ANSWER TO A QUESTION RAISED BY CAYLEY AS REGARDS A PROPERTY OF ABSTRACT GROUPS.

BY PROFESSOR G. A. MILLER.

(Read before the American Mathematical Society, September 10, 1908.)

IN 1859 Cayley * gave an enumeration of the possible abstract groups of order 8, and at the end of the note devoted to this subject he considered briefly the groups defined by two operators s_1, s_2 satisfying the following conditions:

$$s_1^m = 1 \qquad s_2^n = 1 \qquad s_1 s_2 = s_2 s_1^k.$$

He remarks, "the group corresponding to $k = 1$ is distinct from that for any other value of k, but I have not ascertained whether the values other than unity do, or do not, give groups distinct from each other." That different values of k *may* lead to distinct groups is very evident, and we shall assume that the question whose answer Cayley was seeking may be expressed as follows: *Given m and n, and that $k \not\equiv 1 \bmod m$, for what admissible values of k are the groups generated by s_1 and s_2 distinct?* Even if this question should be more general than the one which Cayley had in mind, it relates to such a fundamental matter as to make a direct answer desirable. Partial answers may be found in various places, especially in a comparatively recent paper by Netto, † which is largely devoted to these elementary groups.

The conditions imposed on s_1 and s_2 are equivalent to the conditions that a cyclic group of finite order m is transformed into itself by an operator of finite order n. As a first result we have that the order of G, the group generated by s_1 and s_2, is mn/l, where l is the number of operators common to the two cyclic groups generated by s_1 and s_2 respectively. Cayley implicitly assumed $l = 1$. When $k \equiv 1 \bmod m$, G is either cyclic or the direct product of two cyclic groups. This special case will be excluded in what follows, as it is not included in the question under consideration. As s_1 and s_2 are supposed to be non-commutative, there is some lowest power of s_2, say s_2^r,

* *Philosophical Magazine*, vol. 18 (1859), p. 34.

† *Crelle*, vol. 128 (1905), p. 243.

which is commutative with s_1, r being a divisor of n. Since a cyclic group of order r has $\phi(r)$ generators, $\phi(r)$ being the totient of r, it results that $\phi(r)$ different values of k give rise to the same group whenever one of them may be used for k. That is, all the numbers which may be used for k can be arranged in sets of $\phi(r)$, such that each set corresponds to the same group. It is not difficult to prove that whenever the values of k belong to two such sets the corresponding groups will also be distinct. In other words, there is a (1, 1) correspondence between these sets of $\phi(r)$ numbers and the distinct groups obtained by using for k all the different numbers belonging to exponent r. This theorem gives a complete answer to the question under consideration and its proof is contained in the following two paragraphs.

Let H be the cyclic group generated by s_1. If the values of k corresponding to two distinct sets of $\phi(r)$ numbers gave rise to the same group, the group corresponding to one of these sets would involve at least two invariant subgroups similar to H, each corresponding to a cyclic quotient group and hence involving all the commutators of G. Moreover, these two subgroups H_1, H_2 would have to be transformed differently by the operators of G. Let P be any Sylow subgroup of odd order p^m contained in H_1. If the operators of P are transformed according to a substitution whose order is prime to p, it is necessary that P be common to H_1 and H_2, and hence it is transformed in the same manner under G. If the order of this substitution is not prime to p, the Sylow constituent of order p^α in the commutator subgroup of G is common to H_1 and H_2, and the generators of P and the corresponding subgroup in H_2 are transformed into themselves multiplied by operators of the same order under G.* Hence in every case the Sylow subgroups of odd order in H_1 and H_2 are transformed in the same manner under G.

