \)-closed normal subgroup of \( G \).

Finally, if (g) holds and \( G/N \) happens to be cyclic, then all of the preceding statements hold for \( N \).

**Proof.** We can deduce from Proposition 1.3 that (b) and (c) are equivalent. Proposition 1.4 shows quickly that (b) implies (a).

We recall Frobenius' reciprocity theorem. If \( \chi \) and \( \eta \) are irreducible characters of \( G \) and \( N \) respectively, then \( \eta \) occurs in the restriction of \( \chi \) to \( N \) with the same multiplicity as \( \chi \) occurs in the character of \( G \) induced by \( \eta \). Moreover, the character of \( G \) induced by \( \eta \) has degree \( |G:N| \eta(1) \). These remarks lead quickly to the equivalence of (d), (e) and (f). In particular, we can conclude from (f) that (d), (e) and (f) hold for any subgroup \( M \) containing \( N \). Since the irreducible characters of a finite group \( H \) separate the \( H \)-orbits in \( H \), we can conclude from property (d) of \( M \) that \( M \)-orbits of \( M \) fall in distinct \( G \)-orbits in \( G \). Namely, \( M \) is \( c \)-closed. It follows that \( N \) is strongly \( c \)-closed in \( G \). If we apply (d) to the trivial character of \( N \), then we can conclude that there exist \( |G:N| \) distinct linear characters of \( G \) whose restriction to \( N \) is trivial. If \( M \) is the intersection of the kernels of these \( |G:N| \) linear characters, then \( N \leq M \) and \( G/M \) must have order at least \( |G:N| \). Consequently \( N = M \) is a normal subgroup of \( G \). Thus we have verified that (d) implies (a). It is obvious that (a) implies (g). Thus (g) is implied by any of the first six statements.
We next show that (g) implies (f) under the assumption that $G/N$ is a cyclic group. It would then follow that all seven statements are equivalent in case $G/N$ is a cyclic group.

Let $\chi$ be an irreducible character of $G$. We may apply Clifford's results [3] to the restriction $\chi|_N$ and obtain the equation,

$$\chi|_N = s\sum_{i=1}^{t} \eta_i,$$

where $s$ is a positive integer and $\eta_i$ are distinct irreducible characters of $N$, conjugate under $G$. However, $N$ is $c$-closed and normal in $G$, thus $t = 1$. In other words $\chi|_N = s\eta$ and our task is to show that $s = 1$. Again we use Clifford's result to conclude that $\chi|_N = \alpha\beta$, where $\alpha$ is the character of a projective irreducible representation of $G/N$ associated to a suitable $[f] \in H^2(G/N, \mathbb{C}^*)$; $\mathbb{C}^*$ is the $G/N$-trivial module of the group of nonzero complex numbers under multiplication. It is well known that $H^2(G/N, \mathbb{C}^*) = 0$ when $G/N$ is cyclic acting trivially on $\mathbb{C}^*$, a divisible group. Thus the projective representation associated to $\alpha$ can be modified until it arises from an ordinary irreducible representation of the same degree. Since $G/N$ is cyclic, we conclude that $\alpha$ must have degree 1. However, Clifford's results also assert that $\alpha$ has degree $s$. Thus $s = 1$ and (f) holds.

(a) implies (f). Suppose that (a) holds. According to Proposition 1.2 $G/N$ is an Abelian group. If $G/N$ is a cyclic group, then the preceding argument showed that (f) holds. If $G/N$ is not cyclic, then we can find a subgroup $M$ strictly between $N$ and $G$. It is clear that (a) holds for the pair $M, N$ as well as the pair $G, M$. By induction we can conclude that every irreducible character of $G$ first restricts to an irreducible character of $M$, then restricts to an irreducible character of $N$. Thus (f) holds. Combining this with our earlier arguments we have verified all of our assertions. Q.E.D.

**Proposition 1.6.** Let $N$ be a normal subgroup of the finite group $G$. Let $h_N$ and $h_G$ be the number of $N$-orbits in $N$ and the number of $G$-orbits in $G$ respectively. Then the following statements are equivalent:

(a) $N$ is strongly $c$-closed in $G$.

(b) $h_G = |G : N| h_N$.

(c) Each coset of $G/N$ contains $h_N$ $G$-orbits. (Each such $G$-orbit is actually an $N$-orbit.)

**Proof.** It is obvious that (c) implies (b).

(b) implies (a). Suppose that (b) holds. It is sufficient to verify (e) of Theorem 1.5. Let $\eta$ be a random irreducible character of $N$. Let $\eta^*$ be the character of $G$ induced by $\eta$. We know that $\eta^* = \sum a_i \chi_i$, $1 \leq i \leq t$, where $a_i$ are positive integers and $\chi_i$ are distinct irreducible character of $G$. The
Frobenius reciprocity theorem tells us that $\chi(A) \geq a_i \eta(1)$. Thus $\gamma^*(1) = |G:N| \gamma(1) \geq \Sigma a_i^2 \eta(1) \geq \gamma(1)$. It follows that at most $|G:N|$ characters of $G$ can occur as components of $\gamma^*$. Since every character of $G$ must occur as $\gamma$ varies we know that the total number of irreducible characters of $G$ is at most $|G:N|$ times the total number of irreducible characters of $N$. It is well known that these numbers are equal to $h_G$ and $h_N$ respectively. We can therefore conclude from (b) that all the $a_i$'s are equal to 1 and each $t$ is equal to $|G:N|$. Thus (c) of Theorem 1.5 holds.

(a) implies (c). Suppose that (a) holds. We now repeat the argument used by Burnside. According to Theorem 1.5 it is enough to show that each coset of $G/N$ contains $h_N$ $N$-orbits. Let $U$ be a coset of $G/N$. We let $N$ act on $U$ as a permutation group by conjugation. Let $x \in N$. In view of Theorem 1.5 (b) $U = N g$ for a suitable $g \in C_G(x)$. Consequently the number of elements in $U$ fixed by $x$ is $|C_N(x)|$. In general, if $N$ is represented as a permutation group on a finite set and $f(x)$ is the number of fixed points of $x$ on $S$, then the number of $N$-orbits in $S$ is equal to $|N|^{-1}\Sigma x \in N f(x)$. Applying this result to the cases $S = U$ and $S = N$ respectively, we can conclude that the number of $N$-orbits in $U$ is $h_N$ as desired. Q.E.D.

In general, a $c$-closed subgroup of a finite group is not necessarily strongly $c$-closed. For example, let $G$ be a non-Abelian $p$-group of order $p^3$. The center of $G$ is $c$-closed, but not strongly $c$-closed. Indeed, none of the $p + 1$ subgroups of order $p^3$ is $c$-closed. The point is that every subgroup of order $p^3$ is an Abelian normal subgroup of $G$. Such subgroups are $c$-closed if and only if they are contained in the center. The center of our groups have order $p$. We also note that $G/Z(G)$ is an Abelian group of order $p^2$. Thus the condition that $G/N$ be cyclic is an essential feature in the proof that (g) of Theorem 1.5 implies the other properties.

If it were possible to show that $A_\sigma(G)$ is not merely $c$-closed but strongly $c$-closed in $A_\sigma(G)$, then we could deduce from Proposition 1.2 that $A_\sigma(G)/A_\alpha(G)$ is an Abelian group. However, the example in Section 3 will show that this is not the case.

