MULTIPLE HOLOMORPHS OF FINITELY GENERATED ABELIAN GROUPS

BY

W. H. MILLS

The object of this paper is to determine all cases in which two or more finitely generated abelian groups have the same holomorph(1). Let G and G' be finitely generated abelian groups and let H be the holomorph of G. Then it will be shown that H is the holomorph of G' if and only if G' is an invariant maximal-abelian subgroup of H isomorphic to G. All such subgroups of H are determined. There are at most four. If G does not contain any elements of order 2, or if G has at least three independent generators of infinite order, then G itself is the only such subgroup(2).

1. **Definitions.** Let G be a group. If σ and τ are two automorphisms of G, then $\sigma\tau$ is defined to be the automorphism such that $(\sigma\tau)g=\sigma(\tau g)$ for all $g\in G$. Under this composition the automorphisms of G form a group A. Consider the set H of all pairs (g, σ), $g\in G$, $\sigma\in A$. We define a composition in H by

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

Under this composition the set H forms a group. If e is the identity of G and I is the identity of A, then (e, I) is the identity of H. Furthermore the inverse of (a, σ) is $(\sigma^{-1}a^{-1}, \sigma^{-1})$. The group H is called the holomorph(3) of G. The mapping $g\rightarrow(g, I)$ gives an imbedding of G in the group H. We identify the element g in G with the element (g, I) in H. Then G is an invariant subgroup of H. If G is abelian, then it is a maximal-abelian subgroup of H, that is, an abelian subgroup not properly contained in any abelian subgroup of H.

Received by the editors February 2, 1951.

(1) This problem was proposed by J. G. Wendel for the case of finite abelian groups. Wendel considered the group algebra of a finite abelian group G over the field of complex numbers. He then considered the group J of all norm preserving automorphisms of this group algebra, where the norm is the sum of the absolute values of the coefficients. Wendel then observed that the group J was the holomorph of G, and asked whether the group G was determined by the abstract group J. The methods of §2 are due, in part, to Wendel who first obtained the fundamental identity (6).

(2) This generalizes the results of G. A. Miller [1]. (Numbers in brackets refer to the references cited at the end of the paper.) Miller used the classical definition of the holomorph as the set of all permutations that transform a regular permutation group into itself. He determined all cases in which two or more isomorphic finite abelian groups have the same holomorph. A slight discrepancy between Miller's paper and this paper is due to the fact that different definitions of the holomorph are used.

(3) Various other definitions of the holomorph have been given. For example the holomorph of a group G is the group of transformations of G generated by the automorphisms of G and the left (or right) multiplications, $g\rightarrow ag$ $(g\rightarrow ga)$.

More generally, if η is any isomorphism of H onto a group H', and if G' is the image of G under this isomorphism, then H' is said to be the holomorph of G'.

2. **Several identities.** We shall now establish several identities for later use. Let H be the holomorph of an abelian group G, and let S be an invariant Abelian subgroup of H. Let (a, σ) be a fixed element of S, b an arbitrary element of G, and τ an arbitrary element of A. Since S is invariant,

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

Therefore, since S is commutative,

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

Comparing first components we obtain

$$a\sigma\tau a = \tau a\tau\sigma\tau^{-1}a. \tag{1}$$

Therefore

$$\text{if} \quad \tau a = a, \quad \text{then} \quad \sigma a = \tau\sigma a. \tag{2}$$

Let θ be the automorphism of G that sends each element into its inverse. Put $\lambda = \sigma^{-1}\theta$. Then, since σ and θ both commute with σ, it follows that $\lambda\sigma\lambda^{-1} = \sigma$. Substituting $\tau = \lambda$ in (1) gives $e = \sigma^{-1}a^{-1}\sigma a$. Applying σ we obtain

$$\sigma^2 a = a. \tag{3}$$

Now S contains $(a, \sigma)(e, \lambda)(a, \sigma)(e, \lambda)^{-1} = (e, \sigma^2)$, $b^{-1}(a, \sigma)b(a, \sigma)^{-1} = \sigma b/b$, and hence $(\sigma a/a)^{-1}(a, \sigma)^2(e, \sigma^2)^{-1} = a^2$. We have established:

$$(e, \sigma^2) \in S, \quad \sigma b/b \in S, \quad \text{and} \quad a^2 \in S. \tag{4}$$

Furthermore S contains $(e, \tau)(\sigma b/b)(e, \tau)^{-1} = \tau(\sigma b/b)$. Now, since S is abelian, (a, σ) commutes with $\tau(\sigma b/b)$. It follows that

$$\sigma\tau(\sigma b/b) = \tau(\sigma b/b). \tag{5}$$

If we put $\tau = I$ in (5), then we obtain

$$\sigma(\sigma b/b) = \sigma b/b. \tag{6}$$

From (6) it follows, by induction on n, that

$$\sigma^n b = b(\sigma b/b)^n \tag{7}$$

and

$$(a, \sigma)^n = (a^n(\sigma a/a)^{n(n-1)/2}, \sigma^n), \tag{8}$$

for all positive integral n. Finally, comparing (3) and (7) we have

$$(\sigma a/a)^2 = e. \tag{9}$$

3. **Additional notation.** We shall now suppose that G and G' are finitely generated abelian groups with holomorphs H and H' respectively. Suppose that G is isomorphic to an invariant subgroup $\mathcal{G}$ of H', and that G' is isomorphic to an invariant subgroup $\mathcal{G}'$ of H. This condition is clearly satisfied if G and G' have isomorphic holomorphs.

