

GROUPS GENERATED BY TWO OPERATORS
SATISFYING TWO CONDITIONS.

BY PROFESSOR G. A. MILLER.

(Read before the American Mathematical Society, October 29, 1910.)

THE largest group G generated by two operators s_1, s_2 satisfying two conditions of the form

$$s_1^{\alpha_1} s_2^{\alpha_2} \dots = 1, \quad s_1^{\beta_1} s_2^{\beta_2} \dots = 1$$

is, in general, of infinite order. For some special values of the exponents $\alpha_1, \alpha_2, \dots; \beta_1, \beta_2, \dots$ the order of G is necessarily finite,* but the general necessary and sufficient condition that the order of G be finite does not seem to be known. We proceed to a consideration of all the possible cases where a series of consecutive exponents is composed of numbers which have the common value unity while all of the other exponents are equal to zero, as these cases appear fundamental in the general problem.

§1. *Consecutive Exponents Equal to Unity While all the Others are Zero.*

It is easy to verify that all these possible cases are included in the following five general forms :

$$\begin{aligned} (s_1 s_2)^\alpha &= (s_2 s_1)^\beta = 1, & (s_1 s_2)^\alpha &= (s_1 s_2)^\beta s_1 = 1, \\ (s_1 s_2)^\alpha &= (s_2 s_1)^\beta s_2 = 1, & (s_1 s_2)^\alpha s_1 &= (s_1 s_2)^\beta s_1 = 1, \\ & & (s_1 s_2)^\alpha s_1 &= (s_2 s_1)^\beta s_2 = 1. \end{aligned}$$

As the first two conditions are equivalent to the single condition $(s_1 s_2)^\delta = 1$, δ being the highest common factor of α and β , the order of G is infinite in this case.† When $\alpha = \beta$ the fourth pair of conditions reduces also to a single condition and hence the order of G must also be infinite in this special case. We proceed to prove that G must be a cyclic group of finite order in each of the other possible cases.

To prove this fact we may first observe that G must be cyclic

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

† *Ibid.*

whenever s_1, s_2 satisfy any one of the given five pairs of conditions except the first, since the cyclic group generated by $s_1 s_2$ includes the operators s_1, s_2 in each of these cases. When either the second or the third pair of conditions is satisfied, the order of $s_1 s_2$ is explicitly a divisor of α and hence the order of G is a divisor of α . That the order of G is exactly α in each of these cases results directly from the fact that it is possible to find two operators in any cyclic group of order α such that they satisfy the conditions imposed upon s_1, s_2 . This result may be expressed as follows :

If two operators s_1, s_2 are such that identity can be obtained by taking them alternately as factors, both when we have an even number and also when we have an odd number of such factors, then they generate a cyclic group whose order divides one-half of this even number, and every cyclic group may be generated by two operators satisfying two such conditions.

To simplify the considerations as regards the two remaining pairs of conditions it may be well to observe the following elementary theorem : If α and β are any two numbers and if G is an arbitrary cyclic group it is always possible to find a pair of generating operators of G such that they satisfy the condition $t_1^\alpha = t_2^\beta$.* When the fourth pair of the given conditions is satisfied it results directly that the order of $s_1 s_2$ is a divisor of $|\alpha - \beta|$. When $\alpha = \beta$ the order of G is infinite, as was observed above. When $\alpha \neq \beta$ G is clearly a cyclic group of order $|\alpha - \beta|$, since it is possible to find two generators of such a cyclic group which satisfy the conditions imposed on s_1, s_2 by these conditions.