We conclude this section with some results concerning the relative position of the group of central automorphisms. We recall that the group of central automorphisms of the group $G$ is precisely the group $C_{A(G)}(A_\eta(G))$.

**Proposition 1.7.** Let $G$ be a group and let $\sigma : G \to G$ be a map. The following statements are all equivalent:

(a) $\sigma \in C_{A(G)}(A_\eta(G))$.

(b) $\sigma \in C_{A(G)}(A_\eta(G))$.

(c) There exists a group homomorphism $f : G \to Z(G)$ such that,
(1) $\sigma(g) = gf(g)$ for all $g \in G$, and
(2) $f(g) \neq g^{-1}$ for $g \in Z(G)$ and $g \neq 1$.
(d) $\sigma \in A(G)$ and $\sigma$ induces the identity map on $G/Z(G)$.

We omit the straightforward proof.

Let $M$ be a normal subgroup of the group $G$. The natural homomorphism of $G$ to $G/M$ induces a homomorphism from $A_c(G)$ to $A_c(G/M)$. If $K/M$ is a subgroup of the center of $G/M$, then we can conclude that $A_c(G)$ induces the trivial map on $K/M$. In particular, when $G$ is a nilpotent group, $A_c(G)$ must induce the identity map on each of the factors of a central series of $G$. A result of Hall [5], Lemma 3.5, p. 9, (a statement of this result can be found in [7], p. 430, where related results on $p$-groups can be found,) can be applied to give the following proposition;

**Proposition 1.8.** Let $G$ be a nilpotent group of class $c$. Then $A_c(G)$ is a nilpotent group of class $c - 1$.

**Corollary.** Let $G$ be a nilpotent group of class $c$. Then $A_c(G)/A_1(G)$ is a nilpotent group of class less than $c$.

The example of Wall [11] shows that the above corollary is the best possible when $c = 2$. For large values of $c$ the Corollary could presumably be improved.

Let $G$ be a $p$-group of finite order. The remark preceding Proposition 1.8 shows quickly that $A_c(G)$ is again a $p$-group. More generally, Burnside showed that the prime divisors of $|A_c(G)|$ must be prime divisors of $|G|$. A generalization of this result can be found in [8], Lemma 3.5. If $|G| = p^n$, it is well known that the $p$-Sylow subgroup of $|A(G)|$ has order at most $p^{n(n-1)/2}$. Thus we have the crude inequality that,

$$\log_p |A_c(G)| \leq \frac{1}{2} (\log_p |G|)^2$$

where $G$ is a $p$-group.

Let $R$ be any commutative ring. We can define multiplication on the set $G = \{(x, y, z) | x, y, z \in R\}$ by the rule

$$\begin{align*}
(1) \quad & (u, v, w)(x, y, z) = (u + x, v + y, vx + w + z).
\end{align*}$$

We let $X$, $Y$, $Z$ denote the three coordinate axes. It is clear that they are isomorphic to the additive group of $R$. Moreover, the coordinate planes $XZ$ and $YZ$ are direct products. It is straightforward to show,

$$\begin{align*}
(2) \quad & (x, y, z)^{-1} = (-u, -v, -w + uv) \quad \text{and the multiplication in } G \text{ is}
\end{align*}$$
associative. Thus $G$ is a group.

(3) $(x, y, z)(a, b, c)(x, y, z)^{-1} = (a, b, ya - xb + c)$.

(4) $[(x, y, z), (a, b, c)] = (0, 0, ya - xb)$.

It is worthwhile to note that (2) holds without the commutativity of $R$, but (3) and (4) require the commutativity of $R$. It is now clear that,

(5) $Z$ is the center as well as the commutator subgroup of $G$. In particular, $G$ is a nilpotent group of class 2. Moreover, $G/Z(G) = G/[G, G]$ is isomorphic to the direct product of $XZ/Z$ and $YZ/Z$; both of these groups are isomorphic to $R$ under addition.

If $\sigma \in A_\epsilon(G)$, then (5) implies that $\sigma$ must induce the identity map on $G/Z(G) = G/[G, G]$. It follows that $\sigma$ is a central automorphism. We can deduce from Proposition 1.7 that $\sigma$ is uniquely associated with two additive homomorphisms $f, g : R \rightarrow R$ so that,

(6) \[ \sigma(a, b, c) = (a, b, f(a) + g(b) + c). \]

By setting $a$ and $b$ in turn to be zero, we can deduce from (3) that,

(7) $\sigma \in A_\epsilon(G)$ if and only if $f(a) \in Ra$ and $g(b) \in Rb$ for all $a, b \in R$.

We can further deduce from (3) that,

(8) $\sigma \in A_\epsilon(G)$ if and only if $f, g \in \text{Hom}_R(R, R)$.

The critical point here is that an $R$-module endomorphism of the commutative ring $R$ is a multiplication. If we let $\text{Hom}_R(R, R)$ be the subgroup of $\text{Hom}(R, R)$ such that each principal ideal of $R$ is mapped into itself (such an additive endomorphism might be called a local multiplication); then,

(9) $A_\epsilon(G)/A_\epsilon(G)$ is isomorphic to the direct product of two copies of $\text{Hom}_R(R, R)/\text{Hom}_R(R, R)$.

As an illustration, we let $R$ be the polynomial ring over the finite field $\mathbf{GF}(p^m)$ in the variable $x$ modulo the ideal generated by $x^n$, where $m, n > 0$.

Thus $|\text{Hom}_R(R, R)| = |R| = p^{mn}$. It is clear that $R\pi^i$, $0 \leq i < n$, are the only ideals of $R$. If we take a basis for $\mathbf{GF}(p^m)$ over $\mathbf{GF}(p)$, we can then extend to one for $R$ over $\mathbf{GF}(p)$ by multiplying them by $\pi^i$, $0 \leq i < n$. It is now easy to show that,

\[ |\text{Hom}_R(R, R)| = (p^m)^m(p^{m(n-1)})^m \cdots (p^m)^m = p^{mn(n+1)/2} \]

It is also clear that $|G| = p^{2mn}$. Thus we have,

\[ \frac{1}{18} \left( \log_p |G| \right)^2 \leq \log_p |A_\epsilon(G)| \leq \frac{1}{2} \left( \log_p |G| \right)^2. \]
The above inequality shows that $A_d(G)/A_d(G)$ is immense when compared with $G$ itself. The examples constructed by Wall are such that $A_d(G)/A_d(G)$ is small when compared with $G$.

2. Automorphisms of an Extension

This section is devoted to some reduction techniques. Most of the relevant cohomological results can be found among the works of Hochschild and Serre [6] and Eilenberg and MacLane [4].

Let $M$ be a normal subgroup of the group $G$. We set $A(G, M)$ equal to $\{\sigma \in A(G) | \sigma(M) = M\}$. It is clear that $A_d(G)$ is a subgroup of $A(G, M)$. Each $\sigma$ in $A(G, M)$ induces $\sigma_M \in A(M)$ and $\sigma_{G/M} \in A(G/M)$. These two automorphisms are related by the fact $G/M$ is homomorphic to a subgroup of $A(M)/A_d(M)$. Let us again observe that for $\sigma \in A_d(G)$ we have $\sigma_{G/M} \in A_d(G/M)$.

