EQUIVALENT RATIONAL SUBSTITUTIONS*

BY

J. F. RITT

1. If, for three rational functions, $\varphi(z)$, $\alpha(z)$, $\beta(z)$, a relation

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

holds, it follows, since $\varphi(z)$ is capable of assuming all values, that $\alpha(z)$ and $\beta(z)$ are identical. On the other hand, a relation

$$\varphi[\alpha(z)] = \varphi[\beta(z)] \tag{1}$$

does not imply the identity of $\alpha(z)$ and $\beta(z)$; the functions

$$\varphi(z) = z^2, \qquad \alpha(z) = z, \qquad \beta(z) = -z$$

weakly illustrate this fact.

We are going to study the relation (1).

If a rational function $\zeta(z)$ is such that $\zeta(z) = \zeta_1[\sigma(z)]$, where $\zeta_1(z)$ and $\sigma(z)$ are rational and $\sigma(z)$ is not linear, we shall call $\sigma(z)$ a *forefactor* of $\zeta(z)$. If $\zeta_1(z)$ is not linear, $\sigma(z)$ will be called a *proper* forefactor of $\zeta(z)$. If

$$\alpha(z) = \alpha_1[\sigma(z)], \qquad \beta(z) = \beta_1[\sigma(z)],$$

all functions involved being rational, (1) becomes

$$\varphi[\alpha_1(z)] = \varphi[\beta_1(z)].$$

It will therefore suffice, in studying (1), to consider those cases in which $\alpha(z)$ and $\beta(z)$ have no common forefactor.

The discussion of the relation (1) for the case in which $\alpha(z)$ and $\beta(z)$ are linear presents no difficulty and may well be omitted. Also, when the three functions in (1) are polynomials, it can be shown by the method of undetermined coefficients (and more conveniently in other ways), that $\alpha(z)$ and $\beta(z)$ are linear functions of each other, so that we are brought back to the case in which $\alpha(z)$ and $\beta(z)$ are linear.

* Presented to the Society, March 1, 1924.

We treat here the case in which $\alpha(z)$ and $\beta(z)$ are of degree at least 2 and have no common forefactor. In § 2 we present cases of this kind, involving polyhedral functions and elliptic functions. There follows the proof of a set of theorems which are listed at the head of § 3. In § 4, we consider systems of relations (1), which lead to sets of rational functions analogous to the polyhedral groups of linear functions.

2. A non-linear rational function will be called *composite* or *prime* according as it does or does not have a proper forefactor. Certain composite functions which are invariant under linear transformations illustrate the relation (1). The rational functions invariant under the polyhedral groups of linear transformations are of this type.

For instance, the dihedral function, $\Phi(z) = z^n + 1/z^n$, invariant under the group generated by $z' = 1/z$ and $z' = \varepsilon z$ ($\varepsilon = e^{2\pi i/n}$), has $\alpha(z) = z + 1/z$ for a forefactor. We have

$$\Phi(z) = \varphi[\alpha(z)] = \varphi[\alpha(\varepsilon z)],$$

where $\alpha(z)$ and $\alpha(\varepsilon z)$ are of degree 2 and have no common forefactor if $n > 2$.

The tetrahedral, octahedral and icosahedral functions, with respect to which we shall limit ourselves to some general indications, also illustrate (1). Some of the relations which they yield involve the monomial forefactors which are visible in the expressions for the functions.* The most convenient way to examine the polyhedral functions from this point of view is by studying the types of imprimitivity of the groups of monodromy of their inverses. How to go about this will be understood through the work of the following section. The groups of monodromy just referred to are regular, and are isomorphic with the polyhedral groups of linear transformations.

Further illustrations of (1) are found in the formulas for the transformation of the periods of $\wp(u)$, in the lemniscatic case, in which there exists a square period-parallelogram, and in the equianharmonic case, in which there are parallelograms composed of two equilateral triangles.

