A FACTORIZATION THEORY FOR FUNCTIONS $\sum_{i=1}^{n} a_i e^{\alpha_i x}$*

BY

J. F. RITT

Introduction. When, in the expression

$$a_0 e^{\alpha_0 x} + \cdots + a_n e^{\alpha_n x},$$

we allow n to assume all positive integral values, and the a's and α's all constant values, we obtain a class of functions which is closed with respect to multiplication; that is, the product of any two functions of the class is also in the class. There arises thus the problem of determining all possible representations of a given function of the class as a product of functions of the class. This problem is solved in the present paper.

To secure a simple statement of results, we subject our functions to some adjustments. Let the terms in each function be so arranged that α_i comes before α_j if the real part of α_i is less than that of α_j, or if the real parts are equal but the coefficient of $(-1)^{1/2}$ in α_i is less than that in α_j.† With this arrangement, it is evident that the first term in a product of several functions is the product of the first terms of those functions. Thus we do not specialize our problem if we limit ourselves to functions with first term unity ($a_0=1$, $\alpha_0=0$), resolving such functions into factors‡ with first term unity. We shall make this limitation, and shall furthermore admit into our work only functions with more than one term, that is, functions distinct from unity.§

Our first theorem states that *if*

$$1 + a_1 e^{\alpha_1 x} + \cdots + a_n e^{\alpha_n x} \tag{1}$$

is divisible by

$$1 + b_1 e^{\beta_1 x} + \cdots + b_r e^{\beta_r x},$$

with no b equal to zero, then every β is a linear combination of $\alpha_1, \cdots, \alpha_n$ with rational coefficients.

---

* Presented to the Society, October 30, 1926; received by the editors in December, 1926.

† We assume, of course, that the α's in a function are distinct from one another.

‡ If $P=P_1 \cdots P_m$, with each P_i a function of our class, P will be said to be *divisible* by each P_i, and each P_i will be called a *factor* of P.

§ One might ask whether unity has factors (of first term unity) which are distinct from unity. That it has none follows from the fact that the last term of the product of several functions is the product of the last terms of those functions.

We shall say that the function (1) is *simple* if there exists a number λ of which every α is an integral multiple. It is easy to see that every simple function has an infinite number of factors. In short, as no α has a negative real part, we may suppose λ to be such that every α is a *positive* integral multiple of λ. For every positive integer r, the simple function is a polynomial in $e^{\lambda x/r}$ of degree at least r. It therefore has at least r factors of the form $1+ce^{\lambda x/r}$. It is a consequence of the theorem stated above that every factorization of a simple function is found in this way.

There exist, in abundance, functions (1) which are not divisible by functions (1) other than themselves. We shall call such functions *irreducible.*

We may now state our theorem of factorization.

THEOREM. *Every function*

$$1 + a_1e^{\alpha_1 x} + \cdots + a_n e^{\alpha_n x},$$

distinct from unity, can be expressed in one and in only one way as a product

$$(S_1S_2 \cdots S_s)(I_1I_2 \cdots I_t),$$

in which $S_1, \cdots, S_s$ are simple functions such that the coefficients of x in any one of them have irrational ratios to the coefficients of x in any other, and in which $I_1, \cdots, I_t$ are irreducible functions.*

Most of our work centers about the proof that a resolution exists. Because a function may have an infinite number of factors, this resolution cannot be accomplished by the process of repeated factorization used in the proofs of most factorization theorems. The uniqueness is easy to establish.

1. **Exponents of factors.** We understand, in everything which follows, that the terms in our functions are ordered in the manner explained in the introduction. Of course, the real part of every coefficient of x will be greater than or equal to zero, and, when the real part is zero, the coefficient of $(-1)^{1/2}$ will be positive.

THEOREM. *If $1+\sum_{i=1}^{n} a_ie^{\alpha_i x}$ is divisible by $1+\sum_{i=1}^{r} b_ie^{\beta_i x}$, with no b zero, then every β is a linear combination of $\alpha_1, \cdots, \alpha_n$ with rational coefficients.*

Let

$$\begin{aligned}(2)\qquad 1 + a_1e^{\alpha_1 x} &+ \cdots + a_ne^{\alpha_n x}\\ &= (1 + b_1e^{\beta_1 x} + \cdots + b_re^{\beta_r x})\,(1 + c_1e^{\gamma_1 x} + \cdots + c_se^{\gamma_s x}),\end{aligned}$$

with no b or c equal to zero. Suppose that there exists a β, say β_j, which is not linear in the α's with rational coefficients.

