PRIME AND COMPOSITE POLYNOMIALS*

BY

J. F. RITT

I. INTRODUCTION

Let $F(z)$ represent any polynomial in z of degree greater than unity.† If there exist two polynomials, $\varphi_1(z)$ and $\varphi_2(z)$, each of degree greater than unity, such that

$$F(z) = \varphi_1[\varphi_2(z)], \tag{1}$$

we shall say that $F(z)$ is *composite*. If no such pair of polynomials exists we shall say that $F(z)$ is *prime*.‡

It will be convenient to omit the variable z and all symbols of aggregation from our notations, writing (1), for instance, $F = \varphi_1\varphi_2$.

If we have

$$F = \varphi_1 \varphi_2 \dots \varphi_r \tag{2}$$

where each $\varphi_i(z)$ is a polynomial of degree greater than unity, prime or composite, we shall say that (2) is a *decomposition* of $F(z)$.

The first result of the present paper is that *any two decompositions of a given polynomial into prime polynomials contain the same number of polynomials; the degrees of the polynomials in one decomposition are the same as those in the other, except, perhaps, for the order in which they occur.*

Two decompositions of $F(z)$ into the same number of polynomials,

$$F = \varphi_1 \varphi_2 \dots \varphi_r, \qquad F = \psi_1 \psi_2 \dots \psi_r,$$

will be said to be *equivalent* if there exist $r-1$ polynomials of the first degree

$$\lambda_1(z), \lambda_2(z), \dots, \lambda_{r-1}(z)$$

such that

$$\psi_1 = \varphi_1\lambda_1, \quad \psi_2 = \lambda_1^{-1}\varphi_2\lambda_2, \quad \dots, \quad \psi_r = \lambda_{r-1}^{-1}\varphi_r.$$

* Presented to the Society, October 29, 1921.

† In this paper the powers of z will be understood to be included among the polynomials.

‡ We should have been glad to use the terms "primitive" and "imprimitive" had not these terms already been applied to polynomials, with a different significance.

Two decompositions of $F(z)$ which are not equivalent will be called *distinct*, whether they contain the same number of polynomials or not.

Our task in the present paper will be, after showing the constancy of the number of prime polynomials in the distinct decompositions of a given polynomial into prime polynomials, to determine those polynomials which have two or more distinct decompositions into prime polynomials.

The results will be easy to understand after we have examined some special cases.

If $F(z)$ is a power of z with an exponent which is not a power of a prime, then to every permutation of the prime factors of the exponent there corresponds a separate decomposition of $F(z)$ into prime powers of z. Here is a situation more general in certain respects. Let

$$\varphi(z) = z^n, \qquad \alpha(z) = z^r\, g(z^n)$$
$$\psi(z) = z^r[g(z)]^n, \qquad \beta(z) = z^n,$$

where $g(z)$ is any polynomial in z. If the degrees of $\varphi(z)$ and $\alpha(z)$ are prime, and unequal to each other, the four polynomials will be prime* and we will have in the equation

$$\varphi\alpha = \psi\beta$$

two distinct decompositions of the same polynomial.

Again, it is well known that for every positive integer n, we have

$$\cos nu = f_n(\cos u),$$

where $f_n(z)$ is the "trigonometric polynomial" of degree n. It is clear that for every pair of integers m and n

$$f_{mn} = f_m f_n = f_n f_m.$$

If, now, in a decomposition of $F(z)$ into prime polynomials

$$F = \varphi_1 \varphi_2 \cdots \varphi_r, \tag{3}$$

we have for an adjacent pair of prime polynomials,

$$\varphi_i = \lambda_1 \pi_1 \lambda_2, \qquad \varphi_{i+1} = \lambda_2^{-1} \pi_2 \lambda_3,$$

where $\lambda_1(z)$, $\lambda_2(z)$ and $\lambda_3(z)$ are linear and where $\pi_1(z)$ and $\pi_2(z)$, of unequal degrees m and n, respectively, are of any of the following three types:†

* It is possible for $\alpha(z)$ to be prime even if its degree is composite. For instance, let n be any prime number, and p and q two prime numbers, so large that $pq > (p+q+2)n$. Let $pq = kn + r$, where $0 < r < n$. The most general polynomial $\alpha(z)$, of degree pq and of the form $z^r g(z^n)$ contains $k+1$ parameters. But the most general composite polynomial of degree pq contains only $p+q+2$ parameters. Hence $\alpha(z)$ is generally prime.

† Case (a) with $m = 2$ can be reduced to Case (b) by a linear transformation.

(a) $\pi_1(z) = f_m(z)$, $\pi_2(z) = f_n(z)$,

(b) $\pi_1(z) = z^m$, $\pi_2(z) = z^r\, g(z^m)$,

(c) $\pi_1(z) = z^r[g(z)]^n$, $\pi_2(z) = z^n$,

it is clear that we have for $F(z)$ a decomposition distinct from (3),

$$F = \varphi_1 \ \dots \ \varphi_{i-1}\psi_1\psi_2\varphi_{i+2} \ \dots \ \varphi_r,$$

in which $\psi_1(z)$ is of degree n and $\psi_2(z)$ of degree m.

It will be shown that *if $F(z)$ has two distinct decompositions into prime polynomials, we can pass from either to a decomposition equivalent to the other by repeated steps of the three types just indicated.* This gives the solution of our problem.

