GROUPS GENERATED BY TWO OPERATORS (s_1, s_2) SATISFYING THE EQUATION $s_1 s_2^2 = s_2 s_1^2$.*

BY

G. A. MILLER

§ 1. *Introduction.*

In 1878 CAYLEY considered the groups generated by two operators (s_1, s_2) satisfying the equation $s_1 s_2 = s_2^2 s_1^2$ and observed the interesting theorem that it is not possible to represent all the operators of such a group in the form $s_1^\alpha s_2^\beta$ except in the special trivial case in which the group is cyclic.† This theorem is of historic interest as it is one of the earliest theorems relating to a general category of abstract groups. More recently NETTO published a few additional general results which may be deduced from this equation and he also determined the possible groups when the orders of s_1, s_2 are both less than 6.‡ The results obtained by NETTO were extended by the author of the present paper, mainly by means of special considerations, as regards the possible groups in which the two generating operators are of order 6.§

For convenience the equation under consideration is written, in the present paper, in the form $s_1 s_2^2 = s_2 s_1^2$, and a number of new general results are deduced from it. By means of these the known results are obtained much more easily than in the earlier papers. It is also proved that the two equations $s_1^5 = 1$, $s_1 s_2^2 = s_2 s_1^2$ imply that $s_2^5 = 1$ and hence either the first or the second of the three generational relations $s_1^5 = 1$, $s_2^5 = 1$, $s_1 s_2^2 = s_2 s_1^2$ given by NETTO in the article cited above is redundant. This is of interest since it proves that the non-cyclic group of order 55 is the only non-abelian group which can be generated by two operators satisfying the two conditions $s_1^5 = 1$, $s_1 s_2^2 = s_2 s_1^2$ and hence it establishes contact between the present paper and the one devoted to the "Finite groups which may be defined by two operators satisfying two conditions."‖

Among the other results the following are perhaps of most interest. There

* Presented to the Society, December 29, 1909.

† CAYLEY, Messenger of Mathematics, vol. 7 (1878), p. 188.

‡ NETTO, Crelle's Journal, vol. 128 (1905), p. 243.

§ Quarterly Journal of Mathematics, vol. 40 (1909), p. 197.

‖ American Journal of Mathematics, vol. 31 (1909), p. 167.

is an infinite system of solvable groups each of which may be generated by two operators which satisfy the three conditions $s_1^6 = 1$, $s_2^6 = 1$, $s_1 s_2^2 = s_2 s_1^2$; but there are only two groups which may be generated by two operators satisfying the three conditions $s_1^7 = 1$, $s_2^7 = 1$, $s_1 s_2^2 = s_2 s_1^2$. Combining these results with those known earlier we may say that the only groups which can be generated by two operators satisfying the three conditions,

$$s_1^\alpha = 1, \qquad s_2^\alpha = 1, \qquad s_1 s_2^2 = s_2 s_1^2,$$

are: The group of order 2 when $\alpha = 2$; the group of order 3 and the tetrahedral group when $\alpha = 3$; the cyclic groups of orders 2 and 4, and the holomorph of the group of order 5 when $\alpha = 4$; the group of order 5 and the non-cyclic group of order 55 when $\alpha = 5$; the cyclic groups of orders 2, 3 and 6, and an infinite system of solvable non-abelian groups when $\alpha = 6$; the group of order 7 and the non-cyclic group of order 203 when $\alpha = 7$. The fact that for $\alpha = 6$ there is an infinite system of possible groups, while there are only two for the larger value 7 of α, is to be emphasized.

§ 2. *General considerations.*

By writing the equation $s_1 s_2^2 = s_2 s_1^2$ in the form $s_1 s_2^2 s_1^{-1} = s_2 s_1$, and raising both members to the same power, there results the formula

$$s_1 s_2^{2n} s_1^{-1} = (s_2 s_1)^n.$$

In a similar manner we obtain the formula

$$s_2 s_1^{2n} s_2^{-1} = (s_1 s_2)^n.$$

From these two formulas we see directly that the three operators s_1^2, s_2^2, $s_1 s_2$ are of the same order, and that either s_1, s_2 have the same order or else the order of one of these operators is an odd number and the order of the other is twice this odd number. These results may be expressed in the form of a theorem as follows: *If two operators satisfy the equation $s_1 s_2^2 = s_2 s_1^2$, their squares are of the same order as their product.*

