# THE AUTOMORPHISMS OF THE HOLOMORPH OF A FINITE ABELIAN GROUP

BY

W. H. MILLS

In 1908 G. A. Miller [4] proved that the holomorph of a finite abelian group of odd order has only inner automorphisms. The group of automorphisms of the holomorph of an arbitrary group was studied by Gol'fand [3] who found some cases in which the outer automorphism group has order one or two. In the present paper I determine explicitly the outer automorphism group $\mathfrak{O}$ of the holomorph $H$ of an arbitrary finite abelian group $G$. If $G$ is the direct product of a group of odd order, a group of order two, and a cyclic group of order $2^n$ where $n \geqq 2$, then $\mathfrak{O}$ is the direct product of a finite number of groups of order two and a non-abelian group $\mathfrak{O}^*$ of order six or eight. If $n=2$ then $\mathfrak{O}^*$ is isomorphic to the symmetric group of order six, and if $n \geqq 3$ then $\mathfrak{O}^*$ is the octic group. In all other cases $\mathfrak{O}$ is either trivial or the direct product of a finite number of groups of order two.

Let $A$ be the group of all automorphisms of the finite abelian group $G$, let $\mathfrak{B}$ be the group of all automorphisms of $H$ that map $G$ onto itself, and let $\mathfrak{I}$ be the group of all inner automorphisms of $H$. Then $\mathfrak{B}/\mathfrak{I}$ can be identified with the first cohomology group $H^1(A, G)$. Thus $H^1(A, G)$ can be regarded as a subgroup of $\mathfrak{O}$. Now $G$ is an invariant subgroup of $H$, and it is known [6] that $H$ has at most four invariant subgroups isomorphic to $G$. It follows that $H^1(A, G)$ has index at most four in $\mathfrak{O}$.

In Part I the first cohomology group $H^1(A, G)$ is determined explicitly—it is either trivial or the direct product of groups of order two. In Part II the results of Part I are combined with the results of [6] to determine $\mathfrak{O}$ explicitly.

## I. $H^1(A, G)$

**1. The role of $H^1(A, G)$.** Let $G$ be a finite abelian group and $A$ its group of automorphisms. The holomorph $H$ of $G$ is defined(1) to be the semi-direct product of $A$ and $G$. Thus $H$ is the group of all ordered pairs $(g, \sigma)$, $g \in G$, $\sigma \in A$, with multiplication given by

$$(g, \sigma)(a, \tau) = (g\sigma a, \sigma\tau).$$

The first eight lower case Roman letters will be used to denote group

Received by the editors June 7, 1956.

(1) There are two other well known definitions of the holomorph. It has been defined as the group of one-to-one mappings of $G$ onto itself that is generated by the automorphisms of $G$ and the left multiplications $g \to ag$. Suppose $G$ is represented as a regular permutation group on $n$ letters. Then, according to the original definition, the holomorph is the normalizer of $G$ in the symmetric group $S_n$. These three definitions are equivalent up to isomorphism.

elements (usually elements of $G$), and the remaining ones to denote non-negative integers. Lower case Greek letters will be used to denote homomorphisms of groups (usually automorphisms of $G$), and capital Greek letters will be used to denote automorphisms of the holomorph $H$ and one dimensional cocycles.

We denote the identity of $G$ by $e$, and that of $A$ by $\epsilon$.

The elements of the form $(g, \epsilon)$ form an invariant subgroup of $H$, the mapping $g \to (g, \epsilon)$ is an imbedding of $G$ in $H$, and we will henceforth identify the element $g$ in $G$ with the element $(g, \epsilon)$ in $H$. On the other hand we will distinguish carefully between the element $\sigma$ in $A$ and the element $(e, \sigma)$ in $H$.

Let $I_{(g,\sigma)}$ denote the inner automorphism of $H$ corresponding to $(g, \sigma)$. Thus

$$I_{(g,\sigma)}(a, \tau) = (g, \sigma)(a, \tau)(g, \sigma)^{-1}.$$

In particular $I_{(e,\sigma)}g = \sigma g$, so that every automorphism of $G$ can be extended to an inner automorphism of $H$.

Let $\mathfrak{A}$ be the group of all automorphisms of $H$, and let $\mathfrak{I}$ be the group of all inner automorphisms of $H$. Let $\mathfrak{B}$ be the group of all automorphisms of $H$ that map $G$ onto itself, and let $\mathfrak{C}$ be the group of all automorphisms of $H$ that act as the identity on $G$. Then $\mathfrak{A} \supseteq \mathfrak{B} \supseteq \mathfrak{C}$ and $\mathfrak{I}$ is an invariant subgroup of both $\mathfrak{A}$ and $\mathfrak{B}$. Let $\mathfrak{O} = \mathfrak{A}/\mathfrak{I}$ be the outer automorphism group of $H$. Our ultimate goal is the determination of $\mathfrak{O}$, and we will begin with the study of $\mathfrak{B}/\mathfrak{I}$.

Suppose $\Omega \in \mathfrak{B}$. The restriction of $\Omega$ to $G$ is an automorphism $\sigma$ of $G$, and we have $\Omega I_{(e,\sigma)}^{-1} g = g$ for all $g \in G$. Hence $\Omega I_{(e,\sigma)}^{-1} \in \mathfrak{C}$. It follows that $\mathfrak{B} = \mathfrak{C}\mathfrak{I}$.

Suppose $\Gamma \in \mathfrak{C}$. Let $\Gamma'$ be the mapping of $A$ into $G$ and $\sigma \to \bar{\sigma}$ the mapping of $A$ into itself such that $\Gamma(e, \sigma) = (\Gamma'\sigma, \bar{\sigma})$ for all $\sigma \in A$. If $g$ is an arbitrary element of $G$ we have $(e, \sigma)g = \sigma g(e, \sigma)$,

$$\Gamma((e, \sigma)g) = (\Gamma'\sigma, \bar{\sigma})g = \bar{\sigma}g(\Gamma'\sigma, \bar{\sigma}),$$

and

$$\Gamma(\sigma g(e, \sigma)) = \sigma g(\Gamma'\sigma, \bar{\sigma}).$$

Hence $\bar{\sigma}g = \sigma g$ for all $g \in G$. Therefore $\bar{\sigma} = \sigma$. Furthermore $(\Gamma'\sigma, \sigma)(\Gamma'\tau, \tau) = \Gamma((e, \sigma)(e, \tau)) = \Gamma(e, \sigma\tau) = (\Gamma'(\sigma\tau), \sigma\tau)$. Comparing first components we obtain

$$(\Gamma'\sigma)(\sigma\Gamma'\tau) = \Gamma'(\sigma\tau) \tag{1}$$

for all $\sigma, \tau$ in $A$. We note that (1) is the condition that $\Gamma'$ be an element of $Z^1(A, G)$, the group of one dimensional cocycles or crossed homomorphisms of $A$ into $G$. Conversely if $\Gamma' \in Z^1(A, G)$, then the mapping $\Gamma$ given by

$$\Gamma(g, \sigma) = (g\Gamma'\sigma, \sigma) \tag{2}$$

is an automorphism of $H$ and hence an element of $\mathfrak{C}$. The mapping $\Gamma \to \Gamma'$ is

an isomorphism of $\mathfrak{C}$ onto $Z^1(A, G)$. Henceforth we will identify the cocycle $\Gamma'$ with the element $\Gamma$ of $\mathfrak{C}$ given by (2). Then we have $\mathfrak{C}=Z^1(A, G)$.

Suppose now that $I_{(a,\tau)}\in\mathfrak{C}$. Then

$$g = I_{(a,\tau)}g = I_a I_{(e,\tau)}g = \tau g$$

for all $g\in G$. Hence $\tau=\epsilon$ and $(a, \tau)=a$. Furthermore

$$I_a(e, \sigma) = a(e, \sigma)a^{-1} = (a\sigma a^{-1}, \sigma).$$

It follows that if $\Gamma\in Z^1(A, G)$, then the condition that $\Gamma$ be an inner automorphism of $H$ is that it be of the form $\Gamma_a$, where

$$\Gamma_a\sigma = a\sigma a^{-1}, \tag{3}$$

$a$ a fixed element of $G$. Now this is the condition that $\Gamma$ be an element of $B^1(A, G)$, the group of one dimensional coboundaries or splitting homomorphisms of $A$ into $G$. Thus $\mathfrak{H}\cap\mathfrak{C}=B^1(A, G)$ and we have

$$\mathfrak{G}/\mathfrak{H} = \mathfrak{C}\mathfrak{H}/\mathfrak{H} \cong \mathfrak{C}/\mathfrak{H}\cap\mathfrak{C} = Z^1(A, G)/B^1(A, G) = H^1(A, G),$$

the first cohomology group of $A$ acting on $G$. The first cohomology group $H^1(A, G)$ is thus isomorphic to $\mathfrak{G}/\mathfrak{H}$ under the natural isomorphism

$$\Gamma B^1(A, G) \to \Gamma\mathfrak{H}.$$

We are now faced with the problem of explicit determination of $H^1(A, G)$ to which we devote the remainder of part I.

2. **Additional notation and preliminary lemmas.** We will write

$$Q = Q_1 \times Q_2 \times \cdots \times Q_m, \tag{4}$$

or $Q=\prod Q_i$, if the $Q_i$ are subgroups of the group $Q$, and $Q$ is the direct product of the $Q_i$. Suppose (4) holds, let $S$ be a subset of $\{1, 2, \cdots, m\}$, and put

$$Q_S = \prod_{i\in S} Q_i.$$

If $\sigma$ is any automorphism of $Q_S$ we identify $\sigma$ with the automorphism $\sigma'$ of $Q$ such that

$$\sigma' g = \begin{cases} \sigma g \text{ if } g \in Q_S, \\ g \text{ if } g \in Q_j, j \notin S. \end{cases}$$

This identification does not depend on $Q_S$ and $Q$ alone, but also on the groups $Q_j, j\notin S$. However we will not have occasion to deal with two decompositions of the same group simultaneously, except in cases where they have a common refinement. Hence we can identify $\sigma$ with $\sigma'$ without danger of ambiguity, and we will do so freely.

We need to know a set of generators for the group of automorphisms of $G$. It is sufficient to settle this question for the prime power case, which is treated in the following lemma.

LEMMA 1. *Let $G^{(p)}$ be a finite abelian group whose order is a power of the prime number $p$. Let $G^{(p)}=D_1\times D_2\times\cdots\times D_l$, where $D_i$ is cyclic of order $m_i$ and $m_1\geqq m_2\geqq\cdots\geqq m_l>1$. Let $d_i$ be a generator of $D_i$, and let $A_i$ be the group of automorphisms of $D_i$. For $1\leqq j\leqq l-1$, let $s_j=m_j/m_{j+1}$, and let $\gamma_j$ and $\delta_j$ be the automorphisms of $D_j\times D_{j+1}$ such that*

$$\gamma_j d_j = d_j d_{j+1}, \qquad \gamma_j d_{j+1} = d_{j+1},$$
$$\delta_j d_j = d_j, \qquad \delta_j d_{j+1} = d_j^{s_j} d_{j+1}.$$

*Then the group of all automorphisms of $G^{(p)}$ is generated by the automorphisms $\gamma_j$, $\delta_j$, $1\leqq j<l$, and the groups $A_i$, $1\leqq i\leqq l$.*

**Proof by induction on $l$.** Lemma 1 is trivial if $l=1$. Suppose that $l>1$ and that Lemma 1 holds for the subgroup $\tilde{G}=D_2\times D_3\times\cdots\times D_l$. Let $\tilde{A}$ be the group generated by the automorphisms $\gamma_j$, $\delta_j$, $1\leqq j<l$, and the groups $A_i$, $1\leqq i\leqq l$. By the induction hypothesis any automorphism $\omega$ of $\tilde{G}$ belongs to $\tilde{A}$. Let $\sigma$ be an arbitrary automorphism of $G^{(p)}$. We write

$$\sigma d_1 = \prod_{i=1}^{l} d_i^{u_i}.$$

We begin by constructing an automorphism $\psi\in\tilde{A}$ such that $\psi d_1=\sigma d_1$. There are two possibilities to be considered: (I) $p\mid u_1$. Here for some $j\geqq 2$ we must have $p\nmid u_j$ and $m_1=m_j$. Therefore $m_1=m_2$, $s_1=1$, and there is an automorphism $\rho$ of $\tilde{G}$ such that

$$\rho d_2 = \prod_{i=2}^{l} d_i^{u_i}.$$

For such a $\rho$ we have

$$\rho\delta_1^{u_1-1}\gamma_1 d_1 = \rho\delta_1^{u_1-1}(d_1d_2) = \rho(d_1^{u_1}d_2) = \sigma d_1,$$

and we put $\psi=\rho\delta_1^{u_1-1}\gamma_1$, which belongs to $\tilde{A}$. (II) $p\nmid u_1$. In this case there exists an automorphism $\tau$ of $D_1$ such that $\tau d_1=d_1^{u_1}$ and an automorphism $\rho'$ of $\tilde{G}$ such that

$$\rho' d_2 = d_2 \prod_{i=3}^{l} d_i^{u_i},$$

where $\rho'$ is understood to be $\epsilon$ if $l=2$. Then

$$\tau\gamma_1^{u_2-1}\rho'\gamma_1 d_1 = \tau\gamma_1^{u_2-1}\rho'(d_1d_2) = \tau\gamma_1^{u_2-1}\left(d_1d_2\prod_{i=3}^{l} d_i^{u_i}\right)$$
$$= \tau\left(d_1\prod_{i=2}^{l} d_i^{u_i}\right) = \sigma d_1,$$

and we put $\psi=\tau\gamma\rho_1^{u_2-1}{}'\gamma_1$, which is an element of $\tilde{A}$.

Thus in both cases we have found an automorphism $\psi \in \tilde{A}$ such that $\psi d_1 = \sigma d_1$. Put $\sigma_1 = \psi^{-1}\sigma$. Then $\sigma_1 d_1 = d_1$. We now write

$$\sigma_1 d_j = \prod_{i=1}^{l} d_i^{v_{ij}}, \qquad 2 \leqq j \leqq l.$$

Let $\psi_1$ be the endomorphism of $\tilde{G}$ given by

$$\psi_1 d_j = \prod_{i=2}^{l} d_i^{v_{ij}}, \qquad 2 \leqq j \leqq l.$$

Since $\sigma_1 d_1 = d_1$ it follows that $\psi_1$ has a trivial kernel. Therefore $\psi_1$ is an automorphism of $\tilde{G}$. Hence $\psi_1 \in \tilde{A}$ and we put $\sigma_2 = \psi_1^{-1}\sigma_1$. Then $\sigma_2 d_1 = d_1$ and

$$\sigma_2 d_j = d_1^{v_{1j}} d_j, \qquad 2 \leqq j \leqq l.$$

Now put $v_j = v_{1j} m_j / m_1$. Since $(\sigma_2 d_j)^{m_j} = e$ it follows that $v_j$ is an integer. For $j \geqq 3$ let $\tau_j$ be the automorphism of $D_2 \times D_j$ such that

$$\tau_j d_2 = d_2^{-1}, \qquad \tau_j d_j = d_2^{m_2/m_j} d_j.$$

Then $(\tau_j \delta_1)^2 d_j = d_1^{m_1/m_j} d_j$ and $(\tau_j \delta_1)^2 d_i = d_i$ for $i \neq j$. It follows that

$$\sigma_2 = \delta_1^{v_2} \prod_{j=3}^{l} (\tau_j \delta_1)^{2v_j} \in \tilde{A}.$$

Therefore $\sigma = \psi \psi_1 \sigma_2 \in \tilde{A}$. This completes the proof of Lemma 1.

We write the finite abelian group $G$ in the form $G = G' \times G^{(2)}$, where $G'$ has odd order, and the order of $G^{(2)}$ is a power of 2. Let $A'$ and $A^{(2)}$ be the groups of automorphisms of $G'$ and $G^{(2)}$ respectively. Then $A = A' \times A^{(2)}$. We write

$$G^{(2)} = C_1 \times C_2 \times \cdots \times C_k,$$

where $C_i$ is cyclic of order $n_i$, $n_1 \geqq n_2 \geqq \cdots \geqq n_k \geqq 2$, and each of these $n_i$ is a power of 2. Let $c_i$ be a generator of $C_i$. For $j > k$ we let $C_j$ be the trivial group, $c_j = e$, and $n_j = 1$. Furthermore we put $r_i = n_i / n_{i+1}$ which must be a non-negative power of 2. If $G$ has odd order, then $G^{(2)}$ is trivial and $k = 0$. We will use the decomposition

$$G = G' \times C_1 \times \cdots \times C_k$$

to identify automorphisms of such groups as $G'$, $G^{(2)}$, $C_i$, $C_i \times C_{i+1}$ with elements of $A$. Let $\lambda$, $\lambda'$, and $\lambda''$ be the automorphisms of $G$, $G'$, and $G^{(2)}$ respectively such that

$$\lambda g = g^{-1}, \qquad \lambda' g' = g'^{-1}, \qquad \lambda'' g'' = g''^{-1}$$

for all $g \in G$, $g' \in G'$, $g'' \in G^{(2)}$. Clearly $\lambda = \lambda' \lambda''$.

