ON THE GROUP OF ISOMORPHISMS OF A CERTAIN EXTENSION OF AN ABELIAN GROUP*

BY

LOUIS C. MATHEWSON

INTRODUCTION

In 1908 Professor G. A. Miller showed that "if an abelian group H which involves operators whose orders exceed 2 is extended by means of an operator of order 2 which transforms each operator of H into its inverse, then the group of isomorphisms of this extended group is the holomorph of H."† The present paper discusses an elaboration of the idea embodied in Professor Miller's thoerem, the successive developments taking an abelian group H each of more general type so that *in toto* it is proved that if G is formed by extending H which has operators of order > 2 by a *certain* operator from its group of isomorphisms which transforms every one of its operators into the same power of itself and which is commutative with no operator of odd order in it, then the group of isomorphisms of G is the holomorph of H, and is a complete group if H is of odd order. If H contains no operators of even order, the "certain operator" is any operator from the group of isomorphisms of H effecting the stated automorphism; if H contains no operator of odd order, the "certain operator" must transform every operator of H into its inverse; if H contains operators of both even and odd orders (a) the order of the automorphism of the operators of odd order effected by the extending operator is to be divisible by 2^n where H contains an operator of order 2^n but none of order 2^{n+1}, or else (b) the extending operator transforms into its inverse every one of H's operators whose order is a power of 2. Obviously it is not necessary that the extending operator be "from its group of isomorphisms," but that it have certain properties possessed by this operator; thus, besides effecting the automorphism required, its first power commutative with all the operators of H must be the identity (from which follows that its first power appearing in H is the identity).

The general method used in establishing each of the successive theorems is the same; two important steps in each proof are showing that H is character-

* Presented to the Society, September 5, 1917.

† Miller, The Philosophical Magazine, vol. 231 (1908), p. 224.

istic in G and that the group of isomorphisms of G contains an invariant subgroup simply isomorphic with H. Throughout the paper use is frequently made of properties of rational integers, these interrelationships being but simple illustrations of the comradeship existing between group theory and number theory. The group of isomorphisms is represented by I and a rational prime (odd unless otherwise specified) by p, and the statement "t transforms every operator of a group into the same power of itself, not the first power" means every operator except the identity.

THEORY

1. THEOREM 1. *If a group G is formed by extending a cyclic group H of order p^m (p an odd prime) by an operator from its group of isomorphisms which transforms every one of its operators into the nth power of itself where $n \not\equiv 1$, mod p, then the I of G is the holomorph of H and is a complete group.*

Let s be a generator of H and let r be the order of the extending operator t (note that r divides $\phi(p^m)$, $= p^{m-1}(p-1)$*); then r is the exponent to which n appertains, mod p^m [Note 1]; and t is from the central of the I of H.†

If s_j is any operator of H, $t^{-1} s_j t = s_j^n$, and ts_j effects the same automorphism of H as does t, while $t^a s_j$, $1 < a < r$ effects a different one. Moreover, ts_j is of order r, for

$$\begin{aligned}(ts_j)^r &= t^{r+1} \cdot t^{-r} s_j t^r \cdot \quad \cdots \quad \cdot t^{-2} s_j t^2 \cdot t^{-1} s_j t \cdot t^{-1} \ddagger \\ &= t (s_j^n)^{\frac{n^r-1}{n-1}} t^{-1} = [ts_j^n t^{-1}]^{\frac{n^r-1}{n-1}} \\ &= s_j^{\frac{n^r-1}{n-1}} \text{ (since } t^{-1} s_j t = s_j^n \text{ gives } s_j = ts_j^n t^{-1}) \\ &= 1 \text{ (since } n^r - 1 \equiv 0, \text{ mod } p^m \text{ and } n - 1 \not\equiv 0, \text{ mod } p\P).\end{aligned}$$

Furthermore, ts_j cannot be of order $< r$, for *if t is an operator from the I of a group H, no other operator effecting the same automorphism of H can be of lower order*, because the order of an operator in the I of a group must be exactly the order of the automorphism it effects. From these properties of ts_j it is evident that, as soon as H has been shown characteristic in G, in all the automorphisms of G t corresponds only to itself or to itself multiplied by some operator of H.