Considering the lemniscatic case, suppose that the periods of $\wp(u)$ are 1 and i. Let m be any integer. We know that

$$\wp(u \mid 1, i) = \Psi[\wp(u \mid m, mi)], \tag{2}$$

$$\wp(u \mid 1, i) = \psi[\wp(u \mid 1, mi)], \qquad \wp(u \mid 1, mi) = \alpha[\wp(u \mid m, mi)], \tag{3}$$

* For these expressions, see, for instance, Appell et Goursat, *Théorie des Fonctions algébriques*, p. 247.

where $\Psi(z)$, $\psi(z)$ and $\alpha(z)$ are rational and of the respective degrees m^2, m and m. Here $\Psi(z) = \psi[\alpha(z)]$.

Since $\wp(u)$ is a homogeneous function of degree -2 in u and its periods, we find, for the lemniscatic case, $\wp(iu) = -\wp(u)$. It follows from (2) that $\Psi(-z) = -\Psi(z)$. Putting

$$\Phi(z) = [\Psi(z)]^2, \qquad \varphi(z) = [\psi(z)]^2,$$

we have

$$\Phi(z) = \varphi[\alpha(z)] = \varphi[\alpha(-z)].$$

To take a simple case, suppose that m is prime. Then $\alpha(z)$ and $\alpha(-z)$ are prime. If they had a common forefactor, they would be linear functions of each other. It would follow, replacing u by iu in the second equation of (3), that

$$\wp(iu \mid 1, mi) \text{ and } \wp(u \mid 1, mi)$$

are linear functions of each other. This is not so, since the period i of the former is not a period of the latter.

We have thus a relation (1) in which the degree of $\varphi(z)$ is double that of $\alpha(z)$ and $\beta(z)$. Similarly, in the equianharmonic case, we find relations in which the degree of $\varphi(z)$ is three times that of the other two functions.*

In every example above, $\beta(z)$ is found from $\alpha(z)$ by subjecting z to a linear transformation. We do not know whether other types of relations exist.

3. We deal with three rational functions, $\varphi(z)$, $\alpha(z)$, $\beta(z)$, of the respective degrees m, n and n, assuming that $n > 1$, that $\alpha(z)$ and $\beta(z)$ have no common forefactor, and that

$$\varphi[\alpha(z)] = \varphi[\beta(z)]. \tag{1}$$

We prove the following theorems:

I. $m > n$.

II. *If* $m \leqq 2n$, $\beta(z) = \alpha[\lambda(z)]$, *where* $\lambda(z)$ *is a linear function such that* $\lambda[\lambda(z)] = z$. *Also* $\varphi[\alpha(z)]$ *has a forefactor of degree* 2, *which is invariant when* z *is replaced by* $\lambda(z)$.

* For other connections in which the above elliptic functions occur, see the following papers of the writer in these Transactions for 1922 and 1923: *Periodic functions with a multiplication theorem, On algebraic functions which can be expressed in terms of radicals, Permutable rational functions.*

III. *If* $m = n + 2$, $\varphi(z)$ *is composite, and* $\varphi(z) = \zeta[\sigma(z)]$, *where* $\sigma(z)$ *is of degree* 2 *and* $\zeta(z)$ *is prime. Every proper forefactor of* $\varphi(z)$ *is a linear function of* $\sigma(z)$. *Also, if* $n > 2$, $\alpha(z)$ *and* $\beta(z)$ *are composite, and each has a forefactor of degree* 2.

IV. *If* $m = n + 1$, $\varphi(z)$ *is prime.*

V. *If* $m \leqq n + 2$, *the inverse of* $\varphi(z)$ *has no more than five critical points; it has at least one critical point at which none of its branches is uniform. The inverses of* $\varphi(z)$ *and of* $\varphi[\alpha(z)]$ *have the same critical points.*

VI. *Each of the* mn *branches of the inverse of* $\varphi[\alpha(z)]$ *can be expressed rationally in terms of two of the* m *branches of the inverse of* $\varphi(z)$.

