# ON THE NON-ISOMORPHISM OF CERTAIN HOLOMORPHS

BY

W. H. MILLS

Let $G$ and $G'$ be finite groups with isomorphic holomorphs. It has been shown that if $G$ and $G'$ are abelian, then $G$ and $G'$ are isomorphic(1). The object of this paper is to show that if $G$ is abelian, then $G'$ is also abelian and hence isomorphic to $G$. Thus if $G$ is not isomorphic to $G'$, then neither $G$ nor $G'$ is abelian(2). In [5] it was pointed out that two finite groups with isomorphic holomorphs are not necessarily isomorphic. In fact if $n \geqq 3$, the dihedral and dicyclic groups of order $4n$ have isomorphic holomorphs.

1. **Definitions.** Let $G$ be a group and let $A$ be its group of automorphisms. The set $H$ of all pairs $(g, \sigma)$, $g \in G$, $\sigma \in A$, forms a group under the composition

$$(g, \sigma)(h, \tau) = (g\sigma h, \sigma\tau). \tag{1}$$

We let $e$ and $I$ be the identity elements of $G$ and $A$ respectively. Then $(e, I)$ is the identity of $H$. Furthermore the inverse of $(a, \sigma)$ is $(\sigma^{-1}a^{-1}, \sigma^{-1})$. The group $H$ is called the holomorph(3) of $G$. By identifying the element $g \in G$ with the element $(g, I)$ we obtain an imbedding of $G$ in $H$. It is clear that $G$ is an invariant subgroup of $H$ and that every automorphism of $G$ can be extended to an inner automorphism of $H$.

The centralizer $G^*$ of $G$ in $H$ is called the conjoint of $G$. Thus $(a, \sigma) \in G^*$ if and only if $(a, \sigma)g = g(a, \sigma)$ for all $g$ in $G$. This is equivalent to $\sigma g = a^{-1}ga$. Thus the conjoint $G^*$ consists of all elements of the form $(a, \tau_a)$, where $\tau_a$ is the inner automorphism corresponding to the element $a$. The mapping $\eta$ defined by

$$\eta(a, \sigma) = (a^{-1}, \tau_a^{-1}\sigma) \tag{2}$$

is an automorphism of $H$ mapping $G$ onto $G^*$. Therefore $G$ is isomorphic to $G^*$ and we can regard $H$ as the holomorph of both $G$ and $G^*$. Now $\eta^2$ is the identity automorphism, and hence $\eta$ maps $G^*$ onto $G$. It follows that $G$ is the centralizer of $G^*$. We note that $G \cap G^*$ is the center of $G$, and that $\eta$ maps

Presented to the Society, December 28, 1951; received by the editors March 22, 1952.

(1) In fact this result is true for abelian groups with a finite number of generators. See [5]. (Numbers in brackets refer to the references cited at the end of the paper.)

(2) G. A. Miller [3, p. 337] has asserted that the cyclic group of order 8 and the octic group have the same holomorph. Since the holomorph of the former group has order 32, and that of the latter has order 64, this is not the case.

(3) The holomorph and the conjoint can also be defined as the normalizer and the centralizer of a regular permutation group in the appropriate symmetric group. The automorphism $\eta$ given by (2) is well known in this setting. See, for example, [4].

every element of $G \cap G^*$ into its inverse. Thus $\eta$ maps every subgroup of $G \cap G^*$ onto itself. Furthermore if $G$ is not an abelian group, then $G \neq G^*$, and since $G$ is an invariant subgroup of $H$ it follows that $\eta$ is an outer automorphism of $H$.

Let $N$ be another group with a holomorph $H'$ isomorphic to $H$. Let $\theta$ be an isomorphism of $H'$ onto $H$. We can identify $h' \in H'$ with $\theta h' \in H$. Then $N$ becomes an invariant subgroup of $H$, and $H$ is the holomorph of $N$ as well as of $G$. Thus if two groups have isomorphic holomorphs we can assume that they have the same group $H$ as holomorph.

2. **Some preliminary lemmas.** We shall now establish several preliminary lemmas for later use.

LEMMA 1. *Let $H$ be the holomorph of a group $G$, and $S$ an invariant subgroup of $H$. Then the subset of $G$ consisting of all first components of the elements of $S$ forms a characteristic subgroup of $G$.*

**Proof.** Let $(g, \sigma)$ and $(h, \tau)$ be arbitrary elements of $S$ and let $\xi$ be an arbitrary automorphism of $G$. Then since $S$ is an invariant subgroup of $H$, $S$ contains the elements

$$(g, \sigma)(e, \sigma^{-1}\tau)(h, \tau)^{-1}(e, \sigma^{-1}\tau)^{-1}$$

and

$$(e, \xi)(g, \sigma)(e, \xi)^{-1}$$

which have $gh^{-1}$ and $\xi g$ as first components. Therefore the first components of $S$ form a characteristic subgroup of $G$.

LEMMA 2. *If $H$ is the holomorph of each of a collection of groups, $G_1, G_2, \cdots$, then the group $G' = \bigcap G_i$ is a characteristic subgroup of each of the groups $G_j$.*

**Proof.** Each $G_i$ is an invariant subgroup of $H$. Hence $G'$ is an invariant subgroup of $H$. Therefore $G'$ is mapped onto itself by each inner automorphism of $H$, and hence by each automorphism of any given $G_j$. Therefore $G'$ is a characteristic subgroup of each $G_j$.

LEMMA 3. *Let $G$ and $N$ be finite groups with the same holomorph $H$, and let $N^*$ be the conjoint of $N$. If every element of $G$ occurs at least once as the first component of an element of $N$, then $G$ and $N$ have the same order, and each element of $G$ occurs exactly once as the first component of an element of $N$, and exactly once as the first component of an element of $N^*$.*

**Proof.** Suppose that $(e, \xi)$ is an element of $N^*$ with first component the identity, and let $g$ be an arbitrary element of $G$. Then $g$ occurs as the first component of an element of $N$, say $(g, \sigma)$. Since the elements of $N$ commute with the elements of $N^*$, it follows that $(e, \xi)(g, \sigma) = (g, \sigma)(e, \xi)$ which implies that $\xi g = g$. Thus $\xi g = g$ for all $g \in G$, and hence $\xi = I$. It follows that $N^*$ does

not contain two elements $(a, \tau)$ and $(a, \mu)$ with the same first component. Hence order $N^* \leqq$ order $G$, and by hypothesis order $G \leqq$ order $N$. Since $N^*$ is isomorphic to $N$, it follows that $N^*$ and $N$ have the same order. Therefore $G$ and $N$ have the same order. It follows immediately that each element of $G$ occurs exactly once as the first component of an element of each of the groups $N$ and $N^*$.

The next lemma is an immediate consequence of Lemma 3.