The analogous problem for fractional rational functions is much more difficult. There is a much greater variety of possibilities, as one sees, without going far, on considering the formulas for the transformation of the periods of the elliptic functions. There are even cases in which the number of prime functions in one decomposition is different from that in another. We shall return to this matter in a later communication.

II. Condition for decomposability

It will give us no extra work to deal in this section with a general rational function, integral or fractional, instead of with a polynomial.*

Let w be a rational function, $F(z)$, of z, so that $z = F^{-1}(w)$. We shall understand the term "group of $F^{-1}(w)$" to mean always the group of monodromy of $F^{-1}(w)$.

We prove the following result:

A necessary and sufficient condition that $F(z)$ be composite is that the group of $F^{-1}(w)$ be imprimitive.†

Consider first the necessity of the condition. Suppose that

$$w = \varphi[\alpha(z)]$$

where $\varphi(u)$ and $\alpha(z)$ are rational functions of degrees m, greater than one, and n, greater than one, respectively. Let w_0 be any point which is not a critical point of $F^{-1}(w)$. Take a small neighborhood of w_0. Consider, in this neighborhood, any branch u_1 of $\varphi^{-1}(w)$. There are precisely n functions of w,

(4) $$z_1, z_2, \dots, z_n,$$

* What the terms "prime," "composite," etc., will mean for a general rational function need not be explained.

† This is a more precise result, as far as the sufficiency of the condition goes, for the case with which we are dealing, than the theorem that an equation with an imprimitive Galois group can be made to depend on two equations of lower degrees.

each uniform in the above neighborhood, such that $\alpha(z_i)=u_1$ $(i=1, 2, \ldots, n)$. The relation $\alpha(z_i)=\alpha(z_1)$ holding for any i, in the above neighborhood, and continuing to hold after any substitution of the group of $F^{-1}(w)$ is applied to it, it is clear that any substitution of the group which replaces z_1 by one of the functions (4) replaces every z_i by such a function. It follows from a well known theorem that the letters (4) constitute a system of imprimitivity of the group of $F^{-1}(w)$.*

We shall say that this system of imprimitivity *is determined by* $\alpha(z)$.

Now we prove the sufficiency of the condition. The function $F^{-1}(w)$, as the inverse of a rational function, has only one pole on its Riemann surface. We shall assume that the value of w which corresponds to this pole is not a critical point of $F^{-1}(w)$. This can always be brought about by replacing $F^{-1}(w)$ by a suitable linear fractional function of itself. The inverse of this new function will be prime or composite together with $F(z)$.

Let z_1 be the branch of $F^{-1}(w)$ which has the pole, and let (4) represent a system of imprimitivity of the group of $F^{-1}(w)$. Consider the function

$$u_1 = z_1 + z_2 + \cdots + z_n.$$

This function is unchanged by those substitutions which interchange the letters of (4) among themselves. As it has a pole, it is changed by any substitution which changes the set (4) into another set. Consequently, if there are m sets such as (4), that is, if $F(z)$ is of degree mn, u_1 is uniform on a Riemann surface of m sheets. Since it has only one pole, it must be the inverse of a rational function of degree m. We will write $w=\varphi(u_1)$. Since u_1 is unchanged by those substitutions which leave z_1 fixed, it is a rational function of z_1 and w; therefore, since $w=F(z_1)$, u_1 is a rational function of z_1 alone. Let $u_1=\alpha(z_1)$. We have $w=F(z_1)=\varphi[\alpha(z_1)]$, and therefore, by the principle of the permanence of functional equations we have identically

$$F(z) = \varphi[\alpha(z)]. \tag{5}$$

In this decomposition of $F(z)$, since $\varphi(u)$ is of degree m, $\alpha(z)$ must be of degree n.

Taking now the case where $F(z)$ is a polynomial, we shall show that there exists a linear function $\lambda(z)$ such that $\varphi\lambda$ and $\lambda^{-1}\alpha$ are polynomials. Thus we would gain no generality, in our study of polynomials, by admitting fractional functions into the decompositions.

Let $\alpha(\infty)=a$. Since $\varphi\alpha$ assumes the value infinity mn times for $z=\infty$, since $\alpha(z)$ can not assume the value a more than n times for $z=\infty$, and since $\varphi(u)$ cannot assume the value infinity more than m times for $u=a$, the values a and ∞ must be assumed precisely n and m times, respectively, by $\alpha(z)$ and

* Netto, *Gruppen- und Substitutionentheorie*, Leipzig, 1908, p. 143.

$\varphi(z)$ at the indicated points. Let $\lambda(z)$ be any linear function such that $\lambda^{-1}(a) = \infty$. Then $\lambda^{-1}\alpha$ assumes the value infinity n times for $z = \infty$, and is therefore a polynomial of degree n. Similarly $\varphi\lambda$ is a polynomial of degree m.

We shall show now that any decomposition of $F(z)$ which is based on the given system of imprimitivity is equivalent to (5). Suppose that $w = \varphi_1(v)$ and $v = \alpha_1(z)$ are two rational functions of degrees m and n, respectively, such that

$$F(z) = \varphi_1[\alpha_1(z)], \tag{6}$$

where, for the functions of (4),

$$\alpha_1(z_1) = \alpha_1(z_2) = \cdots = \alpha_1(z_n). \tag{7}$$

Let $v_1 = \alpha_1(z_1)$. By (7), v_1 is unchanged by those substitutions which interchange the functions (4) among themselves. It is therefore a rational function of u_1 and w, and as $w = \varphi(u_1)$, it is a rational function of u_1 alone. Thus $\alpha_1(z)$ is a rational function of $\alpha(z)$, and as it is of the same degree as $\alpha(z)$, it must be a linear function of $\alpha(z)$. This settles the equivalence of (5) and (6).

