5. Further Remarks

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **21 (1975)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **12.07.2024**

Proof. The commensurability of the frequencies implies there is a number α such that all the frequencies $\alpha_1, \ldots, \alpha_n$ are positive integer multiples of α. Then $f(z)$ is a polynomial in $e^{\alpha z}$ and can be factorised as a finite product of factors of the shape $1 - ae^{\alpha z}$. Since $f(z), g(z)$ have infinitely many common zeros, at least one of these factors, say $1 - ae^{\alpha z}$, has infinitely many zeros in common with $g(z)$. So $g(z)$ has infinitely many zeros of the shape $z = (2k\pi i - \log a)/\alpha$, $k \in \mathbf{Z}$. Hence the exponential polynomial $g^*(z) = g\left((2\pi iz - \log a)/\alpha\right)$ vanishes on an infinite subset M of $\mathbf{Z}$, and by the lemma it follows that $g^*(z)$ vanishes on an arithmetic progression $\{d_0 + nd : n \in \mathbf{Z}\}$, $d \neq 0$. Then, as remarked above, the exponential polynomial $h^*(z) = 1 - \exp(2\pi i/d)\, d_0 \exp(2\pi i/d)\, z$ divides $g^*(z)$ in the ring E. It follows that the exponential polynomial $h(z) = 1 - \exp\left((2\pi i/d)\, d_0 + (1/d) \log a\right) . e^{(\alpha/d)z}$ divides $g(z)$ in E. Since $h(z)$ divides $1 - ae^{\alpha z}$, and *a fortiori* $f(z)$, we have the assertion.

We shall show in section 5 that, conversely, the theorem implies the Skolem-Mahler-Lech theorem for sequences $\{c_\nu\}$ where $c_\nu = \sum b_j e^{\beta_j z}$, the coefficients b_j being constants. This observation leads us to remark that, more generally an affirmative answer to the problem implies the following:

Suppose that the exponential polynomials f, g have infinitely many zeros in common. Then the common zeros are located in a finite number of half-strips. Further for each such half-strip the common zeros are distributed "almost periodically" in the sense that there is a constant c such that the number of common zeros in the half-strip which are in absolute value less than R is $cR + O(1)$.

This remark, which follows immediately from (2) in section 2 can be considered as a generalisation of the Skolem-Mahler-Lech theorem. Since, in general, we do not know sufficient conditions for some infinite set of points to be the zeros of an exponential polynomial this generalisation tells only part of the conjectured truth.

5. Further Remarks

In this note we have considered the ring E, often called the ring of exponential sums, though it is arguably more natural to consider the ring

$$E' = \{a_1(z)\, e^{\alpha_1 z} + \ldots + a_n(z)\, e^{\alpha_n z} : a_1(z), \ldots, a_n(z) \in \mathbf{C}[z], \alpha_1, \ldots, \alpha_n \in \mathbf{C}, n \in \mathbf{N}\},$$

more properly called the ring of exponential polynomials. Indeed E' has the very natural description: $f \in E'$ if and only if f satisfies a homogeneous linear differential equation with constant coefficients. The results mentioned in section 2 generalise *mutatis mutandis* to apply to the ring E'. Similarly, the factorisation theory of section 3 generalises to apply to the ring E'; one need only observe that if $\sum a_j(z)e^{\alpha_j z}$ factorises non-trivially in E' then $\sum a_j(\beta)e^{\alpha_j z}$ must factorise in E for all $\beta \in \mathbf{C}$; or one applies Ritt's argument in the polynomial ring $\mathbf{C}[z][y_1, ..., y_p]$ rather than $\mathbf{C}[y_1, ..., y_p]$. Furthermore, it is known that if g/f is an entire function, where $g, f \in E'$ then $g/f = h/a$ where $h \in E'$ and, if $f(z) = \sum a_j(z)e^{\alpha_j z}$, then a is a polynomial such that a divides $\gcd(a_1(z), ..., a_n(z))$; indeed this result is valid in the ring of general exponential polynomials in several complex variables, see Berenstein and Dostal [1] for details and references. Finally, we note that the Skolem-Mahler-Lech theorem applies to elements of E' so that the theorem of section 4 generalises to state that if a simple exponential sum (necessarily in E) and any general exponential polynomial (in E') have infinitely many common zeros than they have a common divisor (which, by the proof, lies in E). Below we refer to elements of E' as exponential polynomials and refer to elements of the subring E as exponential sums.