Now since G and $\mathcal{G}'$ are finitely generated abelian groups, they can be written as direct products

$$G = G(\infty) \times G(p_1) \times \cdots \times G(p_M), \tag{10}$$

$$\mathcal{G}' = G'(\infty) \times G'(p_1) \times \cdots \times G'(p_M), \tag{11}$$

where $G(\infty)$ and $G'(\infty)$ are groups with no elements of finite order except for the identity; $p_1, \cdots, p_M$ are distinct primes; and $G(p_i)$ and $G'(p_i)$ consist of all elements, of G and $\mathcal{G}'$ respectively, whose orders are integral powers of p_i. By allowing the groups $G(p_i)$ and $G'(p_i)$ to contain only the identity, we can assume that the same primes occur in the decompositions (10) and (11), and that 2 is one of these primes. The groups $G(p_i)$ and $G'(p_i)$ are finite abelian invariant subgroups of H. We now put

$$\begin{gathered} F(\infty) = \prod_{i=1}^{M} G(p_i), \qquad F'(\infty) = \prod_{i=1}^{M} G'(p_i), \\ F(2) = G(\infty) \prod_{p_i \neq 2} G(p_i). \end{gathered} \tag{12}$$

Since the groups $G'(p_i)$ and $\mathcal{G}'$ are invariant abelian subgroups of H, it follows that the identities of §2 hold if (a, σ) is an element of one of these groups.

4. **Elements of maximal prime power order.** Let p be one of the primes $p_1, \cdots, p_M$. Let p^m and $p^{m'}$ be the maximal orders of the elements of $G(p)$ and $G'(p)$ respectively. We need the following:

LEMMA 1. *If $(a, \sigma) \in \mathcal{G}'$, $b \in G(p)$, and $m \geqq 1$, then $(\sigma b/b)^{p^{m-1}} = e$.*

Proof. Since $b \in G(p)$, it follows that $\sigma b/b \in G(p)$, and therefore $(\sigma b/b)^{p^m} = e$. Suppose $(\sigma b/b)^{p^{m-1}} \neq e$. Then $b^{p^{m-1}} \neq e$. Hence b and $\sigma b/b$ are both elements of $G(p)$ of maximal order. Therefore there exists an automorphism $\tau \in A$ such that $\tau(\sigma b/b) = b$. By (5) we have $\sigma b = b$ or $\sigma b/b = e$, which implies that $(\sigma b/b)^{p^{m-1}} = e$.

LEMMA 2. $m = m'$.

Proof. Let (a, σ) be an element of $G'(p)$. Then

$$(a, \sigma)^{p^{m'}} = e = (e, I).$$

Comparing second components, we see that $\sigma^{p^{m'}} = I$. If $b \in G$, then from (7) we have $(\sigma b/b)^{p^{m'}} = e$. Hence $\sigma b/b \in G(p)$ and therefore $(\sigma b/b)^{p^m} = e$. Since b is an arbitrary element of G, (7) yields $\sigma^{p^m} = I$. Now by (8)

$$e = (a, \sigma)^{p^{m'+1}} = (a^{p^{m'+1}}(\sigma a/a)^{p^{m'+1}(p^{m'+1}-1)/2}, \sigma^{p^{m'+1}}) = a^{p^{m'+1}}.$$

Hence $a \in G(p)$. Therefore $a^{p^m} = e$. By Lemma 1 we have $(\sigma a/a)^{p^{m-1}} = e$ if $m \geqq 1$. It follows that

$$(13) \qquad (a, \sigma)^{p^m} = (\sigma a/a)^{p^m(p^m-1)/2} = e,$$

for any value of m. Now (13) holds for all $(a, \sigma) \in G'(p)$. Hence $m' \leqq m$. By symmetry $m \leqq m'$. Therefore $m' = m$.

Let $N(p)$ and $N'(p)$ denote the number of elements of $G(p)$ and $G'(p)$ respectively of maximal order p^m.

LEMMA 3. $N'(p) \geqq N(p)$.

Proof. If $m = 0$, then $G(p)$ and $G'(p)$ both consist of the identity alone, and $N'(p) = N(p) = 1$. We suppose that $m > 0$. Let (a, σ) be a fixed element of $G'(p)$ of order p^m. In the proof of Lemma 2 we established that $\sigma^{p^m} = I$ and $a^{p^m} = e$. If the order of σ is p^m, then by (7) there exists a $b \in G$ such that $\sigma b/b$ has order p^m. By (4), $\sigma b/b \in G'(p)$. Hence $G'(p)$ contains an element (a, σ) of order p^m, where $\sigma^{p^{m-1}} = I$. We distinguish two cases:

Case I. The order of a is p^m. Here we can choose $\tau_1, \tau_2, \cdots, \tau_{N(p)}$ so that $\tau_i a$ runs through the $N(p)$ elements of $G(p)$ of order p^m. Then

$$(14) \qquad (e, \tau_i)(a, \sigma)(e, \tau_i)^{-1} = (\tau_i a, \tau_i \sigma \tau_i^{-1})$$

are $N(p)$ distinct elements of $G'(p)$ of order p^m. Thus in this case $N'(p) \geqq N(p)$.

Case II. $a^{p^{m-1}} = e$. In this case we have, by (8),

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

Clearly $(\sigma a/a)^{p^{m-1}} = e$, and by (9) we have $(\sigma a/a)^2 = e$. It follows that $p = 2$ and $m = 2$. Furthermore the order of $\sigma a/a$ is exactly 2. Therefore the order of σ and the order of a are both 2. If a is a square, say $a = g^2$, then the order of $\sigma g/g$ is 4, which contradicts Lemma 1. Therefore a is not a square. Put $b = \sigma a/a$. If b is not a square, then there exists an automorphism τ such that $\tau(\sigma a/a) = \tau b = a$, and then (5) yields $\sigma a = a$, which is a contradiction. Therefore b is a square. Put $b = c^2$. Then the order of c is 4 and $\sigma a = ab = ac^2$. Let B_1 and B_2 be the cyclic groups generated by c and a respectively. We can write $G(2)$ as a direct product, $G(2) = B_1 \times B_2 \times \cdots \times B_t$, where the B_i are cyclic groups of order 2 and 4. We shall show that $t = 2$. Suppose $t \geqq 3$, and let d be a generator of B_3.

(i) Suppose d has order 4. Choose $\tau \in A$ such that $\tau a = a$, $\tau c = d$. Then by (2) we have $\sigma a = \tau\sigma a$, or $ac^2 = ad^2$, or $c^2 = d^2$, which is a contradiction. Therefore B_1 is the only one of the groups B_i of order 4.

