POLYNOMIALS $f[\phi(x)]$ REDUCIBLE IN FIELDS IN WHICH $f(x)$ IS IRREDUCIBLE*

BY LOUIS WEISNER

1. *Introduction.* Professor Ritt recently had occasion to consider the irreducible polynomials which become reducible when each argument is replaced by a power of itself.†

His results suggest the related problem of determining all polynomials $\phi_1(x_1, \cdots, x_m), \cdots, \phi_m(x_1, \cdots, x_m)$, such that $f[\phi_1, \cdots, \phi_m]$ is reducible, $f(x_1, \cdots, x_m)$ being irreducible. There is no such problem for functions of one variable, as every polynomial in a single variable can be factored into linear factors. If, however, we restrict ourselves to a field R, the problem arises: Given a polynomial $f(x)$ with coefficients in R and irreducible in R; to determine all polynomials $\phi(x)$ with coefficients in R such that $f[\phi(x)]$ is reducible in R. The present paper is devoted to a solution of this problem.

2. *Reducibility of $\phi(x)-x_i$ in R'.* Let

$$f(x) = (x - x_1)(x - x_2) \cdots (x - x_n) \tag{1}$$

be a polynomial with coefficients in R and irreducible in R; and let $\phi(x)$ be an arbitrary polynomial with coefficients in R. An irreducible factor $A(x)$ of

$$f[\phi(x)] = [\phi(x) - x_1] \cdots [\phi(x) - x_n] \tag{2}$$

has a root in common with one of the equations $\phi(x) = x_i$, say $\phi(x) = x_1$. Let $a_1(x)$ be the greatest common divisor of $A(x)$ and $\phi(x) - x_1$, and

$$\begin{cases} \phi(x) - x_1 = a_1(x)b_1(x) \\ \qquad A(x) = a_1(x)c_1(x), \end{cases} \tag{3}$$

* Presented to the Society, February 25, 1928.

† J. F. Ritt, *A factorization theory for functions* $\sum_{i=1}^{i=n} a_i e^{\alpha_i x}$, Transactions of this Society, vol. 29 (1927), pp. 584–596.

where $b_1(x)$, $c_1(x)$ are polynomials (which may be constants) with coefficients in the field R' obtained by adjoining $x_1, \cdots, x_n$ to R.

The coefficients of the powers of x in (3) are rational functions of $x_1, \cdots, x_n$ with coefficients in R and are therefore unaltered by the group G of $f(x)=0$ relative to R. Let us apply to (3) some substitution of G which changes x_1 to x_i obtaining

$$(4)\qquad \begin{cases} \phi(x) - x_i = a_i(x)b_i(x) \\ \qquad A(x) = a_i(x)c_i(x), \end{cases}$$

where $a_i(x)$, $b_i(x)$, $c_i(x)$ denote what $a_1(x)$, $b_1(x)$, $c_1(x)$, respectively, become when subjected to this substitution. The coefficients of

$$Q(x) \equiv a_1(x) \cdots a_n(x),$$

being invariant under G, are in R. As $A(x)$ is irreducible in R and has a root in common with $Q(x)$, $A(x)$ is a divisor of $Q(x)$. But $A(x)$ is divisible by each of the polynomials $a_1(x), \cdots, a_n(x)$, which are relatively prime as they are divisors of the relatively prime polynomials $\phi(x)-x_1, \cdots, \phi(x)-x_n$ respectively. Thus, $A(x)$ and $Q(x)$ are equal up to a constant factor, which, without loss of generality, may be taken as unity, so that

$$(5)\qquad A(x) = a_1(x) \cdots a_n(x).$$

The polynomial $a_i(x)$ is irreducible in R'. Otherwise, let

$$(6)\qquad a_1(x) = d_1(x)e_1(x),$$

where $d_1(x)$, $e_1(x)$ are (non-constant) polynomials with coefficients in R': these coefficients are rational functions of $x_1, \cdots, x_n$ with coefficients in R, in which form we suppose them to be expressed. Applying to (6) a substitution of G which changes x_1 to x_i, we obtain

$$a_i(x) = d_i(x)e_i(x),$$

where $d_i(x)$, $e_i(x)$ are what $d_1(x)$, $e_1(x)$, respectively, become under this substitution. Thus $d_1(x) \cdots d_n(x)$ is a polynomial with coefficients in R, of degree less than that of

$A(x)$, and divides $A(x)$. As this conflicts with the irreducibility of $A(x)$ in R, $a_i(x)$ is irreducible in R'.