By transforming the given formulas with respect to s_1^{-1}, s_2^{-1}, respectively, we obtain

$$s_1^2 s_2^{2n} s_1^{-2} = (s_1 s_2)^n \qquad s_2^2 s_2^{2n} s_1^{-2} = (s_2 s_1)^n,$$

and hence

$$(A) \qquad s_1 s_2^{2n} s_1^{-1} s_2^2 s_1^{-2n} s_2^{-2} = s_2 s_1^{2n} s_2^{-1} s_1^2 s_2^{-2n} s_1^{-2} = 1.$$

The commutator of s_1, s_2 is $s_1^{-1} s_2^{-1} s_1 s_2 = s_1 \cdot s_1^{-2} s_2^{-1} \cdot s_1 s_2 = s_1 s_2^{-1}$, and hence

$$(B) \qquad (s_1^{-1} s_2^{-1} s_1 s_2)^2 = (s_1 s_2^{-1})^2 = s_1^3 \cdot s_1^{-2} s_2^{-1} \cdot s_1 s_2^{-1} = s_1^3 s_2^{-3}.$$

The group generated by the two commutators $s_1 s_2^{-1}$, $s_2^{-1} s_1$ is invariant under

the group G generated by s_1, s_2 since

$$s_1^{-1} s_2^{-1} s_1^2 = s_1 \cdot s_1^{-2} s_2^{-1} s_1^2 = s_1 s_2^{-2} s_1 = s_1 s_2^{-1} \cdot s_2^{-1} s_1,$$

$$s_2^{-1} \cdot s_2^{-1} s_1 \cdot s_2 = s_2^{-1} s_1^2 s_2^{-1} = s_2^{-1} s_1 \cdot s_1 s_2^{-1}.$$

As the quotient group of G with respect to this group is cyclic it results that this invariant subgroup is the commutator subgroup of G. That is, *if two operators satisfy the equation* $s_1 s_1^2 = s_2 s_1^2$, *they generate a group whose commutator subgroup is generated by two conjugate commutators and whose commutator quotient is cyclic.*

The commutator $s_1 s_2^{-1}$ is transformed into $s_2^{-1} s_1$ by each of the two operators s_1, s_2. It is also transformed into the same operator by each of the two operators s_1^3, s_2^3, since $(s_1 s_2^{-1})^2 = s_1^3 s_2^{-3}$. The two operators $s_1 s_2 s_1$, $s_2 s_1 s_2$ must have the same order since they may be obtained by transforming $s_2 s_1^2$, $s_1 s_2^2$ by s_1^{-1}, s_2^{-1} respectively. Hence $s_2^{-2} s_1 s_2 s_1 s_2^2$, $s_1^{-2} s_2 s_1 s_2 s_1^2$ must also have the same order. The last two operators are equal respectively to $s_2^{-1} s_1^4$, $s_1^{-1} s_2^4$, as may be seen by employing the relation $s_1 s_2^2 = s_2 s_1^2$. This fact was proved by Netto by means of more lengthy considerations. For convenience in the following applications the equation $s_1 s_2^2 = s_2 s_1^2$ is written also in the following forms:

$$s_2^{-2} s_1^{-1} = s_1^{-2} s_2^{-1}, \qquad s_1^{-1} s_2 = s_2^2 s_1^{-2}, \qquad s_2^{-1} s_1 = s_1^2 s_2^{-2}.$$

Throughout the following two paragraphs it will be assumed that s_1 and s_2 are both of odd order. Hence formula (A) may be written in the simpler form

$$(A') \qquad s_1 s_2^m s_1^{-1} s_2^2 s_1^{-m} s_2^{-2} = s_2 s_1^m s_2^{-1} s_1^2 s_2^{-m} s_1^{-2} = 1,$$

where m is an arbitrary integer. If we let $m = 1$ there results

$$(A'') \qquad s_1 s_2 s_1^{-1} s_2^2 s_1^{-1} s_2^{-2} = s_1 s_2 s_1^{-2} s_2 s_1 s_2^{-2} = 1.$$

From the last equation we have

$$s_2 (s_1 s_2^{-1})^m s_2^{-1} = s_1 (s_1 s_2^{-1})^m s_1^{-1}.$$

Hence $s_1 s_2^{-1}$, $s_2^{-1} s_1$ are commutative. That is, *if two operators of odd order satisfy the equation* $s_1 s_2^2 = s_2 s_1^2$ *they generate a solvable group whose commutator subgroup is either cyclic or the direct product of two cyclic groups.*