VII. *The group of monodromy of the inverse of* $\varphi(z)$ *is at least doubly transitive when* $m = n + 1$, *and only simply transitive when* $m > n + 1$.

VIII. *In the set of functions* $\varphi(z)$ *which satisfy the relation* (1) *with* $\alpha(z)$ *and* $\beta(z)$, *there is one in terms of which every other can be expressed rationally.*

III is illustrated by the dihedral function of degree 8 and by the octahedral function, which is of degree 24. IV is illustrated by the dihedral function of degree 6, and by the tetrahedral function (degree 12).

The proofs will be based on notions presented in our paper *Prime and composite polynomials.** That paper will be referred to as "*A*".

We write

$$w = \Phi(z) = \varphi[\alpha(z)] = \varphi[\beta(z)].$$

With respect to the group of monodromy of $\Phi^{-1}(w)$, the mn branches of $\Phi^{-1}(w)$ break up into m systems of imprimitivity, each of n branches, such that, if the branches

$$z_1, z_2, \ldots, z_n$$

constitute one of these systems, we have

$$\alpha(z_1) = \alpha(z_2) = \cdots = \alpha(z_n).\dagger$$

Similarly, $\beta(z)$ determines m systems of imprimitivity. From the fact that $\alpha(z)$ and $\beta(z)$ have no common forefactor, it follows that no system of imprimitivity determined by $\alpha(z)$ can have more than one branch in common with any system determined by $\beta(z)$. For if two such systems had more than one branch in common, their common branches would also form a system of imprimitivity. This new system would be determined by a rational

* These Transactions, vol. 23 (1922), p. 51.

† *A*, p. 53.

function which would be a forefactor both of $\alpha(z)$ and of $\beta(z)$ (A, p. 55, lines 15–19).

Let u_1 be any branch of $\varphi^{-1}(w)$. Since $\alpha(z) \not\equiv \beta(z)$, the set of n branches z_i of $\Phi^{-1}(w)$ for which $\alpha(z_i) = u_1$ has no branch in common with the set for which $\beta(z_i) = u_1$. Hence the n branches such that $\alpha(z_i) = u_1$ are distributed among n distinct systems determined by $\beta(z)$, each system corresponding to a separate branch of $\varphi^{-1}(w)$ other than u_1. This proves I.

To prove II, let $z_1, \ldots, z_n$ be the n branches such that $\alpha(z_i) = u_1$, and let $z_1', \ldots, z_n'$ be the n branches, distinct from those which precede, such that $\beta(z_i') = u_1$. The functions $\beta(z_i)$ are n branches of $\varphi^{-1}(w)$, distinct from each other and from u_1, and so also are the n functions $\alpha(z_i')$. As $m \leqq 2n$, it must be that for some p and q, $\alpha(z_p') = \beta(z_q)$. It is permissible to let $p = q = 1$. We have thus

$$\alpha(z_1) = \beta(z_1'); \qquad \alpha(z_1') = \beta(z_1). \tag{4}$$

Let w describe any closed path for which z_1 stays fixed. By the first equation of (4), $\beta(z_1')$ also stays fixed, so that z_1' is replaced by a branch which is together with z_1' in a system of imprimitivity determined by $\beta(z)$. Similarly, from the second equation of (4), z_1' is replaced by a branch which is together with z_1', in a system determined by $\alpha(z)$. But as no system determined by $\alpha(z)$ has more than a single branch in common with any system determined by $\beta(z)$, z_1' stays fixed when z_1 stays fixed. Thus z_1' is a rational function of z_1 and w, and as w is a rational function of z_1, z_1' is a rational function of z_1 alone. Let $z_1' = \lambda(z_1)$. Then (4) becomes

$$\alpha(z_1) = \beta[\lambda(z_1)]; \qquad \alpha[\lambda(z_1)] = \beta(z_1). \tag{5}$$

We find from (5), putting $\lambda_2(z) = \lambda[\lambda(z)]$,

$$\alpha[\lambda_2(z_1)] = \alpha(z_1); \qquad \beta[\lambda_2(z_1)] = \beta(z_1). \tag{6}$$

This shows that $\lambda_2(z_1)$ is a branch of $\varphi^{-1}(w)$ which lies together with z_1 in systems determined by $\alpha(z)$ and by $\beta(z)$. Hence $\lambda_2(z_1) = z_1$. By the principal of the permanence of functional equations, $\lambda_2(z) = z$ for every z, so that $\lambda(z)$ is linear. Also (5) holds for every z.