It will next be shown that the orders of the operators in the tail of G either divide r or divide p^m.§ Let $t^a s_j$ be such an operator, $1 \leqq a < r$ which is $\leqq \phi(p^m)$. The cases will be considered separately.

* Mathews, *Theory of Numbers* (1892), p. 18.

† Miller, these Transactions, vol. 1 (1900), p. 397.

‡ Miller, Blichfeldt, and Dickson, *Finite Groups* (1916), § 24.

¶ Cf. Gauss, *Disquisitiones Arithmeticæ* (1801), § 79.

§ Cf. Miller, these Transactions, vol. 4 (1903), p. 156.

Case I. If $n^a \not\equiv 1$, mod p, the order of $t^a s_j$ divides r.

$$(t^a s_j)^r = t^{a(r+1)} \cdot t^{-ra} s_j t^{ra} \cdot \quad \cdots \quad \cdot t^{-2a} s_j t^{2a} \cdot t^{-a} s_j t^a \cdot t^{-a}$$

$$= t^a (s_j^{n^a})^{\frac{n^{ra}-1}{n^a-1}} t^{-a} = [t^a s_j^{n^a} t^{-a}]^{\frac{n^{ra}-1}{n^a-1}}$$

$$= s_j^{\frac{n^{ra}-1}{n^a-1}}$$ (since $t^{-1} s_j t = s_j^n$ gives $t^{-a} s_j t^a = s_j^{n^a}$, whence $s_j = t^a s_j^{n^a} t^{-a}$)

$= 1$, because $n^r = 1$, mod p^m, so that $n^{ra} - 1$ is divisible by p^m while in this first case $n^a - 1$ is not divisible by p.

Case II. If $n^a \equiv 1$, mod p, the order of $t^a s_j$ divides p^m.

$$(t^a s_j)^{p^m} = t^a \cdot t^{-ap^m} s_j t^{ap^m} \cdot \quad \cdots \quad \cdot t^{-2a} s_j t^{2a} \cdot t^{-a} s_j t^a \cdot t^{-a}$$

$= t^a (s_j^{n^a})^{\frac{n^{ap^m}-1}{n^a-1}} t^{-a} = s_j^{\frac{n^{ap^m}-1}{n^a-1}} = 1$. For suppose p^b $(b > 0)$ is the highest power of p dividing $n^a - 1$; then $n^a \equiv 1$, mod p^b, and $(n^a)^{p^m} \equiv 1$, mod p^{m+b} [Note 2]. Hence,

$$\frac{n^{ap^m} - 1}{n^a - 1} \equiv 0, \qquad \text{mod } p^m.$$

NOTE 1. *If p is an odd prime and $n \not\equiv 1$, mod p, and if n appertains to the exponent q, mod p^m, then it appertains, mod p^{m+1}, to q or else to pq.*

Obviously the exponent to which n appertains, mod p^{m+1}, is not less than q. Let $n^q = l + kp^m$. Two cases will be made.

If $k \equiv 0$, mod p, evidently n appertains to the exponent q, mod p^{m+1}.

If $k \not\equiv 0$, mod p, let n appertain to exponent v, mod p^{m+1}, or $n^v = l + lp^{m+1}$.

Subtracting the preceding equation gives $n^q (n^{v-q} - 1) = (lp - k) p^m$. Since neither n^q nor $(lp - k)$ is divisible by p, $n^{v-q} - 1$ is divisible by p^m but not by p^{m+1}, so that $v - q \equiv 0$, mod q, or v is a multiple of q. On raising n^q to the ath power there results $n^{aq} = (l + kp^m)^a = l + akp^m + Np^{m+1}$ (where N is a positive integer). From the last member, evidently the first value a can take so that n^{aq} shall be $\equiv 1$, mod p^{m+1} is the value p. Hence the proposition.

