ON ALGEBRAIC FUNCTIONS WHICH CAN BE EXPRESSED IN TERMS OF RADICALS*

BY

J. F. RITT

I. INTRODUCTION

We consider, in this paper, an irreducible algebraic relation

$$F(w, z) = 0,$$

of degree n in w and of genus p, and seek to determine those cases in which w can be expressed in terms of z by means of radicals. Why the results obtained here should not have been found before this time is a question which has puzzled us as much as it will puzzle the reader.

Our results for the case in which n is prime are fairly complete. We show first that *if n is prime, and if w can be expressed in terms of radicals, then for every genus except zero there exists an upper bound for n*. For any given genus the mechanisms of the possible Riemann surfaces for w can be determined in a finite number of steps.

For the case of genus zero our problem becomes that of finding all rational functions whose inverses can be expressed in terms of radicals. Given one such function, others can be obtained by performing linear transformations upon the function and upon the variable. We show that all rational functions of prime degree with inverses expressible in terms of radicals can be thus obtained from functions of the following types:

(*a*) *The powers of w.*

(*b*) *The polynomials which occur in the formulas for the multiplication of the argument in the function* $\cos u$.

(*c*) *The fractional rational functions which occur in the formulas for the transformations of the periods of the function $\wp u$.*

(*d*) *For the case of $n \equiv 1 \pmod 4$, the fractional rational functions met, in the lemniscatic case ($g_3 = 0$), in the formulas for the multiplication of the argument of $\wp^2 u$ by $\alpha \pm \beta i$, where $\alpha^2 + \beta^2 = n^2$.*

(*e*) *For the case of $n \equiv 1 \pmod 6$, the fractional rational functions met, in the equianharmonic case ($g_2 = 0$), in the formulas for the multiplication of the arguments of $\wp' u$ and $\wp'^2 u$ by $\alpha \pm \beta i \sqrt{3}$, where $\alpha^2 + 3\beta^2 = n^2$.*

The functions just described are already known to have inverses expressible

* Presented to the Society, October 30, 1920, and October 29, 1921.

in terms of radicals. We prove here that they are the only such rational functions of prime degree.

What we have done for the case in which n is composite is to determine all polynomials whose inverses can be expressed in terms of radicals. In stating our result we employ the terms of our paper *Prime and composite polynomials.** A polynomial $F(z)$ is there called *composite* if there exist two polynomials, $\phi_1(z)$ and $\phi_2(z)$, each of degree greater than unity, such that $F(z) = \phi_1[\phi_2(z)]$. Otherwise, $F(z)$, if of degree greater than unity, is called prime. Let

$$F = \phi_1 \phi_2 \cdots \phi_r,$$

where each $\phi_i(z)$ is a prime polynomial, and is understood to be substituted for z in the polynomial which precedes it.

We show that *if the inverse of $F(z)$ can be expressed in terms of radicals, each $\phi_i(z)$, if not of degree 4, can be obtained by means of linear transformations either from a prime power of z or from a trigonometric polynomial of prime degree.* We will have, that is, if $\phi_i(z)$ is of degree $m \neq 4$,

$$\phi_i = \lambda_1 \pi \lambda_2,$$

where $\lambda_1(z)$ and $\lambda_2(z)$ are linear and where either $\pi(z) = z^m$ or else $\cos mu = \pi(\cos u)$.

The work for this case, with n composite, consists mainly in the proof of a theorem on substitution groups.

II. Functions with a prime number of values

If the degree n in w of the irreducible algebraic relation

$$F(w, z) = 0 \tag{1}$$

is prime, and if w can be expressed in terms of radicals, the group of monodromy of (1) is either the metacyclic group or one of its transitive subgroups. The group of monodromy must contain a substitution of order n. We number the branches of w in such a way that the group contains the substitution $(1\ 2 \cdots n)$, and represent the metacyclic group with the formula

$$\nu' \equiv a\nu + b \pmod{n} \qquad \begin{pmatrix} a = 1, 2, \cdots, n-1 \\ b = 0, 1, 2, \cdots, n-1 \end{pmatrix}. \tag{2}$$

The non-identical substitutions with $a = 1$ displace every index ν. The substitutions with $a \neq 1$ leave a single index fixed. If a substitution of the metacyclic group consists of more than one cycle, its cycles are all of the same order.