Finally, if w describes a closed path for which z_1 stays fixed, $\lambda(z_1)$ also stays fixed, whereas if z_1 is replaced by $\lambda(z_1)$, $\lambda(z_1)$ is replaced by $\lambda_2(z_1) = z_1$. This shows that z_1 and $\lambda(z_1)$ form a system of imprimitivity

with respect to the group of $\Phi^{-1}(w)$,* and hence that $\Phi(z)$ has a forefactor of degree 2 which is invariant when z is replaced by $\lambda(z)$ (A, p. 54). This completes the proof of II.

Considering III, let the branches of $\varphi^{-1}(w)$ be $u_1, u_2, \ldots, u_{n+2}$. Let $z_1, \ldots, z_n$ be the branches of $\Phi^{-1}(w)$ such that $\alpha(z_i) = u_{n+2}$. These branches are distributed among n systems of imprimitivity determined by $\beta(z)$ which are distinct from the system for which $\beta(z_i) = u_{n+2}$. We may suppose that

$$\beta(z_i) = u_i \qquad (i = 1, 2, \ldots, n). \tag{7}$$

Suppose that w describes a closed path in such a way that u_{n+2} is replaced by itself. Then $z_1, \ldots, z_n$ are interchanged among themselves. Consequently u_{n+1} is replaced by itself. Hence u_{n+1} is a rational function of u_{n+2} and w, and as $w = \varphi(u_{n+2})$, u_{n+1} is a rational function of u_{n+2} alone. We have

$$\varphi(u_{n+2}) = \varphi(u_{n+1}) = \varphi[\lambda(u_{n+2})],$$

and therefore, identically, $\varphi(u) = \varphi[\lambda(u)]$. Hence $\lambda(u)$ is linear, and u_{n+1} is a linear function of u_{n+2}.

On the other hand, no u_i with $i \leqq n$ is a linear function of u_{n+2}. For, assuming the existence of such a u_i, let w describe a closed path in such a way that z_i is replaced by z_j, a branch among $z_1, \ldots, z_n$ distinct from z_i. This circuit leaves u_{n+2} fixed, but, according to (7), replaces u_i by u_j, an impossibility if u_i is to be a linear function of u_{n+2}.

Thus if a substitution of the group of $\varphi^{-1}(w)$ leaves u_{n+2} fixed, it also leaves u_{n+1} fixed. If it replaces u_{n+2} by $u_{n+1} = \lambda(u_{n+2})$, it must replace u_{n+1} by $u_i = \lambda[\lambda(u_{n+2})]$. Here u_i is a linear function of u_{n+2}, and being distinct from u_{n+1}, it must be identical with u_{n+2}. It follows that u_{n+1} and u_{n+2} form a system of imprimitivity of the group of $\varphi^{-1}(w)$. Hence $\varphi(z)$ is composite and of the form $\zeta[\sigma(z)]$ where $\sigma(z)$ is of degree 2.

Suppose that $\varphi(z)$ has a proper forefactor which is not a linear function of $\sigma(z)$. That forefactor must determine systems of imprimitivity distinct from those determined by $\sigma(z)$ (A, p. 55, lines 4 et seq.). Suppose that that one of the new systems which contains u_{n+2} contains another branch u_i, where $i \neq n+1$. Let u_j $(j < n+1)$ be a branch not in this system. If w describes a path which replaces z_i by z_j, u_{n+2} stays fixed, whereas u_i is replaced by u_j, and we witness the disruption of a system of imprimitivity. Thus every proper forefactor of $\varphi(z)$ is a linear function of $\sigma(z)$. This also means that $\zeta(z)$ is prime.

