COMMUNICATIONS ON PURE AND APPLIED MATHEMATICS, VOL. XII, 487–500 (1959)

On a Theorem Concerning Exponential Polynomials*

HAROLD N. SHAPIRO

1. Introduction

In the three papers, [1, 2, 3], the following theorem has evolved concerning exponential polynomials of the form

$$F(x) = \sum_{j=1}^{m} A_j^x P_j(x), \tag{1.1}$$

wherein the A_j, as well as the coefficients of the polynomials $P_j(x)$, are taken from a field K of characteristic 0.[1]

THEOREM 1.1. (Skolem, Mahler, Lech) *If the function $F(x)$ of (1.1) vanishes for infinitely many integers $x = x_i$, then there exists an integer Δ and a certain set of least positive residues modulo Δ, $d_1, \cdots, d_l$, such that $F(x)$ vanishes for all integers $x \equiv d_i \pmod{\Delta}$, $i = 1, \cdots, l$, and $F(x)$ vanishes only finitely often on other integers.*

In the following we let V denote the set of all $F(x) \not\equiv 0$ which have infinitely many integer zeros. We shall refer to any Δ having the property described in Theorem 1.1 as a *period* of $F(x)$. Since it is clear that if Δ is a period of $F(x)$, any multiple of Δ is also a period, we single out the smallest positive period and call it the *basic period* of $F(x)$. In Section 3 it will follow as a simple corollary of other results that every period of $F(x)$ is a multiple of its basic period. We propose here to study simple arithmetic properties of the basic period and its relationship to the A_j. For example, if $F(x) \in V$ it is a simple consequence of Theorem 1.1 (see Section 2) that there exist ratios A_j/A_k which are roots of unity. As a consequence of our results we obtain, for example, that the basic period of $F(x)$ must be a divisor of the least common multiple of the orders of these roots of unity. Thus we see that the size of the basic period is limited by the A_j, uniformly with respect to the polynomials $P_j(x)$.

In Section 4 various additive decompositions of functions $F(x)$ (as

*This paper represents results obtained under the sponsorship of the Office of Naval Research contract No. Nonr-285(32).

[1] $A_i \neq A_j$ if $i \neq j$, $A_j \neq 0$, $P_j(x) \not\equiv 0$ for $m \geq 1$.

described in Theorem 1.1) are considered in which the summands are again of the form (1.1) and the integer zeros of the summands determine the integer zeros of $F(x)$. Such a decomposition is obtained, having the further property that the basic period of each summand is the least common multiple of the roots of unity which "appear in it" and divides the basic period of $F(x)$.

In Section 5 the decomposition theorem is applied to obtain a "divisibility" theorem in the ring of exponential polynomials of the form (1.1). This theorem asserts, roughly, that an $F(x)$ which has infinitely many integer zeros possesses a "factorization" which makes this fact obvious.

Finally, in Section 6, several of the results of the preceding sections are transliterated into results concerning coefficients in the Taylor expansion of rational functions.

2. A Simple Lemma

A familiar result arising in the theory of ordinary linear differential equations with constant coefficients asserts that if $A_1, \cdots, A_m$ are distinct complex numbers,[2] then the functions $A_1^x, \cdots, A_m^x$ are linearly independent over the ring of polynomials with complex coefficients. The following generalization of this result seems to be less familiar.

LEMMA 2.1. *Let $A_1, \cdots, A_m$ be distinct non-zero elements of a given field K of characteristic 0, and assume that $F(x)$ of the form (1.1) vanishes for all positive integers (or even for all sufficiently large integers), where the $P_j(x)$ are polynomials with coefficients in K. Then $P_j(x) \equiv 0$, $j = 1, \cdots, m$.*

Proof: Consider the set $\mathfrak{F}$ of all $F(x)$ of the form (1.1). Define the *level* of $F(x)$ to be

$$m + \sum_{j=1}^{m} (\text{degree } P_j(x)).$$

The lemma asserts that no function of $\mathfrak{F}$ can vanish for all sufficiently large integers x. We prove this by induction on the level of $F(x)$.

An $F(x) \in \mathfrak{F}$ for which $m = 1$ clearly satisfies the lemma, since then $F(x) = cA^x$, and $F(x) = 0$ for infinitely many x implies that $c = 0$. In particular, then, the lemma certainly holds for all functions of $\mathfrak{F}$ of level one.