* That is, the α's.

We shall call a set of numbers $m_1, \cdots, m_p$ *independent* if there does not exist a relation $\sum q_i m_i = 0$, with the q's rational, and not all zero.

Let $m_1, \cdots, m_p$ be an independent set of numbers such that every α is a linear combination of the m's with rational coefficients. We shall use the symbol m_0 to represent the β_j considered above. Then $m_0, m_1, \cdots, m_p$ are independent.

We can certainly adjoin new m's to those we already have so as to form an independent set

$$m_0,\ m_1,\ \cdots,\ m_p,\ \cdots,\ m_t$$

such that every α, β and γ is linear in the numbers of this set with rational coefficients.

Every β has a *unique* representation of the form $\sum_{i=0}^{t} q_i m_i$, with rational q's. We select those β's for which q_0 is a maximum, say u_0, of those selected we pick out such for which q_1 is a maximum, say u_1, and continue in this fashion for all the q's, obtaining a certain β, call it B, with a representation $\sum u_i m_i$. Because $\beta_j = m_0$, we have $u_0 \geqq 1$.

We now adjoin to the γ's a $\gamma_0 = 0$, and call the term unity, in the second factor of the right member of (2), $e^{\gamma_0 x}$. Of course, γ_0 is linear in the m's with zero coefficients. Similarly, we adjoin a β_0 to the β's.

We choose from among the γ's a $C = \sum v_i m_i$ with the v's determined successively as maxima. Because $\gamma_0 = 0$, we have $v_0 \geqq 0$.

The multiplication of the factors in the second member of (2) yields a term in $e^{(B+C)x}$. From the manner in which B and C are determined, we see that $B+C$ cannot equal any other $\beta+\gamma$. Hence the term in $e^{(B+C)x}$ does not cancel out and $B+C$ must be an α.

But as the expression for $B+C$ in the m's involves m_0 with a coefficient at least unity, and as the α's depend only on $m_1, \cdots, m_p$, the equality of $B+C$ with an α would imply that the m's are not independent. This proves that the β's are linear in the α's with rational coefficients.

2. **Selection of basis.** We are going to prove the existence of an independent set of numbers $\mu_1, \cdots, \mu_p$, such that every α is a linear combination of the μ's with *positive* rational coefficients.

Each α has either a positive real part, or a zero real part and a positive coefficient for $(-1)^{1/2}$. Thus, if δ is a sufficiently small positive quantity, the product of each α by $e^{-\delta(-1)^{1/2}}$ will have a positive real part. We choose such a δ, and let $A_i = e^{-\delta(-1)^{1/2}}\alpha_i$ $(i = 1, \cdots, n)$.

Let $m_1, \cdots, m_p$ be any independent set of numbers in terms of which the A's can be expressed linearly with rational coefficients. Suppose that

$$A_i = q_{i1}m_1 + \cdots + q_{ip}m_p \qquad (i = 1, \cdots, n), \tag{3}$$

all q's being rational. We shall determine an independent set of numbers $M_1, \cdots, M_p$ such that the m's are linear in the M's with rational coefficients, and such that the coefficients in the expressions of the A's, in terms of the M's, found from (3), are all positive.

We associate with each m_i $(i=1, \cdots, p)$, p rational numbers t_{ij} $(j=1, \cdots, p)$, choosing for each t_{ij} a rational number close to the real part of m_i (how close the approximation should be will be made clear below), and taking care that the determinant $|t_{ij}|$ does not vanish. We determine M's through the equations

$$m_i = t_{i1}M_1 + \cdots + t_{ip}M_p \qquad (i = 1, \cdots, p). \tag{4}$$

The coefficient of M_j in the expression for A_i in terms of the M's is

$$q_{i1}t_{1j} + q_{i2}t_{2j} + \cdots + q_{ip}t_{pj}.$$

If t_{ij} is very close to the real part of m_i, this coefficient will be, according to (3), very close to the real part of A_i, and will therefore be positive.

