ON THE HOLOMORPH OF A CYCLIC GROUP*

BY

G. A. MILLER

It is known that the holomorph (K) of a cyclic group (G) is a complete group and that its commutator subgroup is G whenever the order (g) of G is odd. When $g > 2$ is even, the commutator subgroup of K is the subgroup of G whose order is $g/2$, and K is never complete.† The main object of this paper is to determine additional useful properties of K whose subgroups are of such fundamental importance. In particular, we shall determine the orders of all the operators of K and some of the properties of its group of isomorphisms when g is even. It will be observed that the generalized FERMAT's theorem follows directly from some of the properties of the group of isomorphisms of G.

Let $g = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ ($p_1, p_2, \cdots, p_m$ being any odd prime numbers) and let $K_0, K_1, K_2, \cdots, K_m$ represent the holomorphs of the cyclic groups ($G_0, G_1, G_2, \cdots, G_m$) of orders $2^{\alpha_0}, p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_m^{\alpha_m}$ respectively. As K is evidently the direct product of these holomorphs ‡ the orders of all the operators of K can be directly obtained from the orders of the operators in these holomorphs. We shall first consider the operators of K_0 ($\alpha_0 > 2$) whose order is known to be $2^{2\alpha_0 - 1}$.

The group of isomorphisms (I_0) of G_0 is known to be the direct product of an operator of order two and a cyclic group which may be so chosen that it is composed of all the operators of I_0 which transform § an operator of order 4 in G_0 into itself. ¶

The orders of the two independent generators (s_1, s_2) of I_0 are therefore $2^{\alpha_0 - 2}$ and 2 respectively.** We shall first determine the orders of all the

* Presented to the Society (San Francisco) December 20, 1902. Received for publication January 3, 1903.

† BURNSIDE, Theory of groups of finite order, 1897, p. 240; MILLER, Quarterly Journal of Mathematics, vol. 31 (1899), p. 382.

‡ Cf. BURNSIDE, l. c.

§ It will be assumed throughout that K_a ($a = 0, 1, 2, \cdots, m$) is represented as a substitution group whose degree is equal to the order of G_a, and that its group of isomorphisms (I_a) is the subgroup composed of all the substitutions which omit the first letter. The two groups K_a and I_a are thus completely determined by G_a even as substitution groups.

¶ Bulletin of the American Mathematical Society, vol. 7 (1901), p. 350.

** Since all the squares of operators of K_0 which occur in G_0 must also be found in the commutator subgroup of K_0, it follows that the quotient group of K_0 with respect to its commutator subgroup is of type ($a - 2, 1, 1$).

operators of K_0 which may be obtained by multiplying G_0 by powers of s_1, where s_1 is supposed to have been so selected that it is commutative with an operator of order 4 in G_0.

Let s represent any operator of highest order in G_0. From the equations

$$(s_1^\alpha s)^2 = s_1^\alpha s s_1^\alpha s = s_1^{2\alpha} s_1^{-\alpha} s s_1^\alpha s = s_1^{2\alpha} s' s^2,$$

where s' is some operator of G_0 whose order is equal to that of s_1^α and hence $s's^2$ is of the same order as s^2, it follows that $s_1^\alpha s$ $(\alpha = 1, 2, \cdots, 2^{\alpha_0 - 2})$ is of the same order as s.* Hence K_0 contains at least 2^{α_0-2} cyclic subgroups of order 2^{α_0}. We shall soon see that this is the exact number of such subgroups and that, with the exception of G_0, they are conjugate in sets of

$$2^0, 2, 2^2, 2^3, \cdots, 2^{\alpha_0-3}.$$

In particular, K_0 contains just two invariant cyclic subgroups of order 2^{α_0}, so that the holomorph of a cyclic group of order 2^{α_0} is at the same time the holomorph of just one other cyclic group of this order. All the substitutions which transform one of these subgroups into the other must therefore transform K_0 into itself and have their squares in K_0.†

If s^2 is substituted for s in the equations of the preceding paragraph it follows in a similar manner that $s_1^\alpha s^2$ is of the same order as s^2 since the order of $s_1^{2\alpha}$ is less than that of s^4. Hence the group generated by s_1 and G_0 contains just 2^{α_0-2} cyclic subgroups of order 2^{α_0-1}. It will, however, be seen that these are just half of the cyclic groups of this order which are found in K_0, the other half being obtained by multiplying the group generated by G_0 and s_1 by the operator s_2.