In the special situation when $M$ is an Abelian normal subgroup of $G$, we can view $M$ as a (left) $\Gamma$-module; $\Gamma = G/M$ acts on $M$ by conjugation as follows:

$$
\begin{align*}
(1) \quad \text{if } \gamma = gM \in \Gamma, \ m \in M, \ \text{then } \gamma \{m\} &= gmg^{-1}.
\end{align*}
$$

When there is no confusion, we also write $g(m)$ for $\gamma \{m\} = gmg^{-1}$. Let $[f] \in H^2(\Gamma, M)$ be the cohomology class of the normalized 2-cocycle $f$ associated to the following exact sequence of groups:

$$
\begin{align*}
(2) \quad 1 &\rightarrow M \rightarrow G \rightarrow \Gamma \rightarrow 1.
\end{align*}
$$

We then obtain the following diagram;

\[
\begin{array}{c}
1 &\downarrow &\downarrow &\downarrow &1 \\
\downarrow & & & & \\
1 &\rightarrow A_1(G, M) &\rightarrow A_1(G, M) &\rightarrow \text{coker} &\rightarrow 1 \\
\downarrow & & & & \\
(3) \quad 1 &\rightarrow A_1(G, M) &\rightarrow A(G, M) &\rightarrow A(\Gamma) &\rightarrow 1 \\
\downarrow & & & & \\
1 &\rightarrow \text{coker} &\rightarrow \Gamma \Lambda(M, [f]) &\rightarrow 1 \\
\downarrow & & & & \\
1 & & & & 1
\end{array}
\]
In the diagram, coker denote the quotient groups which do not concern us. \( A^1(G, M) \) is the kernel of the map that sends \( \sigma \in A(G, M) \) onto \( \sigma_{G/M} \in A(\Gamma) \). Thus \( A^1(G, M) \) consists of all \( \sigma \in A(G) \) such that \( \sigma \) fixes each coset of \( G/M \).

We now recall that an automorphism \( \sigma_M \) of \( M \) is called \( \Gamma \)-semilinear if there exists a \( a, \in A(\Gamma) \) such that,

\[
(4) \quad \sigma(\gamma)(m) = \sigma(m)(\gamma(m)), \quad \gamma \in \Gamma, \ m \in M.
\]

Such a pair \( \sigma = (\sigma_T, \sigma_M) \) then defines a homomorphism (in fact, an automorphism) \( \sigma : H^2(\Gamma, M) \to H^2(\Gamma, M) \) according to the following formula involving each (normalized) 2-cocycle \( g \):

\[
(5) \quad (\sigma g)(\alpha, \beta) = \sigma(g(\sigma_T^{-1}(\alpha), \sigma_T^{-1}(\beta))), \quad \alpha, \beta \in \Gamma.
\]

The group \( \Gamma L(M, [f]) \) is defined to be the collection of \( \sigma_M \)'s for which \( sf \) and \( f \) are cohomologous for at least one choice of \( \sigma_T \).

Let us now select (normalized) coset representatives \( r_\alpha \) for \( \Gamma \) in \( G \) subordinating the 2-cocycle \( f \). Thus we have,

\[
(6) \quad r_\alpha r_\beta = f(\alpha, \beta) r_{\alpha\beta}, \quad r_1 = 1, \ \alpha, \beta \in \Gamma.
\]

For each \( \sigma \in A(G, M) \) the induced pair \( (\sigma_T, \sigma_M) \) is \( \Gamma \)-semilinear and \( \sigma(r_\alpha) = a_{\sigma_T(\alpha)} r_{\sigma_T(\alpha)} \) for suitable \( a_{\sigma_T(\alpha)} \in M \), where \( \alpha \) ranges over \( \Gamma \). The map \( g \) sending \( \beta \) onto \( a_\beta \) is a 1-cochain of \( \Gamma \) in \( M \). A straightforward calculation shows that \( sf \) and \( f \) differs by the coboundary of \( g \). Thus \( \sigma \) determines \( \sigma_M \in \Gamma L(M, [f]) \). Conversely, given \( (\sigma_T, \sigma_M) \in \Gamma L(M, [f]) \) so that \( sf \) and \( f \) are cohomologous, we can reverse our steps and construct \( \sigma \) in \( A(G, M) \).

Such a \( \sigma \) depends, among other things, on the choice of \( \sigma_T \). We define \( A_3(G, M) \) to be the kernel of the surjective homomorphism in the diagram; it then consists of all \( \sigma \in A(G) \) which keeps each element of \( M \) fixed. \( A^1_3(G, M) \) is then defined to be \( A_3(G, M) \cap A^1(G, M) \); it consists of all \( \sigma \in A(G) \) that induces the identity map on \( M \) as well as on \( G/M = \Gamma \). One checks easily that the diagram (3) is exact and commutative. Our problem is to find out how \( A_3(G) \) and \( A_1(G) \) meet each of the three normal subgroups of \( A(G, M) \).

We deduce from the fact that \( M \) is commutative the relation, \( M \leq C_G(M) \leq G \). \( M \) is \( \Gamma \)-faithful if and only if \( M = C_G(M) \); in this instance, \( M \) is said to be a self-centralizing normal subgroup. When \( G \) is a prime-power group, any maximal Abelian normal subgroup of \( G \) is of this type. In general such subgroups need not exist. (For example, take \( G \) to be the direct product of a nontrivial Abelian group with a non-Abelian simple group.) At the other extreme, \( M \) is \( \Gamma \)-trivial if and only if \( G = C_G(M) \); in other words, \( M \) is contained in the center of \( G \).

**Proposition 2.1.** If \( M \) is \( \Gamma \)-faithful in the preceding notation, then \( A_3(G, M) = A^1_3(G, M) \leq A^1(G, M) \).
Proof. Let $\sigma \in A_1(G, M)$. Then $\gamma(m) = \sigma M(\gamma(m)) = \sigma \gamma(\sigma_M(m)) = \sigma_r(\gamma)(\sigma_M(m))$ holds for all $m \in M, \gamma \in \Gamma$. Since $M$ is $\Gamma$-faithful, we have $\sigma_r(\gamma) = \gamma$ for all $\gamma \in \Gamma$ and $\sigma \in A_1(G, M)$ as asserted. Q.E.D.

**Proposition 2.2.** Continuing with the preceding notations, let $I(M)$ be the subgroup of $A_1(G)$ induced by $M$. Then,

(a) $I(M) \leq A_1(G, M)$.

(b) There is an isomorphism between $A_1^1(G, M)$ and the group of (normalized) 1-cocycles of $\Gamma$ in $M$; this isomorphism carries $I(M)$ onto the group of (normalized) 1-coboundaries.

(c) $H^1(\Gamma, M) \cong A_1^1(G, M)/I(M)$.

Proof. (c) is obviously a consequence of (b). (a) follows from the fact that $\Gamma$ is both Abelian and normal. If $\sigma \in A^1_1(G, M)$, then $\sigma(m r_a) = ma_r \sigma$. Using formula (5) together with the fact that both $\sigma_r$ and $\sigma_M$ are identities, we conclude easily that $a_r$ is a (normalized) 1-cocycle of $\Gamma$ in $M$. Conversely, we can reverse the steps and reconstruct $\sigma \in A_1^1(G, M)$ from the normalized 1-cocycle $\{a_r | \alpha \in \Gamma\}$. It is straightforward to check that this is the isomorphism desired in (b). Q.E.D.