Now let g and τ be arbitrary elements of G and A respectively. Then, since $\sigma^2 = I$, it follows that $(\sigma g/g)^2 = e$. By (5) we have $\sigma\tau(\sigma g/g) = \tau(\sigma g/g)$ and therefore $\tau(\sigma g/g) \neq a$. Since this is true for arbitrary τ, it follows that $\sigma g/g$ is either e or c^2. Therefore

$$\tau(\sigma g/g) = \sigma g/g \tag{15}$$

for all $g \in G$, $\tau \in A$. Hence (1) yields

$$\sigma\tau a/\tau a = \tau(\sigma\tau^{-1}a/\tau^{-1}a) = \sigma\tau^{-1}a/\tau^{-1}a. \tag{16}$$

(ii) Suppose d has order 2. Choose τ such that $\tau a = d$, $\tau^{-1}a = ad$. Then from (16) we have $\sigma d/d = \sigma(ad)/(ad) = c^2\sigma d/d$, or $c^2 = e$, a contradiction. Therefore $t = 2$ and $G(2) = B_1 \times B_2$. Hence $N(2) = 4$.

Now $\sigma(ac)/(ac) = c^2\sigma c/c$, and $\sigma c/c$ is either e or c^2. By replacing, if necessary, c by ac we can assume that $\sigma c = c$. Now choose $\xi \in A$ such that $\xi c = ac$, $\xi a = a$, and $\xi f = f$ if $f \in F(2)$. Put $\rho = \xi\sigma\xi^{-1}$. Then $\rho a = ac^2$ and $\rho c = c^3$. Clearly $\rho \neq \sigma$, and therefore

$$\begin{gathered} (a, \sigma), \qquad (a, \sigma)^3 = (ac^2, \sigma), \\ (e, \xi)(a, \sigma)(e, \xi)^{-1} = (a, \rho), \\ (a, \rho)^3 = (ac^2, \rho) \end{gathered} \tag{17}$$

are four distinct elements of $G'(2)$ of order 4. It follows that $N'(2) \geqq 4 = N(2)$. This completes the proof of Lemma 3.

By symmetry we have $N(p) \geqq N'(p)$. Thus we have:

LEMMA 4. $N'(p) = N(p)$.

We shall now re-examine the two cases of Lemma 3 in the light of Lemma 4.

5. **The case p odd.** If $p \neq 2$, then Case II is impossible and we have only Case I left. Then we have $(a, \sigma) \in G'(p)$ where a is of order p^m. Since $G'(p)$ is an invariant abelian subgroup of H, we can apply (4), and hence $a^2 \in G'(p)$. Since a is an element of odd order, it follows that $a \in G'(p)$. Therefore $(e, \tau)a(e, \tau)^{-1} = \tau a \in G'(p)$ for all $\tau \in A$. Now the elements τa generate $G(p)$. Hence $G(p) \subseteq G'(p)$. By symmetry $G'(p) \subseteq G(p)$. Thus we have proved:

LEMMA 5. *If $p \neq 2$ then $G'(p) = G(p)$.*

6. **The case $p = 2$.** We write $G(\infty)$ and $G(2)$ as the direct product of fixed nontrivial cyclic groups:

$$G(\infty) = G_1 \times G_2 \times \cdots \times G_k, \qquad G(2) = C_1 \times C_2 \times \cdots \times C_t$$

where $k \geqq 0$, $t \geqq 0$, and the order of C_i is greater than or equal to that of C_{i+1}. Let g_i be a generator of the group G_i. Let α and β be generators of C_1 and C_2 respectively, and let u, v, and w be the orders of C_1, C_2, and C_3 respectively. If $t < 3$ it is understood that $w = 1$; if $t < 2$, that $v = 1$, $\beta = e$; and if $t = 0$, that $u = 1$, $\alpha = e$. Then u, v, and w are powers of 2 and $u \geqq v \geqq w$. We put

$$F_j = \prod_{i=j+1}^{t} C_i, \qquad j = 1, 2,$$

where, if $t \leqq j$, F_j is understood to consist of the identity alone.

Suppose $p=2$. Then $2^m=u$. If $u=1$ then $G'(2)=G(2)$ trivially. We suppose that $u>1$. We have either Case I or Case II.

Case I. $G'(2)$ contains an element (a, σ) of order u, where a has order u and $\sigma^{u/2}=I$. Here the $N(2)$ elements (14) constitute the entire set of elements of $G'(2)$ of order u. Now every element of $G(2)$ of order u occurs once and only once as the first component of one of the elements (14). Therefore $G'(2)$ contains an element of order u with α as its first component, say (α, ψ). Furthermore if (α_1, σ_1) and (α_1, σ_2) are elements of $G'(2)$ of order u with the same first component, then $\sigma_1=\sigma_2$ and the order of α_1 is u. In particular if τ is an automorphism of G such that $\tau\alpha=\alpha$, then $(e, \tau)(\alpha, \psi)(e, \tau)^{-1}=(\alpha, \tau\psi\tau^{-1})$ and (α, ψ) are such elements, and hence $\tau\psi\tau^{-1}=\psi$. Thus we have

$$\text{(18)} \qquad \text{if} \quad \tau\alpha = \alpha, \quad \text{then} \quad \tau\psi = \psi\tau.$$

Suppose $(e, \tau) \in G'(2)$. Then it follows that the order of (e, τ) is less than u, and hence the order of $(\alpha, \psi)(e, \tau)=(\alpha, \psi\tau)$ is u. Therefore $\psi\tau=\psi$ or $\tau=I$. Combined with Lemma 5 this yields:

LEMMA 6. *If Case* I *holds for $p=2$, then $F'(\infty)$ contains no elements of the form (e, τ), $\tau \neq I$.*

In particular (4) gives us $(e, \psi^2) \in G'(2)$ and hence $\psi^2=I$. Then (7) yields $(\psi g/g)^2=e$ for all $g \in G$.