The M's are independent. For, let a relation

$$Q_1M_1 + \cdots + Q_pM_p = 0 \tag{5}$$

hold, with the Q's rational and not all 0. Because $|t_{ij}| \neq 0$, the equations

$$t_{1j}q_1 + \cdots + t_{pj}q_p = Q_j \qquad (j = 1, \cdots, p)$$

give a set of rational values, not all 0, for $q_1, \cdots, q_p$. Hence (5) implies an impossible relation $\sum q_i m_i = 0$.

If now we put $\mu_i = e^{\delta(-1)^{1/2}} M_i$ $(i=1, \cdots, p)$, we have an independent set of quantities $\mu_1, \cdots, \mu_p$ of which every $\alpha_i = e^{\delta(-1)^{1/2}} A_i$ is a linear combination with *positive* rational coefficients.

In what follows, we shall use only the fact that the coefficients just secured are *non-negative*.

3. **Expressions for β's and γ's.** Of course, every γ, as well as every β, in (2), is linear in the α's with rational coefficients. We say that, in the expression for each β and γ in terms of the μ's found in § 2, the coefficients are all non-negative. Let the contrary be assumed, and to fix our ideas, suppose that some β involves a μ with a negative coefficient. As we have perfect freedom in assigning subscripts to the μ's, we assume that some β involves μ_1 with a negative coefficient.

Of all β's, we select those for which the coefficient of μ_1 is a minimum, of those selected we take such for which the coefficient of μ_2 is a minimum, and continue in this fashion until μ_p is determined as a minimum. We find in this way a definite β, call it B, *with a negative coefficient for* μ_1.

We now adjoin to the γ's a $\gamma_0=0$, and regard the term unity in the second factor of the second member of (2) as being $e^{\gamma_0 x}$. We find, as above, a γ, call it C, with coefficients determined successively as minima. The coefficient of μ_1 in C is not positive, for $\gamma_0=0$.

On multiplying together the factors in the second member of (2), we find a term in $e^{(B+C)x}$, which cannot be cancelled. Hence $B+C$ must be an α. This is impossible, because the coefficient of μ_1 in $B+C$ is negative. Our statement is proved.

More generally, let the first term of (2) be represented by P, and suppose that

$$P = P_1 \cdots P_m, \tag{6}$$

where each subscripted P is, like P itself, a function of the form (1). When μ's are chosen as in § 2, each coefficient of x in each P_i is linear in the μ's with non-negative rational coefficients.

4. **The identities.** As we may replace the μ's by any submultiples of themselves, we may assume that the coefficients of x in the first member of (6) are linear in the μ's with non-negative *integral* coefficients. We make this assumption.

We now associate with each $e^{\mu_i x}$ a variable y_i. We express each exponential in (6) as a product of non-negative rational powers of the exponentials $e^{\mu_i x}$, and replace each $e^{\mu_i x}$ by y_i.

Equation (6) becomes a relation in the y's which holds when each y_i is replaced by $e^{\mu_i x}$. We say that this relation in the y's is an identity in the y's.*

If it were not, there would exist a sum of rational powers of the y's, not identically zero, which would vanish when each y_i is replaced by $e^{\mu_i x}$. But, because the μ's are independent, any two of the products of powers of the y's would yield terms of the form he^{kx} (h and k constants), with distinct k's. As a sum

$$h_1 e^{k_1 x} + \cdots + h_q e^{k_q x}$$

cannot vanish for every x if the k's are distinct from one another and the h's are not all zero, our statement that the relation in the y's is an identity is proved.

5. **The polynomial problem.** We may replace each y_i by a positive integral power of itself in such a way that the sums of rational powers of

* If more than one fractional power of a y_i appears in the relation, the exponents should be reduced to a common denominator, and the various powers of the y_i regarded as integral powers of a single fractional power of the y_i.

the y's obtained from the P_i's of (6) go over into polynomials in the y's. The relation in the y's thus found is, of course, an identity.

We have now a method for obtaining every representation of P as a product $P_1 \cdots P_m$. First we find an independent set of μ's in terms of which the coefficients of x in P can be expressed linearly, with non-negative integral coefficients. We then replace each $e^{\mu_i x}$ in P by a variable y_i, so that P becomes associated with a polynomial $Q(y_1, \cdots, y_p)$. We replace the y's, in all possible ways, by positive integral powers of themselves, obtaining a family of polynomials $Q(y_1^{t_1}, \cdots, y_p^{t_p})$. To each resolution of each of the latter polynomials into factors with first term unity, there corresponds a factorization of P.* All factorizations of P are found in this way.