If, in (5), $\alpha(z)$ is a prime function, the systems of imprimitivity determined by $\alpha(z)$ cannot be broken up into smaller systems of imprimitivity. For, were that possible, the sum of the functions of that smaller set which contained z_1 would be a rational function of z_1, while u_1 would be a rational function of the sum, so that $\alpha(z)$ would be composite.

As the group of $F^{-1}(w)$ has only a finite number of systems of imprimitivity, there are only a finite number of possibilities for $\varphi_r(z)$ in (2). It follows by a quick induction that $F(z)$ *has only a finite number of distinct decompositions.*

III. The invariant integers*

Suppose that a polynomial $F(z)$ has two *distinct* decompositions into prime polynomials

$$F = \varphi_1\varphi_2 \cdots \varphi_r, \qquad F = \psi_1\psi_2 \cdots \psi_s. \tag{8}$$

We propose to show that r *equals* s, and that *the degrees of the polynomials* ψ *are the same as the degrees of the polynomials* φ *except for the order in which they occur.*

The theorem just stated is certainly true if the degree of $F(z)$ does not exceed six. It will suffice therefore to show that it holds for polynomials of degree n if it holds for the polynomials of all lower degrees.

If $\varphi_r(z)$ and $\psi_s(z)$ determine the same systems of imprimitivity, they are, as was

* The group-theoretic part of the present section consists mainly of a proof that Jordan's incorrect result on the invariance of the factors of imprimitivity of a group, *Traité des Substitutions*, p. 34, and Giornale di Matematiche, vol. 10 (1872), p. 176, holds when the group contains a substitution which permutes all of the letters in a single cycle.

shown in the preceding section, linear functions of each other. Making the substitution $\varphi(z)=u$ in both representations of $F(z)$, we are led to the consideration of a polynomial of degree less than n. The induction is thus carried through for this special case.

To handle the case where $\varphi_r(z)$ and $\psi_s(z)$ determine distinct types of imprimitivity, it will be desirable to determine the possible systems of imprimitivity of the group of $F^{-1}(w)$. This is made possible, fortunately, by the fact that $F^{-1}(w)$, if $F(z)$ is a polynomial of degree n, has a branch point of order $n-1$ at infinity. If the branches of $F^{-1}(w)$ are suitably numbered the substitution corresponding to this branch point may be written in a single cycle

$$(12 \cdots n). \tag{9}$$

Every system of imprimitivity of the group of $F^{-1}(w)$ is respected by this substitution. Suppose that there is a type of imprimitivity in which the letters break up into p sets, with h letters in each set, so that $n=hp$. Let the elements of the set which contains 1, arranged in order of magnitude, be

$$1, a_1, a_2, \ldots, a_{h-1}. \tag{10}$$

The (a_1-1)th power of (9), since it replaces 1 by a_1, interchanges the letters of (10) among themselves. It cannot disturb the cyclic order of the letters. Hence it must replace each letter by the one which follows it cyclically. We must therefore have $a_1=p+1$, and the set (10) is

$$1, \quad p+1, \quad 2p+1, \quad \cdots, \quad (h-1)\,p+1. \tag{11}$$

If we operate on the elements of (11) with the $(\nu-1)$th power of (9) we obtain the set $\nu+ip$ $(i=1, 2\ldots, h-1)$, which is also a system of imprimitivity.

Thus, given any divisor h, of n, the group of $F^{-1}(w)$ can have at most one type of imprimitivity with h letters in each set. Hence, if, in (8), $\varphi_r(z)$ and $\psi_s(z)$ determine distinct types of imprimitivity, these polynomials must be of different degrees.

Suppose then, that $\varphi_r(z)$ is of degree h, with $n=hp$, and that $\psi_s(z)$ is of degree k, with $n=kq$. The type of imprimitivity determined by $\varphi_r(z)$ has the sets

$$\nu+ip \qquad \begin{pmatrix}\nu=1, 2, \ldots, p\\ i=0, 1, \ldots, h-1\end{pmatrix}, \tag{12}$$

each value of ν determining one set, and the type of imprimitivity determined by $\psi_s(z)$ has the sets

$$\nu+iq \qquad \begin{pmatrix}\nu=1, 2, \ldots, q\\ i=0, 1, \ldots, k-1\end{pmatrix}. \tag{13}$$

We shall prove now a fact which will be of the greatest importance in the following section, namely that *h and k are relatively prime.* Suppose that h and k had a factor δ in common. The substitution (9) and its powers have a type of imprimitivity with δ letters in each set, each set of which is contained in a set of (12) and in a set of (13). Hence by the next to the last paragraph of §II, the existence of the factor δ would lead to the conclusion that $\varphi_r(z)$ and $\psi_s(z)$ are not prime.

As n is divisible by hk, the substitution (9) and its powers have systems of imprimitivity containing hk letters. Let I denote that one of these systems which contains z_1. Then I can be considered as consisting either of k sets of (12) or of h sets of (13). As no set of (12) has more than one letter in common with a set of (13), each of the k sets of (12) has precisely one letter in common with each of the h sets of (13).

