ON IRREDUCIBLE POLYNOMIALS IN SEVERAL VARIABLES WHICH BECOME REDUCIBLE WHEN THE VARIABLES ARE REPLACED BY POWERS OF THEMSELVES*

BY

ELI GOURIN

Let $Q(x_1, \cdots, x_s)$ be a polynomial in $x_1, \cdots, x_s$, irreducible in the field of all constants. There exist, in certain cases, integers $t_1, \cdots, t_s$ such that the polynomial $Q(x_1^{t_1}, \cdots, x_s^{t_s})$ is *reducible.*

The determination of the integers t for which reducibility occurs is a problem which arose in an investigation of J. F. Ritt on the factorization of exponential forms.† The case of real interest is that in which Q has at least three terms. We shall, in this introduction, limit ourselves to the discussion of the results for this case. The relatively simple case of two terms is treated in Part III.

For a fairly general, but not perfectly general, type of polynomial Q, consisting of more than two terms, Ritt proved that the sets t break up into a finite number of classes, the sets of any one class being, from a certain point of view, equivalent.

In the present paper, we obtain information relative to the sets t which, in certain respects, is final. Our results are embodied in the following theorems, in which each t_i is understood to be a positive integer.

THEOREM I. *Let $Q(x_1, \cdots, x_s)$ be an absolutely irreducible polynomial, consisting of more than two terms. Suppose that at least one set $t_1, \cdots, t_s$ exists such that $Q(x_1^{t_1}, \cdots, x_s^{t_s})$ is reducible. Then there exists one and only one finite aggregate of sets*

$$(\alpha) \qquad t_{11}, \cdots, t_{1s}; \cdots; t_{n1}, \cdots, t_{ns}$$

which fulfill the following conditions:

(1) *For every i, $Q(x_1^{t_{i1}}, \cdots, x_s^{t_{is}})$ is reducible.*

(2) *If $Q(x_1^{t_1}, \cdots, x_s^{t_s})$ is reducible, there exists one and only one set $t_{j1}, \cdots, t_{js}$ such that each t_k is an integral multiple of t_{jk} and such that if $t_k = a_k t_{jk}$ $(k=1, \cdots, s)$, then the irreducible factors of $Q(x_1^{t_1}, \cdots, x_s^{t_s})$ are found by replacing each x_k by $x_k^{a_k}$ in the irreducible factors of $Q(x_1^{t_{j1}}, \cdots, x_s^{t_{js}})$.*‡

---

* Presented to the Society, February 23, 1929; received by the editors in February, 1930.

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

‡ That is, if in any irreducible factor of $Q(x_1^{t_{j1}}, \cdots, x_s^{t_{js}})$ each x_k is replaced by $x_k^{a_k}$ the resulting polynomial will be irreducible.

We shall call each of the n sets of (α) a basic set.* With respect to such sets we obtain

THEOREM II. *Let* $M=\max(M_1, \cdots, M_s)$, *where* M_i *is the degree of* $Q(x_1, \cdots, x_s)$ *in* x_i. *For any element* t_{ij} *of any of the basic sets of* Q *we have* $t_{ij} \leqq M^2$.

Furthermore, *the bound* M^2 *is the smallest possible bound. We construct polynomials* Q *for which this bound is actually attained.*

The above results are stronger than those of Ritt in the following respects. Ritt deals with a type of polynomial Q which he calls *primary* (see §1), and supposes that one of the terms of Q is unity. In our case, Q is any polynomial with more than two terms. But the chief advance of the present paper is the determination of the best upper bound, M^2, for the elements of the basic sets. The bound given by Ritt for the case with which he deals is δ^{s+4}, where δ is the degree of Q. It may be remarked that our method of proof is essentially simpler than that of Ritt. His complicated first lemma is eliminated entirely.

In Part II, we define a set $t_1, \cdots, t_s$ as *minimal* if $Q(x_1^{t_1}, \cdots, x_s^{t_s})$ is reducible, but if no $Q(x_1^{\tau_1}, \cdots, x_s^{\tau_s})$ with each τ_i a submultiple of t_i, at least one τ_i a proper submultiple of its t_i, is reducible.

We prove, for a polynomial Q consisting of more than two terms,

THEOREM III. *Those elements of a minimal set which are distinct from unity are equal to each other, and their common value is a prime number which does not exceed the greatest prime less than* M^2.

Furthermore we construct polynomials for which the upper bound given in Theorem III is actually attained.

I. BASIC SETS

1. We shall say that two polynomials, neither identically zero, are equivalent if their ratio is a constant.

Let it be understood that no term of the polynomial $Q(x_1, \cdots, x_s)$ has a zero coefficient and that each x is present in some term of Q with an exponent greater than 0. Following Ritt, we shall say that Q is *primary* in x_i if the highest common factor of the exponents of x_i in all the terms of Q is unity. If Q is primary in each of its variables, we say, simply, that Q is *primary*.

Let $t_1, \cdots, t_s$ be positive integers. Consider the group G of substitutions which replace the variables $x_1, \cdots, x_s$ by $\epsilon_1^{k_1}x_1, \cdots, \epsilon_s^{k_s}x_s$, respectively,

* Assuming the existence of these sets, it is easy to conclude that no infinite system of distinct sets satisfying the conditions (1) and (2) of the theorem can exist. See also §6.

where ϵ_i is a primitive t_ith root of unity and k_i is an arbitrary integer. G is of order $t_1 t_2 \cdots t_s$.

The $t_1 t_2 \cdots t_s$ transforms of a given polynomial by means of G can be grouped into classes of equivalent polynomials. A set of transforms obtained by choosing one polynomial from each such class will be referred to as a *complete set of transforms.*

2. We shall prove the following lemma:

LEMMA I. *If* $Q(x_1, \cdots, x_s)$ *is irreducible and* $Q^{(t)} = Q(x_1^{t_1}, \cdots, x_s^{t_s})$ *is reducible, then the irreducible factors* $Q_1, \cdots, Q_N$ *of* $Q^{(t)}$ *form a complete set of transforms obtained from any one of them.*

Because Q is irreducible, no monomial can be a factor of Q. Hence $Q^{(t)}$ can have no monomial factor, either. Thus Q_1 contains at least two terms.