PROPOSITION 1. *The assertion that, if a simple exponential sum and an exponential polynomial have infinitely many zeros in common then they have a non-trivial common divisor in the ring E', is equivalent to the Skolem-Mahler-Lech theorem.*

Proof. In one direction the implication is the content of the theorem of section 4 and the remarks above. Conversely, take, without loss of generality, the exponential sum to be $1 - e^z$ and consider the exponential polynomial as the product of its Ritt factors, that is, a polynomial, a finite number of simple exponential sums whose sets of frequencies are pairwise incommensurable, and a finite number of irreducible exponential polynomials. Firstly, $1 - e^z$ and an irreducible exponential polynomial can have at most finitely many common zeros because otherwise the irreducible exponential polynomial has a non-trivial divisor in E. Secondly, $1 - e^z$ and a polynomial, obviously have at most finitely many common zeros. Thirdly, a simple exponential sum is a finite product of terms of the shape $1 - ae^{\alpha z}$; if α is irrational so that 1 and α are incommensurable, then $1 - e^z$ and $1 - ae^{\alpha z}$ have at most one common zero. On the other hand, if α is rational, say $\alpha = r/d$, then the common zeros of $1 - e^z$ and $1 - ce^{\alpha z}$ are the zeros of finitely many functions of the shape $1 - \exp(2\pi i d_0/d) \exp z/d$ and so occur in arithmetic progressions. Hence the common zeros are a finite union of arithmetic progressions (which may have common difference zero). In particular, if an exponential polynomial has infinitely many integer zeros, and so, infinitely many zeros in common with $1 - e^{2\pi i z}$ then these integer zeros are a finite union of arithmetic progressions, and this is the content of the Skolem-Mahler-Lech theorem.

PROPOSITION 2. *Every pair f, g of exponential polynomials has a greatest common divisor* (gcd) *h in the ring E'* (in the usual sense that h is a common divisor of f and g in E' and every common divisor of f and g in E' divides h in E').

Proof. The Ritt factorisation theory implies one need only consider the cases where f is a polynomial, a simple exponential sum, or an irreducible exponential polynomial. If f is a polynomial the gcd is again a polynomial, and if f is irreducible it is a unit or an associate of f. Finally if f is simple then the gcd is a product of a polynomial and a finite number of functions of the shape of $h(z)$ as constructed in the proof of the theorem of section 4, that is, of functions the set of zeros of each of which is an arithmetic progression.

Shields [14] remarks that the above proposition has been obtained by W. D. Bouwsma (unpublished).

We call the abovementioned greatest common divisor the "Ritt gcd" of the two exponential polynomials f and g, and observe that one can also define a function-theoretic gcd of f and g as follows: (see, for example, Titchmarsh [18], Chapter 8).

Let $z_1, z_2, \ldots$ be the common zeros of f and g. Then the exponent of convergence ρ' of these numbers is at most the exponent of convergence of the zeros of f, hence at most the order of f. Thus $\rho' \leqslant 1$. By the Weierstrass factorisation theorem the canonical product h of $z_1, z_2, \ldots$ is an analytic function, and by Borel's theorem the order ρ of h equals ρ'. By virtue of the Hadamard factorisation theorem every entire function of order $\rho \leqslant 1$ with zeros $z_1, z_2, \ldots$ and no others is the product of $h(z)$ and a unit factor of the shape $e^{\alpha + \beta z}$. Hence $h(z)$ is uniquely determined up to a normalisation. We call the function $h(z)$ so defined the "Hadamard gcd" of the functions f and g. The Shapiro problem can now be posed as follows: *Is it the case that apart from a possible polynomial factor, the Hadamard* gcd *of two exponential polynomials coincides with their Ritt* gcd*?* It is equivalent to ask whether the Hadamard gcd of two exponential polynomials is indeed an exponential polynomial and so has exact order 0 or 1.