Consider those substitutions of the group of $F^{-1}(w)$ which either leave z_1 fixed or replace it by some other letter of I. If we can show that these substitutions interchange the letters of I among themselves, we will know that I *is a system of imprimitivity of the group of* $F^{-1}(w)$. Such a substitution replaces the set of (12) to which z_1 belongs by another set of (12). Since both of these sets of (12) contain elements of each of the h sets of (13) which make up I, the substitution must interchange the h sets of (13), and hence the letters of I, among themselves.

There is a polynomial $\mu(z)$, of degree hk, which determines the system of imprimitivity just shown to exist. We have $F=\sigma\mu$ where $\sigma(z)$ is some polynomial, and also

$$\mu = \zeta\varphi_r, \qquad \mu = \xi\psi_s$$

where $\zeta(z)$ and $\xi(z)$ are polynomials of degrees k and h respectively.

The polynomial $\zeta(z)$ must be prime. If not, the set I would break up into several new systems of imprimitivity, each of these systems containing more than one set of (12). Such a new system would have more than one letter, but less than k letters, in common with each of the h sets of (13) of which I is composed. Thus the sets of (13) would break up into smaller systems of imprimitivity, and $\psi_s(z)$ could not be prime. Similarly, $\xi(z)$ must be prime.

Consider the two decompositions

$$F = \varphi_1\varphi_2 \cdots \varphi_r, \qquad F = \sigma\zeta\varphi_r. \tag{14}$$

We have

$$\varphi_1\varphi_2 \cdots \varphi_{r-1} = \sigma\zeta,$$

and since the members of this last equation are of degree less than n, the second member, with $\sigma(z)$ decomposed into prime polynomials, would contain the same

number of polynomials as the first, with the same degrees. Similar remarks apply to the two decompositions

$$F = \psi_1\psi_2 \cdots \psi_s, \qquad F = \sigma\xi\psi_s. \tag{15}$$

We need only to compare the situations described in (14) and (15) to complete the induction necessary for the proof of our theorem.

We shall now make clear by what kind of steps it is possible to pass from one of the decompositions of (8) to the other. We say that there is a sequence of decompositions of $F(z)$, beginning with the first of (8) and ending with the second, such that any decomposition is either equivalent to the one which precedes it, or else can be formed from the one which precedes it by taking two adjacent prime polynomials, $\varphi(z)$ and $\alpha(z)$ of the latter, and replacing $\varphi\alpha$ by $\psi\beta$, where $\psi(z)$ has the same degree as $\alpha(z)$ and $\beta(z)$ the same degree as $\varphi(z)$. That is, two consecutive decompositions, if not equivalent, have the forms

$$F = \zeta_1 \cdots \zeta_i\varphi\alpha\zeta_{i+3} \cdots \zeta_r$$

and

$$F = \zeta_1 \cdots \zeta_i\psi\beta\zeta_{i+3} \cdots \zeta_r$$

respectively.

This result is readily seen to hold if the degree of $F(z)$ does not exceed six. We shall prove that it holds for polynomials of degree n if it holds for polynomials of all lower degrees.

If ϕ_r and ψ_r, in (8), determine the same systems of imprimitivity, they are linear functions of each other. Let $\psi_r = \lambda\varphi_r$, and put $\psi'_{r-1} = \psi_{r-1}\lambda^{-1}$. It is possible to pass from the first of the two decompositions

$$\varphi_1\varphi_2 \cdots \varphi_{r-1}\,\varphi_r, \qquad \psi_1\psi_2 \cdots \psi_{r-2}\psi'_{r-1}\varphi_r$$

to the second by steps of the types described above, since

$$\varphi_1\varphi_2 \cdots \varphi_{r-1}$$

is of degree less than n. The second of these two decompositions is equivalent to the second of (8).

If φ_r and ψ_r determine distinct systems of imprimitivity we can pass from the first decomposition of (8) to the decomposition $\sigma\zeta\varphi_r$ by steps of the above types,* since $\sigma\zeta$ is of degree less than n. We can pass from the second decomposition of (8) to the decomposition $\sigma\xi\psi_r$ by similar steps. It needs only one step to pass from $\sigma\zeta\varphi_r$ to $\sigma\xi\psi_r$.

Consider any three consecutive decompositions of the sequence. To fix our ideas, suppose that the second is equivalent to the first, and that the third results

* We understand of course that σ is decomposed into prime polynomials.

from the second by a change of $\varphi\alpha$ into $\psi\beta$ as above described. It is clear that we could suppress the second decomposition and pass from the first to a decomposition equivalent to the third by redecomposing a polynomial $\varphi\alpha$.

Continuing this suppression of equivalent decompositions, we see that there exists a sequence of decompositions, beginning with the first of (8), and ending with one equivalent to the second, each one of which is obtained from the preceding by redecomposing a polynomial $\varphi\alpha$.

IV. The two-polynomial problem

The results of the preceding section reduce our problem to the following: *Under what circumstances can we have*

$$\varphi\alpha = \psi\beta,$$

*where $\varphi(z)$ and $\beta(z)$ are two prime polynomials of degree m, greater than unity, and $\psi(z)$ and $\alpha(z)$ two prime polynomials of degree n, greater than unity?**

In our treatment of this problem we shall not have occasion to impose the condition that the polynomials be prime. We shall assume only that each system of imprimitivity determined by $\alpha(z)$ has precisely one letter in common with each system of imprimitivity determined by $\beta(z)$. For this it is necessary and sufficient that m and n be relatively prime.