Now let $\lambda_i$ and $\xi_i$ be the automorphisms of $C_i$ such that

$$\lambda_i c_i = c_i^{-1}, \qquad \xi_i c_i = c_i^{5}.$$

Let $\eta_i$ and $\theta_i$ be the automorphisms of $C_i \times C_{i+1}$ such that

$$\eta_i c_i = c_i c_{i+1}, \qquad \eta_i c_{i+1} = c_{i+1},$$
$$\theta_i c_i = c_i, \qquad \theta_i c_{i+1} = c_i^{r_i} c_{i+1}.$$

We note that $\lambda_i$ and $\xi_i$ generate the group of automorphisms of $C_i$. Hence, according to Lemma 1, the automorphisms $\lambda_i$, $\xi_i$, $1 \leqq i \leqq k$, and $\eta_j$, $\theta_j$, $1 \leqq j < k$, generate $A^{(2)}$. It is clear that $\lambda_i = \xi_i = \epsilon$ for $i > k$, and $\eta_j = \theta_j = \epsilon$ for $j \geqq k$.

Let $J$ be the center of $H$. Then $(a, \sigma) \in J$ if and only if

$$(a, \sigma) = g(a, \sigma)g^{-1} = (ag\sigma g^{-1}, \sigma)$$

and

$$(a, \sigma) = (e, \tau)(a, \sigma)(e, \tau)^{-1} = (\tau a, \tau\sigma\tau^{-1})$$

for all $g \in G$, $\tau \in A$. It follows that $(a, \sigma) \in J$ if and only if $\sigma = \epsilon$ and $\tau a = a$ for all $\tau \in A$. Thus we have the following result:

LEMMA 2. *The center $J$ of $H$ is the group of all characteristic elements of $G$.*

LEMMA 3. *If $G$ has a nontrivial characteristic element $h$, then $n_1 > n_2$ and $h = c_1^{n_1/2}$. Conversely if $n_1 > n_2$, then $c_1^{n_1/2}$ is a characteristic element of $G$.*

**Proof.** Let $h$ be a nontrivial characteristic element of $G$. We have $h = \lambda h = h^{-1}$ and hence $h$ has order 2. Therefore $h \in G^{(2)}$ and $n_1 \geqq 2$. If $h \neq c^{n_1/2}$ then there is an automorphism $\tau$ of $G^{(2)}$ such that $\tau h = hc_1^{n_1/2} \neq h$. Thus $h = c_1^{n_1/2}$. If $n_1 = n_2$ then interchanging the roles of $C_1$ and $C_2$ we obtain $h = c_2^{n_2/2}$, a contradiction. Therefore $n_1 > n_2$.

Conversely if $n_1 > n_2$, then $c_1^{n_1/2}$ is the only element of $G$ of order 2 of the form $g^{n_1/2}$, $g \in G$. Thus $n_1 > n_2$ implies that $c_1^{n_1/2}$ is a characteristic element of $G$.

Combining Lemmas 2 and 3 we obtain $J$ explicitly:

LEMMA 4. *The center $J$ of $H$ is trivial if $n_1 = n_2$. If $n_1 > n_2$ then $J$ has order two and is generated by $c_1^{n_1/2}$.*

Now put

$$N_j = G' \times \prod_{i \neq j} C_i, \qquad N_{j,j'} = G' \times \prod_{i \neq j, j'} C_i.$$

Let $J'$, $J^{(2)}$, $K_j$, and $K_{j,j'}$ be the groups of characteristic elements of $G'$, $G^{(2)}$, $N_j$, and $N_{j,j'}$ respectively. Applying Lemma 3 to these various groups we obtain the following information:

LEMMA 5. *$J'$ is trivial and $J^{(2)} = J$. If $3 \leqq j < j'$, then $K_j = K_{j,j'} = J$. If*

*$2 \leqq j < j'$, then $K_j$ and $K_{j,j'}$ are subgroups of $C_1$ of order at most two. If $2 \leqq j < j'$ and $n_1 > n_2$, then $K_j = K_{j,j'} = J$. Furthermore $K_1 \subseteq C_2$ and $K_{1,2} \subseteq C_3$. If $n_2 = n_3$ then $K_1$ is trivial, and if $n_2 > n_3$ then $K_1$ has order two. If $n_3 = n_4$ then $K_{1,2}$ is trivial, and if $n_3 > n_4$ then $K_{1,2}$ has order two.*

LEMMA 6. *Suppose that $G = Q_1 \times Q_2$ and that $\overline{J}$ is the group of characteristic elements of $Q_1$. Let $\tau$ be an automorphism of $Q_2$. If $\Gamma \in Z^1(A, G)$, then $\Gamma\tau \in \overline{J} \times Q_2$ and $\Gamma(\tau^2) \in Q_2$. Furthermore if $\overline{Z}$ is the group of all cocycles $\overline{\Gamma}$ such that $\overline{\Gamma}\tau \in Q_2$, then $[Z^1(A, G) : \overline{Z}]$, the index of $\overline{Z}$ in $Z^1(A, G)$, is at most two.*

**Proof.** Let $\sigma$ be any automorphism of $Q_1$. Then $\sigma\tau = \tau\sigma$ and hence

$$(\Gamma\sigma)(\sigma\Gamma\tau) = (\Gamma\tau)(\tau\Gamma\sigma).$$

Since $G$ is abelian this can be written

$$(\Gamma\tau)^{-1}(\sigma\Gamma\tau) = (\Gamma\sigma)^{-1}(\tau\Gamma\sigma).$$

Now $g^{-1}\sigma g \in Q_1$ and $g^{-1}\tau g \in Q_2$ for all $g \in G$. Therefore $(\Gamma\tau)^{-1}(\sigma\Gamma\tau) \in Q_1 \cap Q_2$, which consists of $e$ alone. Hence $\sigma\Gamma\tau = \Gamma\tau$. Since this holds for any automorphism $\sigma$ of $Q_1$ we must have $\Gamma\tau \in \overline{J} \times Q_2$. We may write $\Gamma\tau = \bar{h}g_2$, $\bar{h} \in \overline{J}$, $g_2 \in Q_2$. Now $\overline{J}$ is the group of characteristic elements of a finite abelian group. Therefore, by Lemma 3, $\overline{J}$ has order 1 or 2. Hence $\bar{h}\tau\bar{h} = \bar{h}^2 = e$ for any $\bar{h} \in \overline{J}$. It follows that $\Gamma(\tau^2) = (\Gamma\tau)(\tau\Gamma\tau) = g_2\tau g_2 \in Q_2$.

Finally we note that the mapping $\Gamma \to \bar{h}$ is a homomorphism of $Z^1(A, G)$ into $\overline{J}$ with kernel $\overline{Z}$. Hence $[Z^1(A, G) : \overline{Z}]$ is at most the order of $\overline{J}$, which in turn is at most 2.

LEMMA 7. *If $G = Q_1 \times Q_2$, if $\tau$ and $\bar{\lambda}$ are automorphisms of $Q_2$, and if $\bar{\lambda}g_2 = g_2^{-1}$ for all $g_2 \in Q_2$, then*

$$(\Gamma\tau)^2 = (\Gamma\bar{\lambda})(\tau\Gamma\bar{\lambda})^{-1} \tag{5}$$

*for all $\Gamma \in Z^1(A, G)$.*

**Proof.** As in Lemma 6 let $\overline{J}$ be the group of characteristic elements of $Q_1$. Since $\overline{J}$ has order one or two it follows that $\bar{\lambda}\bar{h} = \bar{h} = \bar{h}^{-1}$ for all $\bar{h} \in \overline{J}$. Hence $\bar{\lambda}g = g^{-1}$ for all $g \in \overline{J} \times Q_2$. We have $\Gamma\tau \in \overline{J} \times Q_2$ by Lemma 6, and therefore $\bar{\lambda}\Gamma\tau = (\Gamma\tau)^{-1}$. Now $\bar{\lambda}$ is in the center of the group of automorphisms of $Q_2$. Therefore $\tau\bar{\lambda} = \bar{\lambda}\tau$,

$$(\Gamma\tau)(\tau\Gamma\bar{\lambda}) = \Gamma\bar{\lambda}(\bar{\lambda}\Gamma\tau) = (\Gamma\bar{\lambda})(\Gamma\tau)^{-1},$$

and (5) follows at once.

If we apply Lemma 7 to the case $Q_2 = G$, $Q_1$ trivial, then we obtain

$$\Gamma^2\tau = (\Gamma\tau)^2 = (\Gamma\lambda)(\tau\Gamma\lambda)^{-1} \tag{6}$$

for all $\tau \in A$, $\Gamma \in Z^1(A, G)$. It follows from (6) that the square of every ele-

ment of $Z^1(A, G)$ is a coboundary. Therefore *every nontrivial element of* $H^1(A, G)$ *has order two.*

LEMMA 8. *If* $n_1 \geqq 8$, *then* $(\Gamma\lambda_1)^{n_1/2} = e$ *for all* $\Gamma \in Z^1(A, G)$.

**Proof.** Let $\tau$ be the automorphism of $C_1$ such that $\tau c_1 = c_1^{1+n_1/2}$. Then $\tau^2 = \epsilon$. By Lemma 6, $\Gamma\lambda_1$ and $\Gamma\tau$ are elements of $C_1 \times K_1$. For any $g \in C_1 \times K_1$ we have $\tau g = g^{1+n_1/2}$. It follows that $\tau\Gamma\lambda_1 = (\Gamma\lambda_1)^{1+n_1/2}$ and

$$e = \Gamma(\tau^2) = (\Gamma\tau)(\tau\Gamma\tau) = (\Gamma\tau)^{2+n_1/2}.$$

Now $n_1$ is a power of 2 and $n_1 \geqq 8$. Hence $2+n_1/2$ is not divisible by 4. Furthermore $\Gamma\tau \in G^{(2)}$ so that the order of $\Gamma\tau$ is a power of 2. Hence $(\Gamma\tau)^2 = e$. Applying Lemma 7 to the case $Q_1 = N_1$, $Q_2 = C_1$, $\tilde{\lambda} = \lambda_1$, we obtain

$$e = (\Gamma\tau)^2 = (\Gamma\lambda_1)(\tau\Gamma\lambda_1)^{-1} = (\Gamma\lambda_1)^{-n_1/2},$$

which is the desired result.

3. **The group** Hom $(A, J)B^1(A, G)$. Let Hom $(A, J)$ be the group of all homomorphisms of $A$ into $J$, the center of $H$. Since $J$ is the group of characteristic elements of $G$ it follows that Hom $(A, J)$ is a subgroup of $Z^1(A, G)$. In this section and the next we determine the factor group $Z^1(A, G)/\text{Hom}\ (A, J) \cdot B^1(A, G)$. We need the following characterization of the group Hom $(A, J) \cdot B^1(A, G)$.

THEOREM 1. *Let* $\Gamma \in Z^1(A, G)$. *Then* $\Gamma \in \text{Hom}\ (A, J)B^1(A, G)$ *if and only if the following conditions hold*:

(i) $\Gamma\lambda_1 \in C_1$.

(ii) $\Gamma\theta_1 \in C_1 \times C_2$.

(iii) $\Gamma\eta_2 \in J \times C_2 \times C_3$.

(iv) *Either* $n_1 \neq 4n_2$ *or* $\Gamma(\lambda_1\eta_1) \in C \times C_3$, *where* $C$ *is the cyclic group generated by* $c_1^2 c_2^{-1}$.

**Proof.** Throughout this proof $i$ and $j$ will always denote positive integers. We have $J \subseteq C_1$. Furthermore if $n_1 = 4n_2$, then $J = C_1 \cap C \subseteq C$. It follows that (i), (ii), (iii), and (iv) hold for any $\Gamma' \in \text{Hom}\ (A, J)$. Let $\Gamma'' \in B^1(A, G)$. Then there is a fixed $a \in G$ such that $\Gamma''\sigma = a\sigma a^{-1}$ for all $\sigma \in A$. Now $g\lambda_1 g^{-1} \in C_1$, $g\theta_1 g^{-1} \in C_1$, $g\eta_2 g^{-1} \in C_3$, and $g\lambda_1\eta_1 g^{-1} \in C$ for all $g \in G$. Hence (i), (ii), (iii), and (iv) hold for any $\Gamma'' \in B^1(A, G)$. Now the conditions (i), (ii), (iii), and (iv) are of such a nature that if they hold for two cocycles $\Gamma'$ and $\Gamma''$, then they hold for their product $\Gamma'\Gamma''$. It follows that (i), (ii), (iii), and (iv) hold for every element of Hom $(A, J)B^1(A, G)$.

To prove the converse let $\Gamma \in Z^1(A, G)$ and suppose that (i), (ii), (iii), (iv) hold. According to Lemma 6 we can write, for $1 \leqq i < k$,

$$\Gamma\theta_i = c_i^{u_i} c_{i+1}^{v_i} h_i,$$

where $h_i \in K_{i,i+1}$ and $u_i$, $v_i$ are integers. We have $h_1 = e$ by (ii). Now $\Gamma\lambda_j$

$\in C_1 \times C_j$ for $j \geqq 2$ by Lemmas 6 and 5. Furthermore $\Gamma\lambda_1 \in C_1$ by (i). Therefore $\theta_i \Gamma\lambda_i = \Gamma\lambda_i$ for all $i$. We observe that $\lambda_i = \theta_i \lambda_i \theta_i$. Hence

$$\Gamma\lambda_i = (\Gamma\theta_i)(\theta_i\Gamma\lambda_i)(\theta_i\lambda_i\Gamma\theta)$$

which reduces to

$$e = (\Gamma\theta_i)(\theta_i\lambda_i\Gamma\theta_i) = c_i^{r_i v_i} c_{i+1}^{2v_i}.$$

Thus $n_i \mid r_i v_i$ which is equivalent to $n_{i+1} \mid v_i$. Therefore $c_{i+1}^{v_i} = e$ and we have

$$\Gamma\theta_i = c_i^{u_i} h_i. \tag{7}$$

It follows at once that $\theta_i \Gamma\theta_i = \Gamma\theta_i$. Combining this with $\theta_i^{n_i/r_i} = \epsilon$ we obtain

$$e = \Gamma(\theta_i^{n_i/r_i}) = (\Gamma\theta_i)^{n_i/r_i}.$$

Therefore $c_i^{n_i u_i/r_i} = e$ and we have $r_i \mid u_i$.

By Lemmas 6 and 5 we have $\Gamma\lambda' \in J^{(2)} \times G' = J \times G'$. Every element of $G'$ has odd order. Therefore every element of $G'$ is a square and we have

$$\Gamma\lambda' = hg'^2,$$

where $h \in J$ and $g' \in G'$.

By Lemmas 6 and 5 we can write

$$\Gamma\eta_1 = c_1^r c_2^s \bar{h},$$

where $\bar{h} \in K_{1,2} \subseteq C_3$. By (i) we have $\Gamma\lambda_1 = c_1^t$ for some integer $t$. By Lemma 8, $t$ is even if $n_1 \geqq 8n_2$. Now put

$$s' = \begin{cases} s & \text{if } n_1 \leqq 4n_2, \\ -t/2 & \text{if } n_1 \geqq 8n_2, \end{cases}$$

and

$$f = g'^{-1} c_1^{s'} \prod_{i=1}^{k-1} c_{i+1}^{u_i/r_i}.$$

Let $\Gamma_f$ be the element of $B^1(A, G)$ corresponding to $f$, i.e. $\Gamma_f\sigma = f\sigma f^{-1}$ for all $\sigma \in A$. Put $\Gamma_1 = \Gamma\Gamma_f$. To prove Theorem 1 it is sufficient to show that $\Gamma_1 \in \mathrm{Hom}\ (A, J)$. As a result of the choice of $f$ we have

$$\Gamma_1\lambda' = h \in J, \tag{8}$$

$$\Gamma_1\theta_1 = h_1 = e, \tag{9}$$

and

$$\Gamma_1\theta_j = h_j \in K_{j,j+1} \subseteq C_1 \qquad \text{for all } j \geqq 2. \tag{10}$$

Furthermore

$$\Gamma_1\eta_1 = c_1^r\bar{h} \text{ if } n_1 \leqq 4n_2 \tag{11}$$

and

$$\Gamma_1\lambda_1 = e \text{ if } n_1 \geqq 8n_2. \tag{12}$$

We note also that (i), (ii), (iii), and (iv) hold for $\Gamma_1$ since they hold for both $\Gamma$ and $\Gamma_f$.