It remains to consider the last one of the five given pairs of conditions. Since s_1 and s_2 are commutative it results that these conditions may also be expressed as follows :

$$s_1^{\alpha+1} s_2^\alpha = s_1^\beta s_2^{\beta+1} = 1.$$

Hence

$$s_1^{\alpha+1} = s_2^{-\alpha}, \quad s_1^{\beta(\alpha+1)} = s_2^{-\alpha\beta} = s_2^{-(\alpha+1)(\beta+1)}.$$

From the last equation it results that $s_2^{\alpha+\beta+1} = s_1^{\alpha+\beta+1} = 1$. Hence the order of G is a divisor of $\alpha + \beta + 1$. Moreover, in any cyclic group whose order is $\alpha + \beta + 1$ it is possible to find two operators which satisfy these conditions and also generate the group. This proves that the order of G is exactly $\alpha + \beta + 1$ whenever s_1, s_2 satisfy this pair of conditions. The preceding considerations constitute a proof of the following theorem :

* *Quarterly Journal of Mathematics*, vol. 36 (1905), p. 51.

If identity can be obtained in two ways by forming the continued product with two operators s_1, s_2 taken alternately as factors, then the largest group G generated by s_1, s_2 is of finite order except when the number of factors in both products is even, or when the number of these factors is the same odd number in both products and the same operator occurs an odd number of times in each. When the total number of times that each factor appears in the two products is the same and the number of factors in each product is odd then G is a cyclic group whose order is this total number.*

§ 2. Conditions Imposed upon the Possible Groups by the Single Relation $(s_1s_2)^\alpha = (s_2s_1)^\beta$, α and β being Relatively Prime.

Since the operators s_1, s_2 are supposed to satisfy the equation

$$(s_1s_2)^\alpha = (s_2s_1)^\beta$$

where α, β are relatively prime, it results immediately from the fact that s_1s_2 and s_2s_1 have the same orders that each of these two operators generates the other. Hence we may assume that

$$s_1s_2 = (s_2s_1)^\gamma.$$

The group G generated by s_1, s_2 involves invariantly the cyclic group generated by s_1s_2 since this cyclic group is generated also by $s_1^{-1} \cdot s_1s_2 \cdot s_1 = s_2s_1$. Hence G involves an invariant cyclic subgroup which gives rise to a cyclic quotient group.

Suppose that the order of s_1s_2 is n . It is evident that n is prime to γ . Moreover, it is possible to select s_1, s_2 so that n is an arbitrary number prime to γ , for a generator of the cyclic group of order n is transformed into its γ th power by an operator s_2 whenever γ is prime to n . If we let t represent this generator and $s_2^{-1}t$ represent s_1 , we have a set of operators which satisfy the given conditions. The order of s_2 is a multiple of the exponent to which γ belongs modulo n , but it is not restricted in any other way. Hence the order of G is any multiple of n multiplied by this exponent, but it is not subject to any other restriction. This proves the following theorem:

If two operators satisfy the condition $(s_1s_2)^\alpha = (s_2s_1)^\beta$, α and β being relatively prime, the order of s_1s_2 may have any arbitrary value n which is prime to α and β , and hence $s_1s_2 = (s_2s_1)^\gamma$. The order of s_2 is an arbitrary multiple of the exponent e to

* Cf. *American Journal of Mathematics*, vol. 31 (1909), p. 182.

which γ belongs modulo n , and hence the order of G , the group generated by s_1 and s_2 , is an arbitrary multiple of en . The group generated by s_1s_2 is invariant under G and leads to a cyclic quotient group and hence all such groups are solvable.

From this theorem it results immediately that if two operators satisfy two conditions of the form

$$(s_1s_2)^\alpha = (s_2s_1)^\beta,$$

α, β being relatively prime, they may always generate an arbitrary cyclic group, since it is always possible to assume that the order of s_1 is arbitrary and that $s_1 = s_2^{-1}$. Hence two operators satisfying two such conditions must always generate a solvable group, but these conditions are insufficient to restrict the order of the possible groups. That is, two such conditions may always be satisfied by the two generators of any group in an infinite system of solvable groups of finite order.

§ 3. Consecutive Exponents Equal to Unity in Both Members of Two Equations.