Suppose that w has q critical points. We consider the elementary substitutions of the group of monodromy, which correspond to single turns

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

around these critical points. Suppose that there are α of them with $a = 1$ and $q - \alpha$ with $a \neq 1$. We designate the orders of the latter by $s_1, s_2, \cdots, s_{q-\alpha}$.

If the genus of (1) is p, we have, according to the well known formula of Riemann,

$$(n-1)\alpha + \sum_{i=1}^{i=q-\alpha} \frac{n-1}{s_i}(s_i - 1) = 2(n-1) + 2p,$$

or

$$\sum_{i=1}^{i=q-\alpha} \frac{1}{s_i} = q - 2 - \frac{2p}{n-1}. \tag{3}$$

Since no s_i is less than 2, the first member of (3) is not greater than $q/2$, and we find from (3)

$$q \leqq 4 + \frac{4p}{n-1}, \tag{4}$$

which shows that when p is given, there exists an upper bound for q, independent of n.

We shall prove now that *if p is not zero, there exists an upper bound for n which depends only on p.*

Suppose first that $q > 4$. We have then from (4),

$$n - 1 \leqq \frac{4p}{q-4} \leqq 4p.$$

If $q = 4$, equation (3) gives

$$\frac{2p}{n-1} = 2 - \sum \frac{1}{s_i}.$$

It is seen quickly that the second member of this last equation is at least equal to $1/6$. We have thus, in this case,

$$n - 1 \leqq 12p.$$

If $q = 3$, equation (3) gives

$$\frac{2p}{n-1} = 1 - \sum \frac{1}{s_i}.$$

The three integers the sum of whose reciprocals is less than unity by as small a positive number as possible are 2, 3 and 7. We have thus for this case

$$n - 1 \leqq 84p.*$$

A closer examination of the problem would lead to smaller bounds for n than those found above.

On being given p, we can, with the help of equation (3) and of the upper

* If $q - \alpha < 3$, we have a stronger inequality.

bounds for n and q, determine the possible Riemann surfaces for w in a finite number of steps. We shall not follow this question further in the present paper.

We consider the case of $p = 0$, which includes the most interesting examples already known of algebraic functions expressible in terms of radicals. We must have $q = 2, 3$ or 4.

Following our paper referred to in the introduction, we shall call the sum of the orders of the branch points of an algebraic function at a given point the *index* of the function at that point. The sum of the indices of the inverse of a rational function of degree n is $2n - 2$.

If, when we represent the substitution at a critical point in the form (2), the coefficient a belongs to the exponent d modulo n, where $d > 1$, the substitution is of order d, and the index at the critical point is $(n - 1)(d - 1)/d$.

We shall consider first those cases in which the Riemann surface for w has a branch point of order $n - 1$. Such a branch point must be present at infinity if w is the inverse of a polynomial. As the index of w at any critical point is at least $(n - 1)/2$, and as the sum of the indices of w is $2n - 2$, we must have, in this case, $q = 2$ or $q = 3$.