It is obvious that every substitution of G leaves $Q^{(t)}$ invariant. Consequently, any polynomial obtained from Q_1 by means of G is, like Q_1, an irreducible factor of $Q^{(t)}$.

Let $Q_1, \cdots, Q_l$ be a complete set of transforms obtained from Q_1. The product $P = Q_1 \cdots Q_l$, for any substitution of G, goes over into a polynomial equivalent to P. Furthermore, as the Q_i's are irreducible, and relatively prime, P must be a factor of $Q^{(t)}$. Accordingly, let

$$Q^{(t)} = P \cdot R. \tag{1}$$

We shall prove that R is a constant.

Consider any single variable, say x_1. Not every term of P can contain x_1, else P, and therefore $Q^{(t)}$, would have a monomial factor. Hence the substitution of G which replaces x_1 by $\epsilon_1 x_1$ and leaves all other variables unchanged must leave P invariant. Consequently, P is a rational function of $x_1^{t_1}$ and, similarly, of $x_i^{t_i}$, for every i. If, in (1), R were not a constant, it would certainly be, as the quotient of $Q^{(t)}$ by P, a rational and, consequently, an integral rational function of every $x_i^{t_i}$. Thus R must be a constant, else Q would be reducible.

We may assume that R is unity. Where this is not so at the start, it can be brought about by multiplying Q_1 by $1/R^{1/N}$.

Our lemma is thus proved.

COROLLARY. *Each* Q_i *in the identity* $Q^{(t)} = Q_1 \cdots Q_N$ *involves every variable* x_j.

3. We assume now that the irreducible factor Q_1 of $Q^{(t)}$ is primary and

contains at least three terms. Because Q_1 is irreducible, it must contain at east one term independent of x_1. Suppose, then, that

$$(2)\quad Q_1 = A_1 x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_s^{\alpha_s} + A_2 x_1^{\beta_1} x_2^{\beta_2} \cdots x_s^{\beta_s} + \cdots + A_\mu x_1^{\mu_1} x_2^{\mu_2} \cdots x_s^{\mu_s} + A_\nu x_2^{\nu_2} \cdots x_s^{\nu_s}$$

where the A's are constants and the last term does not contain x_1.

From (2) we find

$$(3)\quad Q_1 = x_2^{\nu_2} \cdots x_s^{\nu_s} U,$$

where

$$(4)\quad U = A_1 x_1^{\alpha_1} x_2^{\alpha_2-\nu_2} \cdots x_s^{\alpha_s-\nu_s} + A_2 x_1^{\beta_1} x_2^{\beta_2-\nu_2} \cdots x_s^{\beta_s-\nu_s} + \cdots + A_\mu x_1^{\mu_1} x_2^{\mu_2-\nu_2} \cdots x_s^{\mu_s-\nu_s} + A_\nu.$$

LEMMA II. *If Q_1 contains at least three terms and is primary, then, for at least one variable $x_i (i \neq 1)$ the exponents $\alpha_1, \beta_1, \cdots, \mu_1$ in U will not be proportional to the corresponding exponents $\alpha_i - \nu_i, \beta_i - \nu_i, \cdots, \mu_i - \nu_i$.*

Suppose that this is not true. Then, since the exponents of x_1 in the various terms of U are all non-negative integers, the exponents of any other variable x_j must be either all non-positive or all non-negative. Let D_j be the greatest common factor of the exponents of x_j in U (if they are non-positive, we shall understand by D_j their common negative divisor of maximum absolute value).

The exponents of x_j in U will, accordingly, be of the form $a_{1j}D_j, \cdots, a_{\mu j}D_j$, where the a's are relatively prime non-negative integers. When $j=1$, $D=1$, because U has the same exponents for x_1 as Q_1. From this fact and the assumed proportionality of the exponents it follows immediately that, for any j, the set of integers $a_{1j}, \cdots, a_{\mu j}$ is identical with the set $\alpha_1, \cdots, \mu_1$. Consequently, U is a polynomial in the product $z = x_1 x_2^{D_2} \cdots x_s^{D_s}$. Then

$$(5)\quad U = C_0 z^n + C_1 z^{n-1} + \cdots + C_{n+1},$$

with constant C's and $n > 1$.

If $z_1, \cdots, z_n$ are the zeros of this latter polynomial, we find, as a consequence from (3) and (5),

$$(6)\quad Q_1 = C_0 x_2^{\nu_2} \cdots x_s^{\nu_s} (z - z_1) \cdots (z - z_n).$$

The product $z = x_1 x_2^{D_2} \cdots x_s^{D_s}$ must involve negative powers; otherwise, by (6), Q would be reducible. Fixing our ideas, let us assume that D_2, $D_3, \cdots, D_k$, but no other D's, are negative. Because the exponents of Q_1 are non-negative, we conclude from (6) that in the expressions

$$(7) \qquad d_2 = \nu_2 + D_2 n, \quad d_3 = \nu_3 + D_3 n, \cdots, d_k = \nu_k + D_k n$$

the d's are non-negative integers.

From (6) and (7) we have that

$$(8) \quad Q_1 = C_0 x_2^{d_2} \cdots x_k^{d_k} x_{k+1}^{\nu_{k+1}} \cdots x_s^{\nu_s} [x_2^{-D_2} \cdots x_k^{-D_k}(z - z_1)] \cdots [x_2^{-D_2} \cdots x_k^{-D_k}(z - z_n)].$$

Each of the factors $x_2^{-D_2} \cdots x_k^{-D_k}(z - z_i)$ is a binomial in which the variables involved have positive exponents. Because n is greater than unity, there are at least two such factors. This result is, however, an absurdity, since Q_1 is irreducible.

Thus in U, for some x_i, the exponents are not proportional to those of x_1.