COROLLARY. *If p is an odd prime and $n \not\equiv 1$, mod p, and if n appertains to the exponent q, mod p^m, then it appertains, mod p^{m-1}, to q or else to q/p.*

For the even prime it is similarly demonstrable that *if $n \equiv 1$, mod 2, and n appertains to the exponent 2^u, mod 2^m, then it appertains, mod 2^{m+1}, to 2^u or else to 2^{u+1}.*

COROLLARY. *If $n \equiv 1$, mod 2, and if n appertains to the exponent 2^u, mod 2^m, then it appertains, mod 2^{m-1}, to 2^u or else to 2^{u-1}.*

NOTE 2. *If $d \equiv 1$, mod p^e, where p is an odd prime $(e > 0)$, then $d^{p^m} \equiv 1$, mod p^{e+m}.* This is readily established by mathematical induction. It is evidently true for $m = 0$. Assume true for mth power of p; i. e., $d^{p^m} = 1 + kp^{e+m}$. Raising to the pth power gives $d^{p^{m+1}} = 1 + (k + M) p^{e+m+1}$, ($M$ is an integer divisible by p) or $d^{p^{m+1}} \equiv 1$, mod p^{e+m+1}. Hence the truth of the proposition.* Furthermore, if p^e is the highest power of p dividing $d - 1$, then p^{e+m} is the highest power of p dividing $d^{p^m} - 1$; because, if mathematical induction is again employed, it will be observed that k would be prime to p while M is a multiple of p.

The proof is similar for the even prime that *if $d \equiv 1$, mod 2^e, $(e > 0)$, then $d^{2^m} \equiv 1$, mod 2^{e+m}.* Similarly, if 2 is the highest power of 2 dividing $d - 1$, then $d^{2^m} - 1$ $(m > 0)$, is divisible by at least 2^{m+2}; and if 2^e, $e > 1$, is the highest power of 2 dividing $d - 1$, then 2^{e+m} is the highest power of 2 dividing $d^{2^m} - 1$, $(m \geqq 0)$.

* Cf. Dirichlet, *Vorlesungen über Zahlentheorie* (1879), p. 333.

From the preceding it is further evident that if $r \geqq p-1$, a can always take a value such that $n^a \equiv 1$, mod p. Then when s_j is of order p^m, or is s, $t^a s$ will likewise be of order p^m; because (as has just been shown) its order divides p^m, and its p^{m-1}th power is

$$(t^a s)^{p^{m-1}} = t^{ap^{m-1}} \cdot t^a (s^{n^a})^{\frac{n^{ap^{m-1}}-1}{n^a-1}} t^{-a} = t^{ap^{m-1}} s^{\frac{n^{ap^{m-1}}-1}{n^a-1}},$$

in which $(n^{ap^{m-1}} - 1)/(n^a - 1)$ is divisible by p^{m-1} but not by p^m. [Note 2.]

Next, in order to show that H is characteristic in G it will be proved that the cyclic subgroup of order p^m generated by an operator of order p^m, such as $t^a s$, from the tail of G is not an invariant subgroup of G. (Note that in $t^a s$, s is of order p^m and $n^a \equiv 1$, mod p.) Transforming by t should, if this subgroup is invariant in G, give an operator commutative with $t^a s$; i. e., $t^{-1}(t^a s)t = t^a s^n$, which if commutative with $t^a s$, requires that $t^a s t^a s^n = t^a s^n t^a s$, or $s t^a s^n = s^n t^a s$, or $t^a s^{n-1} = s^{n-1} t^a$. But this cannot be satisfied since the rth power of t is the first power of t commutative with s and since by hypothesis $n - 1$ is not divisible by p. Accordingly, H is the only invariant cyclic subgroup of order p^m in G and is therefore characteristic.

Since any automorphism of G is determined by an automorphism of the characteristic subgroup H and some one of the p^m operators of order r (that is, t, ts, ts^2, etc.), the I of G can be represented as a transitive substitution group on p^m letters. Now the I of G contains an invariant cyclic subgroup E simply isomorphic with H. For, suppose v is an operator from the I of G leaving the operators of H invariant but transforming t into ts, where s is of order p^m. Then $v^{-1} t v = ts$ gives $v^{-2} t v^2 = ts^2$, etc., from which it is seen that v is of the same order as s. Hence E is a cyclic subgroup of order p^m.