If $q = 2$, w must have two branch points of order $n - 1$. Subjecting z to a suitable linear transformation, we may suppose that one of these points is at infinity and the other at zero. The surface thus obtained is recognized as that for $w = z^{1/n}$. The functions uniform on it are rational functions of $z^{1/n}$. Of these, the only ones which are inverses of polynomials are linear integral functions of $z^{1/n}$

If $q = 3$, the remaining two critical points of w, since each has an index not less than $(n - 1)/2$, must each have precisely $(n - 1)/2$ as index. Subjecting z to a suitable linear transformation, we may suppose that the branch point of order $n - 1$ is at infinity, and the other two critical points at $z = 1$ and $z = -1$ respectively. The substitutions at the latter points are of the form

$$\nu' \equiv -\nu + h_1, \qquad \nu' \equiv -\nu + h_2 \pmod{n},$$

respectively. The substitution at infinity, the result of following the second of these two by the first, is

$$\nu' \equiv \nu + h_1 - h_2 \pmod{n}.$$

As this substitution is of period n, we have $h_1 \not\equiv h_2$. If we renumber the branches of w, giving to the branch numbered ν the number μ determined by the congruence

$$\nu \equiv (h_1 - h_2)\mu + \frac{n+1}{2} h_1 \pmod{n}, \tag{5}$$

the three elementary substitutions become

$$\mu' \equiv -\mu, \qquad \mu' \equiv -\mu - 1, \qquad \mu' \equiv \mu + 1 \pmod{n}.$$

Thus only one mechanism is possible for the surface of w. Now it is well known that the trigonometric polynomial of degree n, $f_n(w)$, defined by the relation

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

has an inverse expressible in terms of radicals, the critical points of the inverse being at 1, -1, and ∞. Hence w must be a rational function of $f_n^{-1}(z)$.

Summarizing the foregoing results, we see that *the only polynomials of prime degree whose inverses can be expressed in terms of radicals are those of the forms* $a(w+b)^n + c$ *and* $af_n(bw+c) + d$, *where* $\cos nu = f_n(\cos u)$.

We consider now the case of $q = 4$. As the index of w at each critical point is at least $(n-1)/2$ and as the sum of the indices is $2n-2$, the index of w is precisely $(n-1)/2$ at each critical point. The corresponding substitutions are all of order 2. Subjecting z to a suitable linear transformation, we may throw one of the critical points to ∞, and so dispose the others that the sum of their affixes e_1, e_2, and e_3 is zero. Let the substitutions at e_1, e_2, and e_3 be respectively

$$\nu' \equiv -\nu + h_1, \qquad \nu' \equiv -\nu + h_2, \qquad \nu' \equiv -\nu + h_3 \pmod{n}.$$

Suppose that h_1 and h_2 are unequal. If we give to the branch of w numbered ν the number μ determined by (5), the three substitutions become

$$\mu' \equiv -\mu, \qquad \mu' \equiv -\mu - 1,$$
$$(h_1 - h_2)\mu' \equiv (h_2 - h_1)\mu + h_3 - h_1 \pmod{n}.$$

As h_3 varies from 0 to $n-1$, we obtain n types of surfaces which, it will be seen below, are all distinct.

If h_1 and h_2 are equal, they must be distinct from h_3, else the surface would not hang together. We can in this case reduce the three substitutions to

$$\mu' \equiv -\mu, \qquad \mu' \equiv -\mu, \qquad \mu' \equiv -\mu - 1 \pmod{n}.$$

Thus, the critical points being disposed as described above, there are at most $n+1$ distinct surfaces for w. To identify these, we construct the elliptic function $\wp(u|\omega_1, \omega_3)$, with $\wp(\omega_i) = e_i$ $(i = 1, 2, 3)$. This is possible, since $e_1 + e_2 + e_3 = 0$. Let

$$\Omega_1 = a\omega_1 + b\omega_3, \qquad \Omega_3 = c\omega_1 + d\omega_3, \tag{6}$$

where $ad - bc = n$. It is well known that there are $n+1$ distinct transformations (6), and that for every transformation, we have

$$\wp(u|\omega_1, \omega_3) = R[\wp(u|\Omega_1, \Omega_3)],$$

where $R(w)$ is a fractional rational function of degree n, whose inverse can

be expressed in terms of radicals. The critical points of $R^{-1}(z)$ will correspond to those values which $\wp(u|\omega_1, \omega_3)$ assumes twice at a point, namely, e_1, e_2, e_3, and ∞. It is easy to show that the $n+1$ Riemann surfaces for the inverses of the functions $R(w)$, occurring in the $n+1$ distinct transformations (6), have distinct mechanisms. The $n+1$ surfaces exhibited above can be none other than these.