LEMMA 4. *If $G$ is a proper subgroup of a finite group $N$ and if $H$ is the holomorph of $N$, then $H$ is not the holomorph of $G$.*

Lemma 4 does not exclude the possibility that a finite group and one of its proper subgroups have isomorphic holomorphs. It seems to be difficult to determine whether or not this can be the case.

LEMMA 5. *Let $H$ be the holomorph of an abelian group $G$, and let $S$ be an invariant subgroup of $H$. Let $(a, \sigma)$ and $b$ be arbitrary elements of $S$ and $G$ respectively. Then $\sigma b/b \in G \cap S$, $a^2 \in G \cap S$, and $(e, \sigma^2) \in S$.*

**Proof.** We need only show that $\sigma b/b$, $a^2$, and $(e, \sigma^2)$ are elements of $S$. Since $S$ is an invariant subgroup of $H$, $S$ contains the commutator $b^{-1}(a, \sigma)b(a, \sigma)^{-1} = \sigma b/b$. Now let $\lambda$ be the automorphism of $G$ that sends each element into its inverse. Then $\lambda$ is in the center of $A$, and since $S$ is invariant, $S$ contains $(e, \lambda)(a, \sigma)(e, \lambda)^{-1} = (a^{-1}, \sigma)$. Hence $S$ contains $(a, \sigma)(a^{-1}, \sigma)^{-1} = a^2$. Finally $S$ contains $a^{-2}(\sigma a/a)^{-1}(a, \sigma)^2 = (e, \sigma^2)$.

3. **The holomorph of a finite abelian group.** In this section we collect certain results about the holomorph of a finite abelian group that will be needed later.

Let $G$ be a finite abelian group with holomorph $H$. Then $H$ contains at most four invariant subgroups isomorphic to $G$. We shall now describe these subgroups explicitly(4).

We write $G$ as the direct product of its Sylow subgroups:

$$G = G(2) \times G(p_1) \times G(p_2) \times \cdots \times G(p_M),$$

where $p_1, \cdots, p_M$ are distinct odd primes and $G(p)$ is the Sylow subgroup of $G$ corresponding to the prime $p$. Of course it is not excluded that $G(2)$ consists of the identity alone. Now write $G(2)$ as a direct product:

$$G(2) = C_1 \times C_2 \times F,$$

where $C_1$ and $C_2$ are cyclic groups of order $u$ and $v$ respectively, $F$ is a group whose elements have maximal order $w$, and $u \geqq v \geqq w$. Clearly $u$, $v$, and $w$ are powers of 2 uniquely determined by the group $G$. Let $\alpha$ and $\beta$ be generators of $C_1$ and $C_2$ respectively. Put $F' = G(p_1)G(p_2) \cdots G(p_M)F$.

(4) See [5] for the determination of these subgroups.

Let $r$ be an odd integer, and $s$ an even integer divisible by $u/v$. Then we define automorphisms $\psi$ and $\omega$ of $G$ as follows:

$$\psi g = \omega g = g \quad \text{if} \quad g \in F',$$
$$\psi\alpha = \alpha^r, \qquad \psi\beta = \alpha^s\beta^r,$$
$$\omega\alpha = \alpha^{1+s}\beta^s, \quad \text{and} \quad \omega\beta = \beta^{1+s}.$$

Let $G(r, s)$ be the group obtained by adjoining $(\alpha, \psi)$ and $(\beta, \omega)$ to the group $F'$. The group $G(r, s)$ is an invariant subgroup of $H$ isomorphic to $G$ if and only if $r$ and $s$ satisfy the following conditions:

(a) $r=1$ or $r=1+u/2$.
(b) $s=0$ or $s=u/2$.
(c) If $u=v$ then $r=s+1$.
(d) If $v=w$ then $s=0$.
(e) If $u \leqq 4$ then $r=1$.

Under these conditions every element of $G$ occurs exactly once as the first component of an element of $G(r, s)$. Conversely if $\mathcal{G}$ is an invariant subgroup of $H$ isomorphic to $G$ such that every element of $G$ occurs at least once as the first component of an element of $\mathcal{G}$, then $\mathcal{G}$ is one of the groups $G(r, s)$ where $r$ and $s$ satisfy the five given conditions. We note that in this case $(\alpha, \psi)$ has order $u$ and $(\beta, \omega)$ has order $v$. Hence there exists an isomorphism of $G$ onto $\mathcal{G}$ that maps $\alpha$ into $(\alpha, \psi)$ and $\beta$ into $(\beta, \omega)$.

If $\mathcal{G}$ is an invariant subgroup of $H$ isomorphic to $G$ such that not all elements of $G$ occur as first components of elements of $\mathcal{G}$, then $u=4$, $v=2$, $w=1$, and $\mathcal{G}$ is the group obtained by putting $r=1$, $s=2$, and then adjoining $(\beta, \psi)$ and $(e, \omega)$ to the group $F'$. We denote this group by $\overline{G}$.

Now let $\mathcal{G}$ be any invariant subgroup of $H$ isomorphic to $G$. Then there exists an automorphism[5] of $H$ mapping $G$ onto $\mathcal{G}$, and hence $H$ is also the holomorph of $\mathcal{G}$. The following properties of $\mathcal{G}$ are consequences of the above mentioned facts.

PROPERTY I. Either $\mathcal{G}=G$; or $\mathcal{G}\cap G$ is the group generated by $\alpha^2$, $\beta^2$, and the elements of $F'$; or $u>v$ and $\mathcal{G}\cap G$ is the group generated by $\alpha^2$, $\beta$, and the elements of $F'$.

**Proof.** By Lemma 2, $\mathcal{G}\cap G$ is a characteristic subgroup of $G$. Furthermore in all cases $\mathcal{G}\cap G$ contains $\alpha^2$, $\beta^2$, and the elements of $F'$. Property I follows at once.

PROPERTY II. There is an isomorphism $\theta$ of $\mathcal{G}$ onto $G$ leaving every element of $\mathcal{G}\cap G$ fixed.

**Proof.** If $\mathcal{G}=G(r, s)$, then

$$\theta(\alpha, \psi) = \alpha^{(1+r)/2}, \quad \theta(\beta, \omega) = \begin{cases} \beta & \text{if} \quad s = 2, \\ \beta^{1+s/2} & \text{if} \quad s \neq 2, \end{cases}$$

[5] See [5, pp. 390–392].

and $\theta f = f$ for all $f \in F'$ define such an isomorphism. If $\mathcal{G} = \overline{G}$, then $\theta(\beta, \psi) = \alpha$, $\theta(e, \omega) = \beta$, and $\theta f = f$ for all $f \in F'$ define a suitable isomorphism $\theta$.

PROPERTY III. If $\theta$ is any isomorphism of $\mathcal{G}$ onto $G$, then $\theta$ can be extended to an automorphism of $H$.