Let $\tau' \in A'$. Applying Lemma 7 to the case $Q_2 = G'$, $Q_1 = G^{(2)}$, $\bar{\lambda} = \lambda'$ we obtain

$$(\Gamma_1\tau')^2 = (\Gamma_1\lambda')(\tau'\Gamma_1\lambda')^{-1} = h(\tau'h)^{-1} = e. \tag{13}$$

Now $\Gamma_1\tau' \in J^{(2)} \times G' = J \times G'$ by Lemmas 6 and 5. Combining this with (13) we see that $\Gamma_1\tau' \in J$ for all $\tau' \in A'$.

Since $A = A' \times A^{(2)}$ and since the automorphisms $\lambda_i$, $\xi_i$, $\theta_i$, $\eta_i$ generate $A^{(2)}$, it is sufficient to show that $\Gamma_1\lambda_i$, $\Gamma_1\xi_i$, $\Gamma_1\theta_j$, and $\Gamma_1\eta_j$ are elements of $J$ for $1 \leqq i \leqq k$, $1 \leqq j < k$.

Now let $u$ be an odd integer and let $\tau_i$ be the automorphism of $C_i$ such that $\tau_i c_i = c_i^u$. Since $h_i^2 = e$ and $\theta_i h_i = h_i$ we have $\Gamma_1(\theta_i^u) = (\Gamma_1\theta_i)^u = h_i^u = h_i$. It follows that $\tau_{i+1}\Gamma_1(\theta_i^u) = \Gamma_1\theta_i$. Hence if we apply $\Gamma_1$ to both sides of the identity $\theta_i\tau_{i+1} = \tau_{i+1}\theta_i^u$, we obtain $\theta_i\Gamma_1\tau_{i+1} = \Gamma_1\tau_{i+1}$. Now $\Gamma_1\tau_{i+1} \in K_{i+1} \times C_{i+1}$, $K_{i+1} \subseteq C_1$, and $e$ is the only element of $C_{i+1}$ left fixed by $\theta_i$. Therefore $\Gamma_1\tau_{i+1} \in K_{i+1}$. In particular

$$\Gamma_1\lambda_j \in K_j \quad \text{and} \quad \Gamma_1\xi_j \in K_j \qquad \text{for all } j \geqq 2. \tag{14}$$

We have $\Gamma_1\theta_1 = \Gamma_1(\theta_1^5) = e$. Therefore if we apply $\Gamma_1$ to both sides of $\theta_1^5\xi_1 = \xi_1\theta_1$, we obtain

$$\theta_1^5\Gamma_1\xi_1 = \Gamma_1\xi_1.$$

Since $\Gamma_1\xi_1 \in C_1 \times K_1 \subseteq C_1 \times C_2$ this implies that

$$\Gamma_1\xi_1 \in C_1. \tag{15}$$

Now we study $\Gamma_1\eta_i$. By Lemma 6 we have

$$\Gamma_1\eta_i \in C_i \times C_{i+1} \times K_{i,i+1}.$$

Applying $\Gamma_1$ to both sides of $\eta_{i+1}\theta_i = \theta_i\eta_{i+1}$ and noting that $\eta_{i+1}\Gamma_1\theta_i = \Gamma_1\theta_i$, we obtain $\Gamma_1\eta_{i+1} = \theta_i\Gamma_1\eta_{i+1}$. It follows that

$$\Gamma_1\eta_j \in C_{j+1} \times K_{j,j+1} \subseteq C_1 \times C_{j+1} \qquad \text{for all } j \geqq 2. \tag{16}$$

Now put $\psi_{i+1} = (\theta_{i+1}\lambda_{i+1}\theta_i)^2$. By (9), (10) and (14), $\Gamma_1(\theta_{i+1}\lambda_{i+1}\theta_i)$ is an element of $C_1$ of order at most 2. Hence $\Gamma_1\psi_{i+1} = e$. Now

$$\psi_{i+1}c_j = \begin{cases} c_j & \text{if } j \neq i+2, \\ c_i^{r_i r_{i+1}} c_{i+2} & \text{if } j = i+2. \end{cases}$$

It follows that $\psi_{i+1}g=g$ if and only if $g\in N_{i+2}$. Furthermore $g^{-1}\psi_{i+1}g\in C_i$ for all $g\in G$. Now

$$\psi_{i+1}\eta_{i+1} = \eta_{i+1}\theta_i^{r_{i+1}}\psi_{i+1}.$$

We apply $\Gamma_1$ to both sides and get

$$\psi_{i+1}\Gamma_1\eta_{i+1} = (\Gamma_1\eta_{i+1})\eta_{i+1}\Gamma_1(\theta_i^{r_{i+1}}) = (\Gamma_1\eta_{i+1})h_i^{r_{i+1}}.$$

Hence $h_i^{r_{i+1}}$ is of the form $g^{-1}\psi_{i+1}g$. Therefore $h_i^{r_{i+1}}\in C_i$. Since $h_1=e$ and $h_j\in C_1$ for $j\geqq 2$, we have $h_i^{r_{i+1}}=e$ for all $i$. Therefore $\Gamma_1\eta_{i+1}\in N_{i+2}$. Combining this with (16) we have

$$\Gamma_1\eta_j \in K_{j,j+1} \subseteq C_1 \qquad \text{for all } j \geqq 2.$$

By Lemma 5 we have $K_{j,j+1}=J$ if $j\geqq 3$. Furthermore $\Gamma_1\eta_2\in J\times C_2\times C_3$ by (iii). Therefore

$$\Gamma_1\eta_j \in J \qquad \text{for all } j \geqq 2. \tag{17}$$

If we apply $\Gamma_1$ to both sides of the identities $\lambda_2=\eta_1\lambda_2\eta_1$ and $\theta_2\eta_1=\eta_1\theta_2$ we obtain

$$(\Gamma_1\lambda_2)(\eta_1\Gamma_1\lambda_2)^{-1} = (\Gamma_1\eta_1)(\eta_1\lambda_2\Gamma_1\eta_1) \tag{18}$$

and

$$(\Gamma_1\theta_2)(\eta_1\Gamma_1\theta_2)^{-1} = (\Gamma_1\eta_1)(\theta_2\Gamma_1\eta_1)^{-1}. \tag{19}$$

Next we will establish:

$$\Gamma_1\lambda_2 \in J, \qquad \Gamma_1\theta_2 \in J \tag{20}$$

and

$$\Gamma_1\eta_1 \in J \times C_2. \tag{21}$$

There are two cases to be considered.

(I) $n_1>n_2$. Here $K_{2,3}=K_2=J$ by Lemma 5. Hence (20) follows from (14) and (10). We have $\Gamma_1\eta_1=c_1^r c_2^{s''}\bar{h}$, where $r$ and $s''$ are integers and $\bar{h}\in K_{1,2}\subseteq C_3$, $\bar{h}^2=e$. It follows from (20) that the left hand sides of both (18) and (19) are equal to $e$. Therefore

$$e = (\Gamma_1\eta_1)(\eta_1\lambda_2\Gamma_1\eta_1) = c_1^{2r}c_2^{r}$$

and

$$e = (\Gamma_1\eta_1)(\theta_2\Gamma_1\eta_1)^{-1} = \bar{h}(\theta_2\bar{h})^{-1}.$$

Therefore $c_1^{2r}=\bar{h}=e$ which implies (21).

(II) $n_1=n_2$. In this case let $\zeta$ be the automorphism of $C_1\times C_2$ such that $\zeta c_1=c_2$, $\zeta c_2=c_1$. We have $\zeta^2=\epsilon$ and $\eta_1=\zeta\theta_1\zeta$. Applying $\Gamma_1$ to these two equalities we obtain $\Gamma_1\zeta=\zeta(\Gamma_1\zeta)^{-1}$ and

$$\Gamma_1\eta_1 = (\Gamma_1\zeta)(\zeta\Gamma_1\theta_1)(\zeta\theta_1\Gamma_1\zeta) = \zeta\{(\Gamma_1\zeta)^{-1}(\theta_1\Gamma_1\zeta)\},$$

since $\Gamma_1\theta_1 = e$ by (9). Now $g^{-1}\theta_1 g \in C_1$ and hence $\zeta(g^{-1}\theta_1 g) \in C_2$ for all $g \in G$. Therefore $\Gamma_1\eta_1 \in C_2$ and (21) is established. It follows from (21) that the right hand sides of both (18) and (19) are equal to $e$. Hence $\Gamma_1\lambda_2 = \eta_1\Gamma_1\lambda_2$ and $\Gamma_1\theta_2 = \eta_1\Gamma_1\theta_2$. Since we already have $\Gamma_1\lambda_2 \in C_1$ by (14) and $\Gamma_1\theta_2 \in C_1$ by (10) these last two equalities imply (20).

We have established that (20) and (21) hold in all cases.

We will next establish:

(22) $$\Gamma_1\lambda_1 \in J,$$

(23) $$\text{either } n_1 = n_2 \text{ or } \Gamma_1\xi_1 \in J,$$

and

(24) $$\Gamma_1\eta_1 \in J.$$

If $r_1 \geqq 8$ then (22) follows from (12). If $r_1 \leqq 4$ then (24) follows from (11) and (21). We will now show that (22), (23) and (24) are equivalent. Then it will follow that all three hold in all cases.

Suppose (22) holds. We apply Lemma 7 with $Q_2 = C_1$, $Q_1 = N_1$, and $\bar{\lambda} = \lambda_1$. Then (5) yields $(\Gamma_1\xi_1)^2 = e$. Combining this with (15) we see that $\Gamma_1\xi_1 \in J$ if $n_1 > n_2$. Thus (22) implies (23).

Next suppose (23) holds and that $r_1 \geqq 8$. We specialize $\tau_i$ to be the automorphism of $C_i$ such that $\tau_i c_i = c_i^{1+r_1}$. Since $8 \mid r_1$ it follows that $\tau_i$ is an even power of $\xi_i$. Furthermore, since $n_1 > n_2$, it follows from (14) and (23) that $\Gamma_1\xi_i \in J$ for all $i$. Therefore $\Gamma_1\tau_i = e$ for all $i$. Now

$$(\eta_1\lambda_2\tau_2\theta_1)^2 = \tau_1\tau_2.$$

We apply $\Gamma_1$ to both sides of this identity, noting that $\Gamma_1\lambda_2 \in K_2 = J$, $\Gamma_1\theta_1 = \Gamma_1\tau_1 = \Gamma_1\tau_2 = e$, and $\Gamma_1\eta_1 = c_1^r c_2^{s''}$, where $c_1^r \in J$ by (21). This gives us

$$e = (\Gamma_1\eta_1)(\eta_1\lambda_2\tau_2\theta_1\Gamma_1\eta_1) = c_1^{r_1 s''}.$$

Therefore $n_1 \mid r_1 s''$, $n_2 \mid s''$, $c_2^{s''} = e$, and $\Gamma_1\eta_1 = c_1^r \in J$. Thus (23) implies (24).

Suppose (24) holds. Then applying $\Gamma_1$ to $(\lambda_1\eta_1)^2 = \epsilon$, we obtain

$$e = (\Gamma_1\lambda_1)(\lambda_1\eta_1\Gamma_1\lambda_1) = c_2^{t'},$$

where $\Gamma_1\lambda_1 = c_1^t$. If $r_1 \leqq 2$, then $c_2^t = e$ implies $c_1^t \in J$. If $r_1 = 4$ then $\Gamma_1(\lambda_1\eta_1) \in C \times C_3$ by (iv), and, since $\lambda_1\Gamma_1\eta_1 \in J \subseteq C$, we have $\Gamma_1\lambda_1 \in (C \times C_3) \cap C_1 = J$. We already know that (22) holds if $r_1 \geqq 8$. Therefore (24) implies (22).

It follows that (22), (23), and (24) hold in all cases.

Combining (17) and (24) we have

$$\Gamma_1\eta_j \in J, \qquad 1 \leqq j < k.$$

From (9), (10), and (20) we obtain

$$\Gamma_1\theta_j \in J, \qquad 1 \leqq j < k.$$

From (14), (20), and (22) we obtain

$$\Gamma_1\lambda_i \in J, \qquad 1 \leqq i \leqq k,$$

and

$$\Gamma_1\xi_i \in J, \qquad 3 \leqq i \leqq k.$$

Furthermore (14) and (23) imply: If $n_1 > n_2$, then $\Gamma_1\xi_1 \in J$ and $\Gamma_1\xi_2 \in J$. To complete the proof of Theorem 1 we need only show that $\Gamma_1\xi_1 \in J$ and $\Gamma_1\xi_2 \in J$ for the case $n_1 = n_2$.

Suppose $n_1 = n_2$. In this case $J$ consists of $e$ alone. As above let $\zeta$ be the automorphism of $C_1 \times C_2$ such that $\zeta c_1 = c_2$ and $\zeta c_2 = c_1$. Since $\zeta = \lambda_1\eta_1\theta_1^{-1}\eta_1$ it follows that $\Gamma_1\zeta = e$. Hence, if we apply $\Gamma_1$ to both sides of the identity $\xi_2 = \zeta\xi_1\zeta$ we obtain $\Gamma_1\xi_2 = \zeta\Gamma_1\xi_1$. Now, by (14) and (15), $\Gamma_1\xi_2 \in C_1$ and $\zeta\Gamma_1\xi_1 \in C_2$. Hence $\Gamma_1\xi_1 = \Gamma_1\xi_2 = e \in J$ and the proof of Theorem 1 is complete.

Let $Z_i$ be the set of all cocycles that satisfy condition (i) of Theorem 1. Clearly $Z_i$ is a subgroup of $Z^1(A, G)$ and we put $m_i = [Z^1(A, G) : Z_i]$, the index of $Z_i$ in $Z^1(A, G)$.

LEMMA i. $m_i \leqq 2$. *If* $m_i = 2$, *then either* $n_1 > n_2 > n_3$ *or* $n_1 = n_2 \geqq 4n_3$.

**Proof.** The inequality $m_i \leqq 2$ follows at once from Lemma 6. Suppose $m_i = 2$ and let $\Gamma \in Z^1(A, G)$, $\Gamma \notin Z_i$. Then $\Gamma\lambda_1 \notin C_1$. From Lemma 6 we have $\Gamma\lambda_1 \in C_1 \times K_1$. Hence $K_1$ is not trivial and Lemma 5 yields $n_2 > n_3$. Thus $n_1 \geqq n_2 \geqq 2n_3$. If $n_1 > 2n_3$ then either $n_1 > n_2 > n_3$ or $n_1 = n_2 \geqq 4n_3$. Thus we need only eliminate the case $n_1 = 2n_3$.

Suppose $n_1 = 2n_3$. Then $\lambda_1\lambda_3 = \phi^2$, where $\phi$ is the automorphism of $C_1 \times C_3$ such that $\phi c_1 = c_1c_3$ and $\phi c_3 = c_1^{-2}c_3^{-1}$. It follows from Lemma 6 that

$$(\Gamma\lambda_1)(\lambda_1\Gamma\lambda_3) = \Gamma(\lambda_1\lambda_3) = \Gamma(\phi^2) \in C_1 \times C_3.$$

Now $\Gamma\lambda_3 \in K_3 \times C_3 \subseteq C_1 \times C_3$. Hence $\lambda_1\Gamma\lambda_3 \in C_1 \times C_3$ and we have $\Gamma\lambda_1 \in C_1 \times C_3$. Now $\Gamma\lambda_1 \in C_1 \times K_1 \subseteq C_1 \times C_2$ by Lemmas 6 and 5. Therefore $\Gamma\lambda_1 \in C_1$, a contradiction. This contradiction establishes Lemma i.

Let $Z_{ii}$ be the group of all cocycles $\Gamma$ satisfying the conditions (i) and (ii) of Theorem 1. Put $m_{ii} = [Z_i : Z_{ii}]$.

LEMMA ii. $m_{ii} \leqq 2$. *If* $m_{ii} = 2$ *then* $n_3 > n_4$.