Proceeding by induction, we assume the theorem true for all functions of $\mathfrak{F}$ of level less than n. Suppose then that $F(x) \in \mathfrak{F}$ is a function of level n which vanishes for all sufficiently large integers x. Hence,

$$F(x) = \sum_{j=1}^{m} A_j^x P_j(x),$$

and

[2] Distinct (mod $2\pi i$) would suffice.

$$n = m + \sum_{j=1}^{m} (\text{degree } P_j(x)).$$

Case 1; $m = 1$. It has already been shown that the lemma holds in this case.

Case 2; $m > 1$. Dividing by A_m^x and taking the first difference, we obtain that

$$0 = \Delta\left\{\frac{F(x)}{A_m^x}\right\} = \sum_{i=1}^{m-1}\left(\frac{A_i}{A_m}\right)^x\left\{\left(\frac{A_i}{A_m} - 1\right)P_i(x+1) + \Delta P_i(x)\right\} + \Delta P_m(x) \tag{2.1}$$

for all sufficiently large integers x. Noting that

$$\frac{A_i}{A_m} \neq \frac{A_j}{A_m}, \qquad i \neq j,\ 1 \leqq i, j \leqq m-1, \tag{2.2}$$

$$\frac{A_i}{A_m} \neq 1, \qquad 1 \leqq i \leqq m-1, \tag{2.3}$$

$$\text{degree}\left[\left(\frac{A_i}{A_m} - 1\right)P_i(x+1) + \Delta P_i(x)\right] = \text{degree } P_i(x), \tag{2.4}$$

(so that certainly $[(A_i/A_m)-1)P_i(x+1)+\Delta P_i(x)] \not\equiv 0$)

$$\text{either } \Delta P_m(x) \equiv 0 \text{ or degree } \Delta P_m(x) < \text{degree } P_m(x), \tag{2.5}$$

we see that $\Delta\{F(x)/A_m^x\}$ is in $\mathscr{F}$, and of level less than n. But this contradicts the inductive hypothesis, which completes the induction and the proof of the lemma.

COROLLARY 2.1. *If $F(x) \in V$, then at least one of the ratios A_i/A_j, $i \neq j$, is a root of unity.*

Proof: Since $F(x)$ vanishes for infinitely many integers x, Theorem 1.1 provides that there is an arithmetic progression such that $F(t\Delta+d) = 0$ for all integers $t \geqq 0$. Hence

$$\sum_{i=1}^{m} (A_i^{\Delta})^t[P_i(t\Delta+d)A_i^d] = 0,$$

for all integers $t \geqq 0$. Thus, if the corollary were false for $i \neq j$, we would have $A_i^{\Delta} \neq A_j^{\Delta}$, so that Lemma 2.1 would imply $P_i(t\Delta+d) \equiv 0$ for all i, and hence $P_i(x) \equiv 0$ for all i.

The above lemma also provides an interesting equivalent formulation of Theorem 1.1:

COROLLARY 2.2. *Theorem* 1.1 *is equivalent to the assertion that for A_i, $i = 1, \cdots, m$, taken from a field K of characteristic* 0, *and such that none of the ratios A_i/A_j, $i \neq j$, are roots of unity, we have that the functions A_i^x, are*

linearly independent over the polynomial ring $K[x]$, even when the domain of x is restricted to any infinite subsequence of the positive integers.

Proof: That Theorem 1.1 implies the assertion given above is immediate from Corollary 2.1. Conversely, assuming the above assertion, consider an $F(x)$ of the form (1.1) which has infinitely many positive integral zeros. We may rewrite $F(x)$ in the form

$$F(x) = \sum_k B_k^x \sum_l \eta_{kl}^x P_{kl}(x),$$

where the η_{kl} are roots of unity, but none of the ratios B^u/B^v are roots of unity. Since the η_{kl} are roots of unity, it follows from our assumed result, that on the sequence of integral zeros of $F(x)$ we have (apart from a finite number of exceptions)

$$\sum_l \eta_{kl}^x P_{kl}(x) = 0 \qquad \text{for all } k. \tag{2.6}$$

Conversely, any positive integer x for which (2.6) holds is a zero of $F(x)$. We next rewrite the equation (2.6) as

$$\sum_i x^i \sum_l a_{ikl} \eta_{kl}^x \equiv 0 \qquad \text{for all } k. \tag{2.7}$$

Apart from a possible finite number of exceptions (for x) this in turn is equivalent to

$$\sum_l a_{ikl} \eta_{kl}^x \equiv 0 \qquad \text{for all } i, k. \tag{2.8}$$

Since the validity of (2.8) depends only on the residue class of x modulo the least common multiple of the orders of the η_{kl}, Theorem 1.1 follows.

The implications of the above argument with regard to the structure of $F(x) \in V$ will be considered in detail in the following sections.