In general, *the order of the product of s_1^α into any operator s^β of G_0 is equal to the least common multiple of the orders of the two factors s_1^α, s^β*, for this order cannot be less than s_1^α, since, the product transforms the operators of G_0 according to a substitution of this order, and from the preceding paragraphs it is clear that it can exceed the order of s_1^α only when the order of s^β exceeds that of s_1^α. In this case the order of the product is equal to the order of s^β. Hence the group generated by G_0 and s_1 contains $3.2^{2(n-1)}$ operators of order 2^n $(0 < n < \alpha_0 - 1)$, $2^{2\alpha_0-4}$ of order 2^{α_0-1}, and 2^{α_0-3} of order 2^{α_0}.

As each of the remaining operators of K_0 must transform an operator of order 4 in G_0 into its inverse and as G_0 contains negative substitutions, all of these operators must be conjugate in sets of 2^{α_0-1}. If s_2 has been so selected

---

* Bulletin, l. c.

† From this it is clear that G_0 has always a *double holomorph* in the same letters as its holomorph. Every non-abelian group has also such a double holomorph since the substitutions which transforms a non-abelian group into its conjoint must transform this conjoint into the given non-abelian group. Abelian groups do not always have such double holomorphs.

that it transforms each operator of G_0 into its inverse (which will be assumed) all the products obtained by multiplying the operators of G_0 by s_2 are of order 2. One half of the products obtained by multiplying G_0 by $s_1^\beta s_2$ ($\beta \not\equiv 0 \bmod 2^{\alpha_0-2}$) are of the same order as s_1^β, since s_1 and s_2 are both found in I_0 and $s_1^\beta s_2$ is of degree $2^{\alpha_0} - 2$. We proceed to prove that the rest are of twice this order.*

None of the operators in question is commutative with $s_1^{2^{\alpha_0-3}}$ or its conjugate, for each of these two conjugates is commutative with $s_1^\beta s_2$ and hence with all the products obtained by multiplying $s_1^\beta s_2$ into the positive substitutions of G_0, but it is commutative with only half the operators of K_0 since its degree is less than 2^{α_0}. If the order of $s_1^\beta s_2$ is $2^\gamma (\gamma > 1)$ the $2^{\gamma-1}$ power of the operators in question must therefore be of order 4; i. e., their order must be twice the order of $s_1^\beta s_2$. If $\gamma = 1$, $s_1^\beta s_2$ transforms s into its $2^{\alpha_0-1} - 1$ power and the theorem clearly remains true.

Combining the results of the last two paragraphs it follows that K_0 contains $3(2^{\alpha_0-1} + 1)$ operators of order 2, $3(2^{2(n-1)} + 2^{\alpha_0+n-3})$ of order $2^n (1 < n < \alpha_0 - 1)$, and $2^{2\alpha_0-3}$ of each of the two orders 2^{α_0-1}, 2^{α_0}. This includes the fact that all the operators of order 2^{α_0} which are contained in K_0 transform an operator of order 4 in G_0 into itself as was stated above. Since the products obtained by multiplying all the operators of G_0 by any given power of s_1 have the same number of conjugates under I_0 as the multiplicands have and since any operator of I_0 has as many conjugates under G_0 as its order has units, it follows that *all the operators of the same order which may be obtained by multiplying G_0 by any one operator of I_0 with the exception of s_2 are conjugate under K_0.*† In particular, the cyclic subgroups of order 2^{α_0} are conjugate in sets of 2^0, 2^0, 2, 2^2, $\cdots$, 2^{α_0-3} as was stated above.

In what precedes it has been explicitly assumed that $\alpha_0 > 2$. When $\alpha_0 = 2$, K_0 is the well known octic group and includes only one cyclic subgroup of order 2^{α_0}. All its other operators are of order 2. When $\alpha_0 = 1$, K_0 coincides with G_0. It remains to determine the orders of all the operators of K_1. It will be seen that the order of the product of any operator of G_1 into any operator whose order is of the form p_1^β in I_1 is the least common multiple of the orders of the two factors. Hence this case is similar to the first part of the preceding case. There is, however, only one invariant cyclic subgroup of order $p_1^{\alpha_1}$ in K_1, as the $p_1 - 1$ subgroups of this order which correspond to the second invariant subgroup in K_0 are conjugate under K_1. We proceed to prove these statements.