All the exponents of the second member of (A'') may be multiplied by 2 without changing its value, since $s_1 s_2 = s_1^2 s_2^2 s_1^{-2}$ and $s_2 s_1 = s_2^2 s_1^2 s_2^{-2}$. Hence the equation

$$s_1^2 s_2^2 s_1^{-4} s_2^2 s_1^2 s_2^{-4} = 1.$$

By employing the given relations between s_1, s_2 and especially those which can be directly obtained from $s_1 s_2^n s_1^{-1} = s_2^2 s_1^n s_2^{-2}$, $s_2 s_1^n s_2^{-1} = s_1^2 s_2^n s_1^{-2}$, it is not difficult

to verify the following equations:

$$(s_1 s_2^{-1})^5 = s_1^3 s_2^{-3} \cdot s_1 s_2^{-1} \cdot s_1^3 s_2^{-3} = s_1^3 s_2^{-4} s_1^2 s_2 s_1 s_2^{-3} = s_1^3 s_2^{-4} s_1^3 s_2^2 s_1^{-1} s_2^{-3}$$
$$= s_1^3 s_2^{-4} s_1^3 s_2^4 s_1^{-2} s_2^{-4} = s_1^3 s_2^{-4} s_1 s_2 s_1^4 s_2^{-5} = s_1^3 s_2^{-3} s_1^2 s_2^{-1} s_1^4 s_2^{-5}$$
$$= s_1^3 s_2^{-2} s_1^{-1} s_2^{-1} s_1^6 s_2^{-5} = s_1 s_2^{-2} s_1^6 s_2^{-5}.$$

Hence it results directly that

$$(B') \qquad (s_1 s_2^{-1})^{4n} = s_2^{-1} (s_1^6 s_2^{-6})^n s_2.$$

From the equations

$$1 = s_2 s_1 s_2^{-1} s_1^2 s_2^{-1} s_1^{-2} = s_2 s_1 s_2^{-2} s_1 s_2 s_1^{-2} = s_2 s_1 s_2^{-1} s_1^2 s_2^{-1} s_1^{-2} = s_2 s_1^3 s_2^{-2} s_1^3 s_2^{-2} s_1^{-3},$$

it follows that $s_2^2 \cdot s_2^{-1} s_1^3 \cdot s_2^{-2} = s_1^3 s_2^2 s_1^{-3}$, and hence the two operators $s_2^{-1} s_1^3$, s_2^2 have the same order. In a similar manner we observe from the equations

$$1 = s_1 s_2^{-1} s_1^{-1} s_2^2 s_1 s_2^{-2} = s_2^{-2} s_1 s_2^{-1} s_1^{-1} s_2^2 s_1 = s_2^{-2} s_1 s_2^{-1} s_1^{-2} s_2 s_1^3$$
$$= s_2^{-2} s_1^3 s_2^{-2} s_1^{-3} s_2 s_1^3 = s_2^2 \cdot s_2^{-4} s_1^3 \cdot s_2^{-2} \cdot s_1^{-3} s_2 s_1^3$$

that $s_2^{-4} s_1^3$ is of the same order as s_2. That is, *when s_1, s_2 are both of odd order all of the following five operators: s_1, s_2, $s_1 s_2$, $s_2^{-1} s_1^3$, $s_2^{-4} s_1^3$ are of the same order.*

§ 3. *Several Special Cases.*

If we add to the equation $s_1 s_2^2 = s_2 s_1^2$ the additional equation $s_1^n = 1$, it is not difficult to determine all the possible groups for the different values of n from 2 to 5. If $n = 2$ it results directly from the former of these equations that $s_1 = s_2^{-1}$ and hence the group (G) generated by s_1, s_2 is of order 2. If $n = 3$ it results from the preceding section that the order of s_2 is either 3 or 6 and that the order of the commutator $s_1 s_2^{-1}$ is either 2 or 4, since $(s_1 s_2^{-1})^2 = s_1^3 s^{-3}$. If s_2 is of order 3 the order of $s_1 s_2^{-1}$ is 2 and hence G is generated by two operators of order 3 whose product is of order 2. It is well known that every pair of operators which satisfy these conditions generate the tetrahedral group. On the other hand, if s_2 is of order 6 when $n = 3$, the order of $s_1 s_2^{-1}$ is 4 and $(s_1 s_2^{-1})^2 = s_2^3$. It is known that the group of order 24 which does not involve a subgroup of order 12 is the only group that can be generated by two operators which fulfil these conditions.*