3. Rank and its Relationship to the Basic Period

For any finite set S of roots of unity we introduce the following notion of *rank*:

DEFINITION. The rank $r(S)$ of a finite set of roots of unity is the least common multiple of the orders of the roots of unity in $\rho^{-1}S$, where $\rho \in S$.

Since $r = r(S)$ is clearly the smallest positive integer such that $\rho^r = \eta^r$ for all $\eta \in S$, it is simply the smallest positive integer such that the r-th power of all numbers in S are equal. From this we see that from the point of view of the above definition it is independent of the choice of ρ in S. We note in particular that if $1 \in S$, then $r(S)$ is simply the least common multiple of the orders of the roots of unity in S.

DEFINITION. If $S_1, S_2, \cdots, S_l$ are given sets of roots of unity, then

$$r(S_1, \cdots, S_l) = \underset{1 \leqq k \leqq l}{\text{l.c.m.}}\, r(S_k)$$

will be called the *rank* of this collection of sets.

Given an $F(x)$ of the form (1.1) we divide the A_j into sets, renotate them and rewrite them so that they may be arrayed as follows:

$$\begin{aligned} &A_1\rho_{10}, A_1\rho_{11}, \cdots, A_1\rho_{1t_1}, \\ &A_2\rho_{20}, A_2\rho_{21}, \cdots, A_2\rho_{2t_2}, \\ &\cdots\cdots\cdots\cdots\cdots, \\ &A_k\rho_{k0}, A_k\rho_{k1}, \cdots, A_k\rho_{kt_k}, \end{aligned}$$

where $\rho_{i0} = 1$ for all i, and $\rho_{ij} \neq 1$ for $j > 0$. Also, the new A_i/A_j, $i \neq j$, are not roots of unity, but the ρ_{ij} *are* roots of unity.

Letting $S_j = (\rho_{i0}, \cdots, \rho_{it_i})$, we call S_i a *primary set* of $F(x)$ and denote by $r(F) = r(S_1, \cdots, S_k)$ the *rank* of $F(x)$. Note that $r(F)$ is simply the least common multiple of the orders of those ratios of the original A_i which are roots of unity.

We may now rewrite $F(x)$ in the form

$$F(x) = \sum_{i=1}^{k} A_i^x F_i(x),$$

where

$$F_i(x) = \sum_{\rho \in S_i} \rho^x P_\rho(x)$$

is also of the form (1.1). An exponential polynomial of this last form, in which all of the exponentiated quantities are roots of unity, we shall call *primary*. The $F_i(x)$ above will be referred to as the *primary components* of $F(x)$.

If, for $F(x) \in V$, Δ is a period, we shall denote by $\mathscr{P}(F, \Delta)$ the set of least positive residues modulo Δ which describe the arithmetic progressions containing all but a finite number of the integer zeros of $F(x)$. If Δ is the *basic* period of $F(x)$ we shall write $\mathscr{P}(F, \Delta) = \mathscr{P}(F)$.

LEMMA 3.1. *If $F \in V$, then $d \in \mathscr{P}(F, \Delta)$ if and only if*

$$\sum_{\substack{\rho \in S_i \\ \rho^{\beta\Delta} = \eta}} \rho^d P_\rho(x) \equiv 0, \qquad i = 1, \cdots, k, \tag{3.1}$$

for every integer $\beta \neq 0$, and every root of unity η.

Proof: Since

$$\sum_{\substack{\rho \in S_i \\ \rho^{\beta\Delta} = \eta^{-1}}} \rho^d P_\rho(x) = \sum_{\substack{\rho \in S_i \\ \rho^{(-\beta)\Delta} = \eta}} \rho^d P_\rho(x),$$

it suffices to consider the case where β is any integer $\geqq 1$. Since by assump-

tion $F(x)$ vanishes for all integers $x \equiv \mathrm{d} \pmod{\Delta}$ this is also true for all integers $x \equiv d \pmod{\beta\Delta}$. Writing $x = t\beta\Delta + d$ we obtain

$$\sum_{i=1}^{k} (A_i^{\beta\Delta})^t \left[A_i^d \sum_{\rho \in S_i} \rho^{t\beta\Delta} \rho^d P_\rho(t\beta\Delta + d)\right] = 0 \tag{3.2}$$

so that

$$\sum_{i=1}^{k} \sum_{\eta} (A_i^{\beta\Delta}\eta)^t A_i^d \Big[\sum_{\substack{\rho \in S_i \\ \rho^{\beta\Delta} = \eta}} \rho^d P_\rho(t\beta\Delta + d)\Big] = 0$$

for all integral $t \geqq 0$. Since the $A_i^{\beta\Delta}\eta$ are all distinct, Lemma 2.1 yields

$$\sum_{\substack{\rho \in S_i \\ \rho^{\beta\Delta} = \eta}} \rho^d P_\rho(t\beta\Delta + d) \equiv 0,$$

which in turn implies (3.1) for $\beta > 0$.