**Proof.** By Lemma 6 the set of all cocycles that satisfy (ii) form a subgroup $Z''$ of $Z^1(A, G)$ of index at most two. We have $Z_{ii} = Z_i \cap Z''$ and hence

$$m_{ii} = [Z_i : Z_i \cap Z''] = [Z_iZ'' : Z''] \leqq [Z^1(A, G) : Z''] \leqq 2.$$

If $n_3 = n_4$, then (ii) is satisfied by all $\Gamma \in Z^1(A, G)$ by Lemmas 6 and 5. Hence if $m_{ii} = 2$ then $n_3 > n_4$.

Let $Z_{iii}$ be the group of all cocycles $\Gamma$ satisfying conditions (i), (ii), and (iii) of Theorem 1. Put $m_{iii}=[Z_{ii}:Z_{iii}]$.

LEMMA iii. $m_{iii}\leqq 2$. *If* $m_{iii}=2$ *then* $n_1=n_2>n_3>n_4$.

**Proof.** By Lemma 6, $\Gamma\eta_2\in C_2\times C_3\times K_{2,3}$ for all $\Gamma\in Z^1(A, G)$. If $n_1>n_2$, then $K_{2,3}=J$, (iii) holds for all $\Gamma\in Z^1(A, G)$, and $m_{iii}=1$. Thus without loss of generality we suppose $n_1=n_2$. Then $J$ is trivial. It follows from Lemma 6 that the set of all cocycles that satisfy (iii) form a subgroup $Z'''$ of index at most two in $Z^1(A, G)$. We have

$$m_{iii} = [Z_{ii}:Z_{ii}\cap Z'''] = [Z_{ii}Z''':Z'''] \leqq [Z^1(A, G):Z'''] \leqq 2.$$

Now suppose $n_3=n_4$. Then $\eta_2=\phi^2$ where $\phi$ is the automorphism of $C_2\times C_3\times C_4$ such that $\phi c_2=c_2c_4$, $\phi c_3=c_3$, $\phi c_4=c_3c_4^{-1}$. It now follows from Lemma 6 that (iii) is satisfied by all $\Gamma\in Z^1(A, G)$, and $m_{iii}=1$. Thus $n_3=n_4$ implies $m_{iii}=1$.

Suppose $n_1=n_2=n_3$. Let $\Gamma\in Z_{ii}$ and let $\zeta$ be the automorphism of $C_1\times C_3$ such that $\zeta c_1=c_3$ and $\zeta c_3=c_1$. Then $\zeta^2=\epsilon$ and $\eta_2=\zeta\theta_1\zeta$. Applying $\Gamma$ to these two equalities we obtain $\Gamma\zeta=(\zeta\Gamma\zeta)^{-1}$ and

$$\Gamma\eta_2 = (\Gamma\zeta)(\zeta\Gamma\theta_1)(\zeta\theta_1\Gamma\zeta) = \zeta\{(\Gamma\theta_1)(\Gamma\zeta)^{-1}(\theta_1\Gamma\zeta)\}.$$

Now $\Gamma\theta_1\in C_1\times C_2$ by (ii). Furthermore $g^{-1}\theta_1 g\in C_1$ for all $g\in G$. Therefore

$$(\Gamma\theta_1)(\Gamma\zeta)^{-1}(\theta_1\Gamma\zeta) \in C_1\times C_2$$

and $\Gamma\eta_2\in C_2\times C_3$. Thus $m_{iii}=1$ if $n_1=n_2=n_3$.

It follows that if $m_{iii}>1$ then $n_1=n_2>n_3>n_4$, and Lemma iii is established.

Now put $m_{iv}=[Z_{iii}:\mathrm{Hom}\ (A, J)B^1(A, G)]$.

LEMMA iv. $m_{iv}\leqq 2$. *If* $m_{iv}=2$ *then* $n_1=4n_2$.

**Proof.** If $n_1\neq 4n_2$, then $m_{iv}=1$ by Theorem 1, and Lemma iv holds. Suppose $n_1=4n_2$ and let $\Gamma\in Z_{iii}$. By Theorem 1, $\Gamma\in\mathrm{Hom}\ (A, J)B^1(A, G)$ if and only if $\Gamma(\lambda_1\eta_1)\in C\times C_3$. Since $\Gamma(\lambda_1\eta_1)\in C_1\times C_2\times K_{1,2}$ we have $\Gamma(\lambda_1\eta_1)=c_1^r(c_1^2c_2^{-1})^s\bar{h}$, where $r$ and $s$ are integers and $\bar{h}$ is an element of $C_3$ such that $\bar{h}^2=e$. Now $(\lambda_1\eta_1)^2=\epsilon$. Hence

$$e = \Gamma(\lambda_1\eta_1)\lambda_1\eta_1\Gamma(\lambda_1\eta_1) = c_2^r,$$

and we have $n_2\mid r$. Now in the case under discussion $C\cap C_1=J$ and $J$ is the cyclic group generated by $c_1^{2n_2}$. Let $D$ be the group generated by $c_1^{n_2}$ and $c_1^2c_2^{-1}$. Then $\Gamma\to c_1^rC$ is a homomorphism of $Z_{iii}$ into $D/C$ with kernel $\mathrm{Hom}\ (A, J)B^1(A, G)$. Hence $m_{iv}\leqq[D:C]=2$, which establishes Lemma iv.

Clearly $[Z^1(A, G):\mathrm{Hom}\ (A, J)B^1(A, G)]=m_im_{ii}m_{iii}m_{iv}$. It follows from Lemmas iii and iv that $m_{iii}$ and $m_{iv}$ cannot both be two. Therefore

$$[Z^1(A, G):\mathrm{Hom}\ (A, J)B^1(A, G)] \leqq 8.$$

It will follow from the results of §4 that this index can actually assume any of the four possible values 1, 2, 4, 8.

4. **Special cocycles.** The four lemmas of §3 give us necessary conditions for $m_v=2$, $v=$i, ii, iii, or iv. In this section we will show, by actual construction of suitable cocycles, that these conditions are also sufficient. This will provide us with a set of generators of the factor group

$$Z^1(A, G)/\text{Hom}\ (A, J)B^1(A, G).$$

Let $\overline{G}$ be a characteristic subgroup of $G$, and let $\overline{A}$ be the group of automorphisms of $\overline{G}$. For any $\sigma\in A$ we let $\bar{\sigma}$ denote the restriction of $\sigma$ to $\overline{G}$. Since $\overline{G}$ is a characteristic subgroup of $G$ it follows that $\bar{\sigma}\in\overline{A}$. In particular $\bar{\epsilon}$ is the identity of $\overline{A}$. If $\overline{\Gamma}\in Z^1(\overline{A}, \overline{G})$, then there is a corresponding element $\Gamma\in Z^1(A, G)$ such that

$$\Gamma\sigma = \overline{\Gamma}\bar{\sigma} \qquad \text{for all } \sigma \in A. \tag{25}$$

Let $\alpha_1, \alpha_2, \cdots, \alpha_m$ be a set of generators of $\overline{A}$ and let $\tilde{\Gamma}$ be a mapping of this set of generators into $\overline{G}$. We will say that $\tilde{\Gamma}$ satisfies the relation(2)

$$\alpha_{l_1}\alpha_{l_2}\cdots\alpha_{l_r} = \bar{\epsilon}$$

if

$$(\tilde{\Gamma}\alpha_{l_1})(\alpha_{l_1}\tilde{\Gamma}\alpha_{l_2})\cdots(\alpha_{l_1}\alpha_{l_2}\cdots\alpha_{l_{r-1}}\tilde{\Gamma}\alpha_{l_r}) = e.$$

Let

$$\begin{cases} \alpha_{l_1}\cdots\alpha_{l_r} = \bar{\epsilon}, \\ \qquad\vdots \\ \alpha_{q_1}\cdots\alpha_{q_u} = \bar{\epsilon} \end{cases} \tag{26}$$

be a set of relations between $\alpha_1, \cdots, \alpha_m$ that is complete in the sense that any other relation can be deduced from it. The following lemma is due to Anne P. Cobbe [1, pp. 43–45].

LEMMA 9. *If $\tilde{\Gamma}$ satisfies each of the relations* (26), *then $\tilde{\Gamma}$ can be extended to an element $\overline{\Gamma}\in Z^1(\overline{A}, \overline{G})$. The extension $\overline{\Gamma}$ is uniquely determined by $\tilde{\Gamma}$.*

Throughout the remainder of the paper we will use the following additional notation:

$$a_i = c_i^{n_i/4}$$

for those $i$ for which $n_i\geqq 4$, and

$$b_j = c_j^{n_j/2}, \qquad 1 \leqq j \leqq k.$$

We are now in a position to proceed to the construction of special cocycles.

(2) For our present purposes it is sufficient to consider only relations in which no negative powers of the $\alpha_i$ occur.

(i) By Lemma i, if $m_i=2$, then either $n_1>n_2>n_3$ or $n_1=n_2\geqq 4n_3$.

(i′) Suppose $n_1>n_2>n_3$. Here we take $\overline{G}$ to be the characteristic subgroup of $G$ generated by $a_1$ and $b_2$. Then $\overline{G}$ is the direct product of a cyclic group of order 4 and one of order 2. Hence $\overline{A}$ is the octic group. Let $\alpha$ and $\beta$ be the automorphisms of $\overline{G}$ defined by

$$\alpha a_1 = a_1 b_2, \qquad \alpha b_2 = a_1^2 b_2,$$
$$\beta a_1 = a_1^3 b_2, \qquad \beta b_2 = b_2.$$

Then $\alpha^2=\bar{\lambda}_1$ and $\alpha\beta=\bar{\theta}_1$, the restrictions of $\lambda_1$ and $\theta_1$ respectively to $\overline{G}$. Furthermore $\alpha$ and $\beta$ generate $\overline{A}$ and a complete set of relations is

$$\alpha^4 = \beta^2 = (\alpha\beta)^2 = \bar{\epsilon}. \tag{27}$$

The mapping $\tilde{\Gamma}'$ of the set $\{\alpha, \beta\}$ into $\overline{G}$ given by

$$\tilde{\Gamma}'\alpha = a_1 b_2, \qquad \tilde{\Gamma}'\beta = e$$

satisfies (27). Hence, by Lemma 9, $\tilde{\Gamma}'$ can be extended to an element $\overline{\Gamma}'$ of $Z^1(\overline{A}, \overline{G})$. This in turn corresponds to an element $\Gamma'\in Z^1(A, G)$ by the correspondence (25). Now

$$\Gamma'\lambda_1 = \overline{\Gamma}'(\alpha^2) = (\tilde{\Gamma}'\alpha)(\alpha\tilde{\Gamma}'\alpha) = b_2 \notin C_1.$$

Thus $\Gamma'\notin Z_i$.

(i″). Suppose $n_1=n_2\geqq 4n_3$. Here we take $\overline{G}$ to be the characteristic subgroup of $G$ generated by $a_1$ and $a_2$. In this case $\overline{G}$ is the direct product of two cyclic groups of order four. Hence $\overline{A}$ has order 96. Let $\gamma$ and $\delta$ be the automorphisms of $\overline{G}$ such that

$$\gamma a_1 = a_1^2 a_2, \qquad \gamma a_2 = a_1 a_2^2,$$
$$\delta a_1 = a_2^3, \quad \text{and} \quad \delta a_2 = a_1 a_2.$$

Then $\gamma$ has order 2, $\delta$ has order 6, and $\gamma\delta^2$ has order 4. The symmetric group of order 24 is characterized, as an abstract group, by the property that it is generated by an element of order 2 and an element of order 3 whose product has order 4. Hence $\gamma$ and $\delta^2$ generate a group $\overline{A}_{24}$ of order 24 isomorphic to the symmetric group. Now $(\gamma\delta^3)^2=\bar{\epsilon}$. It follows that $\delta^3$ commutes with every element of $\overline{A}_{24}$. Therefore $\delta^3\notin\overline{A}_{24}$. It follows that $\gamma$ and $\delta$ generate a group $\overline{A}_{48}$ of order 48 and that a complete set of relations (3) for this group is

$$\gamma^2 = \delta^6 = (\gamma\delta^2)^4 = (\gamma\delta^3)^2 = \bar{\epsilon}. \tag{28}$$

Now

$$(\bar{\lambda}_1\gamma)^2\delta^3 = \bar{\epsilon}. \tag{29}$$

(3) The group $\overline{A}_{48}$ is isomorphic to the direct product of the symmetric group of order 24 and the group of order 2. The set of relations (28) for this group is due to G. A. Miller [5].

It follows that $(\bar{\lambda}_1\gamma)^2 \notin \overline{A}_{24}$, and hence $\bar{\lambda}_1 \notin \overline{A}_{48}$. Therefore $\gamma$, $\delta$, and $\bar{\lambda}_1$ generate $\overline{A}$. A complete (though redundant) set of relations for $\overline{A}$, with respect to this set of generators, is (28), (29), and

$$\bar{\lambda}_1^2 = \bar{\lambda}_1\delta\bar{\lambda}_1\gamma\delta\gamma = \bar{\epsilon}.$$

This set of relations is satisfied by the mapping $\bar{\Gamma}''$ of $\{\gamma, \delta, \bar{\lambda}_1\}$ into $\overline{G}$ given by

$$\bar{\Gamma}''\gamma = \bar{\Gamma}''\bar{\lambda}_1 = a_1^2a_2^2, \qquad \bar{\Gamma}''\delta = e.$$

By Lemma 9, $\bar{\Gamma}''$ can be extended to an element $\overline{\Gamma}'' \in Z^1(\overline{A}, \overline{G})$, and $\overline{\Gamma}''$ in turn corresponds to a cocycle $\Gamma'' \in Z^1(A, G)$. Clearly

$$\Gamma''\lambda_1 = \bar{\Gamma}''\bar{\lambda}_1 = a_1^2a_2^2 \notin C_1.$$

Hence $\Gamma'' \notin Z_i$.

Combining Lemma i with the existence of $\Gamma'$ and $\Gamma''$ we see that

$$m_i = \begin{cases} 2 \text{ if } n_1 > n_2 > n_3, \\ 2 \text{ if } n_1 = n_2 \geqq 4n_3, \\ 1 \text{ otherwise.} \end{cases}$$

Put

$$\Gamma_i = \begin{cases} \Gamma' & \text{if } n_1 > n_2 > n_3, \\ \Gamma'' & \text{if } n_1 = n_2 \geqq 4n_3. \end{cases}$$

Then $\Gamma_i$ is an element of $Z^1(A, G)$, defined whenever $m_i = 2$, such that $\Gamma_i \notin Z_i$.