When $n = 4$ it results from the preceding section that s_2 is also of order 4 and that $s_1 s_2$ is of order 2. Hence, $s_2 s_1 = s_1^{-1} s_2^{-1}$, and $s_1^{-2} \cdot s_1 s_2^{-1} \cdot s_1^2 = s_1^{-1} s_2^{-1} \cdot s_1^2 = s_2 s_1^3 = s_2 s_1^{-1} = (s_1 s_2^{-1})^{-1}$. On the other hand, $s_1^{-1} \cdot s_1 s_2^{-1} \cdot s_1 = s_2^{-1} s_1 = s_2^3 s_1^{-3} = (s_1 s_2^{-1})^{-2}$. That is, s_1^2 transforms $s_1 s_2^{-1}$ both into its 4th power and also into its

*Transactions of the American Mathematical Society, vol. 8 (1907), p. 4. An operator is said to fulfil the condition $s_1^n = 1$ if it is of order n; it is said to satisfy this condition if its order is a divisor of n.

inverse, and hence the order of $s_1 s_2^{-1}$ is 5. Since s_1 transforms $s_1 s_2^{-1}$ into the inverse of its square, it has been proved that *G is the holomorph of the group of order 5 when $n = 4$*. From the preceding section it results that the order of s_2 is either 5 or 10 when $n = 5$. We shall now prove that it cannot be 10. This will be done by assuming that s_1, s_2 fulfil the conditions $s_1^5 = 1$, $s_2^{10} = 1$, $s_1 s_2^2 = s_2 s_1^2$ and by showing that this assumption leads to a contradiction.

Suppose that s_1, s_2 fulfill the three conditions

$$s_1^5 = 1, \qquad s_2^{10} = 1, \qquad s_1 s_2^2 = s_2 s_1^2.$$

From formula (A) of the preceding section we obtain

$$s_1 s_2^6 s_1^{-1} s_2^2 s_1^{-1} s_2^{-2} = 1.$$

Hence

$$s_1 s_2^5 \cdot s_2 s_1^2 \cdot s_1^2 s_2^2 s_1^{-1} \cdot s_2^{-2} = s_1 s_2^5 s_1 s_2^2 s_1 s_2 s_1 s_2^{-2} = s_1 s_2^5 s_1 s_2^2 s_1 s_2^2 s_1^2 s_2^{-4}$$

$$= s_1 s_2^5 s_1 s_2^3 s_1^{-1} s_2^{-4} = s_1 s_2^5 s_1 s_2^5 s_1^{-2} s_2^5 = 1.$$

From the last of these equations it is evident that the conjugates of s_2^5 with respect to s_1^{-1}, s_2^{-2} are commutative, since the product of two operators of order 2 $(s_1 s_2^5 s_1^{-1}, s_1^2 s_2^5 s_1^{-2})$ is of order 2. Transforming this last equation by s_1^{-1} leads to the equation

$$s_1^3 s_2^5 s_1^{-3} = s_1 s_2^5 s_1^{-1} \cdot s_1^2 s_2^5 s_1^{-2} = s_2^5.$$

Since s_1^3 is commutative with s_2^5 and since s_1^3 generates s_1 it results that s_1 is commutative with s_2^5, and hence we have $s_2^{10} = s_2^5 = 1$. As this is contrary to the hypothesis, it has been proved that *the two equations $s_1^5 = 1$, $s_1 s_2^2 = s_2 s_1^2$ imply that $s_2^5 = 1$.*

We proceed to determine all the groups which can be generated by two operators satisfying the two conditions