We put

$$w = F(z) = \varphi(u) = \psi(v),$$

where

$$u = \alpha(z), \qquad v = \beta(z).$$

There will be five Riemann surfaces to consider, those namely for $F^{-1}(w)$, $\varphi^{-1}(w)$, $\psi^{-1}(w)$, $\alpha^{-1}(u)$ and $\beta^{-1}(v)$.

It will be very important to see how the surface for $F^{-1}(w)$ is related to those for $\varphi^{-1}(w)$ and $\alpha^{-1}(u)$. Suppose that for $u=c$, $\alpha^{-1}(u)$ has a critical point with a certain number of cycles. Since $\varphi^{-1}(u)$ assumes no value more than once on its Riemann surface, $F^{-1}(w)$ will surely have a critical point for $w=\varphi(c)$. If the value c is assumed by a branch u_1 of $\varphi^{-1}(w)$ which is uniform in the neighborhood of $\varphi(c)$, those branches z of $F^{-1}(w)$ for which $\alpha(z)=u_1$ will be ramified at $\varphi(c)$ like the branches of $\alpha^{-1}(u)$ for $u=c$. If the value c is assumed by a cycle of r branches of $\varphi^{-1}(w)$, each cycle of $\alpha^{-1}(u)$ at $u=c$ will lead to a cycle of $F^{-1}(w)$ at

* An idea which presents itself naturally is to consider this problem as one in undetermined coefficients. One might hope, for instance, with a judicious use of linear transformations, to show without actually determining the coefficients of the polynomials, that aside from Cases (*b*) and (*c*) mentioned in the introduction there is only one possibility, which would, of course, have to be Case (*a*). A study of the equations for the coefficients convinces me that such a plan would not be easy to carry out, and that the function-theoretic methods used here are not far-fetched.

$\varphi(c)$, with r times as many sheets. If $\varphi^{-1}(w)$ has a critical point for $w=d$, and if $\alpha^{-1}(u)$ has no critical point for any value of $\varphi^{-1}(d)$, then each cycle of $\varphi^{-1}(w)$ at d leads to n cycles of the same number of sheets for $F^{-1}(w)$ at d.

In any case, if $\varphi^{-1}(w)$ has no uniform branches at d, $F^{-1}(w)$ will have no uniform branches at d.

If the branches of $\varphi^{-1}(w)$ are $u_1, u_2, \ldots, u_m$, the group of $F^{-1}(w)$ will have m systems of imprimitivity

$$U_1, U_2, \ldots, U_m,$$

with n letters z in each set, such that for every letter of U_i we have $\alpha(z)=u_i$. Similarly, if the branches of $\psi^{-1}(w)$ are $v_1, v_2, \ldots, v_n$, the group of $F^{-1}(w)$ will have n systems of imprimitivity

$$V_1, V_2, \ldots, V_n,$$

with m letters z in each set.

If w moves around a closed path the sets U are permuted like the branches of $\varphi^{-1}(w)$, and the sets V like the branches of $\psi^{-1}(w)$.

The following fact will be fundamental in our work:

*If a substitution of the group of $F^{-1}(w)$ interchanges the letters of some set U_i among themselves, it interchanges the sets V with a substitution similar to that which it effects on the letters of U_i.**

This follows from the fact that U_i contains precisely one letter of each set V.

It will be convenient in what follows to call the sum of the orders of the branch points of an algebraic function at a given critical point the *index* of the function at the point. Since the Riemann surface of the inverse of a rational function is of genus zero, the sum of the indices of the inverse of a rational function of degree m, for all of its critical points, is $2m-2$. The sum of the indices of the inverse of a polynomial of degree m, for all of its critical points excluding infinity, is $m-1$. If the inverse of a rational function of degree m has a critical point for which none of its branches is uniform, its index at that point is at least $m/2$.

We are going to derive some relations between the critical points of $\alpha^{-1}(u)$ and those of $\psi^{-1}(w)$. Similar results will hold for $\beta^{-1}(v)$ and $\varphi^{-1}(w)$.

Consider a critical point $u=c$ of $\alpha^{-1}(u)$. As u makes a turn around c the branches of $\alpha^{-1}(u)$ undergo a certain substitution. Suppose that $\varphi^{-1}(w)$ has a branch u_i which is uniform in the neighborhood of $\varphi(c)$ and assumes there the value c. As w makes a turn about $\varphi(c)$ the value of u_i makes a turn about c. The letters of the set U_i will undergo a permutation similar to that of the branches of $\alpha^{-1}(u)$ for the point c. The sets V must consequently undergo a similar permutation.

* In saying that two substitutions are similar, we will mean that they consist of the same number of cycles, with an equal number of letters in corresponding cycles.

Hence, in this case, $\psi^{-1}(w)$ has a critical point for $w=\varphi(c)$, with a substitution similar to that of $\alpha^{-1}(u)$ for $u=c$. The index of $\psi^{-1}(w)$ at $\varphi(c)$ equals the index of $\alpha^{-1}(u)$ at c.

If a value d is assumed at $\varphi(c)$ by another branch of $\varphi^{-1}(w)$, also uniform at $\varphi(c)$, then $\alpha^{-1}(u)$ must have a critical point at d, with a substitution similar to that which it has at c. In this case the index of $\psi^{-1}(w)$ at $\varphi(c)$ is less than the sum of the indices of $\alpha^{-1}(u)$ for c and d.