**Proof.** As noted above there exists an automorphism of $H$ mapping $G$ onto $\mathcal{G}$. Any automorphism of $G$ can be extended to an automorphism of $H$. Property III is an immediate consequence of these two facts.

PROPERTY IV. Suppose the order of $G$ is a power of 2, $u > v$, and that $G$ is not the group of order 8 and type (4, 2). Suppose $\beta \notin \mathcal{G}$ and let $\zeta$ be the automorphism of $G$ such that $\zeta g = g^{1+u/2}$, for all $g \in G$. Then there is an isomorphism of $G$ onto $\mathcal{G}$ that maps $\beta$ into $(\beta, \zeta)$.

**Proof.** The case $u = 4$, $v = 2$, $w = 1$, is excluded by hypothesis. Hence $\mathcal{G}$ is one of the groups $G(r, s)$. Since $\beta \notin \mathcal{G}$, it follows that $\omega \neq I$ and hence $s \neq 0$. This implies $v > w$ by condition (d) and $s = u/2$ by condition (b). Since $u > v$ we have $\beta^s = e$ and hence $\omega = \zeta$. Hence there is an isomorphism of $G$ onto $\mathcal{G}$ that maps $\beta$ into $(\beta, \zeta)$.

PROPERTY V. If $\mathcal{G} = G(r, s)$ and if the order of $G$ is a power of 2, then $(\alpha, \psi)$ and its conjugates in $H$ generate $\mathcal{G}$.

**Proof.** $(\alpha, \psi)$ is an element of $\mathcal{G}$ of maximal order. Hence the conjugates of $(\alpha, \psi)$ are the elements of $\mathcal{G}$ of maximal order. Hence these elements generate $\mathcal{G}$.

If $G$ has odd order then $G$ itself is the only invariant abelian subgroup of $H$ isomorphic to $G$. Hence we have:

PROPERTY VI. If $G$ has odd order, then $G$ is a characteristic subgroup of $H$.

Property VI enables us to prove the following theorem.

THEOREM 1. *If $H$ is the holomorph of an abelian group $G$ of odd order, then $H$ has only inner automorphisms*(6).

**Proof.** Let $\theta$ be any automorphism of $H$. By Property VI, $\theta$ maps $G$ onto itself. Hence there exists an inner automorphism $\rho$ of $H$ such that $\theta\rho$ leaves every element of $G$ fixed. Let $\lambda$ be the automorphism of $G$ that maps every element of $G$ onto its inverse. Then $\theta\rho$ maps $(e, \lambda)$ into an element of the form $(b, \lambda)$. Choose $c$ such that $c^2 = b$. If $\tau_c$ is the inner automorphism of $H$ corresponding to the element $c$, then $\Theta = \theta\rho\tau_c$ maps $(e, \lambda)$ and every element of $G$ into itself. Now let $\sigma$ be an arbitrary element of $A$. Then $\Theta(e, \sigma)$ is of the form $(d, \sigma)$. Since $(e, \lambda)$ commutes with $(e, \sigma)$ it follows that $\Theta(e, \lambda) = (e, \lambda)$ and $\Theta(e, \sigma) = (d, \sigma)$ commute with each other. Hence $\lambda d = d$ or $d^2 = e$, which implies that $d = e$. It follows at once that $\Theta$ is the identity automor-

(6) This was first proved by G. A. Miller [2]. Miller established Property VI and then used an earlier result of Burnside [1] to prove the theorem. Burnside's result states that if $G$ is an abelian group of odd order, and if $G$ is a characteristic subgroup of its holomorph $H$, then $H$ has only inner automorphisms. Burnside's result is equivalent to the statement that the first cohomology group $H^1(A, G)$ is trivial. This is not true for the cyclic group of order 4.

phism of $H$. Hence $\theta$ is an inner automorphism.

Now let $p$ be a prime dividing the order of $G$. Each automorphism $\phi$ of the Sylow subgroup $G(p)$ can be identified with the automorphism $\phi'$ of $G$ such that $\phi' g = \phi g$ for $g \in G(p)$ and $\phi' g = g$ for any $g \in G$ with order relatively prime to $p$. Then the holomorph $H_p$ of $G(p)$ can be regarded as a subgroup of the holomorph $H$ of $G$. Clearly $H_p$ is an invariant subgroup of $H$. $H_p$ is not necessarily a characteristic subgroup of $H$. However, we can now establish:

LEMMA 6. *$H_p$ contains a nontrivial characteristic subgroup of $H$.*

**Proof.** Let $\theta$ be any automorphism of $H$. Then $\theta$ maps $G$ onto one of the groups $\mathcal{G}$ listed above. By inspection of the possible groups $\mathcal{G}$ we see that $\theta$ maps $G(p)$ onto a subgroup $\theta G(p)$ of $H_p$. The set of all such subgroups $\theta G(p)$ clearly generates a nontrivial subgroup of $H_p$ that is a characteristic subgroup of $H$.

Let $H_1, H_2, \cdots, H_t$ be the holomorphs of the nontrivial Sylow subgroups of $G$. It is easily shown that $H$ is the direct product of the $H_i$:

$$H = H_1 \times H_2 \times \cdots \times H_t. \tag{3}$$

We shall now show that each of the groups $H_i$ is indecomposable in the sense that it cannot be written as the direct product of two nontrivial subgroups.

THEOREM 2. *Let $G$ be an abelian group of prime power order. Then $H$, the holomorph of $G$, is indecomposable.*

**Proof.** Suppose $H = S_1 \times S_2$ is a decomposition of $H$ into the direct product of two of its subgroups. Let $(g_1, \sigma_1)$ and $(g_2, \sigma_2)$ be arbitrary elements of $S_1$ and $S_2$ respectively. Then $(g_1, \sigma_1)(g_2, \sigma_2) = (g_2, \sigma_2)(g_1, \sigma_1)$. Comparing first components we have $g_1 \sigma_1 g_2 = g_2 \sigma_2 g_1$ or $\sigma_1 g_2 / g_2 = \sigma_2 g_1 / g_1$. Now $S_1$ and $S_2$ are invariant subgroups of $H$ and hence, by Lemma 5, $\sigma_1 g_2 / g_2 \in S_1$ and $\sigma_2 g_1 / g_1 \in S_2$. It follows that $\sigma_1 g_2 / g_2 = \sigma_2 g_1 / g_1 = e$ or

$$\sigma_1 g_2 = g_2 \quad \text{and} \quad \sigma_2 g_1 = g_1. \tag{4}$$

Now let $\delta$ be an element of $G$ of maximal order. Then $\delta$ can be written in the form

$$\delta = (a, \sigma)(b, \tau), \tag{5}$$

where $(a, \sigma) \in S_1$ and $(b, \tau) \in S_2$. Comparing first components of (5) and using (4) we have $\delta = a \sigma b = ab$. Since $G$ is an abelian group of prime power order, it follows that either $a$ or $b$ has maximal order. Without loss of generality we may suppose that $a$ is an element of $G$ of maximal order. Now by Lemma 1, the set of all first components of elements of $S_1$ forms a characteristic subgroup $G'$ of $G$. Now $G'$ contains $a$, an element of maximal order. Hence $G' = G$, and every element of $G$ occurs as first component of an element of $S_1$. Now if $(g_2, \sigma_2)$ is an element of $S_2$, then by (4) we have $\sigma_2 g = g$ for all $g \in G$.