$$s_1^5 = 1, \qquad s_1 s_2^2 = s_2 s_1^2.$$

As $s_1^{-3} \cdot s_1 s_2^{-1} \cdot s_1^3 = s_1^{-2} s_2^{-1} s_1^3 = s_2^{-2} s_1^2 = s_2^3 s_1^{-3} = (s_1 s_2^{-1})^{-2}$ according to formula (B) of the preceding section, it results that $s_1^{-15}(s_1 s_2^{-1}) s_1^{15} = (s_1 s_2^{-1})^{-32}$ and hence the order of $s_1 s_2^{-1}$ must divide 33. To prove that this order is 11 or 1 we may proceed as follows: $s_1^{-6} \cdot s_1 s_2^{-1} \cdot s_1^6 = s_1^{-1} s_1 s_2^{-1} s_1 = s_2^{-1} s_1 = (s_1 s_2^{-1})^4$. Multiplying both members of the last equation by $s_1^3 s_2^{-3} = (s_1 s_2^{-1})^2$, we find that $(s_1 s_2^{-1})^6 = s_1^3 s_2 s_1$; hence $(s_1 s_2^{-1})^{11} = s_2 s_1^{-1} \cdot s_1^3 s_2 s_1^{-1} s_2 s_1 = s_2 s_1^2 s_2 s_1^{-1} s_2 s_1 = s_1 s_2^3 s_1^{-1} s_2 s_1$ $= s_1 \cdot s_2^{-2} s_1^{-1} \cdot s_2 s_1 = s_1 \cdot s_1^{-2} s_2^{-1} \cdot s_2 s_1 = 1$. As $s_1 s_2^{-1}$ is of order 11 or 1 it results that G is either the non-cyclic group of order 55 or the group of order 5. That is, *the group of order 5 and the non-cyclic group of order 55 are the only two groups which can be generated by two operators which satisfy both of the conditions $s_1^5 = 1$, $s_1 s_2^2 = s_2 s_1^2$.*

§ 4. *Groups whose Two Generators satisfy the Three Conditions* $s_1^6 = 1,\ s_2^6 = 1,\ s_1 s_2^2 = s_2 s_1^2$.

In the preceding section we considered all the possible groups when the order of at least one of the operators s_1, s_2 is less than 6. Hence we shall assume throughout the present section that each of these operators is actually of order 6. We shall first prove that each of the two commutators $s_1 s_2^{-1}$, $s_2^{-1} s_1$ which generate the commutator subgroup of G must transform the square of the other into its inverse. This interesting fact may be established as follows:

$$s_2^{-1} s_1 \cdot s_1 s_2^{-1} \cdot s_1^{-1} s_2 = s_2^{-1} s_1^2 s_2^{-1} \cdot s_1^{-1} s_2 = s_2^{-1} s_1^2 s_2 s_1^{-2}.$$

Hence it results that

$$s_2^{-1} s_1 (s_1 s_2^{-1})^2 s_1^{-1} s_2 = s_2^{-1} s_1^2 s_2 \cdot s_1^{-2} s_2^{-1} \cdot s_1^2 s_2 s_1^{-2} = s_2^{-1} s_1^2 \cdot s_2^{-1} s_1 \cdot s_2 s_1^{-2}$$
$$= s_2^{-1} \cdot s_1^{-2} s_2^{-1} \cdot s_1^{-2} = s_2^{-3} s_1^{-3} = (s_1 s_2^{-1})^{-2}.$$

In a similar manner we may prove that $s_1 s_2^{-1}$ transforms $s_2^{-1} s_1$ into its inverse, as follows:

$$s_1 s_2^{-1} \cdot s_2^{-1} s_1 \cdot s_2 s_1^{-1} = s_1 s_2^{-2} s_1 s_2 s_1^{-1} = s_1 s_2^{-1} s_1^2 s_2^{-1} s_1^{-1},$$

$$s_1 s_2^{-1} (s_2^{-1} s_1)^2 s_2 s_1^{-1} = s_1 s_2^{-1} \cdot s_1^2 s_2^{-2} \cdot s_1^2 s_2^{-1} s_1^{-1} = s_1 s_2^{-2} s_1^3 s_2^{-1} s_1^{-1}$$
$$= s_1^{-1} s_2^{-1} \cdot s_1^{-2} s_2^{-1} \cdot s_1^{-1} = s_1^{-1} s_2^{-3} s_1^{-2} = (s_2^{-1} s_1)^{-2}.$$

Having proved that the commutator subgroup of G is generated by two operators each of which transforms the square of the other into its inverse we proceed to consider this general category of groups. That is, we shall consider the category of groups generated by t_1, t_2 where no restrictions are imposed on t_1, t_2 except that they satisfy the two equations

$$t_1^{-1} t_2^2 t_1 = t_2^{-2}, \qquad t_2^{-1} t_1^2 t_2 = t_1^{-2}.$$

These conditions imply that $(t_1 t_2)^2 = (t_2 t_1)^{-2}$, and hence each of the three cyclic groups generated by the operators t_1^2, t_2^2, $(t_1 t_2)^2$ respectively is invariant under the group K generated by t_1, t_2. Any two of these three cyclic subgroups have at most two common operators, since each one of the three operators t_1, t_2, $t_1 t_2$ transforms into their inverses all the operators of two of these three cyclic groups and those of the third into themselves. That is, all the operators of the three groups $\{t_2^2, (t_1 t_2)^2\}$, $\{t_1^2, (t_1 t_2)^2\}$, $\{t_1^2, t_2^2\}$ are transformed into their inverses by t_1, t_2, $t_1 t_2$ respectively.