4. We shall prove the following lemma:

LEMMA III. *If an irreducible factor Q_1 of $Q^{(t)} = Q(x_1^{t_1}, \cdots, x_s^{t_s})$ consists of at least three terms, and is primary, then each t_j, where j is among the numbers $1, 2, \cdots, s$, satisfies the relation $t_j \leqq M^2$.*

It follows from Lemma I that, if $Q^{(t)} = Q_1 \cdots Q_N$, and Q_1 consists of more than two terms and is primary, then each of the Q_i's contains, likewise, more than two terms and is primary.

We conclude further from Lemma II, and from the expression of Q_1 as given in (2), that there exists a subscript i such that at least two numbers in the set $\alpha_1, \beta_1, \cdots, \mu_1$ are not proportional to two corresponding numbers in the set $\alpha_i - \nu_i, \beta_i - \nu_i, \cdots, \mu_i - \nu_i$. Changing, if necessary, the subscripts of the variables as well as the notation of the exponents in (2), we may assume that the numbers α_1, β_1 are not proportional to $\alpha_2 - \nu_2, \beta_2 - \nu_2$ and that the determinant $\alpha_1(\beta_2 - \nu_2) - \beta_1(\alpha_2 - \nu_2)$ is positive.

Let n_1 be the degree of Q_1 in x_1 and n_2 the degree in x_2. Let m_1 and m_2 be, respectively, the degrees of Q in the same variables. Because Q_1 is primary, there will be no two equivalent polynomials among the t_1 polynomials $Q_1(\epsilon_1^{k_1} x_1, x_2, \cdots, x_s)$ $(k_1 = 0, 1, \cdots, t_1 - 1)$.

Suppose, indeed, that, for distinct values p and q of k_1, the corresponding polynomials Q_{1p} and Q_{1q} satisfy a relation

$$Q_{1p} = cQ_{1q},$$

where c is a constant. It is easy to see from (2) that c must be unity and that

$$\epsilon_1^{p\alpha_1} = \epsilon_1^{q\alpha_1}, \cdots, \epsilon_1^{p\mu_1} = \epsilon_1^{q\mu_1},$$

or

$$\frac{\alpha_1(p - q)}{t_1} = I_\alpha, \cdots, \frac{\mu_1(p - q)}{t_1} = I_\mu,$$

where the I's are integers. Because $\alpha_1, \cdots, \mu_1$ are relatively prime, $p-q$ must be divisible by t_1, which implies that $p=q$.

It follows therefore from Lemma I that N is at least equal to t_1. By comparing the degrees in x_1 of both sides of the identity

$$Q^{(t)} = Q_1 \cdot Q_2 \cdots Q_N, \tag{9}$$

we find that

$$t_1 n_1 \leqq t_1 m_1, \quad \text{or} \quad n_1 \leqq m_1. \tag{10}$$

Similarly, we find that

$$t_2 n_2 \leqq t_2 m_2, \quad \text{or} \quad n_2 \leqq m_2. \tag{11}$$

Let us now denote by Q_{uv} any of the polynomials which are obtained from Q_1 by placing $\epsilon_1^u x_1$ for x_1 and $\epsilon_2^v x_2$ for x_2, where u is among the numbers $0, 1, \cdots, t_1-1$ and v among the numbers $0, 1, \cdots, t_2-1$.

These $t_1 t_2$ polynomials may form several sets of equivalent polynomials. Suppose, therefore, that, for two pairs of integers (u_1, v_1) and (u_2, v_2), the corresponding polynomials $Q_{u_1 v_1}$ and $Q_{u_2 v_2}$ are equivalent. It follows then from (2) by considering the first two and the last terms, that the following relations must be satisfied:

$$\epsilon_1^{\alpha_1 u_1} \epsilon_2^{\alpha_2 v_1} = c\epsilon_1^{\alpha_1 u_2} \epsilon_2^{\alpha_2 v_2}, \qquad \epsilon_1^{\beta_1 u_1} \epsilon_2^{\beta_2 v_1} = c\epsilon_1^{\beta_1 u_2} \epsilon_2^{\beta_2 v_2}, \qquad \epsilon_2^{\nu_2 v_1} = c\epsilon_2^{\nu_2 v_2},$$

where c is a constant. This implies that

$$\frac{\alpha_1(u_2 - u_1)}{t_1} + \frac{\alpha_2(v_2 - v_1)}{t_2} = I_1 + e, \tag{12}$$

$$\frac{\beta_1(u_2 - u_1)}{t_1} + \frac{\beta_2(v_2 - v_1)}{t_2} = I_2 + e, \tag{13}$$

$$\frac{\nu_2(v_2 - v_1)}{t_2} = I_3 + e, \tag{14}$$

where the I's are integers and e is a rational fraction.

Subtracting (14) from (12) and (13), we find that

$$\frac{\alpha_1(u_2 - u_1)}{t_1} + \frac{(\alpha_2 - \nu_2)(v_2 - v_1)}{t_2} = I_4,$$

$$\frac{\beta_1(u_2 - u_1)}{t_1} + \frac{(\beta_2 - \nu_2)(v_2 - v_1)}{t_2} = I_5,$$

and, solving for $(u_2-u_1)/t_1$ and $(v_2-v_1)/t_2$, we have

$$\frac{(u_2-u_1)\Delta}{t_1} = I_6, \tag{15}$$

$$\frac{(v_2-v_1)\Delta}{t_2} = I_7, \tag{16}$$

where $I_4, \cdots, I_7$ are integers and Δ is the determinant $\alpha_1(\beta_2-\nu_2) - \beta_1(\alpha_2-\nu_2)$.

Let $d_i (i=1, 2)$ be the highest common factor of Δ and $t_i (i=1, 2)$. Then

$$\Delta = d_1\delta_1 = d_2\delta_2, \quad t_1 = d_1\tau_1, \quad t_2 = d_2\tau_2,$$

where $\delta_1, \delta_2, \tau_1, \tau_2$ are positive integers.

Substituting these expressions in (15) and (16) we find that

$$\frac{u_2-u_1}{\tau_2}\delta_1 = I_6, \tag{17}$$

$$\frac{v_2-v_1}{\tau_2}\delta_2 = I_7. \tag{18}$$

Since the pairs (δ_1, τ_1) and (δ_2, τ_2) are relatively prime, the relations (17) and (18) can be satisfied only if (u_2-u_1) is divisible by τ_1 and (v_2-v_1) by τ_2.

