4. The Theorem of Skolem-Mahler-Lech

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **27.04.2024**

The factorisation theory implies that we need consider only two cases of the Shapiro problem. Namely, firstly the case where at least one of the exponential polynomials f, g is simple. We settle this case, in the affirmative in section 4. Secondly one must take the case where at least one of the exponential polynomials is irreducible. Then an affirmative answer to the problem is equivalent to the truth of the following conjecture:

Let f, g be exponential polynomials and let f be irreducible. Then if f and g have infinitely many zeros in common, f divides g in the ring E (equivalently, g/f is an entire function).

Equivalent to this conjecture is: *if f, g are distinct irreducible exponential polynomials then f and g have at most finitely many common zeros.* This last formulation can be rephrased in terms of polynomials (with constant term 1):

Let $f(y) = f(y_1, \ldots, y_p)$, $g(y)$ be distinct polynomials irreducible in $\mathbf{C}[y]$ in the strong sense that for all sets $t_1, \ldots, t_p$ of positive integers, the polynomials $f(y^t) = f(y_1^{t_1}, \ldots, y_p^{t_p})$, $g(y^t)$ are so irreducible. Denote by $V \subset \mathbf{C}^p$ the set of common zeros of $f(y)$ and $g(y)$. Let $\mu_1, \ldots, \mu_p$ be numbers linearly independent over $\mathbf{Q}$. Then the curve $\{(e^{\mu_1 z}, \ldots, e^{\mu_p z}) : z \in \mathbf{C}\}$ meets V in at most finitely many points.

4. The Theorem of Skolem-Mahler-Lech

The following result was proved by Skolem [15] for the field of rational numbers, by Mahler [5] for the field of algebraic numbers, and by Lech [4] and Mahler [6] for arbitrary fields of characteristic zero (the assertion is false in fields of characteristic p):

Let $\{c_\nu\}$ be a sequence whose elements lie in a field of characteristic zero and satisfy a linear homogeneous recurrence relation

$$c_\nu = b_1 c_{\nu-1} + b_2 c_{\nu-2} + \ldots + b_n c_{\nu-n}, \qquad \nu = n, n+1, \ldots \tag{3}$$

Denote by $\mathrm{M} \subset \mathrm{N}$ the set of indices ν such that $c_\nu = 0$. Then M is a finite union of arithmetic progressions (the progressions may have common difference 0 and so consist of a single point). Hence those c_ν equal to zero occur periodically in the sequence from a certain index on.

It is well-known that there exist elements $\beta_1, \ldots, \beta_m$, namely the distinct zeros of the polynomial

$$z^n - b_1 z^{n-1} - b_2 z^{n-2} - \ldots - b_n, \tag{4}$$

and polynomials $p_1, \ldots, p_m$ where $1 + \deg p_j$ is the multiplicity of β_j as a zero of (4), $j = 1, 2, \ldots, m$, such that for all $\nu = 0, 1, 2, \ldots$

$$c_\nu = \sum_{j=1}^{m} p_j(\nu)\beta_j{}^\nu \tag{5}$$

Conversely any sequence $\{c_\nu\}$ where c_ν is given by (5) satisfies a relation of the shape (3). Hence, after writing $\beta_j = e^{\alpha j}$ a special case (namely, where the zeros of (4) are distinct) of the Skolem-Mahler-Lech theorem is:

LEMMA. *Let $f(z) = \sum a_j e^{\alpha_j z}$ be an exponential polynomial. Denote by* $\mathrm{M} \subset \mathbf{Z}$ *the subset of the integers* $\mathbf{Z}$ *on which f vanishes. Then* M *is a finite union of arithmetic progressions* $\{d_0 + nd : n \in \mathbf{Z}\}$; (and if M is infinite at least one common difference d is non-zero).

Proof. The assertion seems broader than the Skolem-Mahler-Lech theorem in that we claim that if $f(z)$ vanishes for all $z = d_0 + nd$, $n \in \mathbf{N}$ then it vanishes for all $z = d_0 + nd$, $n \in \mathbf{Z}$. This is not difficult to show directly, see for example [16], theorem 2. However the broader assertion is already implied by the proof of the Skolem-Mahler-Lech theorem which we outline for its intrinsic interest: Let K be the field $K = \mathbf{Q}(e^{\alpha 1}, ..., e^{\alpha n}; a_1 ..., a_n)$; then one shows there is a valuation $|\ |_\mathfrak{p}$ of K such that $|p|_\mathfrak{p} = 1/p$ for some rational prime p and

$$|e^{\alpha_j d} - 1|_\mathfrak{p} < p^{-1/(p-1)}, \qquad j = 1, 2, ..., n,$$

for some natural number $d > 0$. Now consider the $\mathfrak{p}$-adic functions $f_l : z \mapsto \sum a_j \exp(\alpha_j l) \exp(d\alpha_j z)$, $l = 0, 1, ... d-1$. These functions are well-defined by $\mathfrak{p}$-adic power series converging for $z \in \mathbf{Z}_p$, the p-adic integers. If $f(z)$ vanishes at infinitely many integers then some f_l, say f_{d_0}, has infinitely many zeros in the compact set $\mathbf{Z}_p$. Hence the $\mathfrak{p}$-adic power series f_{d_0} vanishes identically, so $f(z)$ vanishes on the set $\{d_0 + nd : n \in \mathbf{Z}\}$ as asserted.

It follows from results mentioned in section 3 that if $f(z)$ vanishes for $z = d_0 + nd$, $n \in \mathbf{Z}$ then the exponential polynomial

$$1 - \exp(2\pi i/d)\, d_0 \exp(2\pi i/d)\, z$$

divides $f(z)$ in the ring E.

THEOREM. *Let $f(z) = \sum a_j e^{\alpha_j z}$ be an exponential polynomial with pairwise commensurable frequencies (a simple exponential polynomial) and let $g(z)$ be an arbitrary exponential polynomial such that $f(z)$ and $g(z)$ have infinitely many common zeros. Then there exists an exponential polynomial $h(z)$, with infinitely many zeros, such that h is a common factor of f and g in the ring of exponential polynomials, E.*

Information on the frequencies of h can be deduced from [19].

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