In our study of $Q(y_1, \cdots, y_p)$ and of the polynomials derived from it, we may limit ourselves to the case in which Q is irreducible. For, if Q is reducible, the factorizations of every polynomial obtained from it by replacing the y's by powers of themselves can be obtained by resolving Q into its irreducible factors, replacing the y's by powers of themselves in those factors, and factoring the polynomials thus obtained.

Our problem thus becomes: *Given an irreducible polynomial* $Q(y_1, \cdots, y_p)$, *to determine for which positive integers* $t_1, \cdots, t_p$ *the polynomial* $Q(y_1^{t_1}, \cdots, y_p^{t_p})$ *is reducible.*

6. **Primary polynomials.** Let $Q(y_1, \cdots, y_p)$ be a polynomial in $y_1, \cdots, y_p$, more definitely, a sum of products of non-negative integral powers of $y_1, \cdots, y_p$, with constant coefficients *distinct from zero*. It is understood that each y_i figures in some term with an exponent greater than zero.

If the highest common factor of all the exponents of y_i in Q is unity, we shall say that Q is *primary* in y_i. If Q is primary in each of its variables, we shall say, simply, that Q is *primary*.

There exists one and only one set of positive integers $t_1, \cdots, t_p$ such that Q can be written in the form $Q'(y_1^{t_1}, \cdots, y_p^{t_p})$, with $Q'(y_1, \cdots, y_p)$ primary. In short, t_i can and must be taken as the highest common factor of the exponents of y_i in Q.

Let $Q(y_1, \cdots, y_p)$ be an irreducible polynomial whose first term is unity. Let $t_1, \cdots, t_p$ be any positive integers. It is evident that every factor of

* The question arises as to whether the coefficients of x obtained, when each y_i is replaced in the factors of $Q(y_1^{t_1}, \cdots, y_p^{t_p})$ by $e^{\mu_i x}$, have positive real parts or zero real parts and positive coefficients for $(-1)^{1/2}$. That the answer is affirmative follows from the facts that unity is a term of each function obtained, and that the first term of a product is the product of the first terms.

$Q(y_1^{t_1}, \cdots, y_p^{t_p})$ has a term independent of the y's. Suppose then that

$$Q(y_1^{t_1}, \cdots, y_p^{t_p}) = Q_1Q_2 \cdots Q_m$$

with each Q_i an irreducible polynomial* in $y_1, \cdots, y_p$ with first term unity.

We associate with each i $(i=1, \cdots, p)$, a primitive t_ith root of unity, ϵ_i. The polynomial $Q(y_1^{t_1}, \cdots, y_p^{t_p})$ undergoes no change when each y_i is replaced by $\epsilon_i^{a_i}y_i$, the a's being any integers. Hence, for such a substitution, the Q_i's go over into constant factors times one another. As each Q_i has unity for a term, the constant factors are unity, so that the Q_i's are interchanged among themselves.

We say that, given any Q_i, there is a substitution of the type described above which converts Q_1 into Q_i. For, suppose that Q_1 is converted only into $j<m$ of the functions, say $Q_1, \cdots, Q_j$. Then the substitutions interchange $Q_1, \cdots, Q_j$ among themselves. Hence the product $Q_1 \cdots Q_j$ is invariant under all of the substitutions.† This means that $Q_1 \cdots Q_j$ is a rational integral function of $y_1^{t_1}, \cdots, y_p^{t_p}$, and hence that $Q(y_1, \cdots, y_p)$ is reducible. Thus Q_1 goes over into every Q_i.

Hence, if Q_1 is primary in certain variables, every Q_i will be primary in those variables.

Similarly, if Q is primary in certain variables, every Q_i will be primary in those variables.