Let us see now conversely, and with a little greater precision, what the nature of a critical point of $\psi^{-1}(w)$ implies with respect to the critical points of $\alpha^{-1}(u)$.

Suppose that at the point $w=e$, $\varphi^{-1}(w)$ has a critical point with the substitution

$$S_1S_2 \ldots S_r, \tag{16}$$

where each S_ρ represents a cycle containing i_ρ letters, and $\psi^{-1}(w)$ a critical point with the substitution

$$T_1T_2 \ldots T_s, \tag{17}$$

each T_ρ representing a cycle containing j_ρ letters.

Consider a cycle S_ρ, and let h be the value which $\varphi^{-1}(w)$ assumes at the branch point corresponding to that cycle. We seek to determine how the branches of $\alpha^{-1}(u)$ behave as u makes a turn around h. For u to turn once around h, w must turn i_ρ times around e. For this turn, the branches of $\psi^{-1}(w)$ undergo a permutation which is the i_ρth power of (17). The function $\alpha^{-1}(u)$ has a critical point for $u=h$ with a substitution similar to the i_ρth power of (17).

Let us get an idea of the index of $\alpha^{-1}(u)$ at h. Consider one of the cycles T_q. If i_ρ is prime to j_q, the i_ρth power of T_q will be a cyclic substitution of order j_q, so that the cycle T_q will contribute j_q-1 to the index of $\alpha^{-1}(u)$ at h. If i_ρ is divisible by j_q, T_q contributes nothing to the index of $\alpha^{-1}(u)$ at h. If i_ρ is not divisible by j_q, then at the worst the i_ρth power of T_q can break up into cycles of two letters, so that T_q must contribute at least $j_q/2$ to the index of $\alpha^{-1}(u)$ at h.

If the sum of the indices of $\alpha^{-1}(u)$ for those points which correspond to the values assumed by $\varphi^{-1}(w)$ at e is less than the index of $\psi^{-1}(w)$ at e we shall say that $\psi^{-1}(w)$ has an *extra point* at e. This convention will apply also with respect to $\beta^{-1}(v)$ and $\varphi^{-1}(w)$.

Such an extra point of $\psi^{-1}(w)$ must exist, for instance, if $\psi^{-1}(w)$ has a critical point at which more than one branch of $\varphi^{-1}(w)$ is uniform, since, $\alpha(z)$ and $\psi(v)$ having the same degree, the sum of the indices of the inverse of one equals the corresponding sum for the other. If $\psi^{-1}(w)$ has an extra point at e, no branch of $\varphi^{-1}(w)$ can be uniform in the neighborhood of e, for, as seen above, every such uniform branch would lead to a critical point of $\alpha^{-1}(u)$ with an index equal to that of $\psi^{-1}(w)$ at e. Also $\psi^{-1}(w)$ cannot have an extra point at infinity, since

$\psi^{-1}(w)$ and $\alpha^{-1}(u)$ have the same index, $n-1$, at infinity. Finally, $\psi^{-1}(u)$ cannot have more than a single extra point. In short, at each extra point of $\psi^{-1}(w)$, the function $\varphi^{-1}(w)$, having no uniform branches, has an index not less than $m/2$, so that, since the sum of the indices of $\varphi^{-1}(w)$ for all of its critical points, excluding infinity, is $m-1$, two such extra points cannot exist.

We are going to show that $\psi^{-1}(w)$ and $\varphi^{-1}(w)$ cannot each have an extra point.

If both functions have an extra point, their extra points must correspond to the same value of w. For at an extra point either of $\psi^{-1}(w)$ or of $\varphi^{-1}(w)$, the function $F^{-1}(w)$, since every one of its branches is permuted, must have an index not less than $mn/2$. There cannot be two such points.

Suppose then that $\psi^{-1}(w)$ and $\varphi^{-1}(w)$ each have an extra point at $w=e$. Neither can have a branch which is uniform at e. The branches of $\varphi^{-1}(w)$ undergo at e a substitution of the form (16) with

$$i_1 + i_2 + \cdots + i_r = m, \tag{18}$$

while the branches of $\psi^{-1}(w)$ undergo a substitution of the form (17), with

$$j_1 + j_2 + \cdots + j_s = n. \tag{19}$$

Suppose that every one of the numbers j has one of the following two properties:*

(a) Two of the numbers i are not divisible by it.

(b) One of the numbers i has no factor in common with it.

Consider j_q, for instance, and suppose that it has the property (a) relative to i_a and i_b. Let h and k be the values which $\varphi^{-1}(w)$ assumes at the branch points corresponding to the cycles S_a and S_b. As i_a is not divisible by j_q, the cycle T_q must contribute at least $j_q/2$ to the index of $\alpha^{-1}(u)$ at h. Similarly it must contribute at least $j_q/2$ to the index of $\alpha^{-1}(u)$ at k. Again, if j_q has the property (b) relative to i_a, T_q contributes precisely j_q-1 to the index of $\alpha^{-1}(u)$ at h.

It is clear that if every j had one of the two properties, the sum of the indices of $\alpha^{-1}(u)$ at the points corresponding to the values which $\varphi^{-1}(w)$ assumes at e would be at least as great as the index of $\psi^{-1}(w)$ at e, so that e could not be an extra point of $\psi^{-1}(w)$.