Hence $\sigma_2 = I$. Therefore $S_2 \subseteq G$.

It follows at once that $\tau = I$ in (5). Hence $\sigma = I$. Therefore $S_1 \cap G$ contains $a$, an element of $G$ of maximal order. Clearly $S_1 \cap G$ is an invariant subgroup of $H$ and hence a characteristic subgroup of $G$. Therefore $S_1 \cap G = G$ or $G \subseteq S_1$. Hence $S_2 \subseteq G \subseteq S_1$. It follows that $S_2$ consists of the identity alone. This proves Theorem 2.

COROLLARY. *The decomposition* (3) *is a decomposition of* $H$ *into the direct product of indecomposable groups.*

4. **The reduction to the prime power case.** As before we suppose that $G$ is a finite abelian group with holomorph $H$. Let $N$ be an arbitrary group with the same holomorph $H$. We shall prove that $N$ is abelian.

The holomorph $H$ has the decomposition (3) into the direct product of the groups $H_i$. Hence the centralizer of any subgroup of $H$ can be written in the form $J_1 \times J_2 \times \cdots \times J_t$ where $J_i \subseteq H_i$. If $N^*$ is the conjoint of $N$, then each of the groups $N$ and $N^*$ is the centralizer of the other in $H$. Hence we can write

$$N = J_1 \times J_2 \times \cdots \times J_t \tag{6}$$

and

$$N^* = K_1 \times K_2 \times \cdots \times K_t,$$

where $J_i$ and $K_i$ are subgroups of $H_i$. Clearly $K_i$ is the centralizer of $J_i$ in $H_i$.

Now suppose that for some $j$, $J_j$ consists of the identity alone. Then $K_j = H_j$. By Lemma 6, $H_j$ contains a nontrivial characteristic subgroup $C$ of $H$. Now there exists an automorphism of $H$ mapping $N^*$ onto $N$. Hence $C \subseteq N$. Therefore $C \subseteq N \cap H_j = J_j$, a contradiction. Therefore (6) is a decomposition of $N$ into the direct product of $t$ nontrivial subgroups $J_i$.

Each $J_i$ is an invariant subgroup of $H$, and hence a characteristic subgroup of $N$. It follows that the holomorph $H$ of $N$ is the direct product of the holomorphs of the groups $J_i$:

$$H = L_1 \times L_2 \times \cdots \times L_t, \tag{7}$$

where $L_i$ is the holomorph of $J_i$. Then comparing the decompositions (3) and (7) we obtain from the Krull-Schmidt theorem the fact that each $L_i$ is isomorphic to one of the groups $H_j$.

Thus $N$ is the direct product of groups $J_i$, each one of which has a holomorph isomorphic to the holomorph of an abelian group of prime power order. The question of the existence of a non-abelian group $N$ and a finite abelian group $G$ with isomorphic holomorphs is reduced to the case where $G$ is a group of prime power order.

Let $n$ be the order of $G$.

5. **The case $n$ odd.** If $H$ is the holomorph of a non-abelian group, then it has the outer automorphism $\eta$ given by (2). Hence by Theorem 1 a group that is not abelian and an abelian group of odd order cannot have isomorphic holomorphs. It follows that if the order of $G$ is a power of an odd prime, then $N$ is abelian. There remains the case where $n$ is a power of 2.

6. **The case $n=2^m$—preliminaries.** We suppose now that $G$ is an abelian group with order $2^m$, $m\geqq 1$. Since $G$ and $N$ have the same holomorph $H$, it follows that every element of $H$ can be written as a pair $(a, \sigma)$, $a\in G$, $\sigma\in A$, or as a pair $[a', \sigma']$, $a'\in N$, $\sigma'$ an automorphism of $N$. We shall use parentheses and brackets to distinguish the two notations. Multiplication of two elements of $H$ is given by (1) for both notations. If $S$ is a subgroup of $H$ we shall write $Q_i(S)$ for the set of all elements $a_i$ that occur as the $i$th component of the elements $(a_1, a_2)$ of $S$. Clearly $Q_2(S)$ is a group. If $S$ is an invariant subgroup of $H$, then $Q_1(S)$ is a characteristic subgroup of $G$ by Lemma 1.

Throughout the remainder of this paper we shall use the notation introduced in §3. Since the order of $G$ is a power of 2, we have $G=G(2)=C_1\times C_2\times F$. Furthermore $u$ is now the maximal order of the elements of $G$.

Let $N^*$ be the conjoint of $N$ and let $\eta$ be any automorphism of $H$ of order 2 that maps $N$ onto $N^*$ and that maps every subgroup of $N\cap N^*$ onto itself. Such an automorphism is given by (2). Clearly $\eta$ maps $G$ onto an invariant subgroup $\mathcal{G}$ of $H$. We have $\eta G=\mathcal{G}$, $\eta\mathcal{G}=G$, $\eta N=N^*$, and $\eta N^*=N$.

LEMMA 7. *Any element contained in three of the four groups $G$, $\mathcal{G}$, $N$, and $N^*$ is contained in the fourth group.*

**Proof.** By Properties II and III of $\mathcal{G}$, there is an automorphism $\theta$ of $H$ mapping $\mathcal{G}$ onto $G$ that leaves every element of $\mathcal{G}\cap G$ fixed. Now $\theta\eta$ maps $G$ onto itself. By Lemma 2, $\mathcal{G}\cap G\cap N$ is a characteristic subgroup of $G$, and hence $\theta\eta$ maps $\mathcal{G}\cap G\cap N$ onto itself. Now $\theta$ leaves every element of $\mathcal{G}\cap G$ fixed and hence maps $\mathcal{G}\cap G\cap N$ onto itself. Therefore $\eta$ maps $\mathcal{G}\cap G\cap N$ onto itself. Furthermore $\eta$ maps $\mathcal{G}$ onto $G$, $G$ onto $\mathcal{G}$, and $N$ onto $N^*$, and hence it maps $\mathcal{G}\cap G\cap N$ onto $G\cap\mathcal{G}\cap N^*$. Therefore

$$\mathcal{G}\cap G\cap N = \mathcal{G}\cap G\cap N^*. \tag{8}$$

Now $G\cap N\cap N^*$ is a subgroup of $N\cap N^*$. Therefore $\eta$ maps $G\cap N\cap N^*$ onto itself. Furthermore $\eta$ maps $G\cap N\cap N^*$ onto $\mathcal{G}\cap N^*\cap N$. Hence

$$G\cap N\cap N^* = \mathcal{G}\cap N\cap N^*. \tag{9}$$

Lemma 7 is an immediate consequence of (8) and (9).