At the end of the preceding section we considered the possible groups when the two conditions may be expressed as follows:

$$(s_1s_2)^{\alpha_1} = (s_2s_1)^{\beta_1}, \quad (s_1s_2)^{\alpha_2} = (s_2s_1)^{\beta_2},$$

where $\alpha_1, \beta_1; \alpha_2, \beta_2$ are two pairs of relatively prime numbers. When these exponents are not relatively prime these conditions are not generally sufficient to restrict the possible groups to solvable groups, and it is evident that whenever each member of the equations involves an even number of operators, the two operators being taken alternately, there can be no upper limit to the order of the possible groups, since any operator and its inverse could be used for s_1, s_2 . It remains therefore only to consider the cases where at least one member involves an odd number of such factors.

When one member involves an odd number of such factors while the other involves an even number the equation is evidently equivalent to one of the following:

$$(s_1s_2)^{\alpha} s_1 = 1, \quad (s_2s_1)^{\beta} s_2 = 1.$$

Hence (s_1, s_2) is the cyclic group generated by s_1s_2 . If the second conditional equation also reduced to one of the form considered in section 1, the matter would require no further

consideration. Hence we may assume that the second equation assumes the following form :

$$(s_1 s_2)^{\alpha_1} s_1 = (s_2 s_1)^{\beta_1} s_2.$$

Since the preceding condition implies that s_1, s_2 are commutative, this equation becomes

$$s_1^{\alpha_1 - \beta_1 + 1} = s_2^{\beta_1 - \alpha_1 + 1} \quad \text{or} \quad s_1^k = s_2^{2-k}.$$

For the same reason the first equation must assume one of the following two forms

$$s_1^l = s_2^{1-l}, \quad s_1^l = s_2^{-1-l}.$$

Hence it results that

$$s_1^{kl} = s_2^{2l-kl} = s_2^{k-kl} \quad \text{or} \quad s_1^{kl} = s_2^{2l-kl} = s_2^{-k-kl}.$$

These conditions fix an upper limit for the order of s_2 and hence also for the order of the cyclic group generated by s_1, s_2 , unless $2l$ is equal either to k or to $-k$. That is, *two equations of the forms $(s_1 s_2)^\alpha s_1 = 1, (s_1 s_2)^{\alpha_1} s_1 = (s_2 s_1)^{\beta_1} s_2$ define a cyclic group of finite order unless $2\alpha + 1 = \alpha_1 - \beta_1$; and two equations of the forms $(s_2 s_1)^\beta s_2 = 1, (s_1 s_2)^{\alpha_1} s_1 = (s_2 s_1)^{\beta_1} s_2$ define a cyclic group of finite order unless $2\beta = \beta_1 - \alpha_1 - 1$.* When the special conditions are satisfied these operators generate a cyclic group whose order has no upper limit.

It remains to consider the possible groups when the two given conditions are of the forms

$$(s_1 s_2)^{\alpha_1} s_1 = (s_2 s_1)^{\beta_1} s_2, \quad (s_1 s_2)^{\alpha_2} s_1 = (s_2 s_1)^{\beta_2} s_2.$$

On multiplying the members of the first equation by the inverses of the members of the second, there results the equation

$$(s_1 s_2)^{\alpha_1 - \alpha_2} = (s_2 s_1)^{\beta_1 - \beta_2}.$$

If the two numbers $\alpha_1 - \alpha_2, \beta_1 - \beta_2$ are relatively prime, this equation implies that the cyclic group generated by $s_1 s_2$ is invariant under (s_1, s_2) , as was observed above. Since each of the two conditional equations implies that s_1, s_2 correspond to the same operator in the quotient group of (s_1, s_2) as regards the invariant subgroup generated by $s_1 s_2$, and as s_1 and s_2 must also correspond to inverse operators in this quotient group, it results that this quotient group is of order 2, if it is not

identity. Suppose that n is the order of $s_1 s_2$. As n is prime to both $\alpha_1 - \alpha_2$ and $\beta_1 - \beta_2$ according to our hypothesis, it results that a positive number x_0 less than n can be found so that $(\beta_1 - \beta_2)x_0 \equiv 1 \pmod n$. Hence $s_2 s_1 = (s_1 s_2)^\delta$, $\gamma \equiv (\alpha_1 - \alpha_2)x_0 \pmod n$. Since s_1^2 is $(s_1 s_2)^\delta$ it is necessary that $\gamma^2 \equiv 1 \pmod n$. From this it results that n is a modulus of the following congruences:

$$(\beta_1 - \beta_2)x_0 \equiv 1, \quad (\alpha_1 - \alpha_2)^2 x_0^2 \equiv 1.$$