From the preceding results it is evident that the abelian group $\{t_1^2, t_2^2, (t_1 t_2)^2\}$ is invariant under K. Each of the three groups

$$\{t_1, t_2^2, (t_1 t_2)^2\},\ \{t_1^2, t_2, (t_1 t_2)^2\},\ \{t_1^2, t_2^2, t_1 t_2\}$$

is also invariant under K since $t_2^{-1} t_1 t_2 = t_2^{-2} t_1^{-1} (t_1 t_2)^2$. As a consequence, the quotient group of K with respect to $\{t_1^2, t_2^2, (t_1 t_2)^2\}$ is either the four group or a subgroup of this group, and K is always solvable. Hence the theorem: *If each of two operators transforms the square of the other into its inverse, these operators must also transform the square of their product into its inverse, and these three squares generate an abelian subgroup which is invariant under the group generated by the two operators. The index of this subgroup is a divisor of* 4.

It is not difficult to construct such groups in which the orders of $t_1^2, t_2^2, (t_1 t_2)^2$ are three arbitrary numbers. To do this we may write, in distinct sets of letters, three cyclic substitution groups of the required orders, each generator being composed of two equal cycles when its order is even. We then select t_1, t_2 in such a way that they generate respectively the first two of these cyclic groups and that their components involving the letters of the other cyclic groups are of order 2, transform the operators of these cyclic groups into their inverses and give a product of the required order. It follows directly from the properties of the dihedral group that these substitutions can be so selected that t_1, t_2 have the given properties, and this establishes the existence of K for any arbitrary set of numbers for the orders of $t_1^2, t_2^2, (t_1 t_2)^2$.

Having established some fundamental properties of the general category of groups which may be generated by two operators, each of which transforms the square of the other into its inverse, we return to the operators under consideration. The three operators,

$$(s_1 s_2^{-1})^2 = s_1^3 s_2^{-3}, \qquad (s_2^{-1} s_1)^2 = s_1^2 s_2^{-3} s_1, \qquad (s_1 s_2^{-2} s_1)^2 = s_1 s_2^{-3} s_1^2,$$

generate an invariant subgroup under the commutator group of G and its index under this group divides 4 according to the general theory. It is easy to verify that these three operators together with their inverses constitute a complete set of conjugates under G and hence the group generated by them is also invariant under G.

These results suffice to prove that G can be constructed when the order of $(s_1 s_2^{-1})^2$ is an arbitrary number. The general method can be easily deduced from the following example. Suppose that the order of $(s_1 s_2^{-1})^2$ is 3. Write the three cyclic substitutions abc, def, ghi and select a substitution of order 3

$$t = adg \cdot beh \cdot cfi$$

which merely permutes the corresponding letters of these cycles. Find a substitution of order 2 which transforms each of the cyclic substitutions into its inverse and is commutative with t. In the present case we may select $ab \cdot de \cdot gh$. For s_1 take the continued product of the second cycle, this substitution of order 2, and t. In the present case

$$s_1 = ab \cdot ef \cdot gh \cdot t = aeicfh \cdot bdg.$$

For s_2 we take the continued product of the first cycle, the component of the given substitution of order 2 which involves the letters of this cycle, and t.