LEMMA 8. *If $k$ is an integer, then $\alpha^{2k}\in N$ if and only if $\alpha^{2k}\in N^*$.*

**Proof.** By Property I, $\alpha^2 \in \mathcal{G} \cap G$. Lemma 8 follows at once from Lemma 7.

LEMMA 9. *If $G \neq N$, then the groups $G \cap N$ and $G \cap N^*$ contain no elements of order $u$.*

**Proof.** $G \cap N$ is a characteristic subgroup of $G$ by Lemma 2 and a proper subgroup of $G$ by Lemma 4. Now $u$ is the maximal order of the elements of $G$. Hence $G \cap N$ contains no elements of order $u$. Similarly $G \cap N^*$ contains no elements of order $u$.

LEMMA 10. *Either $G \cap N \subseteq N^*$ or $G \cap N^* \subseteq N$.*

**Proof.** If $G \cap N \subseteq \mathcal{G}$, then $G \cap N \subseteq \mathcal{G} \cap G \cap N \subseteq N^*$ by Lemma 7. Similarly if $G \cap N^* \subseteq \mathcal{G}$, then $G \cap N^* \subseteq N$. Thus it is sufficient to consider the case $G \neq N$, $G \cap N \not\subseteq \mathcal{G}$, and $G \cap N^* \not\subseteq \mathcal{G}$.

Let $g$ be an element of $G \cap N$ such that $g \notin \mathcal{G}$. Then $g$ is not of order $u$ by Lemma 9. By Property I, we have $u > v$ and $g$ is of the form $\alpha^{2k}\beta^q f$ where $q$ is odd and $f \in F$. Since $G \cap N$ and $G \cap \mathcal{G}$ are characteristic subgroups of $G$ it follows that $G \cap N$ contains an element of the form $\alpha^{2k}\beta$ which is not contained in $\mathcal{G}$. Since $\alpha^2 \in \mathcal{G}$ by Property I, it follows that $\mathcal{G}$ contains no elements of the form $\alpha^{2k}\beta$. We can suppose that $k$ is the smallest positive integer such that $\alpha^{2k}\beta \in N$. Similarly $N^*$ contains an element of the form $\alpha^{2k'}\beta$ and we can suppose that $k'$ is the smallest positive integer such that $\alpha^{2k'}\beta \in N^*$. Clearly $k$ and $k'$ are both powers of 2. Without loss of generality we can suppose that $k' \mid k$. Now $\alpha^{2k}\beta$ is an element of $G$ and $N$ but not an element of $\mathcal{G}$. Hence by Lemma 7 it is not an element of $N^*$. Therefore $k' \neq k$ and so $2k' \mid k$. Now since $G \cap N^*$ is a characteristic subgroup of $G$ it follows that $\alpha^{4k'} \in G \cap N^*$. Hence $\alpha^{2k} \in N^*$, and by Lemma 8 we have $\alpha^{2k} \in N$. Therefore $\beta \in N$. Furthermore since $\alpha^{2k}\beta \notin N^*$ we have $\beta \notin N^*$. Also $k' \geqq 1$ and so $k \geqq 2$. Therefore $\alpha^2 \notin N$. Thus we have $u > v \geqq 2$, $\beta \in N$, $\beta \notin N^*$, and $\alpha^2 \notin N$.

It follows from Lemma 5 that $\alpha$ does not occur as the first component of an element of $N$. Hence by Lemma 1 no element of order $u$ occurs as first component of an element of $N$. Therefore if $\zeta$ is the automorphism of $G$ such that $\zeta g = g^{1+u/2}$ for all $g \in G$, then $(e, \zeta) \in N^*$.

Now if $G$ is the group of order 8 and type (4, 2), then $\alpha^2$ is contained in the center of $H$ and hence belongs to $N$, a contradiction. Except in this case, by Property IV, there is an isomorphism of $G$ onto $\mathcal{G}$ that maps $\beta$ into $(\beta, \zeta)$. Therefore $\eta$ followed by a suitable inner automorphism of $H$ maps $\beta$ into $(\beta, \zeta)$. Now since $\beta \in N$ it follows that $(\beta, \zeta) \in N^*$. This yields $\beta \in N^*$, a contradiction. This completes the proof of Lemma 10.

Having established Lemma 10 we can now assume, without loss of generality, that $G \cap N \subseteq N^*$. Since $N^*$ is the centralizer of $N$ it follows that $G \cap N$ is contained in the center of $N$. We shall now use this fact to establish several identities.

Let $(a, \sigma)$ and $(b, \tau)$ be elements of $N$, and let $g$ be an arbitrary element of

$G$. Then by Lemma 5, $a^2$ and $\sigma g/g$ are elements of $G\cap N$ and hence belong to the center of $N$. Therefore

$$a^2(a, \sigma) = (a, \sigma)a^2$$

and

$$(b, \tau)(\sigma g/g) = (\sigma g/g)(b, \tau).$$

These two identities yield

$$(\sigma a/a)^2 = e \tag{10}$$

and

$$\tau(\sigma g/g) = \sigma g/g. \tag{11}$$

We can rewrite (11) in the form $\tau\sigma g = \tau g \sigma g/g$. Interchanging $\sigma$ and $\tau$ we obtain $\sigma\tau g = \sigma g \tau g/g$. Hence we have $\tau\sigma g = \sigma\tau g$. This holds for all $g \in G$. Therefore $\tau\sigma = \sigma\tau$. It follows that the commutator $(a, \sigma)(b, \tau)(a, \sigma)^{-1}(b, \tau)^{-1}$ is an element of $G\cap N$. We have proved the following lemma:

LEMMA 11. *The commutator subgroup of $N$ is a subgroup of $G\cap N$.*

If we put $(b, \tau) = (a, \sigma)$, then (11) becomes

$$\sigma(\sigma g/g) = \sigma g/g. \tag{12}$$

Using (12) we can show, by induction on $k$, that

$$\sigma^k g = (\sigma g/g)^k g \tag{13}$$

and

$$(a, \sigma)^k = (a^k(\sigma a/a)^{k(k-1)/2}, \sigma^k) \tag{14}$$

for all positive integral $k$.