Hence $(\beta_1 - \beta_2)^2 \equiv (\alpha_1 - \alpha_2)^2 \pmod n$. The value of n must therefore be a divisor of $|(\beta_1 - \beta_2)^2 - (\alpha_1 - \alpha_2)^2|$, and as the order of (s_1, s_2) cannot exceed $2n$, this proves that the two conditions under consideration generally restrict the order of the group generated by s_1, s_2 . In fact, we have proved the theorem:

The largest group generated by two operators which satisfy the two equations

$$(s_1 s_2)^{\alpha_1} s_1 = (s_2 s_1)^{\beta_1} s_2, \quad (s_1 s_2)^{\alpha_2} s_1 = (s_2 s_1)^{\beta_2} s_2,$$

where $\alpha_1 - \alpha_2$ and $\beta_1 - \beta_2$ are two relatively prime numbers, is solvable and has an order which divides $2|(\beta_1 - \beta_2)^2 - (\alpha_1 - \alpha_2)^2|$.

When this group is abelian it must be cyclic.* As an illustration of the fact that two such equations may define a cyclic group and also a non-cyclic group of order $2|(\beta_1 - \beta_2)^2 - (\alpha_1 - \alpha_2)^2|$ we may use the following two sets of equations:

$$\begin{aligned} (s_1 s_2)^2 s_1 &= s_2 s_1 s_2, & s_1 s_2 s_1 &= (s_2 s_1)^3 s_2; \\ (s_1 s_2)^2 s_1 &= (s_2 s_1)^3 s_2, & s_1 s_2 s_1 &= s_2 s_1 s_2. \end{aligned}$$

From the first set we obtain $s_1 s_2 = (s_2 s_1)^{-2} = s_2 s_1$, since $(s_1 s_2)^3 = 1$; and hence the first equation reduces to $s_1^2 = 1$ while the second becomes $1 = s_1 s_2^3$ or $s_1 = s_2^3$. Hence we may assume that s_2 is of order 6 and that $(s_1 s_2)$ is the cyclic group of order 6, since such operators clearly satisfy each of the two conditional equations of the first set.

On the other hand, the second set of equations implies that $s_1 s_2 = (s_2 s_1)^2$, and hence s_1^2 is again unity. As s_1 transforms $s_1 s_2$ into its inverse, it results that (s_1, s_2) is the symmetric group of order 6 in this case. It is also easy to verify that if we assume that s_1, s_2 are two operators of order 2 whose product is of order 3, the given conditional equations will be satisfied. It should not be assumed that the order of $s_1 s_2$ is

* *American Journal of Mathematics*, vol. 31 (1909), p. 182.

always equal to $|(\beta_1 - \beta_2)^2 - (\alpha_1 - \alpha_2)^2|$. In fact, this number is 5 when $(s_1s_2)^3s_1 = (s_2s_1)^4s_2$ and $s_1s_2s_1 = s_2s_1s_2$ but s_1s_2 in this case is identity, as may easily be verified. All that has been proved is that the order of s_1s_2 must always divide $|(\beta_1 - \beta_2)^2 - (\alpha_1 - \alpha_2)^2|$ when the two numbers $\alpha_1 - \alpha_2, \beta_1 - \beta_2$ are relatively prime. By assigning different values to the exponents $\alpha_1, \alpha_2, \beta_1, \beta_2$ so that $\alpha_1 - \alpha_2, \beta_1 - \beta_2$ are relatively prime we may thus obtain defining relations for an indefinite number of solvable groups of finite order. For instance, it is easy to verify that the two equations

$$(s_1s_2)^4s_1 = (s_2s_1)^3s_2, \quad (s_1s_2)^7s_1 = (s_2s_1)^8s_2$$

define the group of order 32 which involves a cyclic subgroup of order 16 while the remaining operators transform the operators of this cyclic group into their seventh powers.