$$s = bc \cdot t = adg \cdot bficeh.$$

It is easy to see that any two substitutions selected in the manner in which s_1, s_2 were chosen must be of order 6 and must also satisfy the equation $s_1 s_2^2 = s_2 s_1^2$. The three cyclic substitutions generate a group whose order is the cube of that of one of the cycles. This is the group generated by

$$(s_1 s_2^{-1})^2,\ (s_2^{-1} s_1)^2,\ (s_1 s_2^{-2} s_1)^2.$$

This abelian invariant subgroup is of index 4 under the commutator subgroup and of index 24 under G. In the special case under consideration G is of order 648 and it is the largest group which can be generated by two operators which satisfy the four conditions:

$$s_1^6 = 1,\ s_2^6 = 1,\ (s_1 s_2^{-1})^6 = 1,\ s_1 s_2^2 = s_2 s_1^2.*$$

If the order of $(s_1 s_2^{-1})^2$ had been even we should have proceeded in the same way except that we should have selected cyclic substitutions whose order is twice that of $(s_1 s_2^{-1})^2$ in place of substitutions like *abc*, *def*, *ghi* whose order is equal to that of $(s_1 s_2^{-1})^2$. But the case where $(s_1 s_2^{-1})^2$ is of odd order is sufficient to prove the theorem: *There is an infinite number of distinct groups each of which is generated by two operators satisfying the three conditions* $s_1^6 = s_2^6 = 1$, $s_1 s_2^2 = s_2 s_1^2$. *All such groups are solvable. The commutator subgroup of each of them is generated by two conjugate operators each of which transforms the square of the other into its inverse, and the order of each of the groups generated by* s_1, s_2 *is a divisor of three times the cube of the order of the commutator of* s_1, s_2.

If the commutator $s_1 s_2^{-1}$ of s_1, s_2 were of odd order, $s_2^{-1} s_1$ would also be of odd order. This is clearly impossible since each of these operators transforms the square of the other into its inverse. That is, *if two operators satisfy the three conditions* $s_1^6 = s_2^6 = 1$, $s_1 s_2^2 = s_2 s_1^2$, *their commutator must be of even order.* This theorem was proved by means of prolix considerations in volume 40 of the *Quarterly Journal of Mathematics*, page 201. It may be remarked that the other results of that article relating to the sets of conditions under consideration follow almost immediately from the theorems of the present paper and may be used to illustrate these theorems.

§ 5. *Groups whose two generators satisfy either the three conditions* $s_1^7 = s_2^7 = 1$, $s_1 s_2^2 = s_2 s_1^2$; *or the conditions* $s_1^9 = s_2^9 = 1$, $s_1 s_2^2 = s_2 s_1^2$.

Throughout the first two paragraphs it will be assumed that the first one of these two sets of conditions is satisfied.

*Quarterly Journal of Mathematics, vol. 40 (1909), p. 203.

By making $n = 1$ in formula B' of section 2 there results $(s_1 s_2^{-1})^4 = s_2^{-1} s_1^{-1} s_2^2$. Hence $(s_1 s_2^{-2})^5 = s_1 s_2^{-2} s_1^{-1} s_2^2 = s_1^{-1} s_2 = (s_2^{-1} s_1)^{-1}$. That is, the group generated by $s_1 s_2^{-1}$ involves $s_2^{-1} s_1$ and is therefore invariant under G. Hence the commutator subgroup of G is the cyclic group generated by $s_1 s_2^{-1}$. Since $s_1^{-1} \cdot s_1 s_2^{-1} \cdot s_1 = s_2^{-1} s_1 = (s_1 s_2^{-1})^{-5}$ it results that $(-5)^7 \equiv 1$ modulo the order of $s_1 s_2^{-1}$. Hence the order of $s_1 s_2^{-1}$ divides $6 \cdot 29 \cdot 449$. To verify that this order is 29 we may proceed as follows:

$$(s_1 s_2^{-1})^{29} = (s_1 s_2^{-1})^4 (s_1^{-1} s_2)^5 = (s_1 s_2^{-1})^4 s_1^{-1} s_2 (s_1^{-1} s_2)^4 = (s_1 s_2^{-1})^4 s_1^{-1} s_2 s_1^{-1} (s_1 s_2^{-1})^{-4} s_1$$

$$= s_2^{-1} s_1^{-1} s_2^2 s_1^{-1} s_2 s_1^{-1} s_2^{-2} s_1 s_2 s_1 = s_2^{-1} s_1^{-1} s_2^4 s_1^{-3} s_2^{-2} s_1 s_2 s_1$$

$$= s_2^{-1} s_1^{-1} s_2^4 s_1^{-2} s_2^{-2} s_1^2 = s_2^{-1} s_1^{-1} s_2^2 s_1 s_2^{-2} s_1 = 1.$$

Since the order of $s_1 s_2^{-1}$ is 29 or 1, G must be the non-cyclic group of order 203 or the group of order 7. It is evident that G may be of order 7. That it may also be of order 203 may be proved in the following manner.