Now $\sigma g/g \in G\cap N$. It follows from Lemma 9 that $(\sigma g/g)^{u/2} = e$. Then by (13) we have $\sigma^{u/2} g = g$ for all $g \in G$. Hence

$$\sigma^{u/2} = I. \tag{15}$$

Now by (14) we have

$$(a, \sigma)^u = (\sigma a/a)^{u(u-1)/2} = e. \tag{16}$$

Let $u'$ be the maximal order of the elements of $N$. Then from (16) it follows that

$$u' \mid u. \tag{17}$$

Hence $u'$ is a power of 2 and $g'^{u'} = e$ for all $g' \in N$.

Let $[a', \sigma']$ be an element of $G$ and $g'$ an element of $N$. Then $G\cap N$ contains the commutator

$$g'^{-1}[a', \sigma']g'[a', \sigma']^{-1} = g'^{-1}a'(\sigma'g')a'^{-1} = g'^{-1}(\sigma'g')x,$$

where $x$ is the commutator of $\sigma'g'^{-1}$ and $a'$. By Lemma 11, $x$ is an element of $G\cap N$ and hence $g'^{-1}\sigma'g'$ is an element of $G\cap N$. Since $G\cap N$ is contained in the center of $N$ it follows that $g'$ and $\sigma'g'$ commute, and we can write $\sigma'g'/g' \in G\cap N$. Now since $[a', \sigma']$ and $\sigma'g'/g'$ are both elements of $G$ they commute. It follows that

$$\sigma'(\sigma'g'/g') = (\sigma'g'/g'). \tag{18}$$

From (18) it follows that

$$\sigma'^k g' = (\sigma'g'/g')^k g' \tag{19}$$

and

$$[a', \sigma']^k = [a'^k(\sigma'a'/a')^{k(k-1)/2}, \sigma'^k] \tag{20}$$

for all positive integral $k$. From (19) we have $\sigma'^{u'}g' = g'$ for all $g' \in N$. Hence $\sigma'^{u'}$ is the identity automorphism of $N$. Now (20) yields $[a', \sigma']^{2u'} = e$ for all $[a', \sigma'] \in G$. Thus we have

$$u \mid 2u'. \tag{21}$$

Now if $u' = 2$, then every element of $N$ other than the identity has order 2 and hence $N$ is abelian. Hence without loss of generality we can suppose

$$u' > 2. \tag{22}$$

We are now in a position to prove that $u$ and $u'$ are equal.

LEMMA 12. $u = u'$.

**Proof.** From (17) and (21) it follows that either $u = u'$ or $u = 2u'$. Suppose $u = 2u'$. Since $u$ is a power of 2, $u'$ is also a power of 2. Let $[a', \sigma']$ be an element of $G$ of maximal order $u$. Then (20) yields

$$e \neq [a', \sigma']^{u'} = (\sigma'a'/a')^{u'(u'-1)/2} = (\sigma'a'/a')^{u'/2}.$$

Thus $G\cap N$ contains the element $\sigma'a'/a'$ of order $u' = u/2$. Now $G$ has at most two proper characteristic subgroups that contain elements of order $u/2$, namely the group of all squares, and the group generated by the elements of order $u/2$, which contains all squares. Therefore, since $G\cap N$ is a characteristic subgroup of $G$, it follows that $g^2 \in G\cap N$ for all $g \in G$. Hence $[a', \sigma']^2 \in G\cap N$ which implies that $\sigma'^2$ is the identity automorphism of $N$. Then (19) yields $(\sigma'a'/a')^2 = e$. Therefore $u' \leqq 2$, which contradicts the assumption (22) that $u' > 2$. It follows that $u = u'$.

Since $u = u' > 2$ we have $4 \mid u$. We now distinguish two cases.

7. **The case $n = 2^m$, $Q_1(N) = G$.** We shall suppose first that $Q_1(N) = G$, in other words that each element of $G$ occurs at least once as the first com-

ponent of an element of $N$. We shall show that in this case $N$ is one of the groups $G(r, s)$ described in §3.

By Lemma 3 each element of $G$ occurs exactly once as the first component of an element of $N$. Let $(\alpha, \sigma)$ be the element of $N$ that contains $\alpha$ as first component. Now $\alpha^2 \in N$ by Lemma 5. Since $G \cap N$ is a characteristic subgroup of $G$, and since $\alpha$ is an element of $G$ of maximal order, it follows that

$$g^2 \in N \quad \text{for all } g \in G. \tag{23}$$

Again by Lemma 5 we have $(e, \sigma^2) \in N$. Now the identity $(e, I)$ is an element of $N$ with first component $e$. Hence $\sigma^2 = I$. It follows from (13) that

$$(\sigma g/g)^2 = e \tag{24}$$

for all $g \in G$. Now if $\tau$ is any element of $A$ such that $\tau\alpha = \alpha$, then $N$ contains the elements $(\alpha, \sigma)$ and

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

and hence $\tau\sigma\tau^{-1} = \sigma$ or $\tau\sigma = \sigma\tau$. It follows that $\tau\sigma\alpha = \sigma\tau\alpha = \sigma\alpha$ for all $\tau \in A$ for which $\tau\alpha = \alpha$. Since $\alpha$ is an element of $G$ of maximal order it follows that $\sigma\alpha$ is an odd power of $\alpha$, say $\sigma\alpha = \alpha^r$. Now (24) yields $(\sigma\alpha/\alpha)^2 = e$ and hence we have

$$r = 1 \quad \text{or} \quad r = 1 + u/2. \tag{a'}$$

Now for each $\tau \in A$ for which $\tau\alpha = \alpha$ and $\tau\beta = \beta$ we have $\tau\sigma\beta = \sigma\tau\beta = \sigma\beta$. Therefore $\sigma\beta = \alpha^s\beta^R$ for suitable integral $s$ and $R$. Since $(\sigma\beta/\beta)^2 = e$ it follows that

$$s = 0 \quad \text{or} \quad s = u/2. \tag{b'}$$

Now let $\tau$ be any element of $A$ such that $\tau\alpha = \alpha$, and put $\tau\beta = \beta c$. Then $\tau\sigma = \sigma\tau$,

$$\sigma\tau\beta = \sigma(\beta c) = \alpha^s\beta^R\sigma c,$$

and

$$\tau\sigma\beta = \tau(\alpha^s\beta^R) = \alpha^s\beta^R c^R.$$

Hence $\sigma c = c^R$. It is possible to choose $\tau$ so that $c = \alpha^{u/v}$. Hence $\alpha^{ru/v} = \sigma\alpha^{u/v} = \alpha^{Ru/v}$. Therefore $ru/v \equiv Ru/v \pmod{u}$ and hence $r \equiv R \pmod{v}$. It follows that $\beta^r = \beta^R$ and without loss of generality we can put $R = r$. If $f$ is an arbitrary element of $F$ it is possible to choose $\tau$ so that $c = f$. Hence $\sigma f = f^r$ for all $f \in F$. Thus we see that $r$ and $s$ determine $\sigma$ completely. We shall now obtain certain further restrictions on $r$ and $s$ that will allow us to conclude that $N$ is abelian.