It follows immediately that these relations will surely not be satisfied if u_1 and u_2 are both among the numbers $0, 1, \cdots, t_1-1$, and v_1 and v_2 both among the numbers $0, 1, \cdots, \tau_2-1$. Thus we can obtain from Q_1, by means of the substitutions of G, at least $t_1\tau_2$ polynomials no two of which are equivalent. This implies that $N \geqq t_1\tau_2$. Comparing the degrees in x_2 of both sides of the identity (9), we find that

$$t_1\tau_2 n_2 \leqq t_2 m_2, \tag{19}$$

or, since $\tau_2 = t_2/d_2$,

$$t_1 \leqq \frac{m_2 d_2}{n_2} \leqq \frac{m_2\Delta}{n_2}. \tag{20}$$

Now Δ stands for the expression $\alpha_1(\beta_2-\nu_2)-\beta_1(\alpha_2-\nu_2)$, which is positive. If, therefore, both $\beta_2-\nu_2$ and $\alpha_2-\nu_2$ are non-negative, then $\Delta \leqq \alpha_1(\beta_2-\nu_2) \leqq \alpha_1 n_2$. If they are both non-positive, then $\Delta \leqq \beta_1(\nu_2-\alpha_2) \leqq \beta_1 n_2$. Finally, if $\beta_2-\nu_2$ is positive and $\alpha_2-\nu_2$ is negative, then

$$\Delta = \alpha_1(\beta_2-\nu_2) + \beta_1(\nu_2-\alpha_2) \leqq n_1(\beta_2-\nu_2) + n_1(\nu_2-\alpha_2) \leqq n_1(\beta_2-\alpha_2) \leqq n_1 n_2.$$

We find, thus, that in all cases $\Delta \leqq n_1 n_2$. Hence, it follows from (20) that

$$t_1 \leqq m_2 n_1, \tag{21}$$

and, from (10), that

$$t_1 \leqq m_2 m_1 \leqq M^2. \tag{22}$$

This result we obtained by considering a particular variable x_1. We can apply the same reasoning to any other variable x_i and prove that, in general,

$$t_i \leqq M^2. \tag{23}$$

Lemma III is proved.

5. We assume, next, that the irreducible polynomial $Q(x_1, \cdots, x_s)$ consists of at least three terms and prove

LEMMA IV. *If Q consists of at least three terms and if the irreducible factor Q_1 of $Q^{(t)}$ is primary, then Q_1 consists, likewise, of at least three terms.*

Suppose that Q_1 contains just two terms.

Because Q_1 is irreducible, a given variable x_i can be present only in one of the two terms. Further, since Q_1 is primary, it can involve only first powers of the variables. Let us assume, therefore, since we are free to interchange the subscripts, that

$$Q_1 = ax_1x_2 \cdots x_k + bx_{k+1} \cdots x_s, \tag{24}$$

where a and b are constants.

We denote by q the ratio $x_{k+1} \cdots x_s/(x_1x_2 \cdots x_k)$, so that $Q_1 = ax_1 \cdots x_k (1+c_1q)$, where $c_1 = b/a$.

It follows from Lemma I that, if $Q^{(t)} = Q_1Q_2 \cdots Q_N$, then each Q_i will be of the form $Q_i = d_i a x_1 \cdots x_k(1+c_iq)$, where d_i and c_i are constants and $d_1 = 1$.

We find, in this way, the following expression for $Q^{(t)}$:

$$Q^{(t)} = Da^N(x_1x_2 \cdots x_k)^N(1 + B_1q^{\alpha_1} + B_2q^{\alpha_2} + \cdots + B_nq^N), \tag{25}$$

where $D = d_1d_2 \cdots d_N$ and the last factor is the product of the N binomials $(1+c_iq)$.

Since $Q^{(t)}$ does not change when $x_i (i = 1, \cdots, k)$ is replaced by $\epsilon_i x_i$, it is easy to see that N and each α_j must be divisible by t_i.

Similarly we conclude that N and each of the α's must be divisible by t_j, where j is among the numbers $k+1, \cdots, s$. Consequently, $N = \nu T$ and $\alpha_j = \gamma_j T$, where T is the least common multiple of the numbers $t_1, \cdots, t_s$, and ν and γ_j are positive integers. Denoting q^T by q_1, we find from (25)

$$Q^{(t)} = Da^N(x_1 \cdots x_k)^{\nu T}(1 + B_1q_1^{\gamma_1} + B_2q_1^{\gamma_2} + \cdots + B_nq_1^{\nu}). \tag{26}$$

The exponent ν is greater than unity. Otherwise $Q^{(t)}$ and, consequently, Q would contain only two terms. Then, the last factor of $Q^{(t)}$ in (26), as a polynomial in one variable of degree higher than unity, is reducible. Let $e_1, \cdots, e_\nu$ be the zeros of this polynomial.

We find from (26), substituting for q_1 its expression in the x's,

$$Q^{(t)} = B_n D a^N [(x_{k+1} \cdots x_s)^T - e_1(x_1 \cdots x_k)^T] \cdots [(x_{k+1} \cdots x_s)^T - e_\nu(x_1 \cdots x_k)^T], \tag{27}$$

which contradicts the assumption that Q is irreducible. Hence Q_1, and, consequently, each Q_i, consists of at least three terms.

6. An immediate consequence of the last two lemmas is the following result: Given an irreducible polynomial $Q(x_1, \cdots, x_s)$ consisting of more than two terms, there can exist only a finite number of sets

$$(\beta) \qquad t_{11}, \cdots, t_{1s}; \cdots; t_{n1}, \cdots, t_{ns}$$

such that the irreducible factors of $Q(x_1^{t_{i1}}, \cdots, x_s^{t_{is}})$ $(i=1, \cdots, n)$ are primary.

We assume that all sets of such nature are present among the n sets of (β) and, furthermore, that no two sets of (β) are identical.