Suppose that t is an operator of order 19 and that $s_1^{-1} t s_1 = t^{24}$. Since 24 belongs to exponent 7 modulo 29 we may assume that s_1 is of order 7 and hence $s_1 t$ is also of order 7. The two operators s_1, $s_1 t$ evidently generate the non-cyclic group of order 203 and $s_1 (s_1 t)^2 = s_1^2 t s_1 t = s_1^3 s_1^{-1} t s_1 t = s_1^3 t^{25} = s_1 t s_1^2$ since $24^2 \equiv 25 \bmod 29$. These results prove that there is only one prime number p which satisfies the condition that it is possible to find a number α belonging to exponent 7 and satisfying the equation $\alpha + 1 \equiv \alpha^2 \bmod p$. This prime number is 29 and α is 24. This result may also be stated as follows: *If α belongs to exponent 7 with respect to a prime number p and if $\alpha + 1 \equiv \alpha^2$ mod p then $p = 29$ and $\alpha = 25$.* We are thus led to a characteristic property of the prime 29. Similar characteristic properties of the primes 5 and 11 may be deduced from the results of section 3, and in what follows we shall establish also such a characteristic property of 19.

When $s_1^9 = s_2^9 = 1$, $s_1 s_2^2 = s_2 s_1^2$ formula B' gives rise to the equations

$$(s_1 s_2^{-1})^{4n} = s_2^{-1} (s_1^{-3} s_2^3)^n s_2 = s_2^{-1} s_1^{-3} (s_1 s_2^{-1})^{-2n} s_1^3 s_2.$$

Since $s_1^3 s_2$ transforms $(s_1 s_2^{-1})^2$ into a power of itself we shall first prove that the order of $s_1^3 s_2$ is 9. This fact is established by the following equations:

$$(s_1^3 s_2)^4 = s_1^3 s_2 s_1^3 s_2 s_1^3 s_2 s_1^3 s_2 = s_1^4 s_2^2 s_1^2 s_2^2 s_1^2 s_2^2 s_1 s_2$$

$$= s_1^4 s_2^3 s_1^2 s_2^{-1} s_1^4 s_2^2 s_1 s_2 = s_1^4 s_2^4 s_1^{-1} s_2^{-1} s_1^6 s_2^2 s_1 s_2$$

$$= s_1^4 s_2^2 s_1^{-2} s_2^{-2} s_1^6 s_2^2 s_1 s_2 = s_1^4 s_2^6 s_1^{-4} s_2^{-1} s_1^{-2} s_2^2 s_1 s_2$$

$$= s_1^4 s_2^6 s_1^{-6} s_2 s_1^{-1} s_2 s_1 s_2 = s_1^4 s_2^6 s_1^3 s_2^3 s_1^{-1} s_2.$$

Hence $(s_1^3 s_2)^3 = s_1^4 s_2^6 s_1^3 s_2^3 s_1^{-4} = s_1^4 s_2^6 \cdot s_1^3 \cdot (s_1^4 s_2^6)^{-1}$.

Since s_1^3 is of order 3 the order of $s_1^3 s_2$ must be 9, and from the fact that this operator transforms $(s_1 s_2^{-1})^2$ into $(s_1 s_2^{-1})^{-4}$ it results that its 9th power transforms $(s_1 s_2^{-1})^2$ into its -512th power. That is, the order of $s_1 s_2^{-1}$ must divide $1026 = 2 \cdot 19 \cdot 27$. In view of this result we are led to inquire whether the order of $s_1 s_2^{-1}$ could be 19. That this is possible results directly from the fact that if t is an operator of order 19, and if $s_1^{-1} t s_1 = t^5$ then s_1, $s_1 t$ satisfy the equation $s_1 (s_1 t)^2 = s_1 t s_1^2$, as $6 \equiv 25 \mod 19$. It is also easy to see that the group of order 36 generated by $s_1 = abc \cdot t_1$, $s_2 = bdc \cdot t_1$, where t_1 is invariant and of order 9, fulfils the conditions imposed upon the generators at the beginning of this paragraph. Hence it has been proved that *there is more than one non-abelian group which involves two generators satisfying the conditions* $s_1^9 = s_2^9 = 1$, $s_1 s_2^2 = s_1 s_2^2$, *but the only prime numbers which divide the order of such a group are* 2, 3, *and* 19.