We conclude that *a necessary and sufficient condition that* $f[\phi(x)]$ *be reducible in* R *is that* $\phi(x)-x_1$ *be reducible in* R', *each irreducible factor of* $\phi(x)-x_1$ *in* R' *giving rise to an irreducible factor of* $f[\phi(x)]$ *in* R *by means of an equation similar to* (5).

3. *Divisors of* $f[\phi(x)]$. Because of the relations which exist among $x_1, \cdots, x_n$ the coefficients of a divisor $a_i(x)$ of $\phi(x)-x_i$ may be expressible in different ways as rational functions of $x_1, \cdots, x_n$ with coefficients in R. We proceed to show that *the coefficients of* $a_i(x)$ *equal rational functions of* x_i *alone with coefficients in* R.

The roots of $A(x)=0$ may be separated into systems

$$\begin{array}{c} x_{11}, x_{12}, \cdots, x_{1p} \\ x_{21}, x_{22}, \cdots, x_{2p} \\ \cdots \\ x_{n1}, x_{n2}, \cdots, x_{np}, \end{array}$$

the quantities in the ith system being the roots of $a_i(x)=0$, which form sets of imprimitivity of the group Γ of $A(x)=0$ relative to R if $f(x)$ and $a_i(x)$ are non-linear. Γ permutes these systems in the same way that G permutes $x_1, \cdots, x_n$ respectively. The subgroup G_i of G which leaves x_i fixed corresponds to the subgroup Γ_i of Γ which permutes the symbols of the ith system among themselves. The coefficients of $a_i(x)$ are unaltered by Γ_i when expressed as elementary symmetric functions of $x_{i1}, \cdots, x_{ip}$ and hence are unaltered by G_i when expressed as rational functions of $x_1, \cdots, x_n$ with coefficients in R. As x_i *belongs* to G_i, every function of the roots of $f(x)=0$ which is unaltered by G_i equals a rational function of x_i with coefficients in R; in particular, this is true of the coefficients of $a_i(x)$.

We therefore change our notation and write $a(x, x_i)$ in place of $a_i(x)$. We have

$$A(x) = a(x, x_1) \cdots a(x, x_n). \tag{7}$$

The point to be emphasized in connection with (7) is that $a(x, x_1)$ is a divisor of $\phi(x)-x_1$ and that the other factors in the right member are obtained from $a(x, x_1)$ by changing x_1 to $x_2, \cdots, x_n$.

The preceding equation, derived on the assumption that $A(x)$ is irreducible in R, may be extended to any divisor of $f[\phi(x)]$. Let

$$A(x) = A_1(x) \cdots A_r(x),$$

where $A_1(x), \cdots, A_r(x)$ are irreducible in R, and hence are expressible in the forms

$$A_1(x) = a_1(x, x_1) \cdots a_1(x, x_n),$$
$$\cdots$$
$$A_r(x) = a_r(x, x_1) \cdots a_r(x, x_n),$$

$a_1(x, x_1), \cdots, a_r(x, x_n)$ being divisors of $\phi(x)-x_1$ with coefficients in R' and irreducible in R'. Define

$$a(x, x_1) = a_1(x, x_1) \cdots a_r(x, x_1).$$

Then we have (7), in which $A(x)$ now denotes any divisor of $f[\phi(x)]$ and $a(x, x_1)$ is a divisor of $\phi(x)-x_1$. *Every divisor of $f[\phi(x)]$ with coefficients in R is of the form* (7). This is clearly true of $f[\phi(x)]$ itself.