Suppose first that k, the number of independent generators of infinite order, is positive. Put $h=\psi g_1/g_1$. Then $\psi g_1=g_1h$, $h^2=e$, and hence $h \in G(2) \subseteq F(\infty)$. Let f be either an element of $F(\infty)$ or one of the infinite generators g_i, $i \geqq 2$. Then we can choose τ such that $\tau g_1=g_1f$ and $\tau b=b$ if $b \in F(\infty)$. Then by (18) we have $\tau\psi=\psi\tau$. Now $\psi\tau g_1=\psi(g_1f)=g_1h\psi f$, and $\tau\psi g_1=\tau(g_1h) =g_1hf$. Hence $\psi f=f$.

If $k \geqq 2$, then $\psi g_i=g_i$ if $i \geqq 2$, and by interchanging the roles of g_1 and g_2 we have $\psi g_1=g_1$. Also, since $\psi f=f$ if $f \in F(\infty)$, we have $\psi=I$, and hence $G(2) \subseteq G'(2)$. Since $N'(2)=N(2)$, it follows that $G(2)=G'(2)$.

If $k=1$ then we have $\psi f=f$ for all $f \in F(\infty)$, and we need only determine $\psi g_1=g_1h$. Now if $\tau\alpha=\alpha$ and $\tau g_1=g_1$, then

$$g_1\tau h = \tau(g_1h) = \tau\psi g_1 = \psi\tau g_1 = \psi g_1 = g_1h.$$

Thus $\tau h=h$ for all τ for which $\tau\alpha=\alpha$, $\tau g_1=g_1$. Since $h^2=e$ this is possible if and only if $h=\alpha^q$, where $q=0$ or $q=u/2$. By (4), $h=\alpha^q \in G'(2)$. If $q=u/2$ then $\alpha \notin G'(2)$ and hence $u>2$. Thus q is even. If $b \in G(2)$ let ψ_b be the automorphism such that

$$\text{(19)} \qquad \psi_b g_1 = g_1 b^q, \quad \text{and} \quad \psi_b f = f \qquad \text{if} \quad f \in F(\infty).$$

Now (α, ψ) and its conjugates generate $G'(2)$. It follows that $G'(2)$ consists of the elements (b, ψ_b), $b \in G(2)$. In this case $G'(2)$ is isomorphic to $G(2)$.

Finally suppose $k=0$. By (18) we see that $\tau\psi\alpha=\psi\alpha$ for all τ for which $\tau\alpha=\alpha$. This can be true only if $\psi\alpha$ is a power of α, say

$$\psi\alpha = \alpha^r, \qquad 1 \leqq r < u. \tag{20}$$

Now we know that $(\psi\alpha/\alpha)^2=e$ or $\alpha^{2(r-1)}=e$. It follows that either $r=1$ or $r=1+u/2$. If $u=2$, then of necessity $r=1$. If $u=4$ then $e\neq(\alpha, \psi)^2=\alpha^{1+r}$. Hence $r=1$ here also. Thus we have:

$$\text{If } u \leqq 4, \text{ then } r = 1. \quad \text{If } u > 4, \text{ then } r = 1 \quad \text{or } r = 1 + u/2. \tag{21}$$

Now if $\tau\alpha=\alpha$ and $\tau\beta=\beta$, then $\tau\psi\beta=\psi\tau\beta=\psi\beta$. Therefore $\psi\beta=\alpha^s\beta^R$ for suitable s and R, where we can suppose $0\leqq s<u$. If $f=\alpha^{u/v}$ or if $f\in F_2$ we can choose τ such that $\tau\alpha=\alpha$, $\tau\beta=\beta f$. Then by (18), $\psi\tau=\tau\psi$. Now $\psi\tau\beta=\psi(\beta f)=\alpha^s\beta^R\psi f$, and $\tau\psi\beta=\tau(\alpha^s\beta^R)=\alpha^s\beta^R f^R$. Thus

$$\psi f = f^R. \tag{22}$$

Now $f=\alpha^{u/v}$ gives $\alpha^{ru/v}=\alpha^{Ru/v}$, whence $r\equiv R(\bmod v)$. Thus we have $\beta^r=\beta^R$ and without loss of generality we can suppose that $R=r$. Now $(\psi\beta/\beta)^2=e$ and hence $\alpha^{2s}{}^2\beta^{(r-1)}=e$, which yields $\alpha^{2s}=e$. Hence we have

$$\psi\beta = \alpha^s\beta^r, \text{ where } s = 0 \text{ or } s = u/2. \tag{23}$$

Also from (22) if $f\in F_2$, then $\psi f=f^r$. Now if $v=w$ we can interchange the roles of C_2 and C_3 to obtain $\psi\beta=\beta^r$, or $s=0$.

$$\text{If } v = w, \text{ then } s = 0. \tag{24}$$

Now choose τ such that $\tau\alpha=\alpha\beta$, $\tau\beta=\beta$. Then $\tau^{-1}\alpha=\alpha/\beta$ and (1) gives $\alpha\psi(\alpha\beta)$ $=\alpha\beta\tau\psi(\alpha/\beta)$ or

$$\alpha^{1+r+s}\beta^r = \alpha^{1+r-s}\beta^{1-s}.$$

Since $\alpha^{2s}=e$ we have $\beta^r=\beta^{1-s}$ or $\beta^{r-1}=\beta^{-s}=\beta^s$. Therefore

$$\text{if } u = v, \text{ then } s = r - 1. \tag{25}$$

Since $u\geqq v\geqq w$, it follows from (24) and (25) that if $u=w$, then $s=0$ and $r=1$. If $u>w$ and if $f\in F_2$, then $\psi f=f^r=f$. Hence in any case

$$\text{if } f \in F_2, \text{ then } \psi f = f^r = f. \tag{26}$$

By (10) and (12), $G=G(2)\times F(2)$ and every element of $F(2)$ has odd order. Hence

$$\text{if } f \in F(2), \text{ then } \psi f = f. \tag{27}$$

We note that r and s determine ψ completely. We have four possibilities:

(i) $r=1$, $s=0$. This is possible for all values of u, v, and w.

(ii) $r=1$, $s=u/2$. By (24) and (25) this is possible only if $u>v>w$.