7. **The first lemma.** LEMMA. *Let $Q(y_1, \cdots, y_p)$ be a primary, irreducible polynomial, of degree δ, consisting of more than two terms and with unity for its term of lowest degree. Suppose that, for certain positive integers $t_1, \cdots, t_p$, the irreducible factors of $Q(y_1^{t_1}, \cdots, y_p^{t_p})$ are primary. Then there exist a polynomial $T(y_1, \cdots, y_p)$ and positive integers $\tau_1, \cdots, \tau_p$ which have the following properties*:

(a) *$T(y_1, \cdots, y_p)$ is primary and irreducible, with unity for its term of lowest degree.*

(b) *The degree of $T(y_1, \cdots, y_p)$, in each variable, does not exceed the corresponding degree of $Q(y_1, \cdots, y_p)$.*

(c) *For every i, $\tau_i/t_i \geqq \delta^{-p}$.*

(d) *The irreducible factors of $T(y_1^{\tau_1}, \cdots, y_p^{\tau_p})$ are primary and consist of more than two terms.*

(e) *The polynomials $T(y_1, y_2^{\tau_2}, \cdots, y_p^{\tau_p})$, $T(y_1^{\tau_1}, y_2, y_3^{\tau_3}, \cdots, y_p^{\tau_p}), \cdots,$ $T(y_1^{\tau_1}, y_2^{\tau_2}, \cdots, y_{p-1}^{\tau_{p-1}}, y_p)$ are all irreducible.*

* The term "polynomial" is being used here in its usual sense, rather than in the sense explained at the head of this section. It will be seen, however, that each Q_i involves every y, so that each Q_i is also a polynomial in $y_1, \cdots, y_p$ in the stricter sense.

† This is true even when $Q_1, \cdots, Q_j$ are not distinct.

For simplicity of notation, we shall take the case of $p=3$; it will be seen that the proof is general.

We write x, y, z instead of y_1, y_2, y_3, and p, q, r instead of t_1, t_2, t_3. We shall show the existence of a $T(x, y, z)$ and of integers π, χ, ρ which have the qualities claimed for T, τ_1, etc. in the statement of our lemma.

Let

$$Q(x,y^q,z^r) = Q_1 \cdots Q_m \tag{7}$$

with each Q_i an irreducible polynomial having unity for a term.

Every Q_i is obtained from Q_1 by replacing y by y times a qth root of unity and z by z times an rth root of unity.

Certainly Q_1 is primary in x. It may or may not be primary in y and in z. Let

$$Q_1 = R(x,y^{q_1},z^{r_1}),$$

with $R(x, y, z)$ primary. Certainly $R(x, y, z)$ is irreducible.

Let the degree of $Q(x, y, z)$ in x be a. We say that $q/q_1 \leqq a$ and $r/r_1 \leqq a$. First m, the number of Q_i's, does not exceed a, because every Q_i contains x. Certainly q is divisible by q_1. Let $k=q/q_1$, and let ϵ be a primitive kth root of unity. Because $R(x, y, z)$ is primary, the k polynomials $R(x, \epsilon^i y^{q_1}, z^{r_1})$, $i=1, \cdots, k$, are all distinct. But as each ϵ^i is a q_1th power of a qth root of unity, each of these polynomials is some Q_i. Hence $k \leqq m$, so that $q/q_1 \leqq a$. Similarly, $r/r_1 \leqq a$.

Let b and c be the respective degrees of $Q(x, y, z)$ in y and z, and a_1, b_1, c_1 the respective degrees of $R(x, y, z)$ in x, y, z. We have, by (7), $a=ma_1$, so that $a_1 \leqq a$. Now, as $mb_1q_1=bq$, and as $q \leqq mq_1$ (proved above), we have $b_1 \leqq b$. Similarly, $c_1 \leqq c$.

Let p_1 be written instead of p. Consider the polynomial $R(x^{p_1}, y, z^{r_1})$. Let

$$R(x^{p_1},y,z^{r_1}) = R_1 \cdots R_{m'},$$

with each R_i an irreducible polynomial having unity for a term.

Certainly R_1 is primary in y. It may not be primary in x and in z. Let

$$R_1 = S(x^{p_2},y,z^{r_2})$$

with $S(x, y, z)$ primary. Of course, $S(x, y, z)$ is irreducible. We show as above that $p_1/p_2 \leqq b_1$, $r_1/r_2 \leqq b_1$, and that a_2, b_2, c_2, the degrees of $S(x, y, z)$ in x, y, z, are respectively not greater than a_1, b_1, c_1.

Let q_2 be written in place of q_1. We are going to prove that $S(x, y^{q_2}, z^{r_2})$ is irreducible.