**Proposition 2.3.** Let $M$ be a left $\Gamma$-module. Let $C$ be the intersection of $\ker(\Gamma \to A(M))$ with the center $Z(\Gamma)$. Then there is a bi-additive map,

$$c : C \times H^1(\Gamma, M) \to H^1(\Gamma, M).$$

Proof. Let $\sigma \in C$. For each (normalized) 2-cocycle $f$ of $\Gamma$ in $M$, we construct the group $G$ with coset representatives $r_a$ subordinating $f$. Let $c(\sigma, f) : \Gamma \to M$ be the 1-cochain defined by the formula,

$$c(\sigma, f)_a = [r_a, r_a] = f(\sigma, \alpha) f(\alpha, \sigma)^{-1}, \alpha \in \Gamma.$$

Straightforward calculations show that we have a normalized 1-cocycle whose cohomology class depends only on the cohomology class of $f$. It is easy to see that this defines a bi-additive map. The idea behind the proposition is the rather simple observation that the inner automorphism of $G$ induced by $r_a$ is an element of $A_1^1(G, M)$. Q.E.D.

Let $M$ be a $\Gamma$-module as before. For each cyclic subgroup $\Delta$ of $\Gamma$ we have the restriction homomorphism, $\text{res}_\Delta : H^q(\Gamma, M) \to H^q(\Delta, M)$. We define $H^q(\Gamma, M)$ to be the intersection of the kernel of $\text{res}_\Delta$ as $\Delta$ range over all the cyclic subgroups of $\Gamma$. (In fact, it is enough to let $\Delta$ range over a complete family of representatives of the conjugacy classes of cyclic subgroups.) The case $q = 1$ (which is all we are interested in) was used by Serre in [10]. According to Serre, the definition of this functor was suggested by Tate. For computational purposes, the following result of Serre may be useful:
Proposition 2.4. (Serre, [10] Proposition 6, p. 9.) Let $M$ be a $\Gamma$-module. Let $N$ be a normal subgroup of $\Gamma$ acting trivially on $M$. Then the canonical injection $i : H^1(\Gamma|N, M) \to H^1(\Gamma, M)$ induces an isomorphism between $H^1_*(\Gamma|N, M)$ and $H^1_*(\Gamma, M)$.

In view of Serre's result, we may assume that $M$ is $\Gamma$-faithful in the computation of $H^1_*(\Gamma, M)$.

Theorem 2.5. Let $\rightarrow M \to G \to \Gamma \to 1$ be an exact sequence of groups, where $G$ corresponds to the 2-cocycle $f$ of the left $\Gamma$-module $M$. Then,

(a) $\{A_\alpha(G) \cap A_1^*(G, M)\}/\{A_\alpha(G) \cap A_1^*(G, M)\}$ is isomorphic to a suitable subgroup of a quotient group of $H^1(G, M)$.

(b) Suppose that $[f] = 0$. $I(M)$ is then equal to $A_\alpha(G) \cap A_1^*(G, M)$ and $H^1_*(\Gamma, M) \cong \{A_\alpha(G) \cap A_1^*(G, M)\}/\{A_\alpha(G) \cap A_1^*(G, M)\}$.

Proof. (a) is an immediate consequence of Propositions 2.2 and 2.3. Indeed, we must factor out the image of $C$ in Proposition 2.3 with respect to the homomorphism $c(\cdot, [f])$.

(b) Assume that $[f] = 0$. We may choose coset representatives so that they form a subgroup of $G$ isomorphic to $\Gamma$ under the natural map. For convenience, we assume that $\Gamma$ is a subgroup of $G$. It is now clear that the subgroup $C$ of $\Gamma$ defined in Proposition 2.3 is part of the center of $G$. This allows us to conclude that $I(M) = A_\alpha(G) \cap A_1^*(G, M)$. Let $\sigma \in A_1^*(G, M)$. Then $\sigma(m\alpha) = ma_\alpha$ for $m \in M$, $\alpha \in \Gamma$, where $a_\alpha$ is a 1-cocycle of $\Gamma$ in $M$ associated to $\sigma$. $\sigma \in A_1^*(G, M)$ if and only if there exist suitable $n \in M$, $\beta \in \Gamma$ (depending on $m$, $\alpha$) such that $n\beta m a_\beta^{-1}n^{-1} = ma_\alpha$. Passing over to $G/M$, we see that the equation is equivalent to $\beta \in C_\Gamma(\alpha)$ and $n\alpha(n)^{-1} \cdot m^{-1} \beta(m) = a_\alpha$.

When $m = 1$, $\sigma \in A_\alpha(G)$, we may conclude that there exists $n_0$ in $M$ such that $a_\alpha = n_0 a_\alpha(n_0)^{-1}$. Conversely, if such an $n_0$ can be found, then we can take $\beta = 1$ and $n = n_0$ in general and conclude that $\sigma \in A_\alpha(G)$. Thus $\sigma \in A_\alpha(G) \cap A_1^*(G, M)$ is equivalent to the statement that the associated 1-cocycle $a_\alpha$ has the property that $a_\alpha = n_\alpha(n)^{-1}$ for a suitable $n \in M$ depending on $\alpha$. The existence of such $n$ together with the cocycle equation satisfied by $a_\alpha$ is completely equivalent to the statement that the restriction of $a_\alpha$ to the cyclic group generated by $\alpha$ in $\Gamma$ is the coboundary determined by $n \in M$.

Q.E.D.

The examples constructed by Wall [11] have two interpretations. His group is the affine group of the line based on the integers mod $2^n$, $n \geq 3$. This group $G$ is the split extension of the additive group by the group of units in the ring. The fact that $A_\alpha(G)/A_\alpha(G)$ is not trivial can either be viewed as a special instance where $G$ admits non-inner automorphisms which are central and class-preserving, or be viewed as a special instance where
$H^1_+(\Gamma, M) \neq 0$, $\Gamma$ is the group of units acting by multiplication on the additive group of the ring. In view of the fact that the group of units in the ring of integers mod odd prime power is a cyclic group, Wall's result cannot be generalized to other primes in the obvious way. In Wall's example, we assert that $A_\cdot(G)/A_\cdot(G)$ is isomorphic to $H^1_+(\Gamma, M)$. The fact that $\Gamma$ is commutative tells us that $A_\cdot(G) \leq A^1(G, M)$. Each $\sigma \in A_\cdot(G)$ therefore induces a $\Gamma$-module automorphism of $M$. Furthermore, $\sigma_M$ preserves the $\Gamma$-orbits of $M$. In particular, $\sigma_M$ must preserve the group of units in $M$ (considered as a ring). As $\sigma_M$ commutes with left multiplication by $\Gamma$, $\sigma$ must be a right multiplication on the group of units in $M$. It is easy to see that right multiplication by units on $M$ can be extended to an element of $A_\cdot(G)$ (this depends on the commutativity of the underlying ring). Thus we can assume that $\sigma_M$ fixes all the units in $M$. However, each element of $M$ can be written as a finite sum of units. Thus $\sigma_M$ is the identity on $M$. We have thus shown that $A_\cdot(G)/A_\cdot(G)$ is covered by $A_\cdot(G) \cap A^1_\cdot(G, M)$. [Recall that $L/K$ is covered by $H$ if $L = K(L \cap H)$.] The standard isomorphism theorem then shows that $A_\cdot(G)/A_\cdot(G)$ is isomorphic to $H^1_+(\Gamma, M)$ through the application of Theorem 2.5 (b).