(iii) $r=1+u/2$, $s=0$. By (21) and (25) we have $u>v$, $u>4$.

(iv) $r=1+u/2$, $s=u/2$. By (21) and (24) we have $u>4$, $v>w$.
In other words:

(A) If $u=v=w$; $u=v\leqq 4$; or if $u\leqq 4$ and $v=w$; then $r=1$, $s=0$.

(B) If $u=4$, $v=2$, $w=1$; $r=1$, and $s=0$ or $s=u/2$.

(C) If $u>v=w$ and $u>4$; then $s=0$, and $r=1$ or $r=1+u/2$.

(D) If $u=v>w$ and $u>4$; then $r=1$ and $s=0$, or $r=1+u/2$ and $s=u/2$.

(E) If $u>v>w$ and $u>4$; then $r=1$ or $r=1+u/2$, and $s=0$ or $s=u/2$.

Now if $f\in F_1$ we can choose $\phi\in A$ such that $\phi\alpha=\alpha f$, and $\phi g=g$ if $g\in F_1$ or if $g\in F(2)$. Then $G'(2)$ contains $(e,\phi)(\alpha,\psi)(e,\phi)^{-1}$. Therefore $G'(2)$ also contains

$$(e,\psi)(\alpha,\psi)^{-1}(e,\phi)(\alpha,\psi)(e,\phi)^{-1}(e,\psi)^{-1} = (f,\phi\psi\phi^{-1}\psi^{-1}).$$

If $f\in F_2$ then $\phi\psi=\psi\phi$ and hence $f\in G'(2)$. Therefore $F_2\subseteq G'(2)$. Now put $f=\beta$ and $\omega=\phi\psi\phi^{-1}\psi^{-1}$. Then $(\beta,\omega)\in G'(2)$ and

$$\begin{aligned} \omega\alpha &= \alpha^{1+s}\beta^{s}, \qquad \omega\beta = \beta^{1+s}, \\ \omega g &= g \text{ if } \quad g\in F_2 \quad \text{or if } g\in F(2). \end{aligned} \tag{28}$$

On the other hand, let $G(2,r,s)$ be the group generated by (α,ψ), (β,ω), and the elements of F_2, where ψ and ω are defined by (20), (23), (26), (27), and (28). Then if $k=0$, $G'(2)$ is one of the groups $G(2,r,s)$, where the possible values of r and s are given by (A), (B), (C), (D), and (E). We note that this holds whether or not $u=1$. If $u=4$, $v=2$, and $w=1$, then Case II leads to one additional possibility.

Case II. $a^{u/2}=e$, $\sigma^{u/2}=I$. Here we have $u=2^m=4$, $v=2$, and $w=1$. Furthermore $N'(2)=N(2)=4$. The four elements (17) are the only elements of $G'(2)$ of order 4.

Suppose $k\geqq 1$ and put $h=\sigma g_1/g_1$. Then $h^2=e$ and (15) gives us $\tau h=h$ for all $\tau\in A$. Furthermore

$$\rho g_1 = \xi\sigma\xi^{-1}g_1 = \xi\sigma g_1 = \xi(g_1h) = g_1h = \sigma g_1.$$

Choose τ so that $\tau f=f$ if $f\in F(\infty)$ and $\tau g_1=g_1a$. Then $(e,\tau)^{-1}(a,\sigma)(e,\tau)=(a,\tau^{-1}\sigma\tau)$ is an element of $G'(2)$ of order 4. Hence $\tau^{-1}\sigma\tau$ is either σ or ρ. Therefore

$$g_1h = \tau^{-1}\sigma\tau g_1 = \tau^{-1}\sigma(g_1a) = \tau^{-1}(g_1hac^2) = g_1hc^2,$$

which is a contradiction. Therefore $k=0$, and G is a finite group in this case.

The four elements (17) generate a group of order 8 isomorphic to $G(2)$. This group must be $G'(2)$. Moreover (a,σ) and $(e,\sigma\rho)$ are a set of independent generators of this group. Furthermore $\alpha^2=c^2$ and β must be either a or ac^2. Therefore $G'(2)$ contains the elements (β,σ) and (β,ρ). Also $\sigma\beta=\rho\beta=\beta c^2=\beta\alpha^2$. Let ψ be the automorphism such that

$$\psi\alpha = \alpha, \quad \psi\beta = \beta\alpha^2, \quad \text{and} \quad \psi f = f \text{ if } f\in F(2). \tag{29}$$

Then $\psi=\sigma$ or $\psi=\rho$. Hence $(\beta, \psi)\in G'(2)$. Now if we put $\omega=\sigma\rho$, then

$$(30) \qquad \omega g = g^3 \quad \text{if} \quad g \in G(2), \qquad \omega f = f \text{ if } f \in F(2).$$

Then we see that (β, ψ) and (e, ω) are a set of independent generators of $G'(2)$.

On the other hand if $u=4$, $v=2$, and $w=1$, let ψ and ω be defined by (29) and (30). Then let $\overline{G}(2)$ be the group generated by (α, ψ) and (e, ω). We see that if Case II holds, then $p=2$, $k=0$, and $G'(2)=\overline{G}(2)$. Thus in all cases we have:

LEMMA 7. *$G'(2)$ is isomorphic to $G(2)$.*

7. **The groups $G(\infty)$ and $G'(\infty)$.** We shall now study the group $G'(\infty)$. We let k and k' be the number of independent generators of $G(\infty)$ and $G'(\infty)$ respectively. If $k=0$, then G is a finite group, H is a finite group, and hence $\mathcal{G}'$ is a finite group. Thus when $k=0$, it follows that $k'=0$, and $G'(\infty)=G(\infty)$ since both groups consist of the identity alone. We now suppose that $k>0$. Then clearly $k'>0$. Let (a, σ) be an element of $\mathcal{G}'$ of infinite order. Then either a or σ has infinite order. If a has infinite order then, by (4), a^2 is an element of $\mathcal{G}'$ of infinite order. If σ has infinite order, then there exists an element $b\in G$ such that $\sigma b/b$ has infinite order. By (4), $\sigma b/b\in\mathcal{G}'$. In either case $G\cap\mathcal{G}'$ contains an element g of infinite order. Let Q be the common maximal order of the elements of $F(\infty)$ and $F'(\infty)$. Then $g^Q\in G(\infty)\cap G'(\infty)$. Now g^Q and its conjugates form a subgroup of $G(\infty)$ with k independent generators. This subgroup is also a subgroup of $G'(\infty)$. Hence $k'\geqq k$. By symmetry $k\geqq k'$, and hence $k'=k$. Therefore $G'(\infty)$ is isomorphic to $G(\infty)$. This result, combined with Lemmas 5 and 7, proves the following:

THEOREM 1. *If G and G' are finitely generated abelian groups, each isomorphic to an invariant subgroup of the holomorph of the other, then G is isomorphic to G'.*

COROLLARY. *If G and G' are finitely generated abelian groups with isomorphic holomorphs, then G and G' are isomorphic.*

8. **Multiple holomorphs.** Let H and H^* be the holomorphs of the groups G and G^* respectively. Suppose that H and H^* are isomorphic and that η' is an isomorphism of H^* onto H. Put $G'=\eta'G^*$, the image of G^* under the isomorphism η'. We can regard H as the holomorph of G'. Thus H is simultaneously the holomorph of G and G'. We call H a multiple holomorph(4) of the groups G and G'.

Now suppose that H is a multiple holomorph of the finitely generated

(4) This definition differs from the definition of G. A. Miller [1]. Miller defined the multiple holomorph of G as the group obtained from H by adjoining certain elements that transform G into its conjugates.

abelian groups G and G'. Then by the corollary to Theorem 1, G and G' are isomorphic. Hence there is an automorphism η of H that sends G onto G'. Furthermore G' is an invariant maximal-abelian subgroup of H isomorphic to G. We shall now determine all such subgroups of H.

9. **Invariant maximal-abelian subgroups.** Let G be any finitely generated abelian group with holomorph H, and $\mathcal{G}$ be any invariant abelian subgroup of H isomorphic to G. Then by putting $G'=\mathcal{G}'=\mathcal{G}$ we can apply the results and notations of the preceding sections.

Suppose first that $k=0$. Then $\mathcal{G}$ is the product of the groups $G'(p)$. When $p\neq 2$, then $G'(p)=G(p)$. Hence $\mathcal{G}=G'(2)F(2)$. We put $G(r, s)=G(2, r, s)F(2)$ and $\overline{G}=\overline{G}(2)F(2)$. Then we see that $\mathcal{G}$ is either $\overline{G}$ or one of the groups $G(r, s)$. We note that $\overline{G}$ is defined only if $u=4$, $v=2$, and $w=1$. The possible values of r and s are given by (A) through (E). It can be easily shown that the groups $\overline{G}$ and $G(r, s)$ are invariant maximal-abelian subgroups of H, under the above mentioned restrictions.

Now we suppose that $k>0$. Suppose that $\mathcal{G}$ contains an element of the form (e, τ). As before we let Q be the common maximal order of the elements of $F(\infty)$ and $F'(\infty)$. Then if τ has infinite order, $(e, \tau)^Q$ adjoined to $G(\infty)\cap G'(\infty)$ gives a subgroup of $G'(\infty)$ with $k+1$ independent generators. Hence τ has finite order, and $(e, \tau)\in F'(\infty)$. Now since $k>0$, Case I holds for $p=2$, and by Lemma 6 we have $\tau=I$. We have proved:

Lemma 8. *If $k>0$, then $\mathcal{G}$ contains no elements of the form (e, τ), $\tau\neq I$.*

Let (a, σ) be any element of $\mathcal{G}$. By (4), $(e, \sigma^2)\in\mathcal{G}$, and Lemma 8 gives us $\sigma^2=I$. Let (a, τ) be another element of $\mathcal{G}$ with the same first component. Then $\mathcal{G}$ contains $(a, \sigma)^{-1}(a, \tau)=(e, \sigma^{-1}\tau)$. Therefore $\sigma=\tau$ by Lemma 8. Thus we have proved:

Lemma 9. *If $k>0$, $(a, \sigma)\in\mathcal{G}$, and $(a, \tau)\in\mathcal{G}$, then $\sigma=\tau$ and $\sigma^2=I$.*

It follows at once that if $(a, \sigma)\in\mathcal{G}$ and $g\in G$, then $\sigma g^2=g^2$. Hence (a, σ) commutes with g^2. We now impose the further condition on $\mathcal{G}$ that it be a maximal-abelian subgroup of H. Then we see that $g^2\in\mathcal{G}$ for all $g\in G$. Let K be the group of all elements of the form g^2f, $g\in G$, $f\in F'(\infty)$. Then K is a subgroup of $\mathcal{G}$ and an invariant subgroup of H.

Lemma 10. *If $k>0$, then K is a proper subgroup of $\mathcal{G}$.*

Proof. $\mathcal{G}$ is a maximal-abelian subgroup of H. Therefore it is sufficient to find an element (g, σ) that does not belong to K but that commutes with all elements of K. Since K does not contain any element with first coefficient g_1, it is sufficient to find an element (g_1, σ) that commutes with all elements of K. Now if $k\geqq 2$, then $G'(p)=G(p)$ for all p. Hence $F'(\infty)=F(\infty)$, $K\subseteq G$, and g_1 is an element with the desired properties. If $k=1$, then $G'(p)=G(p)$ for all $p\neq 2$, and $G'(2)$ consists of the elements (b, ψ_b), $b\in G(2)$, ψ_b defined by (19).

In this case let ν be the automorphism such that $\nu g = g^{1+q}$ if $g \in G(2)$, and $\nu f = f$ if $f \in F(2)$. Then (g_1, ν) is an element that commutes with all elements of K. This completes the proof of Lemma 10.