We pass finally to the case in which $q = 3$ and in which no branch point of order $n-1$ exists. We must have, by (3),

$$\frac{1}{s_1} + \frac{1}{s_2} + \frac{1}{s_3} = 1.$$

There are the three possibilities:

(*a*) $\qquad s_1 = s_2 = \tfrac{1}{4}, \qquad s_3 = \tfrac{1}{2};$

(*b*) $\qquad s_1 = s_2 = s_3 = \tfrac{1}{3};$

(*c*) $\qquad s_1 = \tfrac{1}{2}, \qquad s_2 = \tfrac{1}{3}, \qquad s_3 = \tfrac{1}{6}.$

Consider Case (*a*). As every s_i is a divisor of $n-1$, we must have $n \equiv 1 \pmod 4$. Subjecting z to a suitable transformation, we can place the critical points with substitutions of order 4 at 0 and ∞ and the third critical point at any point e_1^2. Normalizing the substitutions at the critical points, we find that there are not more than two distinct mechanisms for the surface. We now take $\wp u$ so that $\wp(\omega_1) = e_1$, $\wp(\omega_2) = 0$, and $\wp(\omega_3) = -e_1$. This corresponds to the lemniscatic case. Now, as $n \equiv 1 \pmod 4$, we have $n = \alpha^2 + \beta^2$, where α and β are integers. In the lemniscatic case, the two functions $\wp^2(\alpha \pm \beta i)u$ are rational functions of $\wp^2 u$.* The rational functions thus obtained can be inverted in terms of radicals. It is not hard to identify their surfaces with those of Case (*a*).

Similarly, it is found that Cases (*b*) and (*c*) lead to the rational functions mentioned in Case (*e*) of the introduction, which are met in the multiplication formulas for the equianharmonic case.†

III. Polynomials of composite degree

We consider a polynomial $w = F(z)$, of prime or composite degree n, and seek those cases in which $F^{-1}(w)$, the inverse of $F(z)$, can be expressed in terms of radicals.‡

* For details relative to complex multiplication in the lemniscatic and equianharmonic cases, see Ritt, *Periodic functions with a multiplication theorem*, these Transactions, vol. 23 (1922), p. 16.

† A detailed discussion of all Riemann surfaces considered in this section is contained in a paper by the writer, *Permutable rational functions*, now in the hands of the editors of these Transactions.

‡ We have interchanged the rôles of w and z in order to conform with the notation of our paper referred to above.

If $F(z)$ is a composite polynomial, that is, if

$$F(z) = \phi_1[\phi_2(z)],$$

where $\phi_1(z)$ and $\phi_2(z)$ are of degrees greater than unity, then if $F^{-1}(w)$ can be expressed in terms of radicals, $\phi_1^{-1}(w)$ and $\phi_2^{-1}(w)$ can also be so expressed, for

$$\phi_1^{-1}(w) = \phi_2[F^{-1}(w)], \qquad \phi_2^{-1}(w) = F^{-1}[\phi_1(w)].$$

We may thus restrict ourselves to the determination of prime polynomials whose inverses can be expressed in terms of radicals.