§ 4. *The Special Case where $(s_1s_2)^{\alpha_1}s_1 = (s_2s_1)^{\beta_1}s_2$ and $(s_1s_2)^{\alpha_1-1}s_1 = (s_2s_1)^{\beta_1+1}s_2$.*

In this special case it is evident that the second equation may be replaced by the simpler one $s_1s_2 = (s_2s_1)^{-1}$. Hence the first equation becomes

$$(s_1s_2)^{\alpha_1}s_1 = (s_1s_2)^{-\beta_1}s_2, \quad \text{or} \quad (s_1s_2)^{\alpha_1+\beta_1+1} = s_2^2.$$

Since s_2s_1 is transformed into its inverse by s_2 and its $(\alpha_1 + \beta_1 + 1)$ -th power is commutative with s_2 it results that the order of s_1s_2 is a divisor of $2(\alpha_1 + \beta_1 + 1)$. On the other hand, it is easy to see that s_1, s_2 may be so selected as to generate the dicyclic group of order $4(\alpha_1 + \beta_1 + 1)$, and hence the order of s_1s_2 is exactly $2(\alpha_1 + \beta_1 + 1)$ whenever the operators s_1, s_2 are subject only to the two conditional equations expressed in the heading of this section. To prove this fact we may assume that $t = s_1s_2$ is an operator of order $2(\alpha_1 + \beta_1 + 1)$ and that $s_1^{-1}ts_1 = t^{-1}$. In the dicyclic group of order $4(\alpha_1 + \beta_1 + 1)$ which involves t we may let s_1 be any operator of order 4 which is not generated by t , and then s_2 may be so selected that $s_1s_2 = t$. The operators s_1, s_2 determined in this manner evidently satisfy the conditions imposed on s_1s_2 by the equations expressed in the heading of the present section. Hence the theorem :

If two operators are restricted only by the two equations $(s_1 s_2)^{\alpha_1} s_1 = (s_2 s_1)^{\beta_1} s_2$, $(s_1 s_2)^{\alpha_1 - 1} s_1 = (s_2 s_1)^{\beta_1 + 1} s_2$ they generate the dicyclic group of order $4(\alpha_1 + \beta_1 + 1)$.

From the symmetry of the equations it results that the same group is generated by s_1, s_2 when they satisfy the two conditions $(s_1 s_2)^{\alpha_1} s_1 = (s_2 s_1)^{\beta_1} s_2$, $(s_1 s_2)^{\alpha_1 + 1} s_1 = (s_2 s_1)^{\beta_1 - 1} s_2$. The close contact of the present paper with the one entitled "Finite groups which may be defined by two operators satisfying two conditions" * should be noted.

FUNDAMENTAL REGIONS FOR CYCLICAL GROUPS OF LINEAR FRACTIONAL TRANSFORMATIONS ON TWO COMPLEX VARIABLES.

BY PROFESSOR J. W. YOUNG.

(Read before the Southwestern Section of the American Mathematical Society, November 26, 1910.)

THE purpose of this note is to call attention to a simple method for obtaining fundamental regions for cyclical groups of linear fractional transformations on two complex variables. The simplicity of the method is due to the fact that the determination of a fundamental region for a group of the specified kind is made to depend merely on the construction of such a region for a simply isomorphic group on a single complex variable. The method, moreover, may be readily extended to the case in which the number of variables is n , and to certain restricted types of groups which are not cyclical and not linear.

Let V be any (non-identical) linear fractional transformation on two complex variables, and let Γ be the cyclical group generated by V , i. e., consisting of all transformations V^n ($n = 0, \pm 1, \pm 2, \dots$). We interpret V as a collineation in a complex plane, and will consider separately each of the five types to which V may belong according to the configuration of its invariant points and lines.

Suppose first that V is of Type I, i. e., has three and only three invariant points forming the vertices of a triangle ABC . Every transformation of Γ then has the same configuration of invariant elements. The group Γ transforms the points on

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