We recall that $Q_1 = R(x, y^{q_1}, z^{r_1})$ is irreducible. Suppose that $S(x, y^{q_2}, z^{r_2})$ is reducible. Then $R_1(x, y^{q_1}, z)$, which equals $S(x^{p_2}, y^{q_2}, z^{r_2})$, can be factored into the form

$$A(x^{p_2}, y, z)B(x^{p_2}, y, z),$$

with $A(x, y, z)$ and $B(x, y, z)$ non-constant rational integral functions.

Let $k = p_1/p_2$ and let ϵ be a primitive kth root of unity. Because $S(x, y, z)$ is primary, the k polynomials $S(\epsilon^i x^{p_2}, y^{q_2}, z^{r_2})$, $i = 1, \cdots, k$, are distinct. But as each ϵ^i is a p_2th power of a p_1th root of unity, each of the k polynomials is obtained from $R_1(x, y^{q_1}, z)$ by replacing x by x times a p_1th root of unity. Hence each of the polynomials is of the form $R_i(x, y^{q_1}, z)$.

Thus, the product of the k functions $A(\epsilon^i x^{p_2}, y, z)$, $i = 1, \cdots, k$, is a factor of $R(x^{p_1}, y^{q_1}, z^{r_1})$, which function equals $Q_1(x^{p_1}, y, z)$. But the product is rational in x^{p_1}, y and z. Thus $Q_1(x, y, z)$ must be reducible. This proves that $S(x, y^{q_2}, z^{r_2})$ is irreducible.

Now, let

$$S(x^{p_2}, y^{q_2}, z) = S_1 \cdots S_{m''},$$

with each S_i an irreducible polynomial having unity for a term. Let

$$S_1 = T(x^{\pi}, y^{\chi}, z),$$

with $T(x, y, z)$ primary (and irreducible). We prove as above that the degree of $T(x, y, z)$ in each variable is not greater than the corresponding degree of $S(x, y, z)$, and that $p_2/\pi \leqq c_2$, $q_2/\chi \leqq c_2$.

Let ρ stand for r_2. It can be shown, as above, that $T(x, y^{\chi}, z^{\rho})$ and $T(x^{\pi}, y, z^{\rho})$ are irreducible (Item (e)).

We wish to show that the irreducible factors of $T(x^{\pi}, y^{\chi}, z^{\rho})$ are primary. That function is a factor of $S(x^{p_2}, y^{q_2}, z^{r_2})$ which is a factor of $R(x^{p_1}, y^{q_1}, z^{r_1})$, a factor of $Q(x^p, y^q, z^r)$. As the irreducible factors of the latter function are primary, those of $T(x^{\pi}, y^{\chi}, z^{\rho})$ are also.

We shall show that each irreducible factor of $T(x^{\pi}, y^{\chi}, z^{\rho})$ contains more than two terms. Let

$$T(x^{\pi}, y^{\chi}, z^{\rho}) = T_1 \cdots T_t,$$

each T_i being irreducible, with unity for its term of lowest degree. Suppose that T_1 has just two terms, and let

$$T_1 = 1 + cx^{\alpha}y^{\beta}z^{\gamma}.$$

Because T_1 is an irreducible factor of $Q(x^p, y^q, z^r)$, the other irreducible factors of $Q(x^p, y^q, z^r)$ are found by multiplying the variables in T_1 by roots of unity. Hence $Q(x^p, y^q, z^r)$ is a polynomial in the product $x^{\alpha}y^{\beta}z^{\gamma}$. Thus the exponents of x, y and z in each term of $Q(x, y, z)$ are respectively proportional to α/p, β/q, γ/r.

Let A be the highest common factor of all the exponents of x which appear in $Q(x, y, z)$, and let B and C be the highest common factors for y and z respectively. Then A, B, C are proportional to $\alpha/p, \beta/q, \gamma/r$, so that $Q(x, y, z)$ is a polynomial in the product $x^A y^B z^C$. Then $Q(x, y, z)$, which has more than two terms, is reducible, for any polynomial in one variable, of more than two terms, is reducible. This absurdity shows that T_1 has more than two terms.

The ratios π/p, χ/q, ρ/r are each at least equal to $1/ab_1c_2 \geqq 1/abc$, and hence are at least equal to δ^{-3}.

The proof of the lemma is completed.