The characteristic subgroup H can be automorphic exactly as any cyclic group of order p^m, because t transforms every operator of H into the same power of itself and because the first power of t appearing in H is the identity. Hence, the order of the I of G is equal to the order of H multiplied by the order of its own group of isomorphisms, which product is the order of the holomorph of H.* Furthermore, since the I of G contains an invariant cyclic subgroup of order p^m and can be written transitively on p^m letters, it is simply isomorphic with the holomorph of H. This last point can be proved directly by showing that operators effecting automorphisms of the characteristic subgroup H, transform the operators of the invariant cyclic subgroup E in exactly the same way. Since H is of odd order, the I of G has the interesting property of being complete, since " the holomorph of any abelian group of odd order is a complete group."†

2. If the order of the cyclic group H is $2p^m$, H contains a characteristic

* Miller, Blichfeldt, and Dickson, loc. cit., p. 46.

† Miller, Mathematische Annalen, vol. 66 (1908), p. 135.

operator of order 2, furthermore G (formed by extending H by an operator from its group of isomorphisms which transforms every one of its operators of order > 2 into the nth power of itself where $n \not\equiv 1$, mod p) would be the direct product of two characteristic subgroups having only the identity in common, one this group of order 2 and the other the non-abelian group formed by extending the cyclic subgroup (of H) of order p^m. The I of this G is thus the holomorph of H.*

3. Now a cyclic group H of order > 2 can be extended by an operator of order 2 which transforms its operators into their inverses, and the group of isomorphisms of the extended group is the holomorph of H. If h (which is the order of the group H) is a number > 6 and has primitive roots, evidently H can be extended by operators from its group of isomorphisms that will transform every operator of order > 2 into the same power of itself other than into its inverse. To have primitive roots h must be of the form 2, 4, p^m, or $2p^m$ (p an odd prime).† As the case $h = 2$ is trivial and $h = 4$ comes under the theorem on inverses, h will be considered to be one of the other forms; that is, $h = p^m$ or $2p^m$. Then since a primitive root n of h ($m > 1$) is a primitive root of all powers of p,‡ the following may be based upon what has just been proved or can be proved independently:

COROLLARY. *If a group G is formed by extending a cyclic group H whose order $h = p^m$ or $2p^m$ by an operator from its group of isomorphisms which transforms every one of its operators of order > 2 into the nth power of itself where n is a primitive root of h, then the I of G is simply isomorphic with G, moreover G is complete if $h = p^m$.*

Here n appertains to the exponent $\phi(h)$, mod h; hence r, the order of the extending operator t, is $\phi(h)$, and the order of G is $h\phi(h)$ so that G itself is seen to be the holomorph of H. H is the only invariant cyclic subgroup of order h in G and is therefore characteristic. If $h = p^m$, G is the holomorph of an abelian group of odd order which is characteristic in it, and hence G is complete.§

4. In case the cyclic group H is of order 2^m ($m > 1$) and $n \equiv 1$, mod 2, r, the order of the extending operator t from the group of isomorphisms of H, divides $\phi(2^m) = 2^{m-1}$ (and if $m > 2$, r is not greater than 2^{m-2}).‖ The attempt to establish a general theorem analogous to the preceding by a similar

* Miller, these Transactions, vol. 1 (1900), p. 396.

† Mathews, loc. cit., §§ 19–29.

‡ Lebesgue, Journal de Mathematiques, vol. 19 (1854), p. 334; cf. also Dirichlet, loc. cit., p. 334.

§ Burnside, *Theory of Groups* (1897), § 169; cf. Miller, Mathematische Annalen, vol. 66 (1908), p. 135.

‖ Weber, *Lehrbuch der Algebra*, Bd. II (1899), § 17; cf. Burnside, loc. cit., also Miller, Bulletin of the American Mathematical Society, vol. 7 (1901), p. 351.

method fails because ts (where s is a generator of H) is not of the same order as t, excepting in the case $t^{-1}st = s^{-1}$, when G is dihedral.* For, suppose $t^{-1}st = s^n$ where the order of t is 2^u, so that n appertains to 2^u, mod 2^m (whence $u < m$). It will be shown that ts is of order 2^u when and only when $n = 2^m - 1$, which means that t transforms the operators of H into their respective inverses so that its order is 2 and $u = 1$.