Suppose first that $u = v$. Then we can choose $\phi \in A$ such that $\phi\alpha = \beta$, and $\phi\beta = \alpha$. Then $N$ contains

$$(\alpha, \sigma)(e, \phi)(\alpha, \sigma)(e, \phi)^{-1} = (\alpha^{1+s}\beta^r, \sigma\phi\sigma\phi^{-1}).$$

Now since $4 \mid u$, it follows that $s$ and $r-1$ are even and hence (23) yields $\alpha^s\beta^{r-1} \in N$. Therefore $(\alpha\beta, \sigma\phi\sigma\phi^{-1}) \in N$. Furthermore there is an automorphism $\xi \in A$ such that $\xi\alpha = \alpha\beta$. Then $(\xi\alpha, \xi\sigma\xi^{-1}) = (\alpha\beta, \xi\sigma\xi^{-1})$ is an element of $N$ and hence $\xi\sigma\xi^{-1} = \sigma\phi\sigma\phi^{-1}$. Now

$$\xi\sigma\xi^{-1}(\alpha\beta) = \xi\sigma\alpha = \xi\alpha^r = (\alpha\beta)^r$$

and

$$\sigma\phi\sigma\phi^{-1}(\alpha\beta) = \sigma(\alpha^r\beta^{r+s}) = \sigma\{\alpha\beta(\alpha^{r-1}\beta^{r+s-1})\} = (\alpha\beta)^{1+s}$$

since $\sigma$ leaves $\alpha^{r-1}$ and $\beta^{r+s-1}$ unchanged and $\alpha^{2r} = \alpha^2$, $\beta^{2r} = \beta^2$. Therefore $(\alpha\beta)^r = (\alpha\beta)^{1+s}$. Thus we have

(c′) if $u = v$, then $r = 1 + s$.

Suppose next that $v = w$. Then there exists a $\gamma \in F$ with order $v$. By interchanging the roles of $\beta$ and $\gamma$ we obtain $\sigma\beta = \beta^r$. Hence we have

(d′) if $v = w$, then $s = 0$.

From (c′) and (d′) we see that if $u = w$ then $r = 1$. If $u > w$ then $f^r = f$ for all $f \in F$. Hence in all cases $\sigma f = f$ for all $f \in F$. It follows that $\sigma$ is the automorphism $\psi$ defined in §3. In order to conclude that $N$ is an abelian group isomorphic to $G$ we need one more restriction on $r$, namely

(e′) if $u \leqq 4$, then $r = 1$.

**Proof of (e′).** We already have $u \geqq 4$. Suppose $u = 4$ and $r \neq 1$. Then $r = 1 + u/2 = 3$, and $(\alpha, \sigma)^2 = \alpha^{1+r} = e$. Hence $(\alpha, \sigma)$ and all its conjugates have order 2. Now $N$ contains at least one element of order 4. Such an element must be of the form $(b, \nu)$ where $b$ has order 2. Choose $\phi \in A$ such that $\phi\alpha = \alpha^{-1}b$, $\phi\beta = \beta$, and $\phi f = f$ for all $f \in F$. Then $N$ contains

$$(\alpha, \sigma)(e, \sigma)^{-1}(\phi\alpha, \phi\sigma\phi^{-1})(e, \sigma) = (b, \phi\sigma\phi^{-1}\sigma).$$

Hence $\nu = \phi\sigma\phi^{-1}\sigma$. Now $\phi$ leaves every element of order 2 fixed and so $\phi\sigma\phi^{-1}\sigma b = \sigma^2 b = b$. It follows that $(b, \phi\sigma\phi^{-1}\sigma)^2 = e$, a contradiction. Thus (e′) is proved.

The conditions (a′) through (e′) are identical to the conditions (a) through (e) of §3. It follows by Property V that $(\alpha, \sigma)$ and its conjugates generate the abelian group $G(r, s)$. Thus $G(r, s) \subseteq N$ and from Lemma 4 we have $G(r, s) = N$. Therefore in this case $N$ is abelian, in fact isomorphic to $G$.

8. **The case $n = 2^m$, $Q_1(N) \neq G$.** There remains the case where $Q_1(N)$ is a proper subgroup of $G$. Since $Q_1(N)$ is a characteristic subgroup of $G$ by Lemma 1, it follows that $Q_1(N)$ contains no elements of order $u$. Since $u' = u$ by Lemma 12, it follows that $N$ contains at least one element of order $u$, say

$(a, \sigma)$. Then $a \in Q_1(N)$ and hence $a^{u/2} = e$. By (15) we have $\sigma^{u/2} = I$. Hence applying (14)

$$e \neq (a, \sigma)^{u/2} = (\sigma a/a)^{u(u/2-1)/4}.$$

Now (10) gives us $(\sigma a/a)^2 = e$, and since $u$ is a power of 2 this implies that $u = 4$. Furthermore $\sigma$, $a$, and $\sigma a/a$ all have order exactly 2. By (13) we have

$$(\sigma g/g)^2 = e \quad \text{for all} \quad g \in G. \tag{25}$$

We have just proved that $G$ is an abelian group whose elements have maximal order 4. Hence $G$ has at most two nontrivial proper characteristic subgroups: the subgroup consisting of all squares which we shall denote by $G_s$, and the subgroup generated by the elements of order 2 which we shall denote by $G_t$. Clearly $G_s \subseteq G_t$. Now $Q_1(N)$, $G \cap N$, $Q_1(N^*)$, and $G \cap N^*$ are characteristic subgroups of $G$. We shall now determine these four groups.

Suppose first that $a$ is a square, say $a = b^2$. Then $\sigma b/b$ has order 4, which contradicts (25). Hence $a$ is not a square. Since $a \in Q_1(N)$ it follows that $Q_1(N) = G_t$.

Now $\sigma a \neq a$ and hence $a(a, \sigma) \neq (a, \sigma)a$. Therefore $a \notin N^*$ or $a \notin G \cap N^*$. Therefore $G \cap N^* \subseteq G_s$. By assumption we have $G \cap N \subseteq N^*$ which is equivalent to $G \cap N \subseteq G \cap N^*$. Also $\sigma a/a$ is a nontrivial element of $G \cap N$. Thus we have $G_s \subseteq G \cap N \subseteq G \cap N^* \subseteq G_s$. Hence

$$G \cap N = G \cap N^* = G_s. \tag{26}$$

An immediate consequence of (26) is that $G \cap N^* \subseteq N$. By Lemma 3, $Q_1(N^*)$ is a proper subgroup of $G$. Hence we can interchange the roles of $N$ and $N^*$ in the above discussion and obtain $Q_1(N^*) = G_t$. Thus we have

$$Q_1(N) = Q_1(N^*) = G_t. \tag{27}$$

Now let $(b, \tau)$ be any element of $N$. If $(b, \tau)$ has order 4, then by the above discussion $\tau^2 = I$. By (16) $(b, \tau)$ cannot have order 3. If the order of $(b, \tau)$ is 1 or 2, then clearly $\tau^2 = I$. Hence if $\tau$ is any element of $Q_2(N)$, then $\tau^2 = I$. It follows that $Q_2(N)$ is an abelian group, the direct product of cyclic groups of order 2.