8. **The second lemma.** LEMMA. *Let $Q(y_1, \cdots, y_p)$ be a primary irreducible polynomial, consisting of more than two terms, and having unity for its term of lowest degree. There exist only a finite number of sets of positive integers $t_1, \cdots, t_p$ such that the irreducible factors of $Q(y_1^{t_1}, \cdots, y_p^{t_p})$ are primary.*

We use the polynomial T and the integers $\tau_1, \ldots, \tau_p$ whose existence was shown in § 7. Let

$$T(y_1^{\tau_1}, \cdots, y_p^{\tau_p}) = T_1 \cdots T_t, \tag{8}$$

with each T_i a primary irreducible polynomial, of more than two terms, with unity for its first term.

Our first step will be to prove that

$$t = \tau_1 = \tau_2 = \cdots = \tau_p,$$

t being the number of factors in the second member of (8). Let ϵ be a primitive τ_1th root of unity. Then the τ_1 polynomials $T_1(\epsilon^j y_1, y_2, \cdots, y_p)$, $j=1, \cdots, \tau_1$, are all distinct, and are among the polynomials T_i. The product of these polynomials is a polynomial in $y_1^{\tau_1}, y_2, \cdots, y_p$ which is a factor of the first member of (8). Hence, if τ_1 were less than t, $T(y_1, y_2^{\tau_2}, \cdots, y_p^{\tau_p})$ would be reducible. Thus $\tau_1 = t$. Similarly, $\tau_2 = t$, etc.

It cannot be that there exist numbers $\lambda_1, \cdots, \lambda_p$ such that, in every term of T_1, the exponents of $y_1, \cdots, y_p$ are respectively proportional to $\lambda_1, \cdots, \lambda_p$. As was shown in § 7, the existence of such λ's would imply the reducibility of T_1.

Let us suppose, then, fixing our ideas, that

$$A y_1^{\alpha_1} y_2^{\alpha_2} \cdots y_p^{\alpha_p}, \qquad B y_1^{\beta_1} y_2^{\beta_2} \cdots y_p^{\beta_p}$$

(A and B constants), are two terms of T_1 with α_1 and α_2 not proportional to β_1 and β_2, that is, with $\alpha_1\beta_2-\beta_1\alpha_2\neq 0$.

As we are free to interchange the letters α and β, we assume that $\alpha_1\beta_2-\beta_1\alpha_2>0$. Then $\beta_2>0$.

There are t^2 ways of multiplying y_1 and y_2 in T_1 by tth roots of unity. As this group of t^2 operations converts T_1 into precisely t distinct polynomials, there must be t of the operations which leave T_1 invariant.

Let

$$y_1' = \epsilon^u y_1, \qquad y_2' = \epsilon^v y_2$$

be any of the t operations which leave T_1 invariant. Then the pair of congruences

$$\begin{aligned} \alpha_1 u + \alpha_2 v &\equiv 0, \\ \beta_1 u + \beta_2 v &\equiv 0 \qquad (\mathrm{mod}\ t), \end{aligned}$$

must have at least t solutions in common, u and v being, in each solution, non-negative integers less than t.

Any solution of the above congruences is also a solution of the congruences

$$(\alpha_1\beta_2 - \beta_1\alpha_2)u \equiv 0, \tag{9}$$

$$v\beta_2 \equiv -\beta_1 u \qquad (\mathrm{mod}\ t). \tag{10}$$

Let h be the highest common factor of $\alpha_1\beta_2-\beta_1\alpha_2$ and t. Then (9) has precisely h solutions in u. Let k be the highest common factor of β_2 and t. Then, for each u satisfying (9), the congruence (10) has at most k solutions in v.*

Hence

$$hk \geqq t,$$

so that either $h\geqq t^{1/2}$ or $k\geqq t^{1/2}$.

Suppose first that $h\geqq t^{1/2}$. Then $\alpha_1\beta_2-\beta_1\alpha_2$ is at least $t^{1/2}$, so that either α_1 or β_2 is at least $t^{1/4}$.

Suppose that $\alpha_1\geqq t^{1/4}$. Then the degree of T_1 is at least $t^{1/4}$. Let a be the degree of $T(y_1, \cdots, y_p)$ in y_1. Then, by (8),

$$at \geqq t \cdot t^{1/4}.$$

We know that a does not exceed the degree of Q in y_1. Hence $a\leqq\delta$, where δ is the degree of Q. Then $t\leqq\delta^4$, so that, by the lemma of § 7, $t_1, \cdots, t_p$ are each not greater than δ^{p+4}.