(ii) By Lemma ii, if $m_{ii} = 2$, then $n_3 > n_4$. Suppose $n_3 > n_4$. We now take $\overline{G}$ to be the characteristic subgroup of $G$ generated by $b_1$, $b_2$, and $b_3$. This $\overline{G}$ is the direct product of three groups of order two, and the corresponding $\overline{A}$ has order 168. Let $\phi$ and $\rho$ be the automorphisms of $\overline{G}$ such that

$$\phi b_1 = b_1b_3, \qquad \phi b_2 = b_3, \qquad \phi b_3 = b_1b_2b_3,$$
$$\rho b_1 = b_1b_2, \qquad \rho b_2 = b_2b_3, \qquad \rho b_3 = b_2.$$

We note that $\phi\rho = \bar{\theta}_1$, the restriction of $\theta_1$ to $\overline{G}$. Furthermore $\rho\phi^5 b_1 = b_3$, $\rho\phi^5 b_2 = b_1b_2$, and $\rho\phi^5 b_3 = b_1$. Hence

$$\phi^7 = \rho^3 = (\phi\rho)^2 = (\rho\phi^5)^4 = \bar{\epsilon}. \tag{30}$$

It is known(4) that (30) and $\phi \neq \bar{\epsilon}$ are sufficient to insure that $\phi$ and $\rho$ generate the simple group of order 168. Therefore $\phi$ and $\rho$ are a set of gener-

(4) This set of generators and relations for the simple group of order 168 is due to Dyck [2, p. 41] and confirmed by Miller [5].

ators for $\overline{A}$ and (30) is a corresponding complete set of relations. Let $\tilde{\Gamma}_{ii}$ be the mapping of $\{\phi, \rho\}$ into $\overline{G}$ given by

$$\tilde{\Gamma}_{ii}\phi = e, \qquad \tilde{\Gamma}_{ii}\rho = b_2.$$

It can be readily verified that $\tilde{\Gamma}_{ii}$ satisfies (30). Hence $\tilde{\Gamma}_{ii}$ can be extended to an element $\overline{\Gamma}_{ii} \in Z^1(\overline{A}, \overline{G})$. By the correspondence (25), $\overline{\Gamma}_{ii}$ corresponds to a cocycle $\Gamma_{ii} \in Z^1(A, G)$. Now $\tilde{\lambda}_1 = \tilde{\epsilon}$. Hence $\Gamma_{ii}\lambda_1 = e$. Furthermore

$$\Gamma_{ii}\theta_1 = \overline{\Gamma}_{ii}(\phi\rho) = \phi\tilde{\Gamma}_{ii}\rho = b_3 \notin C_1 \times C_2.$$

Thus we have constructed a cocycle $\Gamma_{ii}$, defined whenever $n_3 > n_4$, such that

$$\Gamma_{ii} \in Z_i, \qquad \Gamma_{ii} \notin Z_{ii}.$$

Combining the existence of $\Gamma_{ii}$ with Lemma ii we obtain

$$m_{ii} = \begin{cases} 2 & \text{if } n_3 > n_4, \\ 1 & \text{if } n_3 = n_4. \end{cases}$$

(iii) By Lemma iii, if $m_{iii} = 2$, then $n_1 = n_2 > n_3 > n_4$. Suppose $n_1 = n_2 > n_3 > n_4$. In this case again we take $\overline{G}$ to be the group generated by $b_1$, $b_2$, and $b_3$. Let $\overline{\Gamma}_{ii}$ be the element of $Z^1(\overline{A}, \overline{G})$ defined above. Let $\pi$ be the projection of $G$ onto $C_1 \times C_2$ such that

$$\pi g = \begin{cases} g & \text{if } g \in C_1 \times C_2, \\ e & \text{if } g \in N_{1,2}. \end{cases}$$

Let $\chi$ be the homomorphism of $G$ onto $\overline{G}$ such that

$$\chi c_i = \begin{cases} b_i & \text{if } i \leqq 3, \\ e & \text{if } i > 3, \end{cases}$$

and $\chi g' = e$ if $g' \in G'$. The kernel of $\chi$ is generated by $G'$ and the elements $c_i^2$, $c_j$, $1 \leqq i \leqq 3$, $j > 3$. Since $n_3 > n_4$ it follows that the kernel of $\chi$ is a characteristic subgroup of $G$. Therefore if $\sigma \in A$, then

$$\tilde{\sigma}\chi g = \chi\sigma g$$

gives a single valued mapping $\tilde{\sigma}$ of $\overline{G}$ onto itself. Now $\tilde{\sigma} \in \overline{A}$, $\sigma \to \tilde{\sigma}$ is a homomorphism of $A$ into $\overline{A}$, and we put

$$\Gamma_{iii}\sigma = \pi\overline{\Gamma}_{ii}\tilde{\sigma}. \tag{31}$$

We must now show that $\Gamma_{iii}$ is a cocycle. Since $n_1 = n_2 > n_3$ it follows that $\pi\chi g = g^{n_1/2}$ for all $g \in G^{(2)}$. Hence for any $g \in G^{(2)}$ we have

$$\sigma\pi\chi g = (\sigma g)^{n_1/2} = \pi\chi\sigma g = \pi\tilde{\sigma}\chi g.$$

Therefore $\sigma\pi\bar{g} = \pi\tilde{\sigma}\bar{g}$ for all $\bar{g} \in \overline{G}$. Now let $\sigma$ and $\tau$ be arbitrary elements of $A$. Since $\overline{\Gamma}_{ii}\tilde{\tau} \in \overline{G}$, we have $\sigma\pi\overline{\Gamma}_{ii}\tilde{\tau} = \pi\tilde{\sigma}\overline{\Gamma}_{ii}\tilde{\tau}$. Hence

$$\begin{aligned}(\Gamma_{iii}\sigma)(\sigma\Gamma_{iii}\tau) &= (\pi\overline{\Gamma}_{ii}\tilde{\sigma})(\sigma\pi\overline{\Gamma}_{ii}\tilde{\tau}) \\ &= (\pi\overline{\Gamma}_{ii}\tilde{\sigma})(\pi\tilde{\sigma}\overline{\Gamma}_{ii}\tilde{\tau}) \\ &= \pi\{(\overline{\Gamma}_{ii}\tilde{\sigma})(\tilde{\sigma}\overline{\Gamma}_{ii}\tilde{\tau})\} \\ &= \pi\overline{\Gamma}_{ii}(\tilde{\sigma}\tilde{\tau}) \\ &= \Gamma_{iii}(\sigma\tau).\end{aligned}$$

Thus $\Gamma_{iii}\in Z^1(A, G)$. We note that if

$$\sigma c_j = \prod_{i=1}^{k} c_i^{q_{ij}}, \qquad 1 \leqq j \leqq k,$$

then $\Gamma_{iii}\sigma$ depends only on the residue classes of the $q_{ij}$ modulo 2, since these residue classes determine $\tilde{\sigma}$ completely. Hence $\Gamma_{iii}\lambda_1 = e$. Furthermore $\Gamma_{iii}\sigma \in C_1\times C_2$ for all $\sigma\in A$. In particular $\Gamma_{iii}\theta_1\in C_1\times C_2$. Finally $\tilde{\eta}_2 = \phi^2\rho\phi^6\rho\phi^5$, $\overline{\Gamma}_{ii}\tilde{\eta}_2 = b_1b_3$, and hence

$$\Gamma_{iii}\eta_2 = b_1 \notin C_2 \times C_3 = J \times C_2 \times C_3.$$

Thus we have a cocycle $\Gamma_{iii}$, defined whenever $n_1 = n_2 > n_3 > n_4$, such that

$$\Gamma_{iii} \in Z_{ii}, \qquad \Gamma_{iii} \notin Z_{iii}.$$

It follows that

$$m_{iii} = \begin{cases} 2 \text{ if } n_1 = n_2 > n_3 > n_4, \\ 1 \text{ otherwise.} \end{cases}$$

(iv) Suppose $n_1 = 4n_2$. We now take $\overline{G}$ to be the characteristic subgroup of $G$ of order 4 generated by $a_1$. In this case $\overline{A}$ has order two and is generated by $\bar{\lambda}_1$. A complete set of relations is

$$\bar{\lambda}_1^2 = \bar{\epsilon}.$$

It follows from Lemma 9 that there is a cocycle $\overline{\Gamma}_{iv}\in Z^1(\overline{A}, \overline{G})$ such that $\overline{\Gamma}_{iv}\bar{\lambda}_1 = a_1$. By (25), $\overline{\Gamma}_{iv}$ corresponds to a cocycle $\Gamma_{iv}\in Z^1(A, G)$ such that

$$\Gamma_{iv}\sigma = \begin{cases} e \text{ if } \sigma a_1 = a_1, \\ a_1 \text{ if } \sigma a_1 = a_1^{-1}. \end{cases}$$

We have $\Gamma_{iv}\lambda_1 = a_1$, $\Gamma_{iv}\theta_1 = \Gamma_{iv}\eta_2 = e$, and $\Gamma_{iv}(\lambda_1\eta_1) = a_1 \notin C\times C_3$. Thus we have a cocycle $\Gamma_{iv}$, defined when $n_1 = 4n_2$, such that

$$\Gamma_{iv} \in Z_{iii}, \qquad \Gamma_{iv} \notin \text{Hom}\,(A, J)B^1(A, G).$$

It follows that

$$m_{iv} = \begin{cases} 2 \text{ if } n_1 = 4n_2, \\ 1 \text{ if } n_1 \neq 4n_2. \end{cases}$$

We have determined all $m_v$, $i \leqq v \leqq iv$, and constructed a cocycle $\Gamma_v$ for each $v$ such that $m_v = 2$. $Z^1(A, G)$ can be obtained from $\mathrm{Hom}(A, J)B^1(A, G)$ by adjoining these $\Gamma_v$; $H^1(A,G)$ can be obtained from $\mathrm{Hom}(A,J)B^1(A,G)/B^1(A,G)$ by adjoining the corresponding cosets $\Gamma_v B^1(A, G)$.

5. Hom $(A, J)$. Our next goal is the determination of the group Hom $(A, J)$. We will discuss the slightly more general problem of the determination of Hom $(A, T)$, where $T$ is an arbitrary group of order two.

We let $e$ denote the identity of $T$ as well as that of $G$. Let $h$ be the other element of $T$. We write

$$G = \prod_p G^{(p)},$$

where $p$ runs over all prime numbers dividing the order of $G$, and $G^{(p)}$ is the Sylow subgroup of $G$ whose order is a power of $p$. Now

$$A = \prod_p A^{(p)},$$

where $A^{(p)}$ is the group of automorphisms of $G^{(p)}$. Under suitable identification Hom $(A^{(p)}, T)$ can be regarded as a subgroup of Hom $(A, T)$ and we have

$$\mathrm{Hom}\,(A, T) = \prod_p \mathrm{Hom}\,(A^{(p)}, T).$$

Now let $p$ be a fixed prime dividing the order of $G$. We will use the notation of Lemma 1. By Lemma 1, $A^{(p)}$ is generated by the automorphisms $\gamma_j$, $\delta_j$, $1 \leqq j < l$, and the automorphisms of $D_i$, $1 \leqq i \leqq l$.

In the sequel $i$ and $j$ will always denote positive integers.

LEMMA 10. *Let* $\Gamma \in \mathrm{Hom}\,(A, T)$. *If* $p$ *is odd, or if* $m_{j+1} = m_{j+2}$, *or if* $j \geqq 2$ *and* $m_{j-1} = m_j$, *then* $\Gamma\gamma_j = \Gamma\delta_j = e$. *If* $m_j = m_{j+1}$ *then* $\Gamma\gamma_j = \Gamma\delta_j$.

**Proof.** Since $\Gamma \in \mathrm{Hom}\,(A, T)$ it follows that $\Gamma\sigma^2 = e$ for all $\sigma \in A$.

Suppose $p$ is odd. Then $\gamma_j$ and $\delta_j$ have odd order and hence they are squares. Thus in this case $\Gamma\gamma_j = \Gamma\delta_j = e$.

Next suppose $m_{j+1} = m_{j+2}$. Then $\gamma_j = \sigma_1^2$ and $\delta_j = \sigma_2^2$, where $\sigma_1$ and $\sigma_2$ are the automorphisms of $D_j \times D_{j+1} \times D_{j+2}$ such that

$$\begin{aligned} \sigma_1 d_j &= d_j d_{j+2}, & \sigma_1 d_{j+1} &= d_{j+1}, & \sigma_1 d_{j+2} &= d_{j+1} d_{j+2}^{-1}, \\ \sigma_2 d_j &= d_j, & \sigma_2 d_{j+1} &= d_{j+1} d_{j+2}, & \sigma_2 d_{j+2} &= d_j^{s_j} d_{j+2}^{-1}. \end{aligned}$$

Hence $\Gamma\gamma_j = \Gamma\delta_j = e$.

Now suppose $j \geqq 2$ and $m_{j-1} = m_j$. Then $\gamma_j = \sigma_3^2$ and $\delta_j = \sigma_4^2$, where $\sigma_3$ and $\sigma_4$ are the automorphisms of $D_{j-1} \times D_j \times D_{j+1}$ such that

$$\begin{aligned} \sigma_3 d_{j-1} &= d_{j-1}^{-1} d_{j+1}, & \sigma_3 d_j &= d_{j-1} d_j, & \sigma_3 d_{j+1} &= d_{j+1}, \\ \sigma_4 d_{j-1} &= d_{j-1}^{-1} d_j, & \sigma_4 d_j &= d_j, & \sigma_4 d_{j+1} &= d_{j-1}^{s_j} d_{j+1}. \end{aligned}$$

It follows that $\Gamma\gamma_j=\Gamma\delta_j=e$.

Finally suppose $m_j=m_{j+1}$. Then $s_j=1$ and $\gamma_j\delta_j=\sigma_5^2$, where $\sigma_5$ is the automorphism of $D_j\times D_{j+1}$ such that

$$\sigma_5 d_j = d_{j+1}, \qquad \sigma_5 d_{j+1} = d_j d_{j+1}.$$

Hence $(\Gamma\gamma_j)(\Gamma\delta_j)=e$ which implies $\Gamma\gamma_j=\Gamma\delta_j$.

LEMMA 11. *Let $\Gamma\in$Hom $(A, T)$. Let $q$ be an integer relatively prime to $p$, and let $\mu_j$ be the automorphism of $D_j\times D_{j+1}$ such that*

$$\mu_j d_j = d_j^q, \qquad \mu_j d_{j+1} = d_{j+1}^q.$$

*If $q\equiv 1 \pmod{s_j}$, then $\Gamma\mu_j=e$.*

**Proof.** Suppose $q\equiv 1 \pmod{s_j}$. Then $\mu_j=\nu^2$ where $\nu$ is the automorphism of $D_j\times D_{j+1}$ such that

$$\nu d_j = d_j^{-1} d_{j+1} \qquad \nu d_{j+1} = d_j^{q-1} d_{j+1}.$$

Hence $\Gamma\mu_j=(\Gamma\nu)^2=e$, which establishes Lemma 11.

For $p$ odd let $u(p)$ denote the number of distinct integers in the set $m_1, m_2, \cdots, m_l$.

LEMMA 12. *If $p$ is odd, then the order of* Hom $(A^{(p)}, T)$ *is at most $2^{u(p)}$.*

**Proof.** Since $p$ is an odd prime, the group $A_i$ of automorphisms of $D_i$ is cyclic. Let $\tau_1$ be a generator of $A_1$. Then $\tau_1 d_1=d_1^q$ for some integer $q$ relatively prime to $p$. For arbitrary $i$ let $\tau_i$ be the automorphism of $D_i$ such that $\tau_i d_i=d_i^q$. Then $\tau_i$ is a generator of the cyclic group $A_i$. By Lemma 1, $A^{(p)}$ is generated by the automorphisms $\tau_i, \gamma_j, \delta_j$, $1\leqq i\leqq l$, $1\leqq j<l$. Let $\Gamma\in$Hom $(A^{(p)},T)$. Then $\Gamma\gamma_j=\Gamma\delta_j=e$ for all $j$ by Lemma 10. If $m_i=m_j$ then $\Gamma\tau_i=\Gamma\tau_j$ by Lemma 11. Let $j_1, j_2, \cdots, j_{u(p)}$ be a set of indices such that $m_{j_1}, \cdots, m_{j_{u(p)}}$ is the complete set of distinct values of $m_i$. Then $\Gamma$ is completely determined by the $\Gamma\tau_{j_i}$, $1\leqq i\leqq u(p)$. Since there are only two possible values for $\Gamma\tau_j$ for each $j$, the order of Hom $(A^{(p)}, T)$ is at most $2^{u(p)}$. This completes the proof of Lemma 12.

Let $m$ be one of the numbers $m_1, \cdots, m_l$. Thus $m$ is a power of $p$. Let $D_s, D_{s+1}, \cdots, D_t$ be those $D_i$ of order $m$. For $\sigma\in A$ we write

$$\sigma d_j = \prod_{i=1}^{l} d_i^{u_{ij}}, \qquad s\leqq j\leqq t.$$

Let $\bar{u}_{ij}$ denote the residue class of $u_{ij}$ modulo $p$, and let $u_\sigma$ be the value of the $t-s+1$ rowed determinant $|\bar{u}_{ij}|$, $s\leqq i\leqq t$, $s\leqq j\leqq t$. Then $\sigma\to u_\sigma$ is a homomorphism of $A$ onto the multiplicative group of residue classes modulo $p$. We now define the mapping $\Upsilon_m$ of $A$ into $T$ as follows:

$$\Upsilon_m\sigma = \begin{cases} e & \text{if } u_\sigma \text{ is a square modulo } p, \\ h & \text{otherwise.} \end{cases}$$

Then $\Upsilon_m \in \text{Hom}\ (A^{(p)}, T)$. If $p$ is odd, then as $m$ runs through its $u(p)$ possible values, $\Upsilon_m$ runs through $u(p)$ independent homomorphisms of $A$ onto $T$.

Combining this with Lemma 12 we obtain:

LEMMA 13. *If $p$ is an odd prime dividing the order of $G$, then the order of* Hom $(A^{(p)}, T)$ *is* $2^{u(p)}$. *Furthermore* Hom $(A^{(p)}, T)$ *is generated by the $u(p)$ homomorphisms of the form $\Upsilon_m$, where $m$ is a power of $p$ and an invariant of the finite abelian group $G$.*

It can be shown that $\Upsilon_m$ depends only on $G$, $T$, and $m$.

We now study Hom $(A^{(2)}, T)$. We know that $A^{(2)}$ is generated by $\lambda_i$, $\xi_i$, $\theta_j$, $\eta_j$, $1 \leqq i \leqq k$, $1 \leqq j < k$. We will put $n_0 = r_0 = \infty$ in the following in order to insure that $n_0 > n_1$ and $r_0 \geqq 8$.