Let (g, σ) be an element of H that is not an element of K. We may suppose that $g = \prod g_i^{n_i}$, where each n_i is either 0 or 1. At least one of the n_i must be 1. Hence there exists a $\tau \in A$ such that $\tau g = g_1$. Hence $(e, \tau)(g, \sigma)(e, \tau)^{-1} = (g_1, \tau\sigma\tau^{-1})$ is an element of $\mathcal{G}$, but not of K. Without loss of generality let $g = g_1$. Now if $\tau g_1 = g_1$, then $(e, \tau)(g_1, \sigma)(e, \tau)^{-1} = (g_1, \tau\sigma\tau^{-1})$ and (g_1, σ) are both elements of $\mathcal{G}$. Hence, by Lemma 9, we see that

$$\text{(31)} \qquad \text{if} \quad \tau g_1 = g_1, \quad \text{then} \quad \tau\sigma = \sigma\tau.$$

Suppose $k \geqq 2$. Let $f \in F(\infty)$ or $f = g_j$, $j \neq 2$. Then there exists a $\tau \in A$ such that $\tau g_1 = g_1$, $\tau g_2 = f g_2$, and $\tau b = b$ if $b \in F(\infty)$. Then by (31) we have $\tau\sigma = \sigma\tau$. Now

$$\tau\sigma g_2 = \tau(g_2(\sigma g_2/g_2)) = f g_2(\sigma g_2/g_2) = f\sigma g_2,$$
$$\sigma\tau g_2 = \sigma(f g_2) = \sigma f \sigma g_2.$$

Hence $\sigma f = f$. In particular we see that $k \geqq 2$ implies that $\sigma f = f$ for all $f \in F(\infty)$.

If $k \geqq 3$, then $\sigma g_j = g_j$ for all $j \neq 2$. By interchanging the roles of g_2 and g_3 we can show that $\sigma g_2 = g_2$. Thus if $k \geqq 3$, then $\sigma = I$ and $\mathcal{G} = G$.

Let Z be the center of H. If $u = v$, then Z consists of e alone. If $u > v$, then Z consists of e and $\alpha^{u/2}$. We note that $Z \subseteq G(2)$ and that Z contains at most two elements. Z consists of all elements of $G(2)$ that are left invariant by all automorphisms of $G(2)$.

Now suppose that $k = 2$. Then $F'(\infty) = F(\infty)$. Furthermore $\sigma f = f$ for all $f \in F(\infty)$ and $\sigma g_1 = g_1$. Put $\sigma g_2 = g_2 h$. Then $h^2 = e$. Now if $\tau g_1 = g_1$ and $\tau g_2 = g_2$, then by (31), $\sigma\tau = \tau\sigma$ and

$$g_2 h = \sigma g_2 = \sigma\tau g_2 = \tau\sigma g_2 = \tau(g_2 h) = g_2 \tau h,$$

or $h = \tau h$. Therefore h is left invariant by all automorphisms of $G(2)$. It follows that $h \in Z$.

Now let z be an arbitrary element of Z and define σ_1 and σ_2 as follows:

$$\sigma_i f = f \quad \text{if} \quad f \in F(\infty), \qquad \sigma_i g_i = g_i,$$
$$\sigma_i g_j = g_j z \qquad \text{if } i \neq j.$$

Let $G(z)$ be the group generated by (g_1, σ_1), (g_2, σ_2) and the elements of $F(\infty)$. Then $G(z)$ is an invariant maximal-abelian subgroup of H isomorphic to G.

We see that if $k = 2$, then $\mathcal{G} = G(z)$ for suitable $z \in Z$.

Suppose $k = 1$. Then $G'(2)$ consists of the elements (b, ψ_b), $b \in G(^2)$, ψ_b defined by (19). Now $(g_1, \sigma)(b, \psi_b) = (b, \psi_b)(g_1, \sigma)$ since G' is commutative. Comparing the first components we get

$$g_1 \sigma b = b \psi_b g_1 = g_1 b^{1+q},$$

or $\sigma b = b^{1+q}$ for all $b \in G(2)$. If $c \in G(p)$, where $p \neq 2$, then $\sigma c = c$. Hence we need only determine σg_1. Put $\sigma g_1 = g_1 h$. Then $h^2 = e$. Now by (2) if $\tau g_1 = g_1$, then $\sigma g_1 = \tau \sigma g_1$ which implies that $g_1 h = \tau(g_1 h)$ or $h = \tau h$. Hence $h \in Z$.

On the other hand let $z \in Z$, and if $u \leqq 2$ let $q = 0$, if $u > 2$ let $q = 0$ or $q = u/2$. Let ψ_b be defined by (19) and σ by

$$\sigma g_1 = g_1 z, \qquad \sigma b = b^{1+q} \quad \text{if} \quad b \in G(2),$$
$$\sigma c = c \quad \text{if} \quad c \in G(p), \qquad p \neq 2.$$

Let $G(q, z)$ be the group generated by (g_1, σ); (b, ψ_b), $b \in G(2)$; and the elements of the groups $G(p)$, $p \neq 2$. Then $G(q, z)$ is an invariant maximal-abelian subgroup of H.

If $k = 1$, then $\mathcal{G}$ is of the form $G(q, z)$.

Thus we have determined the invariant maximal-abelian subgroups of H isomorphic to G. We see that there are at most four such subgroups. If G does not contain any elements of order 2, or if G contains at least three independent generators of infinite order, then G is the only such subgroup.