The above argument establishes the necessity of (3.1). That (3.1) is sufficient to imply that $d \in \mathscr{P}(F, \Delta)$ follows easily from (3.1) with $\beta = 1$.

LEMMA 3.2. *If $F \in V$, then $d \in \mathscr{P}(F, \Delta)$ if and only if for all integral β and all integers t (positive or negative)*

$$\sum_{\rho \in S_i} \rho^{t\beta\Delta + d} P_\rho(x) \equiv 0, \qquad i = 1, \cdots, k. \tag{3.3}$$

Proof: The necessity of (3.3) follows immediately by multiplying (3.1) by η^t and summing over η. The sufficiency of (3.3) follows by taking $\beta = 1$ and $x = t\Delta + d$.

LEMMA 3.3. *If $F(x)$ is of the form (1.1) and vanishes for all but a finite number of integers in the progression $x \equiv d \pmod{\gamma}$, then it vanishes for all integers in this progression.*

Proof: From the hypothesis it follows that (3.3) holds (with Δ replaced by γ). Let $\tilde{d}$ denote the least positive residue of d modulo γ, with $d = t_1\gamma + \tilde{d}$. Replacing t by $t - t_1$ in (3.3) ($\Delta = \gamma$, $\beta = 1$) we obtain

$$\sum_{\rho \in S_i} \rho^{t\gamma} \rho^{\tilde{d}} P_\rho(x) \equiv 0, \qquad i = 1, \cdots, k,$$

and the desired result follows from Lemma 3.2.

THEOREM 3.1. *Let $F \in V$, then the basic period of F divides $r(F)$.*

Proof: Let Δ be the basic period of F, and write $r = r(F)$. We may take $\tau = (r, \Delta) = \alpha r + \beta\Delta$, where α and β are integers. Then for $d \in \mathscr{P}(F)$

$$F(\tau t + d) = \sum_{i=1}^{k} A_i^{\tau t + d} \sum_{\rho \in S_i} \rho^{\tau t} \rho^d P_\rho(\tau t + d).$$

Since $\rho^{\tau t} = \rho^{\alpha r t + \beta\Delta t} = \rho^{\beta\Delta t}$, this becomes

$$F(\tau t+d) = \sum_{i=1}^{k} A_i^{\tau t+d} \sum_{\rho \in S_i} \rho^{t\beta\Delta+d} P(\tau t+d) \equiv 0$$

by virtue of (3.3).

Since Lemma 3.3 then insures that for $\bar{d}$, the least positive residue of d modulo τ, $F(x)$ vanishes for all $x \equiv \bar{d} \pmod{\tau}$ if $d \in \mathscr{P}(F)$, it follows that τ is a period for F. Since $\tau \leqq \Delta$, the basic period, we obtain that $\tau = \Delta$ and hence that Δ divides r.

For $F(x)$ of the form (1.1), let $r^*(F)$ denote the least common multiple of $r(F)$ and the orders of any of the A_j which are roots of unity. Clearly, $r^*(F) = \text{l.c.m. } r(F),\ r(F+1)$.

COROLLARY 3.1. *Let $F(x)$ be of the form* (1.1). *Then as x takes on positive integral values, at most $r^*(F)$ values of $F(x)$ can repeat themselves infinitely often.*

Proof: For $F(x)$ of the form (1.1), in equation

$$F(x)-c = 0, \tag{3.4}$$

$F(x)-c$ is again of the form (1.1). Thus, if there are infinitely many integer solutions to (3.4) and $c \neq 0$, these solutions fill out a certain number of progressions modulo $r^*(F)$. If $c = 0$, they fill out a certain number of arithmetic progressions modulo $r(F)$, and since $r(F)$ divides $r^*(F)$ certainly also a certain number of arithmetic progressions modulo $r^*(F)$. From this the corollary is immediate.

COROLLARY 3.2. *If for an $F(x)$ of the form* (1.1) *no A_i is a root of unity, then the equation $F(x) = c$ can have an infinite number of integer solutions only if $c = 0$.*

Proof: Considering equation (3.4), if no A_i is a root of unity, one of the S_i for $F(x)-c$ consists only of 1. Then taking $t = 0$ in the corresponding equation, (3.3) yields $c = 0$.

Actually, the above corollary is just a manifestation of the following extension of Corollary 2.1.