Let $u(4)$ denote the number of positive values of $i$ such that $r_i \geqq 4$, and let $u(8)$ denote the number of positive values of $i$ such that $r_i \geqq 8$. Let $u(\eta)$ be the number of values of $i$ such that $n_{i-1} > n_i$ and $n_{i+1} > n_{i+2}$. Let $u(\theta)$ be the number of values of $i$ such that $n_{i-1} > n_i > n_{i+1} > n_{i+2}$. Let $\Gamma \in \text{Hom}\ (A^{(2)}, T)$.

We note that $\lambda_k = \epsilon$ if $n_k = 2$, and that $\xi_k = \epsilon$ if $n_k \leqq 4$. From Lemma 11 it follows that

$$\Gamma\lambda_i = \Gamma\lambda_{i+1} \qquad \text{if } r_i \leqq 2$$

and

$$\Gamma\xi_i = \Gamma\xi_{i+1} \qquad \text{if } r_i \leqq 4.$$

It follows that at most $u(4)$ of the $\Gamma\lambda_i$ are independent and that at most $u(8)$ of the $\Gamma\xi_i$ are independent. From Lemma 10 it follows that $\Gamma\eta_i = \Gamma\theta_i = e$ if either $n_{i+1} = n_{i+2}$ or $n_{i-1} = n_i$. Furthermore $\Gamma\eta_i = \Gamma\theta_i$ if $n_i = n_{i+1}$. It follows that at most $u(\eta)$ of the $\Gamma\eta_i$ are different from $e$, and that $\Gamma\theta_j$ is independent of $\Gamma\eta_j$ for at most $u(\theta)$ values of $j$. Thus the order of Hom $(A^{(2)}, T)$ is at most $2^{u(2)}$, where

$$u(2) = u(4) + u(8) + u(\eta) + u(\theta).$$

We shall now construct $u(2)$ independent homomorphisms of $A^{(2)}$ onto $T$. For any $\sigma \in A$ we write

$$\sigma c_j = \prod_{i=1}^{k} c_i^{q_{ij}}, \qquad 1 \leqq j \leqq k.$$

Let $r = 4$ or 8. Choose $s$ and $t$ such that $s \leqq t$, $r_j < r$ if $s \leqq j < t$, $r_{s-1} \geqq r$, $r_t \geqq r$. For each $r$ there are $u(r)$ possible choices of $s$ and $t$. Let $\bar{q}_{ij}$ denote the residue class of $q_{ij}$ modulo $r$. Let $q_\sigma$ be the value of the $t-s+1$ rowed deter-

minant $|\bar{q}_{ij}|$, $s \leqq i \leqq t$, $s \leqq j \leqq t$. The mapping $\sigma \to q_\sigma$ is a homomorphism of $A$ onto the multiplicative group of odd residue classes modulo $r$. For $r=4$ we put

$$\Lambda_t\sigma = \begin{cases} e \text{ if } q_\sigma \equiv 1 \pmod 4, \\ h \text{ if } q_\sigma \equiv -1 \pmod 4. \end{cases}$$

For $r=8$ we put

$$\Xi_t\sigma = \begin{cases} e \text{ if } q_\sigma \equiv \pm 1 \pmod 8, \\ h \text{ if } q_\sigma \equiv \pm 3 \pmod 8. \end{cases}$$

The $u(4)$ mappings $\Lambda_t$ and the $u(8)$ mappings $\Xi_t$ are elements of Hom $(A^{(2)}, T)$. Furthermore

$$\Lambda_t\xi_j = \Lambda_t\theta_j = \Lambda_t\eta_j = e \text{ for all } j,$$

and

$$\Lambda_t\lambda_j = \begin{cases} h \text{ if } s \leqq j \leqq t, \\ e \text{ otherwise.} \end{cases}$$

Moreover

$$\Xi_t\lambda_j = \Xi_t\theta_j = \Xi_t\eta_j = e \text{ for all } j,$$

and

$$\Xi_t\xi_j = \begin{cases} h \text{ if } s \leqq j \leqq t, \\ e \text{ otherwise.} \end{cases}$$

Now let $s$ be one of the $u(\eta)$ integers such that $n_{s-1} > n_s$ and $n_{s+1} > n_{s+2}$. Let $\bar{q}_{ij}$ denote the residue class of $q_{ij}$ modulo 2, and let $\mathfrak{M}_\sigma$ be the $2\times 2$ matrix $(\bar{q}_{ij})$, $s \leqq i \leqq s+1$, $s \leqq j \leqq s+1$. Then $\sigma \to \mathfrak{M}_\sigma$ is a homomorphism of $A$ into the group of nonsingular $2\times 2$ matrices over the field of two elements. This group of $2\times 2$ matrices is isomorphic to the symmetric group of order 6 and has an invariant subgroup $S$ of order 3 consisting of

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Put

$$\Psi_s\sigma = \begin{cases} e \text{ if } \mathfrak{M}_\sigma \in S, \\ h \text{ if } \mathfrak{M}_\sigma \notin S. \end{cases}$$

The $u(\eta)$ mappings $\Psi_s$ are elements of Hom $(A^{(2)}, T)$. For each of them we have

$$\Psi_s\lambda_j = \Psi_s\xi_j = e \text{ for all } j,$$
$$\Psi_s\theta_j = \Psi_s\eta_j = e \text{ for } j \neq s,$$

and $\Psi_s\eta_s = h$, while $\Psi_s\theta_s$ may be either $e$ or $h$.

Finally let $s$ be any positive integer such that $n_{s-1} > n_s > n_{s+1} > n_{s+2}$. We put

$$\Theta_s\sigma = \begin{cases} e \text{ if } 2r_s \mid q_{s,s+1}, \\ h \text{ otherwise.} \end{cases}$$

Then $\Theta_s \in \text{Hom}\ (A^{(2)}, T)$. There are $u(\theta)$ such $\Theta_s$ and for each one

$$\Theta_s\lambda_j = \Theta_s\xi_j = \Theta_s\eta_j = e \text{ for all } j$$

and

$$\Theta_s\theta_j = \begin{cases} e \text{ if } j \neq s, \\ h \text{ if } j = s. \end{cases}$$

We see that the $u(2)$ homomorphisms $\Lambda_t$, $\Xi_t$, $\Psi_s$, $\Theta_s$ are independent. Therefore the order of Hom $(A^{(2)}, T)$ is $2^{u(2)}$ and the homomorphisms $\Lambda_t$, $\Xi_t$, $\Psi_s$, $\Theta_s$ form a basis for it.

It can be shown that the homomorphisms $\Lambda_t$, $\Xi_t$, $\Psi_s$, $\Theta_s$ are independent of the decomposition of $G^{(2)}$ into the direct product of cyclic groups $C_i$ and of the choice of generators $c_i$.

Summarizing the results of this section we obtain:

THEOREM 2. *The order of* Hom $(A, T)$ *is* $2^u$, *where* $u = \sum u(p)$, *the sum being taken over all primes dividing the order of* $G$. *There is a basis for* Hom $(A, T)$ *consisting of the elements* $\Upsilon_m$, *where* $m$ *runs over the odd prime power invariants of* $G$, $\Lambda_t$ *for those positive* $t$ *such that* $r_t \geqq 4$, $\Xi_t$ *for those positive* $t$ *such that* $r_t \geqq 8$, $\Psi_s$ *for those* $s$ *such that* $n_{s-1} > n_s$ *and* $n_{s+1} > n_{s+2}$, *and* $\Theta_s$ *for those* $s$ *such that* $n_{s-1} > n_s > n_{s+1} > n_{s+2}$.

6. $H^1(A, G)$. In §2 we showed that every nontrivial element of $H^1(A, G)$ has order 2. Therefore $H^1(A, G)$ is either trivial or the direct product of cyclic groups of order 2. It follows that $H^1(A, G)$ is isomorphic to the direct product of the two factor groups

$$Z^1(A, G)/\text{Hom}\ (A, J)B^1(A, G) \text{ and } \text{Hom}\ (A, J)B^1(A, G)/B^1(A, G).$$

The first of these two factor groups was determined in §3 and §4, while the latter is isomorphic to Hom $(A, J)$/Hom $(A, J) \cap B^1(A, G)$.

Now if $n_1 = n_2$, then $J$ is trivial and hence

$$H^1(A, G) = Z^1(A, G)/\text{Hom}\ (A, J)B^1(A, G).$$

If $n_1 > n_2$, then $J$ has order 2 and Hom $(A, J)$ is given by Theorem 2 with $T = J$. Thus to complete the determination of $H^1(A, G)$ we need only determine the intersection Hom $(A, J) \cap B^1(A, G)$ under the assumption $n_1 > n_2$.

If $n_1 > n_2$, then we use the notation of §5 with $T = J$ and $h = b_1 = c_1^{n_1/2}$. We note that if $\Lambda_1$ is defined, then $r_1 \geqq 4$, $\Lambda_1\sigma = a_1\sigma a_1^{-1}$ for all $\sigma \in A$, and hence

$$\Lambda_1 = \Gamma_{a_1} \in \text{Hom } (A, J) \cap B^1(A, G).$$

Similarly if $\Theta_1$ is defined, then $n_1 > n_2 > n_3$ and

$$\Theta_1 = \Gamma_{b_2} \in \text{Hom } (A, J) \cap B^1(A, G).$$

Conversely we have:

LEMMA 14. *If* $\Gamma$ *is a nontrivial element of* Hom $(A, J) \cap B^1(A, G)$, *then* $\Gamma$ *is either* $\Lambda_1$, $\Theta_1$, *or* $\Lambda_1\Theta_1$.

**Proof.** If $n_1 = n_2$ then Lemma 14 is trivial. Suppose $n_1 > n_2$ and let $a$ be an element of $G$ such that $\Gamma_a \in$ Hom $(A, J)$. Then $a\sigma a^{-1} \in J$ for all $\sigma \in A$. Letting $\sigma$ run through the automorphisms of $N_1$ we obtain $a \in C_1 \times K_1$. If $a \notin C_1$, then $K_1$ is not trivial, $n_2 > n_3$, $a$ is of the form $a'b_2$ with $a' \in C_1$, and $\Gamma_a = \Gamma_{a'}\Theta_1$. Hence without loss of generality we may suppose $a \in C_1$. Then $a^2 = a\lambda_1 a^{-1} \in J$ and thus $a^4 = e$. Now $a = c_1^q$ for some integer $q$. Hence $a\eta_1 a^{-1} = c_2^{-q} \in J \subseteq C_1$. Therefore $n_2 \mid q$ and $n_1 \mid r_1 q$. Hence $a^{r_1} = e$. Thus if $a \notin J$, then $a^2 \neq e$, $r_1 \geqq 4$, $\Lambda_1$ is defined, $aa_1^{-1} \in J$, and $\Gamma_a = \Gamma_{a_1} = \Lambda_1$. On the other hand if $a \in J$, then $\Gamma_a$ is the identity element of the group Hom $(A, J)$. Thus Lemma 14 is established.

It now follows that if $n_1 > n_2$, then a set of representatives of a basis of Hom $(A, J)B^1(A, G)/B^1(A, G)$ can be obtained from the basis of Hom $(A, J)$ given in Theorem 2 by deleting $\Lambda_1$ and $\Theta_1$ (if they are defined). We now sum up in the following theorem.

THEOREM 3. *Let* $G$ *be a finite abelian group and* $A$ *its group of automorphisms. Let* $\mathfrak{S}$ *be the set of all* $v$ *for which* $\Gamma_v$ *is defined,* $\text{i} \leqq v \leqq \text{iv}$. *If* $n_1 = n_2$, *then the cosets* $\Gamma_v B^1(A, G)$, $v \in \mathfrak{S}$, *form a basis of* $H^1(A, G)$. *If* $n_1 > n_2$, *then there is a set of representatives of a basis of* $H^1(A, G)$ *that consists of the elements* $\Gamma_v$ *for all* $v \in \mathfrak{S}$, $\Upsilon_m$ *for all odd prime power invariants* $m$ *of* $G$, $\Lambda_t$ *for all* $t > 1$ *such that* $r_t \geqq 4$, $\Xi_t$ *for all positive* $t$ *such that* $r_t \geqq 8$, $\Psi_s$ *for all* $s$ *such that* $n_{s-1} > n_s$ *and* $n_{s+1} > n_{s+2}$, *and* $\Theta_s$ *for all* $s > 1$ *such that* $n_{s-1} > n_s > n_{s+1} > n_{s+2}$. *In both cases* $H^1(A, G)$ *is either trivial or the direct product of groups of order two.*

## II. THE OUTER AUTOMORPHISM GROUP OF $H$

In Part II we will complete the determination of the outer automorphism group of $H$. Throughout Part II we will use the notation of Part I. In particular $H$ is the holomorph of the finite abelian group $G$, $\mathfrak{O}$ and $\mathfrak{I}$ are the outer and inner automorphism groups of $H$ respectively, $\mathfrak{A}$ is the group of all automorphisms of $H$, and $\mathfrak{B}$ is the group of all automorphisms of $H$ that map $G$ onto itself.

7. **Invariant subgroups of $H$ isomorphic to $G$.** In this section we will collect certain results[5] about the invariant subgroups of $H$ isomorphic to $G$.

[5] Most of these results can be found in [6] in somewhat different form. We will appeal to [6] only for the result that there are no invariant subgroups of $H$ isomorphic to $G$ other than the ones listed in this section.

In particular we will list all these subgroups and, for each such subgroup $G^*$, we will construct an automorphism of $H$ that maps $G$ onto $G^*$ and leaves $G \cap G^*$ fixed elementwise.

Let $A^*$ be the group of all elements of $H$ of the form $(e, \sigma)$, $\sigma \in A$.

LEMMA 15. *Let $G^*$ be an invariant subgroup of $H$ isomorphic to $G$ and suppose that every element of $G$ occurs as the first component of an element of $G^*$. Let $\omega$ be any isomorphism of $G$ onto $G^*$. For any $g \in G$ let $g^*$ denote the first component of $\omega g$. Then there exists a unique extension $\Omega$ of $\omega$ to an automorpism of $H$ that maps $A^*$ onto itself. For any $\sigma \in A$ we have $\Omega(e, \sigma) = (e, \sigma^*)$ where*

$$\sigma^* g^* = (\sigma g)^*. \tag{32}$$

*Furthermore if $\Omega'$ is any automorphism of $H$ that maps $G$ onto $G^*$ and $A^*$ onto itself, then $\Omega^{-1}\Omega' \in \mathfrak{g}$. If $\Omega^*$ is any automorphism of $H$ that maps both $G$ and $A^*$ onto themselves, then $\Omega^* \in \mathfrak{g}$.*

**Proof.** Since $G$ and $G^*$ are finite and have the same order it follows that every element of $G$ occurs exactly once as the first component of an element of $G^*$. Hence the mapping $g \to g^*$ is a one-to-one mapping of $G$ onto itself. Suppose that $\Omega$ is an automorphism of $H$ mapping $A^*$ onto itself such that $\omega$ is the restriction of $\Omega$ to $G$. For any $\sigma \in A$ we put $\Omega(e, \sigma) = (e, \sigma^*)$. Now

$$\Omega\sigma g = \Omega\{(e, \sigma)g(e, \sigma)^{-1}\} = (e, \sigma^*)(g^*, \phi_g)(e, \sigma^*)^{-1}$$

where $\omega g = (g^*, \phi_g)$. Comparing first components we obtain (32), which determines $\sigma^*$ uniquely. Since $\Omega$ is completely determined by its effect on $G$ and $A^*$ it follows that there is at most one automorphism of $H$ with the required properties.

We must now prove the existence of $\Omega$. For any $\sigma \in A$ let $[\sigma]$ denote the automorphism of $G^*$ induced by the inner automorphism $\mathrm{I}_{(e,\sigma)}$ of $H$. Since every element of $G$ occurs as the first component of an element of $G^*$ it follows that the mapping $\sigma \to [\sigma]$ is one-to-one of $A$ into the group of automorphisms of $G^*$. Since $A$ and the group of automorphisms of $G^*$ have the same finite order it follows that $\sigma \to [\sigma]$ is an isomorphism of $A$ onto this group of automorphisms. Let $\sigma^*$ be the automorphism of $G$ such that $[\sigma^*] = \omega\sigma\omega^{-1}$. Then the mapping $\Omega$ given by

$$\Omega(g, \sigma) = \omega g(e, \sigma^*)$$

is a one-to-one mapping of $H$ onto itself. Clearly $\Omega g = \omega g$ for all $g \in G$ and $\Omega$ maps $A^*$ onto itself. Furthermore

$$\begin{aligned}\{\Omega(a, \sigma)\}\{\Omega(b, \tau)\} &= \omega a\{[\sigma^*]\omega b\}(e, \sigma^*\tau^*) \\ &= \omega(a\sigma b)(e, \sigma^*\tau^*) \\ &= \Omega\{(a, \sigma)(b, \tau)\}.\end{aligned}$$

Hence $\Omega$ is an automorphism with the desired properties.