We shall prove that if Q is primary, then the sets (β) are the basic sets of Q referred to in the introduction. Let, indeed, $t_1, \cdots, t_s$ be a set of exponents for which $Q^{(t)}$ is reducible, and let $P(x_1, \cdots, x_s)$ be one of the irreducible factors of $Q^{(t)}$. If α_j is the greatest common factor of the exponents of x_j in P, so that

$$P(x_1, \cdots, x_s) = Q_1(x_1^{\alpha_1}, \cdots, x_s^{\alpha_s})$$

where $Q(x_1, \cdots, x_s)$ is primary, we conclude from Lemma I that

$$Q^{(t)} = Q_1(x_1^{\alpha_1}, \cdots, x_s^{\alpha_s}) \cdots Q_N(x_1^{\alpha_1}, \cdots, x_s^{\alpha_s}). \tag{28}$$

This implies that $Q^{(t)}$ is an integral rational function in $x_j^{\alpha_j}(j=1, \cdots, s)$.

Because Q is primary, each t_j must be divisible by the corresponding α_j. If, therefore, $t_j=\alpha_j\tau_j$, we find from (28) that

$$Q(x_1^{\tau_1}, \cdots, x_s^{\tau_s}) = Q_1(x_1, \cdots, x_s) \cdots Q_N(x_1, \cdots, x_s) \tag{29}$$

where the Q_i's are primary.

Consequently, the set $\tau_1, \cdots, \tau_s$ must be one of the sets (β).

Hence, given any set of t's for which $Q^{(t)}$ is reducible, there always exists, among the sets (β), one and only one set, say $t_{k1}, \cdots, t_{ks}$, such that, for every i, $t_i=\alpha_i t_{ki}$ and such that the irreducible factors of $Q^{(t)}$ are obtained by replacing in the irreducible factors of $Q(x_1^{t_{k1}}, \cdots, x_s^{t_{ks}})$ each x_i by $x_i^{\alpha_i}$.

Furthermore, any other aggregate (γ) of sets having the two properties just stated must be identical with the aggregate (β). We shall prove, first, that any set of (β) belongs to (γ). Otherwise, we must conclude that there exists in (β) a set, say $t_{i1}, \cdots, t_{is}$, whose elements are integral multiples of the corresponding elements of some set of (γ), one element, at least, a proper multiple. Let $\tau_1, \cdots, \tau_s$ be the elements of this latter set. Each τ_j is, in its turn, a multiple of the corresponding element in some set, say $t_{k1}, \cdots, t_{ks}$, of (β), distinct from the set $t_{i1}, \cdots, t_{is}$. The elements of the two chosen sets of (β) satisfy, therefore, relations of the form $t_{ij}=a_j t_{kj}$, at least one of the a's being greater than unity. Moreover, the irreducible factors of $Q(x_1^{t_{i1}}, \cdots, x_s^{t_{is}})$ can be found by replacing in the irreducible factors of $Q(x_1^{t_{k1}}, \cdots, x_s^{t_{ks}})$ each x_j by x^{a_j}, which is an absurdity. Hence each set of (β) belongs to (γ). Similarly it can be shown that each set of (γ) belongs to (β). The two aggregates are therefore identical.

The sets (β) are thus the basic sets of Q.

7. Suppose, next, that the polynomial Q is not primary. Let λ_j be the greatest common factor of the exponents of x_j in Q. We have, then, that

$$Q(x_1, \cdots, x_s) = Q'(x_1^{\lambda_1}, \cdots, x_s^{\lambda_s})$$

where $Q'(x_1, \cdots, x_s)$ is primary.

Consider the basic sets (β) of Q'. In any of these sets, say $t_{i1}, \cdots, t_{is}$, we replace each t_{ij} by τ_{ij}, where $\tau_{ij}=t_{ij}/d_{ij}$ and d_{ij} is the greatest common factor of t_{ij} and λ_j. We obtain in this way, say, n sets

$$(\beta') \qquad \tau_{11}, \cdots, \tau_{1s}; \cdots; \tau_{n1}, \cdots, \tau_{ns}.$$

We shall prove that the sets (β') have the qualities necessary for them to be a system of basic sets of Q.

We verify, first, that, for any $i(i=1, \cdots, n)$, the polynomial $Q(x_1^{\tau_{i1}}, \cdots, x_s^{\tau_{is}})$ is reducible. We have, indeed, denoting λ_j/d_{ij} by λ_{ij}, that

$$Q(x_1^{\tau_{i1}}, \cdots, x_s^{\tau_{is}}) = Q'(x_1^{\lambda_{i1}t_{i1}}, \cdots, x_s^{\lambda_{is}t_{is}}).$$

The latter polynomial is obviously reducible.

Further, if, for a given set of t's, $Q^{(t)}$ is reducible, we find from (28) that

$$(30) \quad Q^{(t)} = Q'(x_1^{t_1\lambda_1}, \cdots, x_s^{t_s\lambda_s}) = Q_1(x_1^{\alpha_1}, \cdots, x_s^{\alpha_s}) \cdots Q_N(x_1^{\alpha_1}, \cdots, x_s^{\alpha_s}).$$

This implies that, for every j, $t_j\lambda_j$ must be divisible by α_j. Hence, if $t_j\lambda_j=\alpha_j\tau_j$ we find from (30) that

$$(31) \qquad Q'(x^{\tau_1}, \cdots, x^{\tau_s}) = Q_1(x_1, \cdots, x_s) \cdots Q_N(x_1, \cdots, x_s)$$

where all the Q_i's are primary.

Consequently, the τ's form one of the sets (β), say the set $t_{k1}, \cdots, t_{ks}$. For every j we have, therefore,

$$t_j = \frac{\alpha_j t_{kj}}{\lambda_j} = \frac{\alpha_j \tau_{kj}}{\lambda_{kj}}.$$

Because τ_{kj} and λ_{kj} are relatively prime, α_j must be divisible by λ_{kj}. Accordingly, let $\alpha_j = \delta_j \lambda_{kj}$, so that $t_j = \delta_j \tau_{kj}$.