Our discussion can easily be formalized into the following proposition;

**Proposition 2.6.** Let $R$ be a commutative ring such that the units of $R$ generate $R$ additively. Let $G$ be the affine group in one variable based on $R$. Then $A_\cdot(G)/A_\cdot(G) \cong H^1_+(U, R)$, where $R$ is considered as a left module over the group $U$ of units in $R$ under left multiplication.

The family of rings considered in Proposition 2.6 is closed under tensor product, but not under direct product. (For example, the direct product of two or more $GF(2)$'s is not in the family while $GF(2)$ obvious is.) The family contains every commutative local ring. In particular, Wall's example is included. Using Dirichlet's unit theorem one can verify that the ring of integers of a totally real number field is in the family. In contrast, polynomial rings are not in the family. One more remark concerning Wall's example. When $R = \mathbb{Z}/2^n\mathbb{Z}$, $\mathbb{Z}$ the ring of rational integers, $n \geq 3$, the group $G$ is nilpotent of class $n - 1$, while $A_\cdot(G)/A_\cdot(G)$ is of class 1.

The next proposition provides some further limitation on the cohomology groups.

Let $Q$ be the fractional field of the ring $\mathbb{Z}$ of rational integers.

**Proposition 2.7.** Let $\Gamma$ be a group and let $M$ be an indecomposable left $\Gamma$-module satisfying both chain conditions on $\Gamma$-submodules. Then the following statements hold:

(a) $M$ is either a vector space over $Q$ or a module over $\mathbb{Z}/p^n\mathbb{Z}$ for some prime $p$. 

(b) Either $Z(\Gamma)$ induces a unipotent group of automorphisms of $M$ or else $H^q(\Gamma, M) = 0$ for every integer $q \geq 0$.

(c) Suppose that $M$ is $\Gamma$-irreducible and $Z(\Gamma)$ does not act trivially on $M$. Then $H^q(\Gamma, M) = 0$ for every integer $q \geq 0$.

Proof. (a). Suppose that $M$ is indecomposable and satisfies both chain conditions. We can deduce from Fitting’s lemma that $\text{Hom}_{\mathbb{C}}(M, M)$ is a completely primary ring with a nilpotent Jacobson radical. (Recall that a ring $R$ is completely primary if $R/\text{rad} \, R$ is a division ring, where $\text{rad} \, R$ is the Jacobson radical of $R$ formed by all $x$ in $R$ such that $1 + Rx$ consists of invertible elements of $R$.) Let $1 \in \text{Hom}_{\mathbb{C}}(M, M)$ be the identity map. If 1 is not torsion, then multiplication by each integer $n > 0$ must be an automorphism of $M$. It follows that $Q$ is contained in the center of $\text{Hom}_{\mathbb{C}}(M, M)$ and $M$ is a $Q$-vector space. If 1 is torsion, then the nonexistence of an idempotent other than 0 and 1 in $\text{Hom}_{\mathbb{C}}(M, M)$ implies that $\mathbb{Z}/p^n\mathbb{Z}$ is contained in the center of $\text{Hom}_{\mathbb{C}}(M, M)$ for some prime $p$. Thus $M$ is a module over $\mathbb{Z}/p^n\mathbb{Z}$.

(b) Suppose that $x \in Z(\Gamma)$ is not unipotent on $M$. It then induces $\sigma \in \text{Hom}_\mathbb{C}(M, M)$ such that $\sigma - 1$ and $\sigma$ are both invertible. As a result, $(\sigma - 1)_x$ and $\sigma_x$ are both automorphisms of $H^q(\Gamma, M)$. It is well known that conjugation by $x$ on $\Gamma$ and multiplication by $x$ on $M$ induce the identity map on $H^q(\Gamma, M)$ for any $x$ in $\Gamma$. When $x \in Z(\Gamma)$, the induced map coincides with $\sigma_x$. Thus $(\sigma - 1)_x = \sigma_x - 1_x = 0$ is an automorphism of $H^q(\Gamma, M)$. It follows that (b) holds.

(c) follows from (b) and Schur’s lemma. Q.E.D.

**Proposition 2.8.** Let $M$ be a normal Abelian subgroup of the group $G$. Suppose that $A_\mathfrak{a}(\Gamma)/A_\mathfrak{a}(\Gamma)$, $\Gamma = G/M$, is known to be solvable of length $m$. Then the following statements hold:

(a) If $M$ is $\Gamma$-trivial, then $A_\mathfrak{d}(G)/A_\mathfrak{d}(G)$ is solvable of length at most $m + 1$.

(b) If the group of units in the ring $\text{Hom}_\mathbb{C}(M, M)$ is solvable of length $n$, then $A_\mathfrak{d}(G)/A_\mathfrak{d}(G)$ is solvable of length at most $m + n + 1$.

Proof. In either case, $A_\mathfrak{d}(G)$ is mapped homomorphically into $A_\mathfrak{d}(\Gamma)$ with kernel $A_\mathfrak{d}(G) \cap A^1(G, M)$. This homomorphism carries $A_\mathfrak{d}(G)$ surjectively onto $A_\mathfrak{d}(\Gamma)$. Thus it is sufficient to show that

$$T = A_\mathfrak{d}(G)[A_\mathfrak{d}(G) \cap A^1(G, M)]/A_\mathfrak{d}(G)$$

$$\cong [A_\mathfrak{d}(G) \cap A^1(G, M)]/[A_\mathfrak{d}(G) \cap A^1(G, M)]$$

is solvable of length at most 1 and $n + 1$ in respective cases.
In case (a) we note that $A_e(G) \leq A_1(G, M)$ automatically. Thus the result follows from Theorem 2.5 (a).

In case (b) $A^1(G, M)/A_1^1(G, M)$ is isomorphic to a subgroup of the group of units in the ring $\text{Hom}_F(M, M)$. Thus the result follows from applying isomorphism theorems together with Theorem 2.5 (a).

**Theorem 2.9.** Let $G$ be a finite solvable group. Then $A_e(G)$ is solvable.

**Proof.** $A_e(G) \cong G/Z(G)$ is clearly solvable. Thus we only need to show that $A_e(G)/A^1_e(G)$ is solvable.

Let $M$ be a minimal normal subgroup of $G$. Since $G$ is solvable, $M$ must be an elementary Abelian $p$-group for some prime $p$.

If $M \subseteq Z(G)$, then by induction and Proposition 2.8 we are finished.

If $M \nsubseteq Z(G)$, then $M$ is an irreducible and nontrivial $\Gamma$-module, where $\Gamma = G/M$. Schur's lemma and Wedderburn's theorem imply that $\text{Hom}_F(M, M)$ has a finite cyclic group of units. Using induction and Proposition 2.8 once more we are again finished.

**Q.E.D.**

**Theorem 2.10.** Let $G$ be a group admitting a composition series. Suppose that for each composition factor $F$ of $G$ the group $A(F)/A_1(F)$ is solvable. Then $A_e(G)/A^1_e(G)$ is solvable.