COROLLARY 3.3. *If $F(x) \in V$ and Δ is its basic period, then for each A_i (in* (1.1)) *there must exist at least one $j \neq i$ such that A_i/A_j is a Δ-th root of unity.*

Proof: If under the hypothesis of the corollary there were an A_i such that A_i/A_j is not a Δ-*th* root of unity for any $j \neq i$, there would be an S_i in which 1 is the only Δ-th root of unity. Then taking $\beta = \eta = 1$ in the corresponding equation, (3.1) yields a contradiction.

COROLLARY 3.4. *If $F \in V$, every period of F is divisible by the basic period.*

Proof: Let Δ be the basic period of $F(x)$ and M any other period. We have $\Delta \leqq M$, and it clearly suffices to consider the case $\Delta < M$. Let

$\mathscr{P}(F, \Delta)$ and $\mathscr{P}(F, M)$ consist, respectively, of $d_1, \cdots, d_u$ and $e_1, \cdots, e_v$. For a given d_i we have for all integers $t \geqq 0$, that $F(t\Delta+d_i) = 0$, so that for all sufficiently large t we must have

$$t\Delta+d_i \equiv e_j \pmod{M} \tag{3.5}$$

for some $e_j \in \mathscr{P}(F, M)$, where e_j depends on t. Letting $\gamma = (\Delta, M)$, (3.5) reduces to

$$t\frac{\Delta}{\gamma} \equiv \frac{e_j-d_i}{\gamma} \left(\mathrm{mod}\ \frac{M}{\gamma}\right), \tag{3.6}$$

wherein we must have $d_i \equiv e_j \pmod{\gamma}$. Since t runs over a complete residue system mod (M/γ), and $(M/\gamma, \Delta/\gamma) = 1$, it follows that for every σ, $0 \leqq \sigma \leqq M/\gamma-1$, there exists an $e_j \in \mathscr{P}(F, M)$ such that

$$e_j \equiv d_i+\sigma\gamma \pmod{M}. \tag{3.7}$$

Similarly, for every j and λ, $0 \leqq \lambda \leqq \Delta/\gamma-1$, there is a $d_i \in \mathscr{P}(F, \Delta)$ such that

$$d_i \equiv e_j+\lambda\gamma \pmod{\Delta}. \tag{3.8}$$

Taking $\sigma = 0$ in (3.7) yields the existence of an e_j such that $e_j \equiv d_i \pmod{M}$. Since $0 \leqq e_j < M$ and $0 \leqq d_i < \Delta < M$, it follows that $e_j = d_i$. Thus $\mathscr{P}(F, \Delta) \subset \mathscr{P}(F, M)$. Now it follows from (3.8) that for any $d \in \mathscr{P}(F, \Delta)$, the integers $d+\lambda\gamma$, $0 \leqq \lambda \leqq \Delta/\gamma-1$, are each congruent modulo Δ to an integer in $\mathscr{P}(F, \Delta)$. Therefore from Lemma 3.3, $F(x)$ vanishes for all of the integers

$$x \equiv d+\lambda\gamma \pmod{\Delta}, \qquad 0 \leqq \lambda \leqq \frac{\Delta}{\gamma}. \tag{3.9}$$

But the progressions in (3.9) taken together constitute the one progression

$$x \equiv d \pmod{\gamma}. \tag{3.10}$$

This implies that γ is a period of $F(x)$, and since $\gamma \leqq \Delta$, that it is the basic period; it follows that $\Delta = \gamma = (\Delta, M)$. Hence Δ divides M.

COROLLARY 3.5. *If for $F(x) \in V$ all the ratios A_i/A_j, $i \neq j$, which are roots of unity, are primitive n-th roots of unity, n is the basic period of F.*

Proof: Clearly $r(F) = n$. From Corollary 3.3 there exists a ratio $A_i/A_j \neq 1$ which is a Δ-th root of unity (Δ the basic period of F), we have that $r(F) = n$ divides Δ. Since Theorem 3.1 implies that Δ divides $r(F)$, it follows that $\Delta = n$.

COROLLARY 3.6. *If $F(x) \in V$, and has primary components $F_i(x)$, $i = 1, \cdots, k$, then $F_i(x) \in V$ and, letting $\tilde{\mathscr{P}}(F)$ denote the set of integer zeros of $F(x)$ apart from a finite number of exceptions, we have*

$$\tilde{\mathscr{P}}(F) = \tilde{\mathscr{P}}(F_1) \cap \tilde{\mathscr{P}}(F_2) \cap \cdots \cap \tilde{\mathscr{P}}(F_k). \tag{3.11}$$

Furthermore if Δ and Δ_i are the basic periods of F and the F_i, respectively, then

$$\Delta \text{ divides } \underset{1 \leq i \leq k}{\text{l.c.m.}}\ \Delta_i . \tag{3.12}$$

Proof: (3.11) is an immediate consequence of (3.3), and (3.12) follows easily from (3.11).