$$(ts)^{2u} = t \cdot t^{-2u} st^{2u} \cdot \cdots \cdot t^{-2} st^2 \cdot t^{-1} st \cdot t^{-1}$$

$$= t(s^n)^{\frac{n^{2u}-1}{n-1}} t^{-1} = s^{\frac{n^{2u}-1}{n-1}},$$

which if equal to the identity, requires that $(n^{2u} - 1)/(n - 1)$ be congruent to zero, mod 2^m. In Note 3 it is shown by number theory that this is true when and only when $n = 2^m - 1$. It may be observed, however, that by use of Note 2 it can be proved easily that the order of $t^a s^c$ divides 2^m.

5. It is now an easy step from Theorem 1 to the following (in which p still represents an odd prime):

THEOREM 2. *If a group G is formed by extending an abelian group H of order p^m, type $(m_1, m_2, \cdots, m_k)$, $m_1 \geqq m_2 \geqq \cdots \geqq m_k$, $m = m_1 + m_2 + \cdots + m_k$, by an operator from its group of isomorphisms which transforms every one of its operators into the nth power of itself where $n \not\equiv 1$, mod p, then the I of G is the holomorph of H and is a complete group.*

NOTE 3. *If n appertains, mod 2^m, to 2^u $(u > 0)$, then a necessary and sufficient condition that*

$$\frac{n^{2^u} - 1}{n - 1} \equiv 0,$$

mod 2^m, is that $n = 2^m - 1$. (It is supposed that $m > 1$, that n is odd and $0 < n < 2^m$).

If $n = 2^m - 1$, then $u = 1$, and substituting shows that this value is sufficient to satisfy the congruence.

It will now be shown that it is necessary that $u \not> 1$ and from this that $n = 2^m - 1$. Let the highest power of 2 dividing $n - 1$ be 2^e. Now e must $= 1$, for if $e > 1$, from Note 2 the highest power of 2 dividing $(n^{2^u} - 1)/(n - 1)$ would be 2^u, which is less than 2^m since 2^u divides $\phi(2^m)$. Accordingly, $e = 1$ and $n = 1 + 2k$ where k is odd. The requirement that $(n^{2^u} - 1)/(n - 1)$ be divisible by 2^m then requires $n^{2^u} - 1$ to be divisible by 2^{m+1}. Squaring $n = 1 + 2k$ gives $n^2 = 1 + k(k + 1)2^2$; hence $n^2 - 1$ is divisible by 2^{b+2} (and by no higher power of 2) where 2^b $(b > 0)$ is the highest power of 2 dividing $k + 1$; and hence by Note 2, $n^{2^u} - 1$ is divisible by 2^{b+u+1} (and by no higher power of 2), so that the requirement that $n^{2^u} - 1$ be divisible by 2^{m+1} would necessitate $b + u + 1 \geqq m + 1$, or $b + u \geqq m$. Again by Note 2, if $u > 1$, $n^{2^{u-1}} - 1$ is divisible by 2^{b+u}, and hence by 2^m (because $b + u \geqq m$). But this is impossible since n appertains to exponent 2^u, mod 2^m. Therefore $u \not> 1$, or $u = 1$. Then $b \geqq m - 1$, so that

$$n = 1 + 2k = 2(k + 1) - 1 = 2(c \cdot 2^{m-1}) - 1 = c \cdot 2^m - 1.$$

Since $n < 2^m$, $c = 1$ and accordingly $n = 2^m - 1$.

* Miller has shown that, if t does not transform the operators of this H into their inverses, the order of ts^c is the least common multiple of the orders of t and s^c. These Transactions, vol. 4 (1903), p. 154.