**Proof.** We induct on the length of a composition series. If $G$ is a simple group, there is nothing to prove. If $G$ is not simple, then let $M$ be a minimal normal subgroup of $G$.

Case 1. $M$ is Abelian.

The existence of a composition series in $G$ implies that $M$ must be a finite group. $M$ is $\Gamma$-irreducible and we can repeat the arguments of Proposition 2.8 and Theorem 2.9 to conclude that $A_e(G)/A^1_e(G)$ is solvable.

Case 2. $M$ is non-Abelian and $G$ has no Abelian normal subgroup other than $1$.

It is clear that $Z(G) = 1$. The minimal normal subgroup $M$ is now the direct product of a finite number of uniquely-determined non-Abelian simple groups $M_j$, $1 \leq j \leq t$. It follows that $A_e(G)$ induces a permutation group on the factors $M_j$. Since $M$ is minimal normal in $G$, $A_e(G)$ is already transitive on the factors $M_j$. Since $Z(G) = 1$, we can identify $G$ with $A_e(G)$ and $M$ with $I(M)$. Let $I$ be the stability group of $M_1$ in $A_e(G)$. (Namely, $I = \{\sigma \in A_e(G) \mid \sigma M_1 \sigma^{-1} = M_1\}$.) The fact that $A_e(G)$ is already transitive tells us that $A_e(G) = A_e(G) I$. The group $I$ now induces a group of automorphisms of $M_1$ and $M_1 \leq A_e(G) \cap I$. It follows that $A_e(G) \cap I$ induces a subgroup between $A(M_1)$ and $A_e(M_1)$. Consequently,

$A_e(G)/A_1^e(G) \cong I/(I \cap A_e(G))$
is isomorphic to a subgroup of a quotient group of \( A(M_1)/A_\psi(M_1) \). This last group is solvable by hypothesis; consequently we are done. Q.E.D.

Let us note that it is not possible to conclude in the preceding theorem that \( A(G)/A_\psi(G) \) is solvable. For example, we take \( G \) to be an elementary Abelian \( p \)-group with at least 4 elements. \( A(G)/A_\psi(G) \) is the general linear group and it is nonsolvable when the group \( G \) has at least 4 elements. It would be more satisfactory to assume in the preceding theorem that \( A_\phi(F)/A_\psi(F) \) is solvable. However, in practice, it is easier to determine \( A(F)/A_\psi(F) \). As we mentioned before, for finite groups Schreier conjectured that \( A(F)/A_\psi(F) \) is solvable whenever \( F \) is simple. For all known finite simple groups this is indeed the case. Thus Theorem 2.10 asserts that \( A(G)/A_\psi(G) \) is solvable for any finite groups manufactured out of known simple groups.

We conclude this section with an example showing that \( H^1_\psi(\Gamma, M) \) can be nontrivial for a faithful and irreducible \( \Gamma \)-module. Of course, Proposition 2.7 (c) implies that \( Z(\Gamma) \) must be 1. We recall that Serre's result tells us that we may assume faithfulness in the computation of \( H^1_\psi(\Gamma) \). This example will also show that \( A_\phi(G)/A_\psi(G) \) need not be trivial for a nonsolvable finite group. However, it seemly likely that \( A_\phi(G)/A_\psi(G) \) is trivial for a simple finite group.

Let \( M \) be the 2-dimensional vector space over GF(4) and let \( \Gamma = SL(2, 4) \) act on \( M \) in the natural way. It is clear that \( M \) is a faithful and irreducible left \( \Gamma \)-module. The group \( G \) will be the split extension of \( M \) by \( \Gamma \). Thus \( G \) is the special affine group in two variables over GF(4). It is known that \( A_\phi(\Gamma)/A_\psi(\Gamma) = 1 \). As a result, we know that \( A_\phi(G) = A_\chi(G) \cap A_\psi(G) \cap A_\epsilon(G, M) \).

We assert that \( A_\epsilon(G, M) \cap A_\phi(G) = A_\psi(G, M) \cap A_\epsilon(M) \). Since \( M \) is faithful we already know that \( A_\psi(G, M) \subseteq A_\epsilon(G, M) \). Suppose that \( \sigma \in A_\phi(G) \cap A_\epsilon(G, M) \) is not in \( A_\psi(G, M) \). Then \( \sigma \) must induce scalar multiplication by an element \( \theta \) of order 3 in GF(4). We know that \( \sigma(m^3) = (m^3)a_\psi \gamma \) for \( m \in M, \gamma \in \Gamma \), where \( a_\gamma \) is a cocycle whose class lies in \( H^1_\psi(\Gamma, M) \). This last assertion follows from examining the case \( m = 0 \) together with the fact that \( \sigma \in A_\psi(G) \). In view of Theorem 2.5 (b), we can modify \( \sigma \) by an element of \( A_\phi(G) \cap A_\psi(G) \) so that we can assume that \( a_\gamma = 0 \) for every \( \gamma \). Since \( \sigma \in A_\phi(G) \), we can find \( \beta \in \Gamma, n \in M \) such that \( (m^3)^{n-1} = n^\beta n^{-1} m^{-1} \). It follows that \( \beta \in C_\gamma(\psi) \) and \( \psi(n) = \beta(m) m^{-1} \). We note that \( M \) is written multiplicatively, thus scalar operators appear as exponents. We now revert back to matrices. Let \( \gamma = \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \). Then \( \beta = \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \) for suitable \( \psi \in GF(4) \). It is clear that \( (\gamma - 1) M = \left( \begin{array}{c} 1 \\ 0 \end{array} \right) \). If \( m \) is taken to be \( \left( \begin{array}{c} 0 \\ 0 \end{array} \right) \), then the desired equation has no solution in \( \beta \) and \( n \). This shows that \( \sigma \) could not exist. Consequently,

\[ A_\epsilon(G, M) \cap A_\phi(G) = A_\epsilon(G, M) \cap A_\psi(G, M) \cap A_\psi(G) \cap A_\epsilon(G, M) \]

Combining Theorem 2.5 (b) with the preceding paragraph, we obtain the result that \( A_\phi(G)/A_\psi(G) \simeq H^1_\psi(\Gamma, M) \).
We know that $\theta$ generates $GF(4)$ over $GF(2)$. Let $S = \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right)$ and $T = \left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right)$. It follows that $S^2 = T^3 = (ST)^5 = 1$. It is well known that these are the generators and the defining relations for the alternating group of degree 5. The following proposition is well known; we provide a sketch of its proof for convenience.

**Proposition 2.11.** Let $F$ be a free group based on the set $X$. Let $M$ be a left $F$-module. The following statements hold:

(a) Each map $f : X \to M$ can be extended uniquely to a normalized 1-cocycle of $X$ in $M$.

(b) If $f(r) = 0$ for each $r \in R$, $R$ a subset of $F$ acting trivially on $M$, then $f$ vanishes on the normal subgroup of $F$ generated by $R$.

(c) Let $N$ be the normal subgroup of $F$ generated by the set $R$ in (b). Then $f$ defines a 1-cocycle of $F/N$ in $M$. Every 1-cocycle of $F/N$ in $M$ can be viewed as a 1-cocycle of $F$ in $M$ which vanishes on $R$.