* Their orders could not exceed this number since they are rot commutative with the operators of order 4 in G_0.

† That these operators form complete sets of conjugates under K_0 follows directly from the fact that K_0/G_0 is abelian. The products of G_0 and s_2 clearly form two complete sets of conjugates under K_0.

Let s represent any operator of G_1 and let t represent any operator whose order is of the form p_1^β in I_1. Suppose that

$$tst^{-1} = s_1 s,\ ts_1 t^{-1} = s_2 s_1,\ \cdots,\ ts_\alpha t^{-1} = s_{\alpha+1} s_\alpha .$$

It is known that the order of $s_{\alpha+1}$ is lower than that of s_α.* From the equations

$$(st)^n = stst^{-1}t^2st^{-2}t^3s\cdots t^{n-1}st^{1-n}t^n$$
$$= ss_1ss_2s_1^2s\cdots s_{n-1}s_{n-2}^{n-1}\cdots s_{n-r-1}^{\frac{(n-1)\dots(n-r)}{r!}}\cdots s_1^{n-1}st^n$$
$$= \cdots s_1^{\frac{n(n-1)}{2}}s^nt^n,$$

where the omitted factors in the last member are of a lower order than s_1, it follows that st is of the same order as it would be if s and t were commutative and independent. That is, the order of st is the least common multiple of the orders of s and t. If the order of t is not of the form p_1^β then st is of the same order as t since t is not commutative with any operator of G_1 besides the identity and I_1 is abelian.

From the results of the preceding paragraph we can readily determine the number of operators of a given order in K_1. *There are just* $\phi(n)p_1^{\alpha_1}$ *operators of order* n *in* K_1, n *representing any divisor of* $p_1^{\alpha_1-1}(p_1-1)$ *which is not of the form* p_1^β. *The orders of the remaining operators are of the form* p_1^β *and there are* $p_1^{2(\beta-1)}(p_1^2-1)$ *of this order whenever* $\beta<\alpha_1$. *When* $\beta=\alpha_1$ *there are* $p_1^{2(\alpha_1-1)}(p_1-1)$ *operators of order* p^β. In exactly the same manner as in the preceding case it may be seen that all the operators of the same order which may be obtained by multiplying the operators of G_1 by any one operator of I_1 form a complete set of conjugates under K_1. Hence the cyclic subgroups of order $p_1^{\alpha_1}$ in K_1 are conjugate in sets of

$$1,\, p_1-1,\, p_1(p_1-1),\, \cdots,\, p_1^{\alpha_1-2}(p_1-1).$$

These results can readily be applied to the holomorph K of the general cyclic group G. In the first place, *K contains only one invariant cyclic subgroup of order g whenever g is not divisible by* 8. *If g is divisible by* 8 *then K contains just two such subgroups, having $g/2$ common operators.* This result follows directly from the facts that K_1 contains only one invariant cyclic subgroup of order $p_1^{\alpha_1}$ and that K_0 contains one or two invariant cyclic groups of order 2^{α_0} according as $\alpha_0<3$ or $\alpha_0 \geqq 3$. The group of isomorphisms of G will be denoted by I and it will be assumed that K is represented as a transitive substitution group of degree g. Hence G must be regular.† Let t represent the

* Bulletin of the American Mathematical Society, vol. 7 (1901), p. 351.

† If a transitive group of degree n contains an invariant cyclic subgroup of order n this cyclic subgroup must be regular. If the subgroup were non-cyclic it would not need to be regular.

substitution of I which transforms a generator s of G into its α'th power. The orders of all the substitutions of K which transform s into its α power are the same as those of the direct product of the divisions in the holomorphs $K_0, K_1, \cdots, K_m$ which transform the generators of $G_0, G_1, \cdots, G_m$ respectively in the same manner as t does. The number of sets of conjugates among these g substitutions is clearly equal to the product of the numbers of the sets of conjugates in the given divisions of $K_0, K_1, \cdots, K_m$.