If P is of order 2^m $(m > 2)$, its group of isomorphisms is the direct product of a cyclic group of order 2^{m-2} and a group of order 2. Hence this group of isomorphisms contains two cyclic subgroups of every order greater than 2 and less than 2^{m-1}, and these two cyclic subgroups correspond to commutator subgroups of different orders. From this it follows that P and the corresponding subgroup in H_2 are transformed in the same

* BULLETIN, vol. 7 (1901), p. 350.

manner whenever P is transformed according to a cyclic group whose order exceeds 2. When a generator of P is transformed into its inverse or into its $(2^{m-1} - 1)$th power, the commutator subgroup is of order 2^{m-1}. In each of these cases, n must be divisible by 4 to insure more than one invariant P, and each such P must therefore be transformed in the same manner under G. Combining these results we have the theorem:

If r is the lowest power of s_2 which is commutative with s_1, the numbers which can be used for k are precisely those belonging to exponent r modulo m, and all of these numbers less than m may be arranged into sets of $\phi(r)$ such that those of the same set, but no others, correspond to the same group.

For the sake of seeing more clearly the nature of the problems included under this theorem, we may consider the special case when $m = 72$ and $n = r = 6$. Since the group of isomorphisms of the cyclic group of order 72 contains 14 operators of order 6, there are 14 numbers which can be used for k, viz., 5, 7, 11, 13, 23, 29, 31, 41, 43, 47, 59, 61, 65, 67. As $\phi(6) = 2$, these numbers may be arranged into pairs, each pair leading to the same group. These seven pairs are as follows:

5, 29; 7, 31; 11, 59; 13, 61; 23, 47; 41, 65; 43, 67.

Only three of these pairs lead to groups involving more than one invariant cyclic subgroup of order 72, viz., 7, 31; 13, 61; 43, 67. The first and last of these three groups involve exactly three invariant cyclic subgroups of order 72, while the second involves six such subgroups. In each case, all of these invariant subgroups are transformed in the same manner under G. It should not be inferred that all the invariant cyclic subgroups of order m are transformed in the same manner under G; the theorem merely implies that two invariant cyclic subgroups of order m which are transformed differently under G cannot both correspond to a cyclic quotient group of G.

When n is a prime number p and G contains more than one invariant cyclic subgroup of order m, it is necessary that $r = n$, and in this case it is easy to prove that m is divisible by p^2 when $p > 2$, and by p^3 when $p = 2$. Moreover, all the commutators of G are invariant and there is only one group for given values of m and n which involves more than one invariant cyclic subgroup of order m. In fact, if G contains more than one subgroup of order m, it is necessary that m is divisible by p, since all the operators of G which are not in the subgroup generated by s_1 have orders which are divisible by p. Moreover, two such cyclic subgroups would have in common all their operators whose orders are prime to p. Hence we have that G is the direct product of its Sylow subgroup of order p^m and its other Sylow subgroups whenever it involves more than one subgroup of order m. As the group of isomorphisms of a cyclic group of order p^α, $p > 2$, is cyclic, we have the theorem:

When n is a prime p and G involves more than one subgroup of order m, these subgroups must be cyclic and invariant, and G is the direct product of the non-abelian group of order p^m involving p cyclic subgroups of order p^{m-1}, and a cyclic group whose order is prime to p.

It results from the last theorem that there is one and only one non-abelian group of order pg which contains more than one invariant cyclic subgroup of order g, whenever g is divisible by p^2 or by p^3 as p is odd or even. When g is not divisible by one of these numbers, there is no such group. In particular, there is one and only one non-abelian group of order $2g$ involving two cyclic subgroups of order g whenever g is divisible by 8 and only then. If we let $n = 2$ in the example considered above, where $m = 72$, there are 7 numbers which can be used for k, viz., 17, 19, 35, 37, 53, 55, 71. The seven corresponding groups are distinct and only one of them (when $k = 37$) contains more than one cyclic subgroup of order 72. When $n = r = p^\alpha$, G cannot contain more than one invariant cyclic subgroup of order m unless m is divisible by $p^{\alpha+1}$ or $p^{\alpha+2}$ according as p is odd or even; and all these cyclic subgroups have in common the operators whose orders are prime to p in the subgroup generated by s_1. The number of these invariant subgroups cannot exceed p^β, where β is the largest number not greater than α which satisfies the condition that m is divisible by $p^{\alpha+\beta}$ when $p > 2$, and by $p^{\alpha+\beta+1}$ when $p = 2$.