4. Decompositions for Functions of V

The decomposition of an $F(x) \in V$ into primary components reduces the problem of determining its zeros to that of determining the zeros of these components, according to Corollary 3.6. However (3.12) does not provide a complete relation between the basic period of F and the basic periods of its components. We shall see, in fact, that as a result of further decomposition of the primary components we know that Δ equals the l.c.m. Δ_i in (3.12).

THEOREM 4.1. *If $F \bullet V$, and has primary components with basic periods as described in Corollary* 3.6, *then each F_i may be decomposed so that*

$$F_i = \sum_j F_{ij}, \tag{4.1}$$

where each $F_{ij} \in V$ and is primary. Also,

$$\tilde{\mathscr{P}}(F_i) = \bigcap_j \tilde{\mathscr{P}}(F_{ij}), \tag{4.2}$$

and, if Δ_{ij} denotes the basic period of F_{ij},

$$\Delta = \underset{i}{\text{l.c.m.}}\ \Delta_i = \underset{i,j}{\text{l.c.m.}}\ \Delta_{ij} = \underset{i,j}{\text{l.c.m.}}\ r(F_{ij}). \tag{4.3}$$

Proof: Let η_{ij} be the different roots of unity which are representable in the form ρ^Δ with $\rho \in S_i$. Set

$$F_{ij}(x) = \sum_{\substack{\rho \in S_i \\ \rho^\Delta = \eta_{ij}}} \rho^x P_\rho(x); \tag{4.4}$$

(4.1) is then immediate and from (3.1) we see that $F_{ij} \in V$, and (4.2) holds. Since the Δ-th power of all the roots of unity ρ which appear in F_{ij} are equal, it follows that

$$r(F_{ij}) \text{ divides } \Delta. \tag{4.5}$$

From Theorem 3.1 we know that Δ_{ij} divides $r(F_{ij})$ so that

$$\Delta_i \text{ divides } \underset{j}{\text{l.c.m.}}\ \Delta_{ij} \text{ divides } \underset{j}{\text{l.c.m.}}\ r(F_{ij}) \text{ divides } \Delta; \tag{4.6}$$

(4.6) together with (3.12) implies (4.3).

We note that if $\Delta < r(F)$, there is a ρ in some S_i such that $\rho^\Delta \neq 1$ and

consequently the corresponding $F_i(x)$ will actually decompose into two or more F_{ij}. Note also that the failure to obtain the relation $\Delta_i = \text{l.c.m.}_j \Delta_{ij}$ stems from the fact that the decomposition of the primary components was "controlled" by the basic period Δ of $F(x)$. One can, however, apply the above process of decomposition to each primary component viewed independently of its relationship to F. This produces, in general, a different decomposition of F in which the properties (4.1), (4.2), (4.3) are retained and for which we also have $\Delta_i = \text{l.c.m. } \Delta_{ij}$. If in this decomposition any of the summands have a basic period smaller than their rank, we can continue the decomposition still further. Thus we obtain

THEOREM 4.2. *Under the hypothesis of Theorem* 4.1, *each primary component* F_i *can be decomposed so that* (4.1), (4.2), (4.3) *hold; and in addition*

$$\Delta_i = \text{l.c.m. } \Delta_{ij}. \tag{4.7}$$

$$\Delta_{ij} = r(F_{ij}). \tag{4.8}$$

Since an exponential polynomial of V can have its basic period equal to its rank and still be decomposable, the F_{ij} of Theorem 4.2 may possibly be decomposed further. That we can achieve a decomposition of $F \in V$ for which all the assertions of Theorem 4.2 hold and for which in addition the F_{ij} cannot be decomposed further, is an immediate consequence of the following

LEMMA. *Let* $F \in V$ *and* $F = G+H$,[3] *where* $G, H \in V$ *and* F, G, H *are primary. In addition let the basic period of* F *be* $r(F)$ *and* $\mathscr{P}(F) = \mathscr{P}(G) \cap \mathscr{P}(H)$. *Then the least common multiple of the basic periods of* G *and* H *equals* $r(F)$.