4. *Construction of $\phi(x)$.* We proceed to prove the converse: if $a(x, y)$ is a polynomial in the independent variables x, y, with coefficients in R, there exists a polynomial $\phi_0(x)$ with coefficients in R such that $f[\phi_0(x)]$ is divisible by

$$A(x) \equiv a(x, x_1) \cdots a(x, x_n) \tag{8}$$

and $\phi_0(x)-x_1$ is divisible by $a(x, x_1)$. Lagrange's interpolation formula suggests taking

$$\phi_0(x) \equiv \sum_{i,j=1}^{i=n,j=p} \frac{x_i A(x)}{(x - x_{ij})A'(x_{ij})}, \tag{9}$$

$x_{i1}, \cdots, x_{ip}$ being the roots of $a(x, x_i)=0$. As the coefficients of

$$\frac{x_i A(x)}{(x - x_{i1})A'(x_{i1})} + \cdots + \frac{x_i A(x)}{(x - x_{ip})A'(x_{ip})}$$

are rational functions of the coefficients of $a(x, x_i)=0$, the coefficients of $\phi_0(x)$ are in R. It is evident that $\phi_0(x_{ij})=x_i$, $(j=1, \cdots, p)$. Hence $\phi_0(x)-x_i$ is divisible by $a(x, x_i)$. As

$$f[\phi_0(x_{ij})] = f(x_i) = 0, \quad \begin{pmatrix} i = 1, \cdots, n \\ j = 1, \cdots, p \end{pmatrix},$$

$f[\phi_0(x)]$ is divisible by $A(x)$.

If $\phi(x)$ is another polynomial with coefficients in R such that $\phi(x)-x_1$ is divisible by $a(x, x_1)$ and $f[\phi(x)]$ is divisible by $A(x)$, then $\phi(x)-\phi_0(x)$ is also divisible by $a(x, x_1)$ and hence by $A(x)$; that is,

$$\phi(x) \equiv \phi_0(x), \qquad (\text{mod } A(x)). \tag{10}$$

Conversely, every polynomial $\phi(x)$ with coefficients in R satisfying this congruence has these properties, $\phi_0(x)$ being distinguished from the others by the fact that its degree is less than that of $A(x)$. The degree of every polynomial $\phi(x)$ of the system (10) excepting $\phi_0(x)$ exceeds that of $A(x)$; hence $f[\phi(x)]$ is reducible. But $f[\phi_0(x)]$ may be of the same degree as $A(x)$ and may be irreducible. For the complete solution of our problem it is necessary to determine those polynomials $a(x, y)$ which lead to a $\phi_0(x)$ such that $f[\phi_0(x)]$ is irreducible.

5. *The Polynomials* $P(x)$. We treat first the case in which $A(x)$ is $f(x)$ itself; that is, we consider the polynomials $\phi(x)$ with coefficients in R such that $f[\phi(x)]$ is divisible by $f(x)$.

If $f[\phi(x)]$ is divisible by $f(x)$, $\phi(x_1)$ is a root of $f(x)=0$; and conversely. Suppose $\phi(x_1)=x_2$. The subgroup of the group G of $f(x)=0$ relative to R which leaves x_1 fixed also leaves x_2 fixed. Hence* there exists a substitution t_2 on the symbols $x_1, \cdots, x_n$ (not necessarily in G) which is commutative with every substitution of G. Let H be the group consisting of the substitutions $t_1=1$, $t_2, \cdots, t_h$ on the symbols $x_1, \cdots, x_n$ which are commutative with all the

* See Miller, Blichfeldt and Dickson, *Finite Groups*, p. 37.

substitutions of G.* The order of H is equal to the number of symbols fixed by the subgroup of G which leaves one symbol fixed. Let $x_1, x_2, \cdots, x_h$ be the symbols fixed by the subgroup of G which leaves x_1 fixed. Then $x_2, \cdots, x_h$ equal rational functions of x_1 with coefficients in R. These functions are readily constructed with the aid of Lagrange's interpolation formula. By a suitable choice of notation we may suppose that t_i changes x_1 to x_i. The functions in question are

$$(11) \qquad P_i(x) \equiv \frac{t_i(x_1)f(x)}{(x - x_1)f'(x_1)} + \cdots + \frac{t_i(x_n)f(x)}{(x - x_n)f'(x_n)},$$

where $t_i(x_j)$ denotes the effect of t_i on x_j. Evidently $P_i(x_j) = t_i(x_j)$.