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

It is permissible to suppose that u_1 and u_2 form a system of imprimitivity with respect to $\sigma(z)$. Consider z_1 and z_2. Let w describe any path for which z_1 stays fixed. Then z_2 must be replaced by some z_i $(i = 2, \ldots, n)$. Also, $u_1 = \beta(z_1)$ stays fixed, so that u_2 does also. Hence z_2 must stay fixed, else $u_2 = \beta(z_2)$ could not. Similarly, if z_1 is replaced by z_2, z_2 is replaced by z_1. Hence z_1 and z_2 form a system of imprimitivity of the group of $\Phi^{-1}(w)$ if $n > 2$, and $\alpha(z)$ has a quadratic forefactor (A, p. 55, lines 15—19). This completes the proof of III.

We now jump to the proof of VII. Let the branches of $\varphi^{-1}(w)$, when $m = n + 1$, be $u_1, \ldots, u_{n+1}$, and let $z_1, \ldots, z_n$ be those branches of $\Phi^{-1}(w)$ for which $\alpha(z_i) = u_{n+1}$. Then (7) holds. If we can prove that it is possible to keep u_{n+1} fixed and replace any other branch u_i by any third branch u_j, we shall know that the group of $\varphi^{-1}(w)$ is doubly transitive. Precisely this is accomplished by letting w describe a path which replaces z_i by z_j. Supposing now that $m > n + 1$, let

$$u_m = \alpha(z_i), \qquad u_i = \beta(z_i) \qquad (i = 1, \ldots, n).$$

It is clear that if u_m stays fixed, the branches $u_i (i = 1, \ldots, n)$ are interchanged among themselves, so that the group of $\varphi^{-1}(w)$ cannot be more than simply transitive. VII is proved.

IV is a corollary of VII, for if $\varphi(z)$ were composite the group of $\varphi^{-1}(w)$ would be imprimitive. It cannot be so, since it is doubly transitive.

We now turn to V, limiting ourselves to the case of $m = n + 2$; that of $m = n + 1$ requires only slight changes. Suppose that

$$\alpha(z_i) = u_{n+2}, \qquad \beta(z_i) = u_i \qquad (i = 1, \ldots, n).$$

Consider a value a of w at which u_{n+2} is uniform, assuming the value b. Let w make a turn about a. The branches $u_i (i = 1, \ldots, n)$ of $\varphi^{-1}(w)$ will be interchanged among themselves with a substitution similar to that undergone by the branches $z_i (i = 1, \ldots, n)$ of $\Phi^{-1}(w)$. We infer first that u_{n+1} is uniform at a, and secondly that the inverse of $\alpha(z)$ has a critical point at b if and only if $\varphi^{-1}(w)$ has a critical point at a.

Now the sum of the orders of all the branch points of the inverse of a rational function of degree n is $2n - 2$, so that the inverse of $\alpha(z)$ cannot have more than $2n - 2$ critical points. Suppose that $\varphi^{-1}(w)$ has r critical points. The sum of the orders of the branch points of $\varphi^{-1}(w)$ is $2m - 2 = 2n + 2$. It is also equal (by the definition of order) to $rm - j - k$, where j is the number of branch points of $\varphi^{-1}(w)$, and k

is the number of places on the Riemann surface of $\varphi^{-1}(w)$ for which w is a critical point, and at which $\varphi^{-1}(w)$ is uniform. Each of the k latter places yields a critical point of the inverse of $\alpha(z)$, so that $k \leqq 2n-2$. Also, as each branch point is at least of order 1, $j \leqq 2n+2$. Hence

$$2n+2 \geqq r(n+2)-(2n+2)-(2n-2)$$

and $r \leqq (6n+2)/(n+2) < 6$. Furthermore the sum of the orders of the branch points which $\varphi^{-1}(w)$ has at a is identical with the corresponding sum for the inverse of $\alpha(z)$ at b, because of the similarity of the substitutions which their branches undergo. Hence if $\varphi^{-1}(w)$ had a uniform branch at each of its critical points, the sum of the orders of the inverse of $\alpha(z)$ would be at least $2n+2$, which is too large. Finally, it is clear that if $\varphi^{-1}(w)$ does not have a critical point at a, $\Phi^{-1}(w)$ does not either. This settles V.