Now $\Omega'$ maps $G$ onto $G^*$. Hence for suitable $\phi \in A$ we have $\Omega'\phi g = \omega g$ for all $g \in G$. Then $\Omega' I_{(e,\phi)}$ is an extension of $\omega$ to an automorphism of $H$ that maps $A^*$ onto itself. Hence $\Omega' I_{(e,\phi)} = \Omega$ by the uniqueness of $\Omega$. Thus $\Omega^{-1}\Omega' \in \mathfrak{g}$. Finally putting $G^* = G$, $\Omega = I$, the identity automorphism of $H$, and $\Omega' = \Omega^*$ this becomes $\Omega^* \in \mathfrak{g}$, which completes the proof.

If $n_1 \geqq 4$ let $\phi_1$ denote the automorphism of $G^{(2)}$ such that

$$\phi_1 g = g^{1+n_1/2}$$

for all $g \in G^{(2)}$. Clearly $\phi_1$ belongs to the center of $A$ and $\phi_1^2 = \epsilon$.

If $n_2 \geqq 2$ put $\phi_2 = \theta_1^{n_2/2}$. Thus

$$\phi_2 c_1 = c_1, \qquad \phi_2 c_2 = c_1^{n_1/2} c_2.$$

Furthermore $\phi_2^2 = \epsilon$.

If $n_1 \geqq 4$ put $\phi_3 = \phi_1 \eta_1^{n_1/2}$. Thus

$$\phi_3 c_1 = c_1^{1+n_1/2} c_2^{n_1/2}, \qquad \phi_3 c_2 = c_2^{1+n_1/2}$$

We have $\phi_3^2 = \epsilon$.

We will now list the invariant subgroups of $H$ isomorphic to $G$.

1. Suppose $n_1 \geqq 8$ and $n_1 > n_2$. In this case let $G_1$ be the group generated by $(c_1, \phi_1)$ and $N_1$. Then $G_1$ is isomorphic to $G$. The group $G_1$ consists of those elements of $H$ of the form $(a, \phi_1)$ where $n_1$ divides the order of $a$ and of those elements of $G$ whose order is not divisible by $n_1$. It follows that $G_1$ is an invariant subgroup of $H$ isomorphic to $G$, that every element of $G$ occurs exactly once as the first component of an element of $G_1$, and that $G \cap G_1$ is generated by $c_1^2$ and $N_1$. Let $\omega_1$ be the isomorphism of $G$ onto $G_1$ such that

$$\omega_1 c_1 = (c_1^{1+n_1/4}, \phi_1)$$

and $\omega_1 g = g$ for all $g \in N_1$. Then $\omega_1$ leaves every element of $G \cap G_1$ fixed. By Lemma 15 there exists an automorphism $\Omega_1$ of $H$ that extends $\omega_1$ and that maps $A^*$ onto itself. By (32) we have

$$(33) \qquad \begin{cases} \Omega_1(e, \sigma) = (e, \sigma) \text{ if } \sigma c_1 = c_1, \\ \Omega_1(e, \xi_1) = (e, \xi_1), \\ \Omega_1(e, \lambda_1) = (e, \lambda_1 \phi_1), \\ \Omega_1(e, \eta_1) = (e, \eta_1^{1+n_1/4}). \end{cases}$$

Since $n_1 \geqq 8$ we have $\phi_1 = \xi_1^{n_1/8}$. Hence $\Omega_1(e, \phi_1) = (e, \phi_1)$. It follows that $\Omega_1^2$ maps both $G$ and $A^*$ onto themselves. Hence $\Omega_1^2 \in \mathfrak{g}$ by the last statement of Lemma 15.

2. Suppose $n_1 > n_2 > n_3$. In this case let $G_2$ be the group generated by $(c_1, \phi_2)$, $(c_2, \phi_1)$, and $N_{1,2}$. Then $G_2$ is isomorphic to $G$ and $G \cap G_2$ is the characteristic subgroup of $G$ generated by $c_1^2$, $c_2^2$, and $N_{1,2}$. Let $F$ be the set of all elements of $G$ that do not belong to $G_2$ and have order divisible by $n_2$ but not by

$n_1$. For any element $a$ of $G$ whose order is divisible by $n_1$ let $\phi_a$ be the unique automorphism of $G$ such that $\phi_a a = a$ and $\phi_a f = hf$ for all $f \in F$, where $h$ is the nonidentity element of $J$. The group $G_2$ consists of the elements of $G \cap G_2$, the elements of $H$ of the form $(f, \phi_1)$, $f \in F$, and the elements of $H$ of the form $(a, \phi_a)$ where $n_1$ divides the order of $a$. It follows that $G_2$ is an invariant subgroup of $H$. Thus $G_2$ is an invariant subgroup of $H$ isomorphic to $G$ and every element of $G$ occurs exactly once as the first component of an element of $G_2$. Let $\omega_2$ be the isomorphism of $G$ onto $G_2$ such that

$$\omega_2 c_1 = (c_1, \phi_2), \qquad \omega_2 c_2 = (c_2, \phi_1),$$

and $\omega_2 g = g$ for all $g \in N_{1,2}$. Then $\omega_2$ leaves every element of $G \cap G_2$ fixed. Let $\Omega_2$ be the automorphism of $H$ that extends $\omega_2$ and maps $A^*$ onto itself. By (32) we have

$$\begin{cases} \Omega_2(e, \sigma) = (e, \sigma) \text{ if } \sigma c_1 \in C_1, \\ \Omega_2(e, \eta_1) = (e, \eta_1 \phi_1). \end{cases} \tag{34}$$

It follows from (34) that $\Omega_2(e, \phi_1) = (e, \phi_1)$ and $\Omega_2(e, \phi_2) = (e, \phi_2)$. Therefore $\Omega_2^2$ acts as the identity on $G$. Since $\Omega_2^2$ maps $A^*$ onto itself it follows from Lemma 15, with $G^* = G$, that $\Omega_2^2 = \mathrm{I}$, the identity automorphism of $H$.

3. Suppose $n_1 \geqq 8$ and $n_2 > n_3$. In this case let $G_3$ be the group generated by $(c_1, \phi_1\phi_2)$, $(c_2, \phi_3)$, and $N_{1,2}$. Then $G_3$ is isomorphic to $G$ and every element of $G$ occurs exactly once as the first component of an element of $G_3$. Furthermore $G \cap G_3$ is the characteristic subgroup of $G$ generated by $c_1^2$, $c_2^2$, and $N_{1,2}$. We now consider two cases:

3a. Suppose $n_1 \geqq 8$ and $n_1 > n_2 > n_3$. In this case $G_1$, $G_2$, $\Omega_1$, and $\Omega_2$ are defined. Moreover $\phi_3 = \phi_1$ and

$$G \cap G_3 = G \cap G_2 \subset G \cap G_1.$$

Hence $\Omega_1\Omega_2$ and $\Omega_2\Omega_1$ both leave $G \cap G_3$ fixed elementwise. Furthermore

$$\Omega_1\Omega_2 c_1 = (c_1^{1+n_1/4}, \phi_1\phi_2) = \Omega_2\Omega_1 c_1$$

and

$$\Omega_1\Omega_2 c_2 = (c_2, \phi_1) = \Omega_2\Omega_1 c_2.$$

It follows that $\Omega_1\Omega_2$ and $\Omega_2\Omega_1$ map $G$ onto $G_3$, that their restrictions to $G$ are identical, and that they both map $A^*$ onto itself. Since $\Omega_1\Omega_2$ is an automorphism of $H$ it follows that $G_3$ is an invariant subgroup of $H$ isomorphic to $G$. Hence $\Omega_1\Omega_2 = \Omega_2\Omega_1$ by Lemma 15. In this case we put $\Omega_3 = \Omega_1\Omega_2$.

3b. Suppose $n_1 \geqq 8$ and $n_1 = n_2 > n_3$. For any $a \in G$ whose order $n_a$ is divisible by $n_1$ let $\theta_a$ be the unique automorphism of $G$ such that $\theta_a a = a$, $\theta_a g' = g'$ for all $g' \in G'$, and $\theta_a g = a^{n_a/2} g$ for every $g \in G$ of order $n_1$ that is independent of $a$.

Then $G_3$ consists of the elements of $G\cap G_3$ and the elements of $H$ of the form $(a, \theta_a\phi_1)$ where $n_1$ divides the order of $a$. It follows that $G_3$ is an invariant subgroup of $H$ isomorphic to $G$. Let $\omega_3$ be the isomorphism of $G$ onto $G_3$ such that

$$\omega_3 c_1 = (c_1^{1+n_1/4}, \phi_1\phi_2), \qquad \omega_3 c_2 = (c_2^{1+n_1/4}, \phi_3),$$

and $\omega_3 g = g$ for all $g\in N_{1,2}$. Then $\omega_3$ leaves $G\cap G_3$ fixed elementwise. Let $\Omega_3$ be the automorphism of $H$ that extends $\omega_3$ and maps $A^*$ onto itself. By (32) we have $\Omega_3(e, \phi_i) = (e, \phi_i)$, $i = 1, 2, 3$. It follows that $\Omega_3^2$ maps both $G$ and $A^*$ onto themselves. Hence $\Omega_3^2\in\mathfrak{g}$ by Lemma 15. In this case we do not need to know $\Omega_3(e, \sigma)$ for all $\sigma\in A$. However if $g^*$ denotes the first component of $\Omega_3 g$, then $g^*g^{-1}$ is a square. Therefore if $\sigma^*$ is the automorphisms of $G$ such that $\Omega_3(e, \sigma) = (e, \sigma^*)$ and if

$$\sigma c_j = \prod_{i=1}^{k} c_i^{q_{ij}}, \qquad \sigma^* c_j = \prod_{i=1}^{k} c_i^{q^*_{ij}}, \qquad 1 \leqq j \leqq k,$$

then it follows from (32) that

$$q_{ij} = q^*_{ij} \pmod 2. \tag{35}$$

4. Suppose $n_1 = 4$ and $n_2 = k = 2$. Then $\Gamma_i$ and $\Omega_2$ are both defined, and $\Gamma_i$ can be regarded as an automorphism of $H$ by (2). Referring to §4 we have $a_1 = c_1$, $b_2 = c_2$, $\Gamma_i = \Gamma'$,

$$\Gamma_i\Omega_2 c_1^{-1} = \Gamma_i(c_1^{-1}, \phi_2) = \Gamma_i(c_1^{-1}, \theta_1) = (c_2, \theta_1),$$
$$\Gamma_i\Omega_2 c_2 = \Gamma_i(c_2, \phi_1) = \Gamma_i(c_2, \lambda_1) = (e, \lambda_1),$$

and $\Gamma_i\Omega_2 g' = g'$ for all $g'\in G' = N_{1,2}$. Since $\Gamma_i$ and $\Omega_2$ are automorphisms of $H$, it follows that $(c_2, \theta_1)$, $(e, \lambda_1)$, and $G'$ generate an invariant subgroup of $H$ isomorphic to $G$. We designate this subgroup by $G_4$. The automorphism $\Gamma_i\Omega_2$ of $H$ maps $G$ onto $G_4$.

Conversely it has been shown [6] that if $G^*$ is an invariant subgroup of $H$ isomorphic to $G$, and $G^* \neq G$, then either

1. $n_1 \geqq 8$, $n_1 > n_2$, and $G^* = G_1$, or
2. $n_1 > n_2 > n_3$ and $G^* = G_2$, or
3. $n_1 \geqq 8$, $n_2 > n_3$, and $G^* = G_3$, or
4. $n_1 = 4$, $n_2 = k = 2$, and $G^* = G_4$.

For each of the groups $G_w$, $1 \leqq w \leqq 3$, we have an automorphism $\Omega_w$ of $H$ that maps $G$ onto $G_w$, leaves $G\cap G_w$ fixed elementwise, maps $A^*$ onto itself, and satisfies $\Omega_w^2\in\mathfrak{g}$. Furthermore $\Omega_1$ is defined if the first two of the inequalities

$$n_1 \geqq 8, \qquad n_1 > n_2, \qquad n_2 > n_3 \tag{36}$$

hold, $\Omega_2$ is defined if the last two of the inequalities (36) hold, and $\Omega_3$ is defined if the first and third of these inequalities hold. Therefore if more than one of

these $\Omega_w$ is defined, then all three of them are and we have $\Omega_3=\Omega_1\Omega_2=\Omega_2\Omega_1$.

Let $\mathcal{P}$ be the subgroup of $\mathcal{O}$ that is generated by the cosets $\Omega_w\mathcal{J}$, where $w$ runs over those values for which $\Omega_w$ is defined, $1\leqq w\leqq 3$. If all three of the inequalities (36) hold, then $\mathcal{P}$ is the four group. If exactly two of these inequalities hold, then $\mathcal{P}$ has order 2. If less than two of them hold, then $\mathcal{P}$ is trivial.

8. **The outer automorphism group of** $H$. The group $G$ is an invariant subgroup of $H$. Hence any automorphism $\Omega$ of $H$ maps $G$ onto a group $G^*$, where $G^*$ is an invariant subgroup of $H$ isomorphic to $G$. As indicated in §7 there are five possibilities for $G^*$, namely $G$, $G_1$, $G_2$, $G_3$, and $G_4$. If $G^*=G$, then $\Omega\in\mathfrak{B}$. If $G^*=G_w$ with $w=1$, 2, or 3, then $\Omega_w^{-1}\Omega\in\mathfrak{B}$. If $G^*=G_4$, then $(\Gamma_i\Omega_2)^{-1}\Omega\in\mathfrak{B}$ and $\Gamma_i\in Z^1(A, G)\subseteq\mathfrak{B}$. It follows that $\mathfrak{A}$ is generated by $\mathfrak{B}$ and those $\Omega_w$ that are defined, $1\leqq w\leqq 3$.

In §1 we showed that $H^1(A, G)$ is isomorphic to $\mathfrak{B}/\mathcal{J}$ under the natural isomorphism $\Gamma B^1(A, G)\to\Gamma\mathcal{J}$. In this section we will identify $H^1(A, G)$ and $\mathfrak{B}/\mathcal{J}$ by means of this isomorphism. Then $\mathcal{O}$ is generated by $\mathcal{P}$ and $H^1(A, G)$, and $\mathcal{P}\cap H^1(A, G)$ consists of the identity alone. We must now study the relations between the elements of $\mathcal{P}$ and those of $H^1(A, G)$. In other words we must study the relations, modulo $\mathcal{J}$, between the $\Omega_w$ and the cocycles of $Z^1(A, G)$.

Henceforth $w$ will denote an integer such that $\Omega_w$ is defined, $1\leqq w\leqq 3$. For any $\sigma\in A$, $\sigma^*$ will denote the element of $A$ such that $\Omega_w(e, \sigma)=(e, \sigma^*)$, and for any $g\in G$, $g^*$ will denote the first component of $\Omega_w g$. This is in agreement with the notation of Lemma 15.

LEMMA 16. *If* $\Omega_w$ *is defined and* $\Gamma\in\mathrm{Hom}\ (A, J)$, *then*

$$\Gamma\Omega_w\equiv\Omega_w\Gamma\pmod{\mathcal{J}}.$$

**Proof.** If $n_1=n_2$, then $J$ is trivial and so is Lemma 16. Hence suppose $n_1>n_2$. Then if $\Omega_3$ is defined we have $\Omega_3=\Omega_1\Omega_2$. Thus without loss of generality suppose that $w=1$ or 2. Since $J\subset G_w$ it follows that $\Gamma$ maps $G_w$ onto itself. Now $\Omega_w^2\in\mathcal{J}$ and hence $\Omega_w$ permutes $G$ and $G_w$. Therefore $(\Omega_w\Gamma)^2$ maps $G$ onto itself. For all $\sigma\in A$ we have

$$(\Omega_w\Gamma)^2(e, \sigma)=((\Gamma\sigma)(\Gamma\sigma^*), \sigma^{**}), \tag{37}$$

since $\Gamma\sigma$ and $\Gamma\sigma^*$ are elements of $J$ and hence left fixed by $\Omega_w$. We distinguish two cases:

*Case* 1. $\Gamma\phi_1=e$. If $w=1$, then $n_1\geqq 8$, $\eta_1^{n_1/4}$ is a square, and it follows from (33) that $\Gamma\sigma=\Gamma\sigma^*$ for all $\sigma\in A$. If $w=2$ it follows from (34) that $\Gamma\sigma=\Gamma\sigma^*$ for all $\sigma\in A$. In either case $(\Omega_w\Gamma)^2$ maps $A^*$ onto itself by (37). It now follows from Lemma 15 that $(\Omega_w\Gamma)^2\in\mathcal{J}$ which is equivalent to $\Gamma\Omega_w\equiv\Omega_w\Gamma\pmod{\mathcal{J}}$.