Proof: Let Δ, $\Delta(G)$ and $\Delta(H)$ be the basic periods of F, G and H, respectively. Since multiplication by a constant does not alter either the basic period or the rank of an exponential polynomial, we may assume that 1 appears as one of the roots of unity in F. Hence we may assume that $r(F)$ equals the least common multiple of the orders of the roots of unity which appear in F. Thus from the hypothesis we have

$$\Delta = r(F) \leqq \text{l.c.m. } \{\Delta(G), \Delta(H)\} \leqq \text{l.c.m. } r(G), \qquad r(H) \leqq r(F),$$

and the desired result follows.

5. A Division Theorem

The following theorem is related to a "divisibility" theorem of Ritt [4] for exponential polynomials with constant coefficients over the field of com-

[3] This decomposition is restricted here to those obtained by grouping the terms appearing in F. It is not permitted to add and subtract new exponentials.

plex numbers. In fact, in the case of the complex number field the theorem given below may possibly be deduced from Ritt's theorem. In the case treated here wherein the exponential polynomials are taken over an arbitrary field K of characteristic 0, an algebraic proof is given which depends upon the decomposition theorems of the previous section.

THEOREM 5.1. *Let Δ be the basic period of $F \in V$. Then*

$$F(x) = \Big\{ \prod_{d \in \mathscr{P}(F)} (\eta^x - \eta^d) \Big\} G(x), \tag{5.1}$$

where η is a primitive Δ-th root of unity and $G(x)$ is an exponential polynomial of the form (1.1).

Proof: From Theorem 4.2 it follows that we may write $F(x)$ in the form

$$F(x) = \sum_k B_k^x H_k(x), \tag{5.2}$$

where the $H_k(x)$ are primary and in V, and

$$\tilde{\mathscr{P}}(F) = \bigcap_k \tilde{\mathscr{P}}(H_k). \tag{5.3}$$

Also, if Δ_k denotes the basic period of $H_k(x)$, we have

$$\Delta = \text{l.c.m.}_k \, \Delta_k , \tag{5.4}$$

$$\Delta = r(H_k), \tag{5.5}$$

and $r(H_k)$ equals the least common multiple of the orders of the roots of unity which appear in H_k. Thus we have

$$H_k(x) = \sum_\rho \rho^x Q_\rho(x), \tag{5.6}$$

where the ρ are Δ-th roots of unity and the $Q_\rho(x)$ are polynomials. Then (5.6) may be rewritten as

$$H_k(x) = \sum_i x^i \Big(\sum_j a_{ij}^{(k)} \rho_j^x \Big), \tag{5.7}$$

where the ρ_j are Δ-th roots of unity.

From (5.3) we obtain that for $d \in \mathscr{P}(F)$, $H_k(x)$ must vanish for all positive integers $x \equiv d \pmod{\Delta}$. It then follows that we must have

$$\sum_j a_{ij}^{(k)} \rho_j^d = 0 \qquad \text{for all } i, k;\ d \in \mathscr{P}(F). \tag{5.8}$$

Letting η be any primitive Δ-th root of unity, we may write $\rho_j = \eta^{n_j}$ so that (5.8) becomes

$$\sum_j a_{ij}^{(k)} (\eta^d)^{n_j} = 0. \tag{5.9}$$

Introducing the polynomials

$$h_i^{(k)}(y) = \sum_j a_{ij}^{(k)} y^{n_j},$$

we see that (5.9) simply asserts that $h_i^{(k)}(y)$ must have the quantities η^d, $d \in \mathscr{P}(F)$, as roots. Thus we can write

$$h_i^{(k)}(y) = \prod_{d \in \mathscr{P}(F)} (y - \eta^d) g_i^{(k)}(y), \tag{5.10}$$

where $g_i^{(k)}(y)$ is a polynomial in y. Then, since

$$\begin{aligned} H_k(x) &= \sum_i x^i h_i^{(k)}(\eta^x) \\ &= \prod_{d \in \mathscr{P}(F)} (\eta^x - \eta^d) \sum_i x^i g_i^{(k)}(\eta^x) \end{aligned}$$

for all k, we obtain (5.1).

If we use the decomposition of $F \in V$ into primary components, and apply an argument analogous to the above to each of the primary components, where instead of the η we use a primitive $r(F)$-th root of unity ζ, we arrive at

THEOREM 5.2. *Given $F \in V$, then for ζ a primitive $r(F)$-th root of unity we have*

$$F(x) = \prod_{d \in \mathscr{P}(F, r(F))} (\zeta^x - \zeta^d)^{m_d} H(x), \tag{5.11}$$

where $H(x)$ is an exponential polynomial of the form (1.1) *which has at most a finite number of integer zeros. Also $m_d \geqq 1$, and*

$$\sum_{d \in \mathscr{P}(F, r(F))} m_d < r(F). \tag{5.12}$$

The assertion (5.1) may now be derived anew as a simple consequence of (5.11).