**Proof.** We set $f(1) = 0$. The cocycle condition forces us to set $f(x^{-1}) = -x^{-1}f(x)$. It then forces us to set $f(uv) = uf(v) + f(u)$. The assertions now follow in a straightforward way from the fact that each element of the free group $F$ has a unique reduced representation in terms of $x$ and $x^{-1}$, $x \in X$.

**Proposition 2.12.** Let $f$ be a normalized 1-cocycle of a group $\Gamma$ in a $\Gamma$-module $M$. Then $f(\gamma^n) = (1 + \gamma + \cdots + \gamma^{n-1}) f(\gamma)$. In particular, if $\gamma^n$ is trivial on $M$ and if $\gamma$ has only the trivial fixed point on $M$, then $f(\gamma^n) = 0$ holds automatically.

The proof is straightforward.

We now return to our example. Suppose that $[f] \in H^1_\times(\Gamma, M)$. We can modify $f$ by a coboundary and assume that $f(T) = 0$. Since $S^2 = 1$ and $GF(4)$ has characteristic 2, we must have $f(S) = Sf(S)$. Thus $f(S) = (\gamma^u)$ for suitable $u \in GF(4)$. Conversely, setting $f(T) = 0$ and $f(S) = (\gamma^u)$ for any $u \in GF(4)$, we obtain a 1-cocycle on the free group generated by $S$ and $T$. Proposition 2.12 shows that $f(S^2) = 0$. Since $T$ and $ST$ are acting without fixed points on $M$ and $T^3$, $(ST)^5$ act trivially on $M$, we can conclude from Proposition 2.12 that $f(T^3) = 0 = f((ST)^5)$. Thus $f$ really defines a cocycle on $\Gamma$ as indicated in Proposition 2.11. We know from the structure of $SL(2, 4)$ that every element of $SL(2, 4)$ has order 3, 5 or 2. Any element of order 2 is conjugate to $S$ in $SL(2, 4)$. Using the fact that $H^q(C, M) = 0$ when $C$ is a finite group of order prime to the order of $M$, we can conclude that the restriction of our cocycle is trivial on every subgroup of order 3 and 5. It is clear that $f(S) = (\gamma^u) = (1 - S)(u^0_{-1})$. Thus $[f] \in H^1_\times(\Gamma, M)$. We still
have to decide when \( f \) is a coboundary. If \( f \) is a coboundary, then 
\[
f'(T) = (1 - T)q^2
\]
for suitable \( a, b \) in \( GF(4) \). However, \( f(T) = 0 \) and \( T \) has no fixed point other than 0 on \( M \), thus \( a = b = 0 \) and \( f \) must be identically 0. 
It is now clear that \( H'_q(T, M) \cong GF(4) \).

3. An Example

We now construct an example of a finite \( p \)-group \( G \) for which \( A_q(G)/A_q(G) \) is a non-Abelian group.

Let \( k = GF(q^n), q \) a power of the prime \( p \). Let \( R \) be a left \( k \)-vector space of dimension \( n, n \leq m \). Let 1, \( \pi, \ldots, \pi^{n-1} \) be a left \( k \)-basis for \( R \) and define multiplication on \( R \) by the rules:

\[
\begin{align*}
(1) & \quad \pi a = a^q \pi \\
(2) & \quad \pi^i \pi^j = \begin{cases} 
\pi^{i+j}, & \text{if } i + j < n, \\
0, & \text{if } i + j \geq n,
\end{cases} \quad \text{where } 0 \leq i, j < n, \pi^n = 1.
\end{align*}
\]

One checks immediately that \( R \) has the following properties:

3. \( R \) is a graded algebra with \( i \)th homogeneous component \( k\pi^i = \pi^i k \), 
\( k \)-vector space of dimension 1 (from the left and from the right), \( 0 \leq i < n \).
4. \( Rx = xR \) holds for every \( x \) in \( R \).
5. \( R\pi^i, 0 \leq i < n \), are the only ideals of \( R \) (left, right, or two-sided). 
They are linearly ordered by inclusion. In particular, \( R\pi \) is the Jacobson radical and \( R \) is completely primary.

It is now clear that we can talk about the lowest degree as well as the lowest 
(left) leading coefficient of an element of \( R \).

\( U_q(R) = U \) shall denote the group of units in \( R \). \( U_q(R) = 1 + R\pi^i, i > 0 \), 
is a \( p \)-group of order \( q^{n-i} \); these groups form a descending chain of normal 
subgroups of \( U_q(R) \).

6. The following statements for the elements \( x, y \in R \) are equivalent:

(a) \( xU_q(R) = U_q(R)y \).
(b) \( x \) and \( y \) have the same lowest degree term.

Proof. We can exclude the obvious cases when \( x \) or \( y \) is 0. It is clear that 
the lowest degree term of any nonzero element of \( R \) can be factored out 
either from the left, or from the right, with the quotient in \( U_q(R) \). In view of 
the fact that \( U_q(R) \) is a group and that multiplication by elements of \( U_q(R) \) 
does not alter the lowest degree term we can conclude that (a) and (b) are 
equivalent. O.E.D.
For $1 \leq i < n$, $U_{i}/U_{i+1}$ is isomorphic to the additive group of $k$ under the map that sends the coset of $x$ onto the $(i\text{th})$ coefficient of $(x-1)$. If $1 \leq j < n-1$, then the commutator map defines a bilinear [over $GF(q)$] map $B_{i,j} : U_{i}/U_{i+1} \times U_{j}/U_{j+1} \rightarrow U_{i+j}/U_{i+j+1}$. This map is nondegenerate when $i+j < n$ and it is trivial when $i+j \geq n$. In terms of the identifications, $B_{i,j}(a, b) = ab^{q^i} - b^{q^i}a^q$, $a, b \in k$ and $i+j < n$.

Proof. If we reduce $R$ by the ideal $Rn+j$, then we can deduce that $[U_i, U_j] \leq U_{i+j}$. This leads immediately to the bi-additivity of the map induced by the commutator map. The fact that $U_n(R) = 1$ implies immediately that $[U_i, U_j] = 1$ when $i+j \geq n$.

If $u = 1 - x, x \in R^{n}$, then $u^{-1} = 1 + \cdots + x^{n-1}$. Suppose now $u = 1 - x \in U_i$ and $v = 1 - y \in U_j$. In view of the fact that $[u, v] = [v, u]^{-1}$ we may assume that $i < j < n$. We now compute $[u, v]$ mod $R^{i+j+1}$ and note that $1 \leq i$. Thus we have,

$$[u, v] = (1 - x)(1 - y)(1 + x + x^2 + \cdots)(1 + y + y^2 + \cdots)$$

$$= (1 - x - y + xy)(1 + x + x^2 + \cdots + x^{n-1} + (1 + x)y + y^2)$$

$$+ \text{element in } R^{n+j+1}$$

$$= 1 - y(1 + x)y + xy + (1 - x^2)y - y(1 + x)y + y^2$$

$$+ \text{element in } R^{n+j+1}$$

$$= 1 - y - xy + xy + y - y^2 + y^2 + \text{element in } R^{n+j+1}$$

$$= 1 + (xy - yx) + \text{element in } R^{n+j+1}.$$  

Let $x$ have lowest term $an^i, a \in k$, and let $y$ have lowest term $bn^j, b \in k$. It is then clear that $[u, v] - 1$ has lowest term $an^ibm^j - bnm^ian^i = (ab^{q^i} - b^{q^i}a^q) \pi^{i+j}$. This verifies the asserted form of $B_{i,j}$. The map $B_{i,j}$ is now clearly bilinear over $GF(q)$. We must now show the nondegeneracy when $i+j < n$. Again, since the situation is symmetric, we only have to show that $B_{i,j}(a, b) = 0$ for all $b \in k$ implies that $a = 0$. If $a \neq 0$, then setting $b = 1$ we conclude that $a = a^q$. Since $i < n \leq m$, we can find $b \in k = GF(q^m)$ so that $b^q \neq b$. This shows that $a$ must be $0$. Q.E.D.