Replacing now in (30) each $x_j^{\delta_j}$ by x_j, we find that

$$(32) \quad Q(x_1^{\tau_{k1}}, \cdots, x_s^{\tau_{ks}}) = Q_1(x_1^{\lambda_{k1}}, \cdots, x_s^{\lambda_{ks}}) \cdots Q_N(x_1^{\lambda_{k1}}, \cdots, x_s^{\lambda_{ks}}).$$

Hence, given a set of t's for which $Q^{(t)}$ is reducible, there exists always in (β') one and only one set, say $\tau_{k1}, \cdots, \tau_{ks}$, such that, for every j, $t_j = \delta_j \tau_{kj}$, and such that the irreducible factors of $Q^{(t)}$ are obtained by replacing in the irreducible factors of $Q(x_1^{\tau_{k1}}, \cdots, x_s^{\tau_{ks}})$ each x_j by $x_j \delta_j$.

We know already that there can exist no other system of sets having the same two properties.

The sets (β') are, therefore, the basic sets of Q.

8. The results obtained in §§6 and 7 verify thus Theorem I, announced in the introduction. We conclude, further, on the basis of Lemma III, that Theorem II of the introduction is likewise true for a primary polynomial Q. If Q is not primary, the upper bound for the elements of its basic sets, as we have seen, cannot exceed the corresponding bound for the basic sets of a primary polynomial whose degrees in the individual variables never exceed the degrees of Q in the same variables. Hence, if t is any element of any of the basic sets of Q, we have, a fortiori, that $t \leqq M^2$. Theorem II is, therefore, true for any polynomial Q.

9. We shall show now that the bound of Theorem II is the smallest possible bound. We shall construct a class of polynomials for which t actually reaches the value M^2.

Consider the polynomial

$$(33) \qquad P_0(x_1, \cdots, x_s) = 1 + x_1 x_2 \cdots x_s + x_1^m,$$

where m is a positive integer greater than unity.

We shall prove that P *is irreducible for any* m. For, if $P_0 = P_1 \cdot P_2$, it is clear that x_1 must be present in both polynomials P_1 and P_2; otherwise, the coefficient of the last term in P_0 would be distinct from unity. This implies, however, that the polynomial

$$R(x_1, x_2) = 1 + x_1 x_2 + x_1^m$$

obtained from P by replacing $x_3, x_4, \cdots, x_s$ by unity, is also reducible. If,

therefore, $R=R_1 \cdot R_2$, we conclude, for the same reason as before, that x_1 must be present in both R_1 and R_2. Because R is linear in x_2, this variable can be present only in one of the factors, say R_1. Hence.

$$1+x_1x_2+x_1^m=R_1(x_1,x_2)R_2(x_1). \tag{34}$$

Any root α of the equation $R_2=0$ must be distinct from zero. Replacing in (34) x_1 by α, we find that

$$1 + x_2\alpha + \alpha^m = 0,$$

where x_2 is arbitrary, which is, of course, an absurdity. Consequently, P_0 is irreducible.

Consider the m polynomials $P_0, P_1, \cdots, P_{m^2-1}$ obtained from P_0 by substituting $\epsilon_1^{k_1}x_1$ for x_1, where ϵ_1 is a primitive m^2th root of unity and k_1 ranges over the numbers $0, 1, \cdots, m^2-1$. Because P_0 is a primary polynomial, there will be no pair of equivalent polynomials in the set thus obtained. On the other hand, it is easy to verify that any polynomial obtained from P_0 by replacing x_1 by $\epsilon_1^{k_1}x_1$, where ϵ_1 and k_1 have the same meanings as above, and by replacing, further, any other variable x_j by $\epsilon_j^{k_i}x_j$, where ϵ_j is a primitive mth root of unity and $k_j=0, \cdots, m-1$, is identical with one of the polynomials P_i. The index i is the smallest non-negative number satisfying the congruence

$$y \equiv [k_1 + m(k_2 + k_3 + \cdots + k_s)] \pmod{m^2}.$$

The product $\Pi(x_1, \cdots, x_s)$ of the m polynomials P_i, therefore, remains invariant for any of the substitutions of the group G described above and, consequently, is an integral rational function in $x_1^{m^2}, x_2^m, \cdots, x_s^m$.

Consider now the polynomial $\Pi_1(x_1, \cdots, x_s)$ obtained from $\Pi(x_1, \cdots, x_s)$ by replacing $x_1^{m^2}$ by x_1 and x_j^m by $x_j (j=2, \cdots, s)$. The polynomial Π_1 is irreducible. For, if

$$\Pi_1 = A(x_1, \cdots, x_s)B(x_1, \cdots, x_s),$$

then

$$\Pi = A(x_1^{m^2}, x_2^m, \cdots, x_s^m)B(x_1^{m^2}, x_2^m, \cdots, x_s^m),$$

a relation which is absurd, considering that the group G is transitive with respect to any of the polynomials P_i the product of which is Π.

Now, the degree of Π in x_1 is m^3, and in any of the remaining variables is m^2. Consequently, the degrees of Π_1 in the same variables are all equal to $m=M$. Furthermore, replacing in Π_1 the variable x_1 by $x_1^{M^2}$ and every other variable x_j by x_j^M, we find that

$$\Pi_1(x_1^{M^2}, x_2^M, \cdots, x_s^M) = P_0 \cdot P_1 \cdots P_{M^2-1}$$

where the P_i's are primary.

Hence Π_1 has, at least, one basic set in which one of the elements, namely t_1, actually attains the value M^2. This proves that the bound of Theorem II is the smallest possible bound.

II. Minimal sets

10. From the definition of a minimal set, as given in the introduction, it follows easily that every minimal set of an irreducible polynomial consisting of more than two terms is necessarily a basic set. For its elements must be integral multiples of the corresponding elements of a particular basic set; no element, however, can be a proper multiple. Hence the minimal sets are finite in number.