That the coefficients of $P_i(x)$ are in R may be seen as follows. Apply to the right member of (11) any substitution s of G, obtaining

$$\frac{s[t_i(x_1)]f(x)}{[x - s(x_1)]f'[s(x_1)]} + \cdots + \frac{s[t_i(x_n)]f(x)}{[x - s(x_n)]f'[s(x_n)]}.$$

As s and t_i are commutative, this expression equals

$$\frac{t_i[s(x_1)]f(x)}{[x - s(x_1)]f'[s(x_1)]} + \cdots + \frac{t_i[s(x_n)]f(x)}{[x - s(x_n)]f'[s(x_n)]},$$

which is clearly the same as the right member of (11), except possibly for the order in which the terms are written. Having shown that the coefficients of $P_i(x)$ are unaltered by G, we conclude that they equal numbers in R.

If $\phi(x)$ is a polynomial with coefficients in R such that

$$\phi(x_i) = P(x_i), \qquad (i = 1, \cdots, n),$$

where $P(x)$ is one of the polynomials (11), $\phi(x) - P(x)$ is divisible by $f(x)$; and conversely. Thus *every polynomial with coefficients in R having the property that* $f[\phi(x)]$ *is divisible by* $f(x)$ *is congruent modulo* $f(x)$ *to one of the polynomials* $P(x)$.

* A method for constructing H when G is known is explained in Burnside's *Theory of Groups*, 2d edition, pp. 224–227.

We note in passing that the polynomials $P(x)$ form a group, the "product" of $P_i(x)$ and $P_j(x)$ being $P_i[P_j(x)]$ reduced modulo $f(x)$. This group is simply isomorphic with the group H previously described.

6. *Determination of all Polynomials $\phi(x)$ such that $f[\phi(x)]$ is Reducible.* As noted at the end of §4 we must consider the case in which $f[\phi_0(x)]$ and $A(x)$ are of the same degree. We have

$$[\phi_0(x) - x_1] \cdots [\phi_0(x) - x_n] = ca(x, x_1) \cdots a(x, x_n),$$

where c is in R. It was shown in §3 that $a(x, x_1)$ is a divisor of one of the factors in the left member, say $\phi_0(x) - x_k$; that is,

$$a(x, x_1) = q[\phi_0(x) - x_k],$$

where q is a *constant* in R. Hence x_k equals a rational function of x_1 with coefficients in R. By taking the equation $f(x_1) = 0$ into account, this rational function may be expressed as a polynomial in x_1 of degree less than n, and then must be one of the polynomials $P(x)$ of §5. Thus

$$a(x, y) = a(x) - qP(y). \tag{12}$$

Conversely, if $a(x, y)$ is of this form, $f[\phi_0(x)]$ and $A(x)$ are of the same degree. If, therefore, we avoid choosing $a(x, y)$ of this form, we may be certain that $f[\phi_0(x)]$ is reducible. However, the polynomials (12) may not be ignored. For, although they lead to polynomials as $\phi_0(x)$ such that $f[\phi_0(x)]$ may be irreducible, other polynomials $\phi(x)$ are determined from (10) with the aid of $\phi_0(x)$ which have the property that $f[\phi(x)]$ is reducible.

7. *Summary.* Each polynomial $a(x, y)$ with coefficients in R determines ∞^1 polynomials $\phi(x)$ such that $f[\phi(x)]$ is reducible, by means of (9) and (10). The only exception occurs when $a(x, y)$ is of the form (12), in which case $\phi_0(x)$ is the only polynomial of the system (10) for which $f[\phi_0(x)]$ may be irreducible.

HUNTER COLLEGE OF THE CITY OF NEW YORK