Our last remark depends on the observation that an affirmative answer to the problem implies: *if the exponential polynomial h is the greatest common* *divisor of exponential polynomials f and g, then the set of zeros of h is all but at most finitely many of the common zeros of f and g.* We have shown this to be the case if at least one of f and g is a simple exponential sum.

We see that a natural formulation of the Shapiro problem is: *If f and g are exponential polynomials, is it the case that there exists an exponential polynomial h, the set of zeros of which is exactly the set of common zeros of f and g?*

We recall that it is not, without qualification, the case that if every zero of $f \in E'$ is a zero of $g \in E'$ then f divides g in the ring E'; for example $(1-e^z)/z$ is not an element of E' (its set of integer zeros in not a finite union of arithmetic progressions). Equivalently, it follows that if $\Pi_{l=1}^{m} (e^{z/2^l}+1)$ divides an exponential polynomial $g(z)$ in the ring E' for all $m = 1, 2, \ldots$ then $1 - e^z$ divides $g(z)$ in E'.

The ideas we have mentioned attack an apparently analytic problem by essentially algebraic methods. Indeed, in a sense, "approximate" methods appear doomed to failure by virtue of the following proposition mentioned to the authors by H. L. Montgomery:

PROPOSITION 3. *Let* $\mu(\mathrm{r})$ *be any positive-real-valued function decreasing to* 0 *as* $\mathrm{r} \to \infty$. *Then there exist exponential polynomials* f, g *such that for every* $\mathrm{r}_0 > 0$ *there is an* $\mathrm{r} > \mathrm{r}_0$ *and a* $z \in \mathbf{C}$ *with* $\mathrm{r}_0 < |z| < \mathrm{r}$ *such that* $0 < |f(z) - g(z)| \leqslant \mu(\mathrm{r})$.

Proof. Define an increasing sequence $\{n_l\}$ of integers by $n_0 = 0$ and $n_{l+1} - n_l \geqslant -\log(\mu(2^{n_l})/2\pi)/\log 2$ and write $\alpha = \sum_{l=0}^{\infty} (-1)^l 2^{-n_l}$. Let $f(z) = 1 - e^{2\pi i z}$ and $g(z) = 1 - e^{2\pi i \alpha z}$, and write $z_l = 2^{n_l}$, $l = 0, 1, 2, \ldots$. Then $f(z_l) = 0$ and $0 < |g(z_l)| = |1 - e^{2\pi i \alpha z_l}| = 2|\sin \pi \alpha z_l| \leqslant \mu(2^{n_l})$, as required. One notices that $f(z), g(z)$ have the property that there are infinitely many pairs z_l, z'_l with $f(z_l) = 0$, $g(z'_l) = 0$ and $|z_l - z'_l| \leqslant 2\mu(|z_l|)$.

REFERENCES

[1] BERENSTEIN, C. A. and M. A. DOSTAL. A lower Estimate for Exponential Sums. *Bull. Amer. Math. Soc. 80* (1974), pp. 687-691.

[2] DICKSON, D. G. Asymptotic Distribution of Exponential Sums. *Publ. Math. Debrecen 11* (1964), pp. 295-300.

[3] JAGER, H. A Note on the Vanishing of Power Sums. *Ann. Univ. Sci. Bud sect. Math. 10* (1967), pp. 13-16.

[4] LECH, C. A Note on Recurring Series. *Ark. Mat. 2* (1953), pp. 417-421.