The order r of the extending operator t divides $\phi(m_1)$ and no operator (other than the identity) is transformed into itself. Evidently ts (where s is any operator of H) effects the same automorphism of H as does t and is of order r. This as well as the following points can be proved by methods exactly like those in the proof of Theorem 1: the orders of the operators $(t^a s)$ outside H divide r if $n^a \not\equiv 1$, mod p, or divide p^m, if $n^a \equiv 1$, mod p; if s is chosen of order p^{m_1}, then the order of $t^a s$ may be p^{m_1} ($n^a \equiv 1$, mod p); that the cyclic subgroup of order p^{m_1} generated by such a $t^a s$ is not an invariant subgroup of G. Hence, the cyclic subgroups of order p^{m_1} in H which are the only ones of this order invariant under every operator of G, are characteristic in G (in fact they form a characteristic set*). Moreover, since no operator outside of H is commutative with each operator of a cyclic subgroup of order p^{m_1} in H, therefore H is the direct product of the only cyclic subgroups of order p^{m_1} that are invariant in G and the cyclic subgroups of G whose orders are powers of p and whose operators are commutative with the individual operators of the said cyclic subgroups of order p^{m_1}. Thus H is characteristic in G, and the remainder of the proof proceeds as in the preceding theorem.

6. From Theorem 2 a more general proposition in which H is an abelian group of odd order is easily deduced. The requirement that $n \not\equiv 1$, mod p, can be made by stating that no operator (excepting the identity) is transformed into itself by the extending operator. It will now be shown that *if a group G is formed by extending an abelian group H of odd order by an operator from its group of isomorphisms which transforms every one of its operators into the same power of itself, not the first power, then the I of G is the holomorph of H and is a complete group.*

Let $h = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, where $p_1, \cdots, p_k$ are distinct odd primes and $p_1 > p_2 > \cdots > p_k$. We may take $k > 1$ since Theorem 2 covers the case for $k = 1$. Let $H_1, \cdots, H_k$ be the abelian subgroups of orders $p_1^{m_1}, \cdots, p_k^{m_k}$, respectively.† If $p_1^{w_1}, \cdots, p_k^{w_k}$ are the respective orders of the cyclic subgroups of largest orders in $H_1, \cdots, H_k$, then the order r of the extending operator t is the least common multiple of the exponents to which n appertains with respect to the moduli $p_1^{w_1}, \cdots, p_k^{w_k}$, n being the power into which t transforms each operator of H. Let s_i be an operator of order p^{w_i} in H_i and let t be made up of the commutative cycles $t_1, \cdots, t_k$ where the order of t_i is r_i and where t_i transforms s_i into its nth power but is commutative with all the other s's ($i = 1, \cdots, k$); then $t = t_1 \cdot \cdots \cdot t_k$.

Evidently ts (where s is any operator of H) is of order r, and the cycle $t_j s_j$ (where s_j is any operator of H_j, $j = 1, \cdots, k$) will always be of order r_j and r is the least common multiple of the r's; and ts transforms H exactly

*American Journal of Mathematics, vol. 38 (1916), p. 21.

† Burnside, loc. cit., § 38.

as t does. It will next be shown that H is characteristic in G. First, H_1 is characteristic in G since the cyclic subgroup generated by s_1 is invariant under G while any cyclic subgroup of order $p_1^{w_1}$ in G outside H would, since p_1 is the largest prime, necessitate that the cycle $t_1^a s_1$ be of order $p_1^{w_1}$ $(0 < a < r)$. According to the proof under Theorem 1 this cyclic subgroup generated by $t_1^a s_1$ would not be invariant in G; hence with argument similar to that in the proof of Theorem 2, H_1 itself is characteristic in G. Next, H_2 is characteristic in G, since the cyclic subgroup generated by s_2 is invariant under G and each of its operators is commutative with each of the operators of H_1. Any cyclic subgroup of order $p_2^{w_2}$ in G and outside of H would not be invariant, for by the proof of Theorem 1, if the cycle $t_2^a s_2$ generated a cyclic subgroup of order $p_2^{w_2}$, this subgroup would not be invariant in G; also, if some power of $t_1 s_1' \cdot t_2 s_2'$ (where s_1' is an operator of H_1 and s_2' is an operator of H_2) generated a cyclic subgroup of order $p_2^{w_2}$, evidently its operators would not be individually commutative with the operators of H_1 (since in such a power the first cycle would not reduce to the identity). The only operators (of G) whose orders divide $p_2^{w_2}$ and which are commutative with the individual operators of H_1 and those of the cyclic subgroup generated by s_2, are operators of H_2. Hence, H_2 is characteristic in G. Similarly, for $H_3, \cdots, H_k$; and hence the proposition as stated. Or, according to the observation made in the introduction that requiring the particular extending operator to be "from the group of isomorphisms of H" is, here, only another way of saying that the order of the extending operator must be the same as that of the automorphism which it effects, the proposition may be stated as follows:

THEOREM 3. *If a group G is formed by extending an abelian group H of odd order by an operator t which transforms every operator of H into the same power of itself, not the first power, where the order of t equals the order of the automorphism it effects, then the I of G is the holomorph of H and is a complete group.*

From § 2 in which the case for $h = 2p^m$ is discussed, it is apparent that from Theorem 3 follows

Corollary. If a group G is formed by extending an abelian group H whose order $h = 2h'$ where h' is odd and > 1, by an operator t which transforms every operator of H of order > 2 into the same power of itself, not the first power, where the order of t equals the order of the automorphism which it effects, then the I of G is the holomorph of H.

7. If H is an abelian group different from those of the preceding theorems, the following may be stated:

THEOREM 4. *If a group G is formed by extending an abelian group H whose order $h = 2^m h'$ where $m > 1$ and h' is odd and > 1, by an operator t which transforms every operator of H into the same power of itself such that no operator of odd order is transformed into its first power and such that the order of t equals*

the order of the automorphism of H which it effects and (*a*) *the order of the automorphism of the operators of odd order which t effects is divisible by 2^n where H contains an operator of order 2^n but none of order 2^{n+1}, or else* (*b*) *t transforms into its inverse every one of H's operators whose order is a power of 2, then the I of G is the holomorph of H.*

If H' is the abelian subgroup of order h' in H, it can be shown to be characteristic in G by a method analogous to that in Theorem 2. The operators whose orders are powers of 2 in H are the only operators in G which are commutative with the individual operators of H'. Hence H is characteristic in G. The product of t multiplied into any operator of H effects the same automorphism of H as does t, and is of the same order as t. This latter statement about orders will be discussed. If t is commutative with the operators of H whose orders are powers of 2, the statement is evident; if t is not commutative with these operators, the cycle in t which transforms these operators into their same powers is, by § 4, always of an order which divides 2^n. Hence part (*a*) of the theorem is proved. In part (*b*), if t transforms each operator of H into its inverse, G is the generalized dihedral group; if t transforms every operator of H into the same power of itself and this transformation takes operators whose orders are powers of 2 into their inverses but operators of odd orders not into their inverses (and none excepting the identity into itself), then one cycle of ts (where s is any operator of H including the identity) is always of order 2 while the order of the other part is a constant > 2. Accordingly, as in the other theorems, the I of G may be written as a transitive substitution group on h letters and contains an invariant subgroup simply isomorphic with H; etc.

8. One part of the preceding theorem is a special case of the proposition that *if G is formed by extending an abelian group H which is the direct product of two groups H' and H'' whose orders are relatively prime and where the order of H'' is not divisible by 4, by an operator t which is commutative with the operators of H' but which transforms every operator of H'' of order > 2 into the same power of itself, not the first power, and where the order of t equals the order of the automorphism of H'' which it effects and is divisible by the order of each operator of H', then the I of G is the holomorph of H.*

This proposition as well as the preceding theorems and Professor Miller's theorem on the I of a generalized dicyclic group* are special cases of the following theorem, each being a case in which it can be proved that H is characteristic in G, that the I of G contains an invariant subgroup simply isomorphic with H, and that the subgroup H can be automorphic just as any abelian group simply isomorphic with H can.

* Miller, Blichfeldt, and Dickson, loc. cit., p. 170; cf. also the theorem following the one on the dicyclic group.

THEOREM 5. *If G is formed by extending an abelian group H by an operator t which transforms every operator of H into the same power of itself and which is such that ts_i ($i = 1, \cdots, h$ where $s_1, \cdots, s_h$ are the operators of H) are all of the same order and have a single characteristic operator of H for their same first power in H, then the I of G is the holomorph of H provided H is characteristic in G.*

The hypotheses here include the points established in the detail of the proof of Theorem 1, so that the last two paragraphs in § 1 give discussion sufficient for showing the truth of this theorem.

DARTMOUTH COLLEGE
June, 1917