We find the same bound for t_1 etc. when $\beta_2\geqq t^{1/4}$.

If $k\geqq t^{1/2}$, then β_2 must be at least $t^{1/2}\geqq t^{1/4}$.

---

* Accurately, either no solutions or k solutions.

We have thus shown that none of the exponents $t_1, \cdots, t_p$ can exceed δ^{p+4}. This proves our lemma.

9. **The factorization theorem.** We proceed now to establish the theorem of factorization for functions

$$P(x) = 1 + a_1 e^{\alpha_1 x} + \cdots + a_n e^{\alpha_n x},$$

stated in the introduction.

Our first step is to take the polynomial $Q(y_1, \cdots, y_p)$ associated with $P(x)$ in § 5, and to resolve it into irreducible factors with unity for term of lowest degree.

From the irreducible factors of Q which consist of two terms, we obtain the simple factors S of our expression for $P(x)$. Let each y_i be replaced, in these irreducible factors, by its $e^{\mu_i x}$ of § 5. Each factor goes over into a simple function $1+ae^{\alpha x}$. We separate these simple functions into sets such that the α's of the functions of any one set have rational ratios to one another, but have irrational ratios to the α's of any other set. The product of the several functions of each set is a simple function. The simple functions obtained from the several sets form precisely such a set of simple factors $S_1, \cdots, S_s$ of $P(x)$ as is mentioned in the introduction.

We now consider any irreducible factor of Q, say $U(y_1, \cdots, y_r)$, consisting of more than two terms.* Let

$$U(y_1, \cdots, y_r) = V(y_1^{m_1}, \cdots, y_r^{m_r}),$$

with $V(y_1, \cdots, y_r)$ primary. Of course, $V(y_1, \cdots, y_r)$ is irreducible. It gives a factor of $P(x)$ when each y_i is replaced by $e^{m_i \mu_i x}$.

Of all the finite number of polynomials $V(y_1^{t_1}, \cdots, y_r^{t_r})$ whose irreducible factors are primary (§ 8), consider one which has a maximum number, q, of irreducible factors. Let the irreducible factors of the function considered be $V_1, \cdots, V_q$. We say that each V_i gives an irreducible factor of $P(x)$ when each y_j in it is replaced by $e^{m_j \mu_j x_j / t_j}$.

Suppose, for instance, that V_1 does not give an irreducible factor of $P(x)$. Then there must be some $V_1(y_1^{u_1}, \ldots, y_r^{u_r})$ which is reducible. Thus, $V(y^{t_1 u_1}, \cdots, y_r^{t_r u_r})$ has more than q irreducible factors. We may replace each $t_i u_i$ by a submultiple v_i of itself, if necessary, so as to get a polynomial $V(y_1^{v_1}, \cdots, y_r^{v_r})$ with *primary* irreducible factors, greater in number than q.†

* Of course, U need not involve all of the p variables in Q. We are supposing that the $r \leqq p$ variables in U are relettered, if necessary, so as to have the designations $y_1, \cdots, y_r$.

† The irreducible factors of $V(y_1^{t_1 u_1}, \cdots, y_r^{t_r u_r})$ are all obtained from one of them by multiplying the variables by roots of unity. Hence the highest common factor of the exponents of any y_i is the same for all of the irreducible factors. This highest common factor will therefore be a factor of the exponents of y_i in $V(y_1^{t_1 u_1} \cdots, y_r^{t_r u_r})$.

We have thus a contradiction of the assumption that q is a maximum.

When we multiply together the simple factors of $P(x)$ which arise from the binomial factors of Q, and the irreducible factors of $P(x)$ which come from the remaining factors of Q, we have precisely such an expression for $P(x)$ as is described in the statement of our theorem.

It remains to prove the uniqueness of the resolution. It is easy to see that the uniqueness will follow if we can show that if P_1 is a factor of P_2P_3, each P_i being an expression like (1), and if P_1 has no factor in common with P_2, then P_1 is a factor of P_3.

Let

$$P_2P_3 = P_1P_4. \tag{11}$$

There corresponds to (11) a relation among polynomials

$$Q_2Q_3 = Q_1Q_4$$

with Q_1 relatively prime to Q_2. Then Q_3 is divisible by Q_1, so that P_3 is divisible by P_1. The question of uniqueness is thus settled.

Columbia University,
New York, N. Y.