There must consequently exist a number j_q which divides into all except perhaps one of the numbers i, and which has a factor in common with that i. That factor of j_q, being a factor of all of the numbers i, is a factor of m, and since m and n are prime to each other it cannot be a factor of n. Thus there is a j which is not divisible by that factor of the numbers i. Let it be j_1, for instance, and let h be the value which $\psi^{-1}(w)$ assumes at the branch point corresponding to the cycle T_1. Since j_1 is not divisible by any i_p, each cycle S_p contributes at least $i_p/2$ to the index of $\beta^{-1}(v)$ at h.

* If the substitution (16) has only one cycle, only the second property need be considered.

Hence the index of $\beta^{-1}(v)$ at h is at least $m/2$. Certainly then, the sum of the indices of $\beta^{-1}(v)$ for the points corresponding to the values assumed by $\psi^{-1}(w)$ at e is not less than $m/2$.

By an argument similar to that employed above, we can show that the sum of the indices of $\alpha^{-1}(u)$ at the points corresponding to the values assumed by $\varphi^{-1}(w)$ at e is at least $n/2$.

Let the indices of $\varphi^{-1}(w)$ and $\psi^{-1}(v)$ at e be

$$\frac{m}{2} + x, \qquad \frac{n}{2} + y,$$

respectively. The numbers x and y, each of which is at least unity, need not be integral.

Suppose, to fix our ideas, that x is not less than y. Since the sums of the indices of $\alpha^{-1}(u)$ and of $\psi^{-1}(w)$ are the same, namely $2n-2$, $\alpha^{-1}(u)$ must have a critical point with a finite affix which does not correspond to a value of $\varphi^{-1}(w)$ at e. Let c be such a critical point of $\alpha^{-1}(u)$. Consider the behavior of $\varphi^{-1}(w)$ at $\varphi(c)$. Since the sum of the indices of $\varphi^{-1}(w)$, excluding the point ∞, is $m-1$, the index of $\varphi^{-1}(w)$ at $\varphi(c)$ is not greater than

$$m - 1 - \left(\frac{m}{2} + x\right) = \frac{m}{2} - x - 1.$$

Hence not more than $m-2x-2$ branches of $\varphi^{-1}(w)$ can be permuted at $\varphi(c)$. Then at least $2x + 2$ branches of $\varphi^{-1}(w)$ are uniform in the neighborhood of $\varphi(c)$. Consequently $\psi^{-1}(w)$ must have a branch point at $\varphi(c)$ with an index at least that of $\alpha^{-1}(u)$ at c, and $\alpha^{-1}(u)$ must have at least $2x + 2$ such points, including c. The index of $\psi^{-1}(w)$ at $\varphi(c)$ is at least unity. Hence the sum of the indices of $\alpha^{-1}(u)$ at the $2x + 2$ or more critical points under consideration exceeds the index of $\psi^{-1}(w)$ at $\varphi(c)$ by at least $2x + 1$, a quantity greater than y. Thus the extra point at e fails to give $\varphi^{-1}(v)$ a sufficiently large index to make up for the situation at the point $\varphi(c)$.

The proof that $\psi^{-1}(w)$ and $\varphi^{-1}(w)$ cannot each have an extra point is complete. It will not be difficult now to settle the two-polynomial problem.

Suppose that it is $\psi^{-1}(w)$ which has no extra point. Then at any critical point of $\psi^{-1}(w)$, $\varphi^{-1}(w)$ cannot have more than one uniform branch. It follows that $\psi^{-1}(w)$ cannot have more than two critical points in addition to infinity.

Suppose first that $\psi^{-1}(w)$ has only one critical point in addition to infinity. At this point, $\psi^{-1}(w)$ must have a branch point of order $n-1$. We see that $\psi(v)$ is of the form $a\,(v + b)^n + c$. At this critical point of $\psi^{-1}(w)$, $\varphi^{-1}(w)$ has at most one uniform branch.

Suppose that for this point the branches of $\varphi^{-1}(w)$ undergo the substitution (16), where, understanding that there may be one cycle which consists of a single

letter, equation (18) holds. If there were two of the numbers i in (18) which were not divisible by n, $\alpha^{-1}(u)$ would have two critical points, distinct from infinity, each with an index not less than $n/2$. Therefore all but one of the numbers i must be divisible by n, so that one i must be prime to n.* It follows that $\alpha^{-1}(u)$ has a branch point of order $n-1$, its only critical point in addition to infinity, and that $\alpha(z)$ is of the form $d\ (z+e)^n + f$.

If w, u, v and z are subjected to appropriate linear transformations, the case under consideration can be reduced to that in which $\psi(v)=v^n$ and $\alpha(z)=z^n$. We have thus to determine under what circumstances it is possible to have

$$\varphi(z^n) = [\beta(z)]^n.$$

We must have, in this case, denoting by ϵ any primitive nth root of unity,

$$\beta(\epsilon z) = \epsilon^r \beta(z)$$

where r is some positive integer not greater than n. Consequently

$$\beta(z) = z^r\, g(z^n),$$

where $g(z^n)$ is a polynomial in z^n. Hence

$$\varphi(u) = u^r [g(u)]^n.$$

Let us summarize these results for the case where $\psi^{-1}(w)$ has only one critical point in addition to infinity. We must have

$$\varphi = \lambda_1\varphi_1\lambda_2, \qquad \alpha = \lambda_2^{-1}\alpha_1\lambda_3,$$
$$\psi = \lambda_1\psi_1\lambda_4, \qquad \beta = \lambda_4^{-1}\beta_1\lambda_3,$$

where $\lambda_1(z)$, $\lambda_2(z)$, $\lambda_3(z)$ and $\lambda_4(z)$ are linear, and where

$$\varphi_1(u) = u^r[g(u)]^n, \qquad \alpha_1(z) = z^n,$$
$$\psi_1(v) = v^n, \qquad \beta_1(z) = z^r[g(z^n)],$$

where r is any positive integer prime to n, and where $g(u)$ is any polynomial in u. If $g(u)=1$, we have the simple case of two power functions.†