Let $A'$ be the subgroup of $N$ consisting of all elements of $N$ of the form $(e, \tau)$. Then $Q_2(A')$ is a subgroup of $Q_2(N)$. There exists a subgroup $\overline{A}$ of $Q_2(N)$ such that $Q_2(N)$ is the direct product of $\overline{A}$ and $Q_2(A')$:

$$Q_2(N) = \overline{A} \times Q_2(A').$$

Now we let $\overline{N}$ be the subgroup of $N$ consisting of all elements with second component in $\overline{A}$. Then $N = \overline{N}A'$.

Now let $(e, \tau)$ be an element of $A'$. Then since $A' \subseteq N$, $(e, \tau)$ must commute with all elements of $N^*$ and hence $\tau$ must leave all elements of $Q_1(N^*)$ fixed. By (27), $Q_1(N^*) = Q_1(N)$ and hence $\tau$ leaves all elements of $Q_1(N)$ fixed.

Now $Q_2(N)$ is abelian. Hence $(e, \tau)$ belongs to the center of $N$. Thus $A'$ is contained in the center of $N$. Clearly $A' \cap \overline{N}$ consists of the identity alone. Hence $N$ is the direct product of $\overline{N}$ and $A'$:

$$N = \overline{N} \times A'. \tag{28}$$

We need now only show that $\overline{N}$ is abelian. To do this we need more information about the groups $G$ and $N$.

If $\lambda$ is the automorphism of $G$ such that $\lambda g = g^{-1}$ for all $g \in G$, then $\lambda$ leaves every element of order 2 fixed and belongs to the center of $A$. Hence $(e, \lambda)$ belongs to the centralizer of $N^*$, that is $(e, \lambda) \in N$. Hence $(e, \lambda) \in A'$.

Now suppose $(e, \phi) \in A'$, $\phi \neq I$. Then there is an automorphism of $N$, and hence an inner automorphism of $H$, sending $(e, \lambda)$ into $(e, \phi)$. But $\lambda$ is in the center of $A$. Hence $\phi = \lambda$. Therefore $A'$ has order 2 and consists of the two elements $e$ and $(e, \lambda)$.

Let $\xi$ be the element of $A$ such that $\xi\alpha = \alpha$, $\xi\beta = \beta^{-1}$, and $\xi f = f$ for all $f \in F$. Then $\xi$ leaves every element of $Q_1(N)$ and $G \cap N^*$ fixed. Let $(b, \tau)$ be any element of $N^*$ and $g$ an element of $G$. Now by Lemma 5, $\tau g/g \in G \cap N^*$. Hence $\xi(\tau g/g) = \tau g/g$ or $\xi\tau g = \xi g \tau g/g$. Clearly $\xi g/g$ is a square and hence an element of $G \cap N$. Now $(b, \tau)$ must commute with $\xi g/g$ and hence $\tau(\xi g/g) = \xi g/g$ or $\tau\xi g = \tau g \xi g/g$. Therefore $\xi\tau g = \tau\xi g$ for all $g \in G$ and hence $\xi\tau = \tau\xi$. It follows that $(e, \xi)$ commutes with all elements of $N^*$ and hence $(e, \xi) \in N$. Thus $(e, \xi) \in A'$. By definition $\xi \neq \lambda$. Hence $\xi = I$, and therefore $\beta^2 = e$. Now $a$ is an element of $G_t$ but not an element of $G_s$. Hence $G$ is not cyclic. It follows that $\beta \neq e$, and hence $\beta$ has order 2. Therefore $G \cap N = G_s$ has order 2 and consists of the two elements $e$ and $\alpha^2$. Clearly both elements of $G \cap N$ are left fixed by all $\phi \in A$. In particular, if $g \in G$, then $\sigma g/g \in G \cap N$ and hence

$$\phi(\sigma g/g) = \sigma g/g \tag{29}$$

for all $g \in G$, $\phi \in A$.

Since $a$ is not a square, we can choose a basis for $G$ that includes $a$. Suppose this basis contains another element of order 2, say $c$. Then there is a $\phi \in A$ such that $\phi a = a$, $\phi c = ac$, and hence $\phi^{-1}c = ac$. Now $N$ contains the element

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

It follows that $\phi\sigma\phi^{-1}$ is either $\sigma$ or $\sigma\lambda$. Now $\sigma\lambda c = \sigma c^{-1} = \sigma c$. Hence, using (29), we have

$$\sigma c = \phi\sigma\phi^{-1}c = \phi\sigma(ac) = \phi\{(ac)\sigma(ac)/(ac)\} = \sigma(ac)/a = \sigma c \sigma a/a \neq \sigma c,$$

a contradiction. Hence any basis for $G$ contains exactly one element of order 4 and exactly one element of order 2. Therefore $Q_1(N)$ has order 4. Since $\overline{N}$ does not contain any elements of the form $(e, \tau)$, $\tau \neq I$, it follows that $\overline{N}$ and $Q_1(N)$ have the same order, namely 4. Hence by (28) $N$ is the direct

product of a group of order 4 and a group of order 2. It follows that $N$ is abelian.

Thus an abelian group of order $2^m$ cannot have a holomorph isomorphic to the holomorph of a group that is not abelian. If we combine this fact with the results of §4 and §5 we obtain the following theorem.

THEOREM 3. *If a group $N$ has a holomorph isomorphic to the holomorph of a finite abelian group, then $N$ is abelian.*

Now in [5] it is shown that two finite abelian groups have isomorphic holomorphs if and only if they are isomorphic. Thus we have:

THEOREM 4. *If a finite abelian group $G$ and an arbitrary group $N$ have isomorphic holomorphs, then $G$ and $N$ are isomorphic.*

## REFERENCES

1. W. Burnside, *Theory of groups of finite order*, Cambridge, 1897.

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

3. ———, *Memoir on the substitution groups whose degrees do not exceed eight*, Amer. J. Math. vol. 21 (1899) pp. 287–337.

4. G. A. Miller, H. F. Blichfeldt, and L. E. Dickson, *Theory and applications of finite groups*, New York, 1938.

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

YALE UNIVERSITY,
NEW HAVEN, CONN.