*Case* 2. $\Gamma\phi_1\neq e$. Here $\Gamma\phi_1=c_1^{n_1/2}$. If $n_2\geqq 2$, then $\Gamma\phi_1=e$ by Lemma 11 with $q=1+n_1/2$ and $j=1$. Hence $n_2=1$. Therefore $\Omega_2$ is undefined, $w=1$, and $n_1\geqq 8$. By (33) we have

$$(\Gamma\lambda_1)(\Gamma\lambda_1^*) = (\Gamma\lambda_1)^2(\Gamma\phi_1) = \Gamma\phi_1 = c_1^{n_1/2},$$

and

$$(\Gamma\sigma)(\Gamma\sigma^*) = (\Gamma\sigma)^2 = e$$

for all $\sigma \in A'$ and for $\sigma = \xi_1$. Since $n_2 = 1$ it follows that $A$ is generated by $\lambda_1$, $\xi_1$, and $A'$. Therefore $(\Omega_w\Gamma)^2 I_{a_1}$ maps $A^*$ onto itself, where $a_1 = c_1^{n_1/4}$ as usual. Clearly $I_{a_1}$ maps $G$ onto itself. Therefore $(\Omega_w\Gamma)^2 I_{a_1}$ also maps $G$ onto itself, and Lemma 15 yields $(\Omega_w\Gamma)^2 I_{a_1} \in \mathfrak{g}$. Hence $(\Omega_w\Gamma)^2 \in \mathfrak{g}$ and Lemma 16 is established.

We now come to the relations between the special cocycles $\Gamma_v$ of §4 and the $\Omega_w$. The key to these relations is the following:

LEMMA 17. *Suppose that $\Gamma_v$ and $\Omega_w$ are defined. Let $\overline{G}$ be the characteristic subgroup of $G$ used to define $\Gamma_v$. Then we have $n_1 \geqq 8$ and $\overline{G} \subseteq G \cap G_w$ with the exception of the case $n_1 > n_2 = k = 2$, $w \neq 1$, $v = \mathrm{i}$.*

**Proof.** We recall that if $v = \mathrm{i}$, then either $n_1 > n_2 > n_3$ and $\overline{G}$ is generated by $a_1$ and $b_2$, or $n_1 = n_2 \geqq 4n_3$ and $\overline{G}$ is generated by $a_1$ and $a_2$. If $v = \mathrm{ii}$ or iii, then $n_3 > n_4$ and $\overline{G}$ is generated by $b_1$, $b_2$, and $b_3$. If $v = \mathrm{iv}$ then $n_1 = 4n_2$ and $\overline{G}$ is generated by $a_1$.

Suppose that $n_1 \leqq 4$. Then $w = 2$ and $n_1 > n_2 > n_3$. This implies $n_1 = 4$, $n_2 = k = 2$, and $v = \mathrm{i}$. Thus $n_1 \leqq 4$ can occur only in the exceptional case.

Now suppose that $n_1 \geqq 8$. If $n_2 = 1$, then none of the $\Gamma_v$ are defined. Therefore $n_2 \geqq 2$. Now $c_1^2$, $c_2^2$, and $c_3$ are elements of $G_w$. Hence $a_1$ and $b_1$ are elements of $G_w$. Furthermore if $n_3 > n_4$, then $n_3 \geqq 2$ and $b_3 \in G_w$. If $n_1 = n_2$, then $a_2 \in G_w$.

Now suppose that $n_1 \geqq 8$ and that $\overline{G} \nsubseteq G \cap G_w$. Since $\overline{G}$ is a subgroup of $G$ we have $\overline{G} \nsubseteq G_w$. Then $v \neq \mathrm{iv}$, $n_2 \geqq 2$, and $b_2 \notin G_w$. If $n_2 \geqq 4$, then $b_2 \in G_w$. Hence $n_2 = 2$. If $w = 1$, then $b_2 = c_2 \in G_w$. Hence $w \neq 1$. If $n_2 = n_3$, then $w = 1$. Therefore $n_2 > n_3$ and we have $n_3 = 1$, $k = 2$, and $v \neq \mathrm{ii}$, iii. Thus $v = \mathrm{i}$ and we have the exceptional case mentioned in the statement of Lemma 17.

LEMMA 18. *Suppose that $\Gamma_v$ and $\Omega_w$ are defined and that the exceptional case of Lemma 17 does not hold. Let $\sigma \in A$ and $(a, \phi) \in G_w$. Then $\Omega_w\Gamma_v\sigma = \Gamma_v\sigma$, $\Gamma_v\sigma^* = \Gamma_v\sigma$, and $\Gamma_v\phi = e$.*

**Proof.** By Lemma 17 we have $n_1 \geqq 8$ and $\overline{G} \subseteq G \cap G_w$. It follows from the construction of $\Gamma_v$ that $\Gamma_v\sigma \in \overline{G}$. Since $\Omega_w$ leaves every element of $G \cap G_w$ fixed we have $\Omega_w\Gamma_v\sigma = \Gamma_v\sigma$. To prove the remaining statements of Lemma 18 we distinguish two cases.

*Case* 1. $v = \mathrm{iii}$. Here $n_1 = n_2$ so that $w = 3$. We recall that $\Gamma_{\mathrm{iii}}\sigma$ depends only on the residue classes of the numbers $q_{ij}$ modulo 2, where

$$\sigma c_j = \prod c_i^{q_{ij}}.$$

Hence $\Gamma_{\mathrm{iii}}\phi_j = e$ for those $\phi_j$ that are defined, $1 \leqq j \leqq 3$. Now $\phi$ is contained in

the group generated by these $\phi_j$. Hence $\Gamma_{iii}\phi = e$. Furthermore $\Gamma_{iii}\sigma^* = \Gamma_{iii}\sigma$ by (35).

*Case* 2. $v \neq iii$. In this case $\Gamma_v\sigma$ depends only on the restriction of $\sigma$ to $\overline{G}$. Since $G_w$ is abelian it follows that $\phi$ leaves every element of $G \cap G_w$ fixed. Therefore $\phi$ leaves every element of $\overline{G}$ fixed and we have $\Gamma_v\phi = e$. Now $\Omega_w\bar{g} = \bar{g}$ for all $\bar{g} \in \overline{G}$ and $\overline{G}$ is a characteristic subgroup of $G$. Hence, by (32) we have

$$\sigma^*\bar{g} = \sigma^*\bar{g}^* = (\sigma\bar{g})^* = \sigma\bar{g}$$

for all $\bar{g} \in \overline{G}$. Therefore $\Gamma_v\sigma^* = \Gamma_v\sigma$ and Lemma 18 is established.

LEMMA 19. *Suppose that* $\Gamma_v$ *and* $\Omega_w$ *are defined. Then* $\Gamma_v\Omega_w = \Omega_w\Gamma_v$ *with the exception of the case* $n_1 > n_2 = k = 2$, $w \neq 1$, $v = i$.

**Proof.** Suppose that the exceptional case $n_1 > n_2 = k = 2$, $w \neq 1$, $v = i$ does not hold. Then Lemma 18 applies. Hence for any $g \in G$ we have

$$\Gamma_v\Omega_w g = \Gamma_v(g^*, \phi) = (g^*, \phi) = \Omega_w g = \Omega_w\Gamma_v g$$

for suitable $\phi \in A$. Applying Lemma 18 again we have, for any $\sigma \in A$,

$$\Gamma_v\Omega_w(e, \sigma) = (\Gamma_v\sigma^*, \sigma^*) = (\Gamma_v\sigma, \sigma^*)$$

and

$$\Omega_w\Gamma_v(e, \sigma) = \Omega_w(\Gamma_v\sigma, \sigma) = (\Gamma_v\sigma, \sigma^*).$$

Therefore $\Gamma_v\Omega_w = \Omega_w\Gamma_v$ and Lemma 19 is established. We will see that $\Omega_w$ and $\Gamma_v$ do not commute in the exceptional case.

It follows from Lemmas 16 and 19 that, except for the case $n_1 > n_2 = k = 2$, the elements of $\mathcal{P}$ and $H^1(A, G)$ commute with each other. Thus $\mathfrak{O} = \mathcal{P} \times H^1(A, G)$ except for this exceptional case.

We now come to the case $n_1 > n_2 = k = 2$. The existence of $G_4$, if $n_1 = 4$, indicates that the cases $n_1 \geqq 8$ and $n_1 = 4$ behave differently. We treat them separately.

Suppose $n_1 \geqq 8$ and $n_2 = k = 2$. In this case we need to determine $(\Omega_2\Gamma_i)^2$ modulo $\mathfrak{I}$. We see that $\Omega_2\Gamma_i$ maps $G$ onto $G_2$. Since $G$, $G_1$, $G_2$, and $G_3$ are the only invariant subgroups of $H$ isomorphic to $G$ it follows that $\Omega_2\Gamma_i$ maps $G_2$ onto one of these groups. Now $(c_1, \phi_2) = (c_1, \theta_1) \in G_2$ and

$$\Omega_2\Gamma_i(c_1, \theta_1) = (c_1^{1+3n_1/4}c_2, \phi_1)$$

which is an element of $G_1$, but not of $G$, $G_2$, or $G_3$. Hence $\Omega_2\Gamma_i$ maps $G_2$ onto $G_1$, and $(\Omega_2\Gamma_i)^2$ maps $G$ onto $G_1$. Since $n_2 = k = 2$ it follows that $A$ is generated by $\lambda_1$, $\xi_1$, $\theta_1$, $\eta_1$, and the elements of $A'$. We have

$$(\Omega_2\Gamma_i)^2(e, \lambda_1) = (e, \phi_1\lambda_1),$$
$$(\Omega_2\Gamma_i)^2(e, \theta_1) = (c_1^{n_1/2}, \phi_1\theta_1),$$

and

$$(\Omega_2\Gamma_i)^2(e, \sigma) = (e, \sigma)$$

for all $\sigma \in A'$, for $\sigma = \xi_1$, and for $\sigma = \eta_1$. Hence $I_{c_2}(\Omega_2\Gamma_i)^2$ maps $A^*$ onto itself. Since $G_1$ is an invariant subgroup of $H$ it follows that $I_{c_2}$ maps $G_1$ onto itself, and hence $I_{c_2}(\Omega_2\Gamma_i)^2$ maps $G$ onto $G_1$. Therefore $I_{c_2}(\Omega_2\Gamma_i)^2 \equiv \Omega_1 \pmod{\mathcal{G}}$ by Lemma 15. Thus we have $(\Omega_2\Gamma_i)^2 \equiv \Omega_1 \pmod{\mathcal{G}}$. We see at once that the cosets $\Gamma_i\mathcal{G}$ and $\Omega_2\mathcal{G}$ generate a group $\mathfrak{O}_8$ of order 8, and that $\mathfrak{O}_8$ is the octic group. Since $k = 2$, neither $\Gamma_{ii}$ nor $\Gamma_{iii}$ is defined. Furthermore $\Gamma_{iv}$ is defined if $n_1 = 8$ and undefined if $n_1 \geqq 16$. If $n_1 \geqq 16$ we put $\mathfrak{O}' = \text{Hom}\ (A, J)\mathcal{G}/\mathcal{G}$, while if $n_1 = 8$ we let $\mathfrak{O}'$ be the group obtained from Hom $(A, J)\mathcal{G}/\mathcal{G}$ by adjoining $\Gamma_{iv}\mathcal{G}$. Then $\mathfrak{O}'$ is the direct product of groups of order 2, and $\mathfrak{O} = \mathfrak{O}_8 \times \mathfrak{O}'$. Referring to Lemma 14 we see that a set of representatives of a basis of Hom $(A, J)\mathcal{G}/\mathcal{G}$ can be obtained by deleting $\Lambda_1$ and $\Theta_1$ from the basis of Hom $(A, J)$ given by Theorem 2.

There remains only the case $n_1 = 4$, $n_2 = k = 2$ to be treated. In this case the invariant subgroups of $H$ isomorphic to $G$ are $G$, $G_2$, and $G_4$. We observed in §7 that $\Gamma_i\Omega_2$ maps $G$ onto $G_4$. Furthermore $\Omega_2$ maps $G_2$ onto $G$ so that $\Gamma_i\Omega_2$ also maps $G_2$ onto $G$. It follows immediately that $\Gamma_i\Omega_2$ maps $G_4$ onto $G_2$, and that $(\Gamma_i\Omega_2)^3$ maps $G$ onto itself. In this case $A$ is generated by $\lambda_1$, $\theta_1$, $\eta_1$, and the elements of $A'$. We have

$$(\Gamma_i\Omega_2)^3(e, \theta_1^2) = (c_1, \theta_1\lambda_1),$$

and

$$(\Gamma_i\Omega_2)^3(e, \sigma) = (e, \sigma)$$

for all $\sigma \in A'$, for $\sigma = \lambda_1$, and for $\sigma = \eta_1$. It follows that $I_{c_2}(\Gamma_i\Omega_2)^3$ maps both $G$ and $A^*$ onto themselves. Hence $I_{c_2}(\Gamma_i\Omega_2)^3 \in \mathcal{G}$ by Lemma 15. Therefore $(\Gamma_i\Omega_2)^3 \in \mathcal{G}$ and we see that the cosets $\Gamma_i\mathcal{G}$ and $\Omega_2\mathcal{G}$ generate a group $\mathfrak{O}_6$ isomorphic to the symmetric group of order 6. In fact if we regard $\mathfrak{O}_6$ as a permutation group on $G$, $G_2$, $G_4$, then it is exactly this symmetric group. In this case $\Gamma_{ii}$, $\Gamma_{iii}$, $\Gamma_{iv}$, $\Omega_1$, and $\Omega_3$ are undefined and we have

$$\mathfrak{O} = \mathfrak{O}_6 \times \text{Hom}\ (A, J)\mathcal{G}/\mathcal{G}.$$

In this case $\Lambda_1$ is undefined and we can obtain a set of representatives of a basis of Hom $(A, J)\mathcal{G}/\mathcal{G}$ by deleting $\Theta_1$ from the basis of Hom $(A, J)$ given by Theorem 2. This set consists of $\Psi_1$ and the $\Upsilon_m$, where $m$ runs through the odd prime power invariants of $G$.

We summarize our results in a final theorem:

THEOREM 4. *If $G$ is the direct product of a cyclic group of order four, a group of order two, and an abelian group of odd order, then $\mathfrak{O}$ is the direct product of the symmetric group of order six and a finite number of groups of order two, $\mathfrak{O} = \mathfrak{O}_6 \times$ Hom $(A, J)\mathcal{G}/\mathcal{G}$. If $G$ is the direct product of a cyclic group of order $2^n$,*

*$n \geqq 3$, a group of order two, and an abelian group of odd order, then $\mathfrak{O}$ is the direct product of the octic group and a finite number of groups of order two, $\mathfrak{O} = \mathfrak{O}_8 \times \mathfrak{O}'$. For all other finite abelian groups $G$, $\mathfrak{O}$ is the direct product of a finite number of groups of order two, in fact $\mathfrak{O} = \mathfrak{P} \times H^1(A, G)$.*

## REFERENCES

1. Anne P. Cobbe, *On the cohomology groups of a finite group*, Quart. J. Math. Oxford Ser. (2) vol. 6 (1955) pp. 34–47.

2. W. Dyck, *Gruppentheoretische Studien*, Math. Ann. vol. 20 (1882) pp. 1–44.

3. Yu. A. Gol'fand, *On the group of automorphisms of the holomorph of a group*, Rec. Math. (Mat. Sbornik) N.S. vol. 27 (1950) pp. 333–350.

4. G. A. Miller, *On the multiple holomorphs of a group*, Math. Ann. vol. 66 (1908) pp. 133–142.

5. ———, *Abstract definitions of all the substitution groups whose degrees do not exceed seven*, Amer. J. Math. vol. 33 (1911) pp. 363–372.

6. W. H. Mills, *Multiple holomorphs of finitely generated abelian groups*, Trans. Amer. Math. Soc. vol. 71 (1951) pp. 379–392.

7. ———, *On the non-isomorphism of certain holomorphs*, Trans. Amer. Math. Soc. vol. 74 (1953) pp. 428–443.

YALE UNIVERSITY,
NEW HAVEN, CONN.