10. Groups with the same holomorph.

THEOREM 2. *If H is the holomorph of a finitely generated abelian group G, and if $\mathcal{G}$ is an invariant maximal-abelian subgroup of H isomorphic to G, then H is also the holomorph of $\mathcal{G}$.*

Proof. Clearly H is the holomorph of $\mathcal{G}$ if and only if there exists an automorphism η of H mapping G onto $\mathcal{G}$. We shall construct such an automorphism. In §9 it was shown that if $\mathcal{G} \neq G$, $\mathcal{G}$ must be one of the groups $\overline{G}$, $G(z)$, $G(q, z)$, or $G(r, s)$. We suppose first that $\mathcal{G}$ is one of the groups $G(z)$, $G(q, z)$, or $G(r, s)$. Then we note that every element of G occurs once and only once as the first component of an element of $\mathcal{G}$. If $g \in G$, let (g, σ_g) be the element of $\mathcal{G}$ with g as its first component. Now if $\tau \in A$, then

$$(e, \tau)(g, \sigma_g)(e, \tau)^{-1} = (\tau g, \tau \sigma_g \tau^{-1}) \in \mathcal{G}.$$

It follows that

$$\sigma_{\tau g} = \tau \sigma_g \tau^{-1}. \tag{32}$$

Let D be the group generated by the set of all elements of the form $\sigma_g h/h$, $g, h \in G$. Then it can be verified directly that if $d \in D$, then $d^2 = e$, $\sigma_g d = d$ for all $g \in G$, and $D \subseteq \mathcal{G}$. Put

$$\eta f = (f, \sigma_f) \tag{33}$$

if $f = g_i$, $f = \alpha$, $f = \beta$, $f \in F_2$, or if $f \in G(p)$, $p \neq 2$. It is clear that (33) determines an isomorphism η of G onto $\mathcal{G}$. For any $g \in G$, let $\eta g = (g^*, \tau_g)$. Then $g \rightarrow g^*$ is a one-to-one mapping of G onto itself and $g^*/g \in D \subseteq \mathcal{G}$ for all $g \in G$. Hence $(g/g^*)(g^*, \tau_g) = (g, \tau_g) \in \mathcal{G}$. It follows that $\tau_g = \sigma_g$ and $\eta g = (g^*, \sigma_g)$. Also if

$d \in D$ and if g and h are elements of G, then $(gd)^* = g^*d$, $d^* = d$, and $\sigma_g h^*/h^* = \sigma_g h/h$. Now

$$\eta(gh) = \eta g \eta h = (g^*, \sigma_g)(h^*, \sigma_h) = (g^*\sigma_g h^*, \sigma_g\sigma_h).$$

Therefore

$$(gh)^* = g^*\sigma_g h^* = g^*h^*(\sigma_g h^*/h^*) = g^*h^*(\sigma_g h/h).$$

Hence

$$g^*h^* = (gh)^*(\sigma_g h/h) = \{gh(\sigma_g h/h)\}^* = (g\sigma_g h)^*. \tag{34}$$

Now if $\mu \in A$, let μ^* be the mapping defined by $\mu^*g^* = (\mu g)^*$. Then μ^* is a one-to-one mapping of G onto itself. By (32) and (34)

$$\begin{aligned}(\mu g)^*(\mu h)^* &= (\mu g\sigma_{\mu g}\mu h)^* = (\mu g\mu\sigma_g h)^* = \{\mu(g\sigma_g h)\}^* \\ &= \mu^*(g\sigma_g h)^* = \mu^*(g^*h^*).\end{aligned}$$

Hence $\mu^* \in A$. It is easily shown that $\mu^{**} = \mu$ and that $\mu^*\nu^* = (\mu\nu)^*$. Hence the mapping $\mu \to \mu^*$ is an automorphism of A. Now the first component of $(e, \mu^*)(\eta h)(e, \mu^*)^{-1}$ is $\mu^*h^* = (\mu h)^*$. It follows that

$$(e, \mu^*)(\eta h)(e, \mu^*)^{-1} = \eta\mu h. \tag{35}$$

We now define $\eta(g, \mu) = \eta g(e, \mu^*)$. Clearly η is a one-to-one mapping of H onto itself, sending G onto $\mathcal{G}$. Furthermore by (35)

$$\begin{aligned}\eta(g, \mu)\eta(h, \nu) &= \eta g(e, \mu^*)\eta h(e, \nu^*) = \eta g\eta\mu h(e, \mu^*)(e, \nu^*) \\ &= \eta(g\mu h)(e, (\mu\nu)^*) = \eta\{(g, \mu)(h, \nu)\}.\end{aligned}$$

Hence η is an automorphism of H.

There remains the case $\mathcal{G} = \overline{G}$. Here $u = 4$, $v = 2$, $w = 1$, $k = 0$. Define

$$\eta\alpha = (\beta, \psi), \quad \eta\beta = (e, \omega), \quad \text{and} \quad \eta f = f \quad \text{if} \quad f \in F(2). \tag{36}$$

Then η is an isomorphism of G onto $\mathcal{G}$. We seek to extend η to an automorphism of H. Now A is the direct product of $A(2)$ and $A'(2)$, where $A(2)$ consists of those automorphisms leaving every element of $F(2)$ fixed, and $A'(2)$ consists of those automorphisms leaving every element of $G(2)$ fixed. Furthermore $A(2)$ is generated by ψ and an automorphism ζ of order 4 such that $\zeta\alpha = \alpha\beta$, $\zeta\beta = \alpha^2\beta$. It can be verified directly that (36),

$$\eta(e, \zeta) = (\alpha, \zeta), \qquad \eta(e, \psi) = (\alpha\beta, \psi),$$

and

$$\eta(e, \tau) = (e, \tau) \quad \text{if} \quad \tau \in A'(2)$$

determine an automorphism η of H mapping G onto $\mathcal{G}$. This completes the proof.

Corollary. *If H is the holomorph of a finite abelian group G, and if $\mathcal{G}$ is an invariant subgroup of H isomorphic to G, then H is also the holomorph of $\mathcal{G}$.*

Proof. It has been shown that under these conditions $\mathcal{G}$ is a maximal abelian subgroup of H. Hence Theorem 2 applies.

Theorem 2 and the corollary to Theorem 1 give us the following:

Theorem 3. *Let G and G' be finitely generated abelian groups and let H be the holomorph of G. Then H is the holomorph of G' if and only if G' is an invariant maximal-abelian subgroup of H isomorphic to G. If G is a finite group then H is the holomorph of G' if and only if G' is an invariant subgroup of H isomorphic to G.*

When either of the groups G and G' is not abelian the problem appears to be much more difficult. It is not true that two finite nonabelian groups with the same holomorph are isomorphic. For example if $n \geqq 3$, the dihedral and dicyclic groups of order $4n$ have the same holomorph.

References

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

2. 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.

Yale University,
New Haven, Conn.