We will show that if the inverse of a *prime* polynomial is expressible in terms of radicals, the degree of the polynomial, if not equal to four, is a prime number. Thus, using the result found for polynomials in the preceding section, we will know that *if* $F(z)$ *has the decomposition into prime polynomials*

$$F = \phi_1 \phi_2 \cdots \phi_r$$

each $\phi_i(z)$ *is either of degree* 4, *or else is of the form* $\lambda_1 \pi \lambda_2$, *where* $\lambda_1(z)$ *and* $\lambda_2(z)$ *are linear and where* $\pi(z)$ *is either a prime power of* z *or a trigonometric polynomial of prime degree.**

We refer to § II of our paper, *Prime and composite polynomials*, for a proof of the fact that *a necessary and sufficient condition that a polynomial be prime is that the group of monodromy of its inverse be primitive.*

It is well known that the degree of a primitive solvable group is a power of a prime. As the substitution corresponding to the branch point at infinity of the inverse of a polynomial of degree n consists of a single cycle of n letters, the proof that prime polynomials whose inverses can be expressed in terms of radicals are either of prime degree or of degree 4 will be complete as soon as we have proved the following theorem on substitution groups:

THEOREM. *A primitive solvable group in* p^m *letters with* p *prime and* $m > 1$ *cannot contain a substitution of order* p^m, *except in the case of* $p = 2$, $m = 2$.

Let G be a primitive solvable group of degree p^m. Suppose that G contains a cyclic subgroup C of order p^m.

It is well known that G contains an invariant transitive abelian subgroup Γ, of order p^m, every substitution of which, except identity, is of order p. As Γ is permutable with C, these two groups generate a group H in G, the order of which is the product of the orders of Γ and C, p^{2m}, divided by the order of the group of substitutions common to Γ and C. The order of H is a power of p greater than p^m. The substitutions of H are all of the form $c\gamma$ where c and γ are substitutions of C and Γ respectively.

The group C is invariant in a subgroup of H of order greater than p^m.

*Certainly if each $\varphi_i(z)$ is of one of the three types described, $F^{-1}(w)$ can be expressed in terms of radicals.

Hence there must be substitutions of H which are not in C, and with respect to which C is invariant. Suppose that $c\gamma$ is such a substitution, where γ is not in C. Then, since

$$\gamma^{-1} c^{-1} C c\gamma = \gamma^{-1} C\gamma = C,$$

C is invariant with respect to certain substitutions γ of Γ, which are not in C.

Let

$$c_1 = (0\ 1\ 2 \cdots \nu \cdots p^m - 1)$$

be the substitution which generates C. We shall determine the group of substitutions which converts c_1 into a power of itself. Let α be a substitution such that

$$\alpha^{-1} c_1 \alpha = c_1^r,$$

where r is any integer not divisible by p. It is evident that α is determined as soon as r, and the index s by which α replaces 0, are given. Consider the substitution given analytically by

$$\nu' \equiv r\nu + s \pmod{p^m}. \tag{7}$$

Noting that c_1 has the representation $\nu' \equiv \nu + 1 \pmod{p^m}$, we see that $\alpha^{-1} c_1 \alpha$ has the representation $\nu' \equiv \nu + r \pmod{p^m}$. Thus α transforms c_1 into c_1^r and replaces 0 by s. The group in which C is invariant is given by (7), where r assumes all values prime to p, and where s is unrestricted.

We shall now impose the condition that a substitution of the form (7) belong to Γ, but not to C. We have for α^p the representation

$$\nu' \equiv r^p \nu + s(r^{p-1} + r^{p-2} + \cdots + 1) \pmod{p^m}.$$

As α is not in C, we cannot have $r \equiv 1 \pmod{p^m}$. Since α belongs to Γ, α^p is identity, so that

$$r^p \equiv 1 \pmod{p^m}, \tag{8}$$

$$s(r^{p-1} + r^{p-2} + \cdots + 1) \equiv 0 \pmod{p^m}. \tag{9}$$

By Fermat's theorem,

$$r^p \equiv r \pmod{p}, \tag{10}$$

so that, by (8) and (10), $r \equiv 1 \pmod{p}$. Let $r = kp + 1$. We have

$$r^{p-i} \equiv (p - i)kp + 1 \pmod{p^2},$$

so that

$$r^{p-1} + r^{p-2} + \cdots + 1 \equiv \sum_{i=1}^{i=p} [(p - i)kp + 1] \pmod{p^2},$$

$$\equiv \frac{kp^2(p-1)}{2} + p \pmod{p^2}.$$

Suppose that $p > 2$. Then $p - 1$ is even and

$$r^{p-1} + r^{p-2} + \cdots + 1 \equiv p \pmod{p^2}. \tag{11}$$

That is, the first member of (11) is divisible by p, but not by p^2. Hence, referring to (9), we see that s is divisible by p^{m-1}.