The following examples may serve to exhibit more clearly some of the properties mentioned above. If $g = 100$ and $\alpha = 9$ the orders of the operators obtained by multiplying G into t are the same as those in the direct product of the cyclic group of order 4 and the division in the holomorph of the cyclic group of order 25 which transforms the operators of this cyclic group into their 9th powers. As all the operators of the latter division are of order 10, t is of order 10 and has 25 conjugates under K. There is another set of 25 conjugates of this order, while the remaining 50 operators of K which transform s into the 9th power are of order 20 and from a single set of conjugates under K. If $g = 100$ and $\alpha = 3$ there are evidently two equal sets of conjugates, each of the 100 operators being of order 20.

It is very easy to determine the degrees of all the substitutions of K. Since the substitution t is in I its degree is less than g. We may suppose that it omits the first letter of G. If it omits any other letter it must be commutative with the substitution in which the first letter is replaced by this second. That is, *if t is of degree $g - \beta$ it is commutative with just β substitutions of G*. The number of its conjugates under G (which is clearly equal to the number of its conjugates under K) is g/β. All the other products obtained by multiplying G by t must be of degree g, otherwise K would contain a transitive subgroup in which the average number of letters would not be $g - 1$.* It is clear that the condition in regard to the average number of letters in the substitutions of a transitive group requires that in each division of K with respect to G this average number is $g - 1$.

The result of the preceding paragraph may be stated as follows: *If any subtitution t of I is commutative with just β substitutions of G its degree is $g - \beta$ and it has g/β conjugates under K.* All the products obtained by multiplying G by t are of degree g, with the exception of these g/β conjugates of t. For instance, in the first example of the next to the preceding paragraph, there are 25 substitutions of degree 96 and 75 of degree 100. In the second example there are 50 of degree 98 and 50 of degree 100.

It is evident that I can be represented as a regular group of degree $\phi(g)$ since each of its substitutions must permute all the generators of G and these generators can be permuted transitively. In fact, this regular group is one of

* Cf. Bulletin of the American Mathematical Society, vol. 2 (1895), p. 75.

the transitive constituents of I and each of its other constituents is also regular. As I is the group formed by combining the $\phi(g)$ numbers by multiplication and replacing the products by their least positive residues modulo g,* FERMAT'S *generalized theorem* ($a^{\phi(g)} \equiv 1 \mod g$) *is merely a statement of the fact that the order of I is divisible by the order of each of its substitutions.*

When $g = p^\alpha$, p being any odd prime, I contains α transitive constituents whose orders are $p^\beta(p-1)$, $\beta = 0, 1, \cdots, \alpha - 1$, respectively. If $\gamma > \delta$ then the constituent of order $p^\gamma(p-1)$ has a $(p^{\gamma-\delta}, 1)$ isomorphism with the constituent of order $p^\delta(p-1)$.† Hence I contains just $p-1$ substitutions of degree $\phi(g)$ and its structure as a substitution group is completely determined. When $p = 2$ I contains only $\alpha - 1$ transitive constituents and the given subgroup of order $p^{\gamma-\delta}$ is generated by a substitution corresponding to s_1 in I_0 as used above. Hence in this case I is also completely determined as a substitution group.

It has been observed that I always contains one transitive constituent of order $\phi(g)$. When $\alpha_0 = 1$ there is one more constituent of this order. In all other cases there is only one such constituent since the group of isomorphisms of every subgroup of I is of a lower order than I. When $\alpha_0 = 0$ there are $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_m + 1) - 1$ transitive constituents in I while there are $(\alpha_0 + 1)(\alpha_1 + 1) \cdots (\alpha_m + 1) - 2$ such constituents in all other cases.‡ As $\phi(g)$ is the order of the constituent formed by the direct product of the constituents representing the permutations of the operators in the subgroups of orders $2^{\alpha_0}, p_1^{\alpha_1}, \cdots, p_m^{\alpha_m}$ respectively it follows that *I contains substitutions of degree $\phi(g)$ only when $g = p^\alpha$.*

The preceding results are sufficient to determine I as a substitution group. It is only necessary to determine the isomorphisms between the given regular constituent of order $\phi(g)$ and the remaining regular constituents. As each of these constituents represents the permutation of the operators of highest order in some subgroup of G, the required isomorphism is equivalent to determining all the permutations of the operators of highest order in G which do not affect the generators of this subgroup. The latter can be directly obtained from the powers of the primes which enter into the order of the subgroup.