As to VI, consider any branch z_i of $\Phi^{-1}(w)$. Let

$$\alpha(z_i) = u_j, \qquad \beta(z_i) = u_k.$$

It is plain that if w describes a path for which u_j and u_k stay fixed, z_i also stays fixed. Hence z_i is a rational function of u_j, u_k, and w, and as w is a rational function of u_j, for instance, z_i is rational in u_j and u_k alone.

Finally, we take VIII. Of all the functions $\varphi(z)$ which satisfy (1) together with a fixed pair of functions $\alpha(z)$ and $\beta(z)$, let $\varphi_0(z)$ be one whose degree is a minimum. Let $\varphi_1(z)$ be any other of the functions $\varphi(z)$. According to a theorem of Lüroth,* there exists a rational $\vartheta(z)$ which is a rational function of $\varphi_0(z)$ and $\varphi_1(z)$, and of which $\varphi_0(z)$ and $\varphi_1(z)$ are rational functions. Of course the degree of $\vartheta(z)$ does not exceed that of $\varphi_0(z)$. Again it is plain that $\vartheta[\alpha(z)] = \vartheta[\beta(z)]$, so that $\vartheta(z)$ is not of lower degree than $\varphi_0(z)$. Hence $\vartheta(z)$ is a linear function of $\varphi_0(z)$, which means that $\varphi_1(z)$ is a rational function of $\varphi_0(z)$. Q. E. D.

4. Let a set of distinct non-linear rational functions

$$\alpha_1(z),\ \alpha_2(z),\ \ldots,\ \alpha_m(z), \tag{8}$$

which do not all have a forefactor in common, be such that for some rational function $\varphi(z)$, *of degree* m,

* Weber, *Lehrbuch der Algebra,* 2d edition, vol. 2, p. 472.

$$\varphi[\alpha_1(z)] = \varphi[\alpha_2(z)] = \cdots = \varphi[\alpha_m(z)].$$

The analogy of the system (8) to a finite group of linear functions is obvious.

Writing $w = \Phi(z) = \varphi[\alpha_i(z)]$ $(i = 1, \ldots, m)$, we shall show that *the branches of* $\Phi^{-1}(w)$ *are linear functions of one another,* and hence that $\Phi(z)$ *is a polyhedral function.*

Let the branches of $\varphi^{-1}(w)$ be $u_1, \ldots, u_m$. Let z_1 be any branch of $\Phi^{-1}(w)$. We may assume that $\alpha_i(z_1) = u_i$ $(i = 1, \ldots, m)$. Thus if w describes a path for which z_1 is replaced by itself, every u_i is replaced by itself. Suppose, on the other hand, that some z_2 does not stay fixed, but is replaced by z_3. It cannot be that $\alpha_i(z_2) = \alpha_i(z_3)$ for every i, else z_2, z_3, and perhaps other branches, would lie together, for every $\alpha_i(z)$, in a system of imprimitivity determined by that $\alpha_i(z)$, and the functions of (8) would have a common forefactor.

Let, then, $\alpha_p(z_2) = u_r$, $\alpha_p(z_3) = u_s$, where $r \neq s$. If z_2 is replaced by z_3, u_r is replaced by u_s, an impossibility if z_1 stays fixed. Hence z_2 is a rational function of z_1 and w, and therefore a rational function of z_1 alone. Thus all of the branches z_i are rational, and therefore linear functions of each other, so that $\Phi(z)$ is a polyhedral function.

Furthermore, the dihedral, tetrahedral, octahedral and icosahedral functions all lead to sets of non-linear functions like (8).

COLUMBIA UNIVERSITY,
NEW YORK, N. Y.