6. Theorems on the Taylor Coefficients of Rational Functions

Theorems of the kind proved in the preceding sections all have counterparts as theorems on the Taylor coefficients of rational functions. This stems from the fact that if a rational function $R(x)$, which vanishes at infinity, has the Taylor expansion

$$R(x) = \sum_{n=0}^{\infty} a_n x^n, \tag{6.1}$$

then the a_n are given by a formula of the form

$$a_n = \sum_i A_i^n P_i(n), \text{ [4]} \tag{6.2}$$

[4] If the rational function $R(x)$ does not vanish at infinity then (6.2) holds.

where the $P_i(n)$ are polynomials in n. Conversely, if the a_n in (6.1) are given by a formula such as (6.2), then $R(x)$ will be a rational function. The A_i in (6.2) will in fact be the reciprocals of the poles of $R(x)$. Thus we see that consideration of the sequence of Taylor coefficients of a rational function is equivalent to the consideration of the values at the positive integers of an exponential polynomial of the form (1.1). Corresponding to the integer zeros of such exponential polynomials we have the vanishing Taylor coefficients. We shall apply the terms period, basic period, etc . . . to rational functions to mean the period, basic period, etc. . . . of the corresponding exponential polynomial which represents the Taylor coefficients. In particular, we shall write $R(x) \in \tilde{V}$ if the rational function $R(x)$ has infinitely many Taylor coefficients which vanish.

Corollary 3.1 then yields

THEOREM 6.1. *For a rational function $R(x)$, let r^* denote the least common multiple of the orders of those roots of unity which are either poles of $R(x)$ or the ratio of two such poles. Then, at most, r^* numbers can repeat infinitely often as Taylor coefficients of $R(x)$.*

The simplest rational functions which, if in $\tilde{V}$, obviously satisfy Theorem 1.1 are those of the form

$$R(x) = \frac{P(x)}{1-x^r}, \tag{6.3}$$

where $P(x)$ is a polynomial. To see this note that for $P(x) = \sum_i b_i x^i$ the Taylor coefficients of the rational function in (6.3) are

$$a_n = \sum_{i \equiv n \pmod r} b_i$$

which clearly depend only on the residue class of n modulo r. Thus we see also that if this rational function is in $\tilde{V}$, then r will be a period. Whether or not r is the basic period in this case will of course depend on further information concerning the polynomials $P(x)$. If $R(x)$ in (6.3) has 1 as a pole, and r is the smallest integer such that $R(x)$ can be represented in the form (6.3), then $r = r(R)$. Thus if r should happen to be the basic period it follows that (6.3) provides the "smallest" representation of that form.

Since it is easily seen that a Taylor coefficient of

$$\frac{P(x)}{(1-x^r)^t} \tag{6.4}$$

can vanish if and only if a corresponding Taylor coefficient of (6.3) vanishes it follows that (6.4) is in $\tilde{V}$ if and only if (6.3) is, and that they then have the same basic period.

THEOREM 6.2. *If* $R(x) \in \tilde{V}$ *and has the basic period* Δ, *then* $R(x)$ *may be written in the form*

$$R(x) = \sum_i \frac{P_i(x)}{(1-(\alpha_i x)^{\Delta_i})^{t_i}}, \tag{6.5}$$

where

$$\frac{P_i(x)}{(1-(\alpha_i x)^{\Delta_i})^{t_i}} \in \tilde{V} \text{ and has basic period } \Delta_i, \tag{6.6}$$

$$\Delta = \text{l.c.m.}_i \, \Delta_i, \tag{6.7}$$

and apart from a finite number of exceptions a Taylor coefficient of $R(x)$ *vanishes if and only if the corresponding Taylor coefficient of each summand vanishes.*

Proof: From Theorem 4.2 we see that in order to obtain the above conclusions we need only show that a rational function $T(x)$ of $\tilde{V}$ which has 1 as a pole, $r = r(t)$ as its basic period and all of its poles roots of unity must be of the form (6.4). This in turn is quite evident.

Bibliography

[1] Skolem, T., *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, Comptes Rendus du Huitième Congrès des Mathématicians Scandinaves, Stockholm, 1934, pp. 163–188.

[2] Mahler, K., *Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen*, Akad. Wetensch. Amsterdam Proc., Vol. 38, 1935, pp. 50–60.

[3] Lech, C., *A note on recurring series*, Ark. Mat., Vol. 2, 1952–1954, pp. 417–421.

[4] Ritt, J. F., *On the zeros of exponential polynomials*, Trans. Amer. Math. Soc., Vol. 31, 1929, pp. 549–640.

Received December, 1958.