(8) $U_j, 1 \leq j \leq n$, is the $j$th term of the descending central series of $U_1$. It is also the $(n-j)$th term of the ascending central series of $U_1$. $U_1$ is nilpotent of class $n-1$. The Frattini subgroup of $U_1$ is $U_2$ so that $U_1$ is generated by elements of $U_1$ which form a basis for $U_1/U_2 \cong GF(q^n)$ over the prime field.

Proof. The first two assertions follow easily from the nondegeneracy of $B_{i,j}, j < n$, and from $B_{i,n} = 0$. The others are then easy consequences.

(9) $GF(q)$ is the center of the ring $R$. In particular, $U_1(R)$ and the center of $R$ have only the identity element of $R$ in common.
Proof. \( R \) is a graded algebra, therefore, the center of \( R \) must be a graded subalgebra. \( GF(q) \) is clearly the 0-component of the center. If \( j > 0 \), then \( a \pi^j \) is in the center implies that \( \pi^j \) must commute with all elements of \( k \), or else \( a = 0 \). The basic assumption that \( k = GF(q^m) \), \( m \geq n > j \), together with \( \pi^j b = b \pi^j \pi^j \) shows that \( \pi^j \) cannot commute with every element of \( k \). Thus \( a = 0 \) and \( GF(q) \) is the center of \( R \). Q.E.D.

We now study the affine group in one variable based on the ring \( R \) constructed above. This group, denoted by \( Aff(R) \), can be described as the group of all matrices of the form \( \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \), \( a \in U \), \( b \in R \), or be described as the split extension of \( R \) by \( U \) where \( R \) is considered as a left \( U \)-module through left multiplication. The exhibited matrix then corresponds to \((b, a)\) with the multiplication given by,

\[
(y, x)(b, a) = (y + xb, xa).
\]

It is easy to see that the following rules hold:

\[
(y, x)^{-1} = (-x^{-1}y, x^{-1}),
\]

\[
(y, x)(b, a)(y, x)^{-1} = (xb + y - xax^{-1}y, xax^{-1}).
\]

We note that \( U \) is identified with the set of all \((0, x)\), \( x \in U \); \( R \) is identified with the set of all \((y, 1)\), \( y \in R \). \( U \) acts on \( R \) through conjugation in \( Aff(R) \).

For each integer \( j \), \( 0 \leq j \leq n \), the \( j \)th special affine group, \( SAff_j(R) \), is defined to be the subgroup of \( Aff(R) \) whose elements have "determinant" in \( U_j(R) \). [Recall that \( U_j(R) = U_j \).] Equivalently, \((y, x)\) is in \( SAff_j(R) \) if and only if \( x \in U_j(R) \).

For each \( u \in U \) we define a map \( \sigma_u : Aff(R) \rightarrow Aff(R) \) by setting \( \sigma_u(b, a) = (bu, a) \). \( \sigma_u \) is obviously bijective. An immediate consequence of (10) is that \( \sigma_u \) is an automorphism of \( Aff(R) \). It is clear that \( \sigma_u \in Aut(SAff_j(R)) \) for \( 0 \leq j \leq n \).

(13) Let \( u \neq 1 \). \( \sigma_u \in Aut(SAff_j(R)) \), \( 0 \leq j \leq n \), if and only if,

(a) \( j = 0 \), and

(b) \( u \in GF(q) - \{0\} \).

Proof. \( R \) is an Abelian normal subgroup of \( SAff_j(R) \). The effect on \( R \) of an inner automorphism depends only the coset of the element determining the inner automorphism modulo \( R \). Formula (12) tells us that an inner automorphism must induce on \( R \) a left multiplication by a suitable element of \( U_j \). However, \( \sigma_u \) induces right multiplication on \( R \). Since \( R \) is a ring, we conclude that \( u \) must be in center of \( R \). (9) tells us that (a) and (b) are both necessary. When (a) and (b) are satisfied, \( \sigma_u \) is the inner automorphism induced by the element \((0, u)\). Q.E.D.
(14) Let $u \neq 1$, $0 \leq j \leq n$. $\sigma_u \in A_\sigma(S\text{Aff}_j(R))$ if and only if,

(a) $u \in U_j$.

(b) for each $a \in U_j$, $b \in R$, there exist $x \in U_j$, $y \in R$ with the following properties:

$$xax^{-1} = a$$

(*)

$$(1 - a)y = bu - xb.$$  

(**)

Proof. (a) is a special instance of (b). We take $a = 1 = b$. Our assertion is an obvious consequence of (12). Q.E.D.

Let us observe that (***) states that $bu - xu$ must lie in the ideal generated by $(1 - a)$. If $a$ is close to 1, then $C_u(a)$ is large, but $(1 - a) \in R$ is small. If $a$ is farther away from 1, then $C_u(a)$ is small, but $(1 - a) \in R$ is large. We must balance (*) and (**) against each other and hope for the best. A "saddle point" occurs when $n = 3$ and $G = S\text{Aff}_3(R)$.

**THEOREM.** Let $n = 3$ and set $G = S\text{Aff}_3(R)$. Then $A_\sigma(G)/A_\sigma(G)$ contains a subgroup isomorphic to the non-Abelian group $U_3(R)$. Thus $A_\sigma(G)/A_\sigma(G)$ is a $p$-group of class at least 2.

Proof. Since $G$ is a $p$-group we already know that $A_\sigma(G)$ is a $p$-group. In view of (13) and (14) we only have to show that (*) and (**) can be solved simultaneously for any $u$ in $U_3(R)$.

**Case 1.** $a \in U_3(R)$.

We know from (8) that $a$ is in the center of $U_1$. Thus (*) is automatic for any $x$ in $U_1$. We let $y$ be 0. (6) then tells us that (**) can be solved for any $u \in U_1$ with $x$ in $U_1$.

**Case 2.** $a \notin U_3(R)$.

In this case $(1 - a) \in R = R\pi$. We take $x = 1$. It then follows that $bu - xb = b(u - 1) \in R\pi$ for any $u \in U_1$. Again we can solve (**). Since $x = 1$, (*) is again automatic. Q.E.D.

In contrast to our earlier examples, the group $U_1$ appears in the factor group

$$(A_\sigma(G) \cap A^1(G, M)) A_\sigma(G)/(A_\sigma(G) \cap A^1(G, M)) A_\sigma(G).$$

The order of the group constructed in the theorem has order $q^{5m}$, $m \geq 3$. Thus the smallest one has order $2^{15}$. 
REFERENCES