Consider now the case where $\psi^{-1}(w)$ has two critical points besides infinity. The index of $\varphi^{-1}(w)$ at each of these points is at least $(m-1)/2$. It follows that the index of $\varphi^{-1}(w)$ at each of these points is precisely $(m-1)/2$, and that at each point $\varphi^{-1}(w)$ has one uniform branch and $(m-1)/2$ branch points of the first order. Of course m must be odd.

At each of the finite critical points of $\psi^{-1}(w)$, the order of the substitution which its branches undergo must be two. Otherwise, since $\varphi^{-1}(w)$ would have, at such a critical point, cycles with a number of sheets not divisible by the order

* If (18) consists of one cycle this result follows immediately.

† Except in the case of $r=m$, $\varphi^{-1}(w)$ will have an extra point.

of the substitution just mentioned, and also a uniform branch, $\psi^{-1}(w)$ would necessarily have an extra point. Hence the index of $\psi^{-1}(w)$ at either of its two finite critical points cannot exceed $n/2$. Hence if n is even, $\psi^{-1}(w)$ has one critical point with $n/2$ branch points, and one critical point with two uniform branches and $n/2-1$ branch points of the first order.* If n is odd, $\psi^{-1}(w)$ must have, at each of its finite critical points, one uniform branch and $(n-1)/2$ branch points of the first order.

Let us take the case in which n is even. At the points which correspond to the values assumed at the critical points of $\varphi^{-1}(w)$ by its uniform branches, $\alpha^{-1}(u)$ has critical points of the types of those of $\psi^{-1}(w)$. Thus $F^{-1}(w)$, since $F=\varphi\alpha$, has one critical point at which all of its branch points are permuted in pairs, and one at which two branches are uniform and the others are permuted in pairs.

We may assume that the branches of $F^{-1}(w)$ are so numbered that the cyclic substitution at infinity, which we shall denote by s_0, is given by the formula

$$\nu' \equiv \nu + 1 \qquad (\text{mod } mn).$$

Let s_1 represent the substitution at the finite critical point where no branches are uniform and s_2 the substitution at the second finite critical point. We have $s_0s_1=s_2$. Suppose that s_1 replaces i by j. Then s_0s_1 replaces $i-1$ by j. But since s_2 is of order two, s_0s_1 must replace j by $i-1$; that is, s_1 must replace $j+1$ by $i-1$. Similarly s_1 must replace $j+2$ by $i-2$, etc. It is clear then that s_1 may be written in the form.

$$\nu' \equiv -\nu + k \qquad (\text{mod } mn),$$

where, since s_1 leaves no branch fixed, k must be odd. If we renumber the branches of $F^{-1}(w)$, giving to the branch numbered ν the number $\mu=\nu-(k-1)/2$, the substitutions s_0 and s_1 become

$$\mu' = \mu + 1, \qquad \mu' = -\mu + 1,$$

respectively.

Similar results are obtained if n is odd.

Thus only one mechanism is possible for the surface of $F^{-1}(w)$. The two finite critical points can be placed at pleasure by subjecting w to an appropriate linear transformation. Hence if $f_{mn}(z)$ is a particular function of degree mn which has two decompositions of the types considered, we will have

$$F = \lambda_1 f_{mn} \lambda_2$$

where λ_1 and λ_2 are linear. But the trigonometric polynomial $f_{mn}(z)$, defined by the relation

$$\cos mnu = f_{mn}(\cos u),$$

* In this case $\varphi^{-1}(w)$ has an extra point.

is precisely of this type.* We may, then, take $f_{mn}(z)$ as a trigonometric polynomial. Now $F(z)$ has the two decompositions.

$$F = \lambda_1 f_m f_n \lambda_2, \qquad F = \lambda_1 f_n f_m \lambda_2.$$

As the group of $F^{-1}(w)$ can have only one type of imprimitivity with a given number of letters in each set, and as any two decompositions based on the same system of imprimitivity are equivalent, we must have

$$\varphi = \lambda_1 f_m \lambda_3, \qquad \alpha = \lambda_3^{-1} f_n \lambda_2,$$
$$\psi = \lambda_1 f_n \lambda_4, \qquad \beta = \lambda_4^{-1} f_m \lambda_2,$$

where $\lambda_3(z)$ and $\lambda_4(z)$ are linear. This settles the case where $\psi^{-1}(w)$ has two critical points in addition to infinity.

A consideration of the material of this section and of the preceding one leads to the statement of results made in the introduction. We shall not enlarge upon that statement.

---

* It is easy to show that the inverses of the trigonometric polynomials have, in addition to infinity, the critical points 1 and -1, where their branches are permuted in pairs.

COLUMBIA UNIVERSITY,
NEW YORK, N. Y.