It has been observed that the group of isomorphisms (I') of K is the same as K itself whenever the order (g) of G is odd. We proceed to find the order of I' when g is even. Representing K as an intransitive substitution group whose transitive constituents are $K_0, K_1, \cdots, K_m$, we shall first determine what groups may correspond in the holomorphisms of K to K_α, α having any one of

* Annals of Mathematics, vol. 2 (1900), p. 77.

† Bulletin of the American Mathematical Society, vol. 7 (1901), p. 350.

‡ Cf. DIRICHLET, *Zahlentheorie*, 1894, p. 17.

the values $1, 2, \cdots, m$. Since every subgroup of G* is a characteristic subgroup of K the group which corresponds to K_a must involve all the letters of K_a. As K_a is a complete group the corresponding group must be either K_a itself or it must involve K_a as one of its transitive constituents. We proceed to prove that in the latter case the other constituents must be the invariant substitution (S') of K, which is not the identity.

This follows immediately from the fact that each of the substitutions of K_a is commutative with all the substitutions in the direct product of the remaining partial holomorphs $K_0, K_1, \cdots, K_m$. As the corresponding group must have the same property with respect to a similar group it is proved that *in any simple isomorphism of K with itself each of the partial holomorphs $K_1, K_2, \cdots, K_m$ either corresponds to itself or to the group obtained by multiplying half its operators by S'.* In these holomorphisms S' cannot be multiplied into an operator of G and hence K_a can correspond to two and only two subgroups of K. The partial holomorph K_0 must always correspond to itself.

From the preceding paragraph it follows that I' contains a subgroup of order 2^m which includes no operator whose order exceeds 2 and which has only the identity in common with I'' the group of cogredient isomorphisms of K. Each of these 2^m operators is commutative with every operator of I'' according to the following evident theorem: *Any operator of the group of isomorphisms which corresponds to a holomorphism obtained by multiplying half the operators of the group by an invariant operator of order 2 is commutative with every operator in the group of cogredient isomorphisms.* Hence I' must always include the direct product of I'' and this abelian group of order 2^m. When $\alpha_0 = 1$ it is clear that I' contains no operators besides this direct product, and when $\alpha_0 = 2$ the order of I' is twice the order of this direct product. We proceed to prove that for all other values of α_0 the order of I' is four times the order of this direct product.

To prove this it is only necessary to determine the order of the group (I'_0) of isomorphisms of K_0. Consider the divisions of K_0 with respect to G_0. One of these contains 2^{α_0-1} substitutions of order 2^{α_0-2} and of degree $2^{\alpha_0} - 2$ while its remaining substitutions are of degree 2^{α_0} and of order 2^{α_0-1}. The substitutions of each of these two sets must correspond to themselves whenever G_0 corresponds to itself. As any two substitutions, one from each of these sets, generate one half of K_0 and as the division which transforms each operator of G_0 into its inverse contains only two substitutions which are commutative with a substitution of the first set, it follows that the number of the operators in I'_0, which transform G_0 into itself, cannot exceed $2^{\alpha_0-1} \cdot 2^{\alpha_0-1} \cdot 2$. Hence the order of I'_0 cannot exceed $4 \cdot 2^{2(\alpha_0-1)}$; i. e. four times the order of the group (I''_0) of cogredient isomorphisms of K_0.

* When g is divisible by 8, G itself is not a characteristic subgroup of K. In this case G has a double holomorph of degree g.

It remains only to prove that I_0' contains operators which transform G_0 into itself but are not found in I_0''. Such an operator of order 2 corresponds to the simple isomorphism of K_0 which may be obtained by multiplying by S' all the operators obtained by multiplying G_0 by all the operators of order 2^{α_0-2} in I_0 in order. Hence the theorem: *The order of the group of isomorphisms of K is 2^m, 2^{m+1} or 2^{m+2} times the order of its group of cogredient isomorphisms as* $\alpha_0 = 1, 2$, or > 2.*

* Cf. BURNSIDE, *Theory of groups of finite order*, 1897, p. 242.