11. Let $t_1, \cdots, t_s$ be the elements of a minimal set belonging to a primary irreducible polynomial Q. Then, in the identity

$$Q^{(t)} = Q_1 \cdots Q_N,$$

each Q_i is primary. It is obvious, further, that not every t_i is unity. Fixing our ideas, let us assume that $t_1 = t_2 = \cdots = t_{j-1} = 1$ and that the remaining $t_j, \cdots, t_s$ are all greater than unity. Consider the t_j polynomials $Q_1(x_1, \cdots, \epsilon_j^{k_j} x_j, \cdots, x_s)$, $k_j = 0, \cdots, t_j - 1$. We have shown above (§4) that, because Q is primary, no two among these polynomials are equivalent. Denoting their product by P, we find that

$$Q(x_1, \cdots, x_{j-1}, x_j^{t_j}, \cdots, x_s^{t_s}) = P \cdot R, \tag{35}$$

where P and R are integral rational functions in $x_j^{t_j}$. However, R must be a constant; else the polynomial

$$Q(x_1, \cdots, x_{j-1}, x_j, x_{j+1}^{t_{j+1}}, \cdots, x_s^{t_s})$$

would be reducible and the set $1, \cdots, 1, t_j, \cdots, t_s$ would not be a minima set. Hence $N = t_j$. Similarly we find that $N = t_k$, for $k = j, j+1, \cdots, s$. Consequently, $t_j = t_{j+1} = \cdots = t_s = t$.

12. Suppose, now, that $t = q \cdot r$, where q and r are positive integers and q is greater than unity. The product of the t polynomials $Q_1(x_1, \cdots, \epsilon_j^{k_j} x_j, \cdots, x_s)$ can then be decomposed into q products $P_0, P_1, \cdots, P_{q-1}$, where the factors of P_i are the r polynomials obtained by assigning to k_j the r values $i, i+q, \cdots, i+(r-1)q$. The polynomial P_i, therefore, will be invariant for any substitution which replaces x_j by $\eta^k x_j$, where $\eta = e^{2\pi i/r}$ and $k = 0, 1, \cdots, r-1$. Consequently, P_i is a rational integral function

in x_j^r. We have, then, that

$$Q(x_1, \cdots, x_{j-1}, x_j^t, \cdots, x_s^t) = P_0(x_1, \cdots, x_j^r, \cdots, x^s) \cdots P_{q-1}(x_1, \cdots, x_j^r, \cdots, x_s)$$

or

$$Q(x_1, \cdots, x_{j-1}, x_j^q, \cdots, x_s^t) = P_0(x_1, \cdots, x_j, \cdots, x_s) \cdots P_{q-1}(x_1, \cdots, x_j, \cdots, x_s)$$

which is a contradiction, unless $r=1$ and $q=t$.

Consequently t is a prime number. Hence, if Q is primary, those elements in a minimal set which are distinct from unity are all equal to one and the same prime number.

13. We shall consider now the case when Q is not primary. Referring to §7, we shall recall that the basic sets of Q are obtained from the basic sets (β) of a certain primary polynomial by substituting for any element in each set (β) a properly chosen factor of the element. It is clear, further, from the way these substitutions were defined, that all minimal sets of Q will be found by effecting the indicated substitutions only in the minimal sets of (β). The elements in each of the latter sets being equal either to unity or to one and the same prime number, it is obvious that the minimal sets of Q will, thus, necessarily have the same structure.

14. Let p be the common value of those elements in a minimal set which are distinct from unity. Because a minimal set is a basic set, and p is a prime number, it follows from Theorem II that $p \leqq P$, where P is the largest prime less than M^2.

The results obtained in §§12, 13, and 14 of this section verify thus Theorem III of the introduction.

15. We shall show now that the bound P, as defined in §14, is the smallest possible bound.

Consider, indeed, the polynomial

$$(36) \quad Q_0(x_1, \cdots, x_s) = 1 + x_1^{m-q} x_2 \cdot x_3 \cdots x_s + x_1^{(m-q)m-P}(x_2 \cdot x_3 \cdots x_s)^m,$$

where m is any integer greater than unity, P is the largest prime less than m^2, and q is the positive integer satisfying the inequalities

$$m^2 - (q+1)m < P < m^2 - qm.$$

We prove, first, that the polynomial Q_0 is primary in all its variables. This is obvious with regard to the variables $x_2, x_3, \cdots, x_s$. If, on the other hand, d is the greatest common divisor of the exponents in x_1, then d must

be a factor of both $m-q$ and P; consequently, if d is distinct from unity, P must be a factor of $m-q$. As $m-q<P$, we have $d=1$.*

We show, next, that Q_0 is irreducible. For, if $Q_0=Q_1\cdot Q_2$, it is clear that x_1 must be present in both Q_1 and Q_2. The polynomial

$$R(x_1, x_2) = 1 + x_1^{m-q}x_2 + x_1^{(m-q)m-P}x_2^m,$$

obtained from Q by replacing each of the variables $x_3, \cdots, x_s$ by unity, is also reducible. Consider the equation $R(x_1, x_2)=0$. Treating x_2 as a function of x_1, we find, by means of Newton's polygon, that for the neighborhood of $x_1=0$

$$x_2 = \epsilon x_1^{-(m^2-qm-P)/m} + \cdots$$

where ϵ is an mth root of unity. Consequently, if x_1 describes a small circle in the complex plane about $x_1=0$, the m branches of x_2 will be permuted in a single cycle. These m branches thus hang together. Hence $R(x_1, x_2)$ cannot be reducible, which implies that Q_0 is irreducible.

Consider the P polynomials $Q_0, Q_1, \cdots, Q_{P-1}$, obtained from Q_0 by substituting $\eta^{k_1}x_1$ for x_1, where η is a Pth root of unity and $k=0, 1, \cdots, P-1$. No two among these polynomials are equivalent. Furthermore, any polynomial obtained from Q_0 by replacing x_1 by $\eta^{k_1}x_1$ and every other variable x_j by $\eta^{k_j}x_j$, where k_j ranges over the same values as k_1, will be identical with one of the polynomials Q_i, say Q_k. The index k is, namely, the smallest non-negative number which satisfies the congruence

$$y(m-q) \equiv (m-q)k_1 + k_2 + \cdots + k_s \pmod{P}.$$

We conclude, also, from the fact that Q is primary in all its variables, that the same set of polynomials Q_i will be obtained from Q_0 by means of every subgroup g_j of substitutions which replace x_j by $\eta^{k_j}x_j$, k_j and η having the same meanings as before, and leave all other variables unchanged.