Suppose then that α has the form

$$\nu' \equiv (kp + 1)\nu + lp^{m-1} \pmod{p^m},$$

where kp is not divisible by p^m. Since Γ is regular, if we can show that α leaves certain indices fixed, we will know that α cannot belong to Γ. Consider the congruence

$$(kp + 1)\nu + lp^{m-1} \equiv \nu \pmod{p^m},$$

or

$$kp\nu + lp^{m-1} \equiv 0 \pmod{p^m}. \tag{12}$$

Since kp is not divisible by p^m, we see that (12) must have roots.

We conclude that for α to belong to Γ and not to C, we must have $p = 2$.

If $p = 2$, we must have, by (8),

$$r^2 \equiv 1 \pmod{2^m}.$$

If $m > 2$, this congruence has the four solutions

$$r \equiv \pm 1, \qquad r \equiv 2^{m-1} \pm 1 \pmod{2^m}.$$

Suppose that $m > 2$, and that $r \equiv 2^{m-1} + 1 \pmod{2^m}$. The highest power of 2 by which $r + 1$ is divisible is the first. Since, by (9), $s(r + 1)$ is divisible by 2^m, we see that s is divisible by 2^{m-1}. That is, α has the form

$$\nu' \equiv (2^{m-1} + 1)\nu + 2^{m-1} l \pmod{2^m}.$$

Since this substitution leaves the index 0, or the index 1, fixed, according as l is even or odd, we cannot have $r \equiv 2^{m-1} + 1 \pmod{2^m}$, if $m > 2$.

Suppose that $m > 2$, and that $r \equiv 2^{m-1} - 1 \pmod{2^m}$. Then, by (9), s must be even. Putting $\nu' = \nu$, we have

$$(2^{m-1} - 2)\nu + 2l \equiv 0 \pmod{2^m}.$$

Now, since $m > 2$, $2^{m-1} - 2$ is divisible by no higher power of 2 than the first, so that the congruence above has roots, and α cannot belong to Γ.

We consider finally the case of $r \equiv -1 \pmod{2^m}$. We have the 2^m substitutions

$$\nu' \equiv -\nu + s \pmod{2^m}, \tag{13}$$

which transform C into itself. If s is even, (13) leaves two letters fixed and cannot belong to Γ. Consider those substitutions for which s is odd. We say that if Γ contains one of them, it contains all of them. For if,

in the substitutions

$$\nu' \equiv -\nu + s_1, \qquad \nu' \equiv -\nu + s_2 \pmod{2^m},$$

s_1 and s_2 are both odd, the substitution $\nu' \equiv \nu + (s_2 - s_1)/2 \pmod{2^m}$, which belongs to C, transforms the first into the second. As Γ is an invariant subgroup, if either of these substitutions belongs to Γ the other does also.

Suppose that Γ contains the two substitutions

$$\nu' \equiv -\nu + 1, \qquad \nu' \equiv -\nu - 1 \pmod{2^m},$$

which we denote by α_1 and α_2 respectively. As Γ is abelian, we have, equating $\alpha_1 \alpha_2$ and $\alpha_2 \alpha_1$,

$$\nu - 2 \equiv \nu + 2 \pmod{2^m},$$

from which it follows that $m = 2$.

In the case of $p = 2$, $m = 2$, the symmetric group in four letters has substitutions of order 4.

The proof of the theorem is completed.

COLUMBIA UNIVERSITY,
NEW YORK, N. Y.