This implies, first, that the product of the P polynomials Q_i, which remains invariant for any substitution of our group, is an integral rational function $R(x_1^P, \cdots, x_s^P)$ in x_j^P, for every x_j. Moreover, since any of the substitutions of the subgroup g_j simply permutes the Q_i's, with respect to which g_j is transitive, we conclude that $R(x_1^P, x_2^P, \cdots, x_j^P, x_{j+1}, \cdots, x_s)$, for every j less than s, is irreducible. For, if such a polynomial were a product

$$R_1(x_1, \cdots, x_s)\cdot R_2(x_1, \cdots, x_s)$$

then

* According to Tchebycheff, given an integer a, greater than unity, there exists always a prime number between a and $2a-1$. If, therefore, P is the greatest prime contained in m^2, then $P>m^2/2$ and, consequently, $P>m$, considering that $m>1$.

$$R(x_1^P, \cdots, x_s^P) = R_1(x_1, \cdots, x_j, \overset{P}{x_{j+1}}, \cdots, x_s^P) \cdot R_2(x_1, \cdots, x_j, \overset{P}{x_{j+1}}, \cdots, x_s^P)$$

and none of the subgroups $g_k (k=j+1, \cdots, s)$ could, therefore, be transitive with respect to the polynomials Q_i.

The polynomial $R(x_1, \cdots, x_s)$ obtained from $R(x_1^P, \cdots, x_s^P)$ by replacing each x_j^P by x_j, is, therefore, also irreducible. If m_i is the degree of Q_0 in x_i, then m_iP is the corresponding degree of $R(x_1^P, \cdots, x_s^P)$. Hence, the degree of $R(x_1, \cdots, x_s)$ in x_i is m_i. Because $m_2=m_3= \cdots =m_s=m$ and both numbers $m-q$ and $(m-q)m-P$ are less than m, we see that max $(m_1, \cdots, m_s)=M=m$. The irreducible polynomial $R(x_1, \cdots, x_s)$ becomes reducible when each x_j is replaced by x_j^P. Hence the set $t_1=P, \cdots, t_s=P$ is either a minimal set of $R(x_1, \cdots, x_s)$, or is obtained from a minimal set whose elements are, then, necessarily equal either to unity or to P. Suppose, fixing our ideas, that its elements $\tau_1=\tau_2= \cdots =\tau_j=P$ and $\tau_{j+1}= \cdots =\tau_s=1$. This implies that $R(x_1^P, \cdots, x_j^P, x_{j+1}, \cdots, x_s)$ is reducible. We have seen, however, that a polynomial of this type is always irreducible unless $j=s$.

The polynomial $R(x_1, \cdots, x_s)$ has, therefore, a minimal set all the elements of which are equal to P, where P is the largest prime less than M[2].

III. Polynomials of two terms

16. We shall, for the sake of completeness, investigate the case in which the irreducible polynomial Q has two terms. Changing subscripts, if necessary, we assume that

$$Q(x_1, \cdots, x_s) = ax_1^{\alpha_1}x_2^{\alpha_2} \cdots x_k^{\alpha_k} + bx_{k+1}^{\alpha_{k+1}} \cdots x_s^{\alpha_s}. \tag{37}$$

Let $t_1, \cdots, t_s$ be a set of positive integers for which $Q^{(t)}$ is reducible. We shall prove that in the identity

$$Q^{(t)} = Q_1 \cdots Q_n, \tag{38}$$

Q_1, and, on the basis of Lemma I*, each Q_i, contains only two terms.

Let λ_i be the greatest common factor of the exponents of x_i in Q_1. We conclude from (37) and (38) that $\alpha_i t_i$ must be divisible by λ_i. Hence if $\alpha_i t_i=\lambda_i\tau_i$ and if P_k is the polynomial obtained from Q_k by replacing each $x_j^{\lambda_j}$ by x_j, we find that

$$ax_1^{\tau_1} \cdots x_k^{\tau_k} + bx_{k+1}^{\tau_{k+1}} \cdots x_s^{\tau_s} = P_1 \cdots P_N, \tag{39}$$

where all the P_i's are primary.

* In the proof of this lemma, as well as Lemma III, no restriction was made with regard to the number of terms in the irreducible polynomial Q.

If each Q_i, and, consequently, each P_i, consisted of more than two terms, then, as a consequence of Lemma III, $\tau_j \leqq M^2$. Because M is unity, each τ_j is unity, which is an absurdity. Hence, each Q_i contains only two terms.

Since P_i is primary and consists of only two terms, its degree in x_j is unity. Comparing the degrees in x_j of both sides of the identity (39) we find that $\tau_j = N$, for every j.

Consider the infinite system of sets

$$(\gamma) \qquad t_{21}, \cdots, t_{2s};\ t_{31}, \cdots, t_{3s};\ \cdots$$

where $t_{kj} = k/d_{kj}$ and d_{kj} is the greatest common factor of α_j and k.

We easily verify that, for any set of (γ), the corresponding $Q^{(t)}$ is reducible.

Further, if, for a given set of t's, $Q^{(t)}$ is reducible, then there exists in (γ) one and only one set, say $t_{i1}, \cdots, t_{is}$, such that each t_j is an integral multiple of t_{ij} and such that if $t_j = \delta_j t_{ij}$, the irreducible factors of $Q^{(t)}$ are found by replacing in the irreducible factors of $Q(x_1^{t_{i1}}, \cdots, x_s^{t_{is}})$ each x_j by x^{δ_j}.

Finally, it can be shown that there exists no other system of sets satisfyin the two condition s just stated.

COLUMBIA UNIVERSITY,
NEW YORK, N. Y.