An analogue of Hilbert's Tenth Problem for the ring of exponential sums

Dimitra Chompitaki
d.hobitaki@gmail.com
Thesis Committee: Mihalis Kolountzakis, Thanases Pheidas (Supervisor), Xavier Vidaux
University of Crete
Department of Mathematics and Applied Mathematics

Introduction

Hilbert's Tenth Problem

Give a procedure which, in a finite number of steps, can determine whether a polynomial equation (in several variables) with integer coefficients has or does not have integer solutions.

Positive Existential Theory, a definition

Definition 1 *The (positive) existential theory of a structure is the set of (positive) existential sentences that are true in the structure.*

We say that the theory (resp. existential theory, positive-existential theory) over a structure is **decidable** if there is an algorithm that determines whether any given sentence (resp. existential sentence, positive-existential sentence) is true or false in the structure. Otherwise the theory is **undecidable**.

Analogues of Hilbert's Tenth Problem for Polynomial Rings and Quadratic Rings

Theorem 2 *(Denef 1975) The positive existential theory of the ring of Gaussian Integers $\mathbb{Z}[i]$, in the language $L = \{0, 1, t, +, \cdot\}$, is undecidable.*

Theorem 3 *(Denef 1978) Let R be an integral domain of characteristic zero; then the positive existential theory of R[t] with coefficients in $\mathbb{Z}[t]$, in the language $L = \{0, 1, t, +, \cdot\}$, is undecidable. (R[t] denotes the ring of polynomials over R, in one variable t.)*

Theorem 4 *(Pheidas-Zahidi 1999) The positive existential theory of a polynomial ring A, with A an integral domain, in the language $L_T = \{0, 1, +, \cdot, T\}$ where T is a symbol for the property "is not a constant", is undecidable.*

An analogue of Hilbert's Tenth Problem for Exponential Sums

Exponential Sums

Define the set of **exponential sums**, denoted by EXP($\mathbb{C}$), to be the the set of expressions

$$a = \alpha_0 + \alpha_1 e^{\mu_1 z} + \cdots + \alpha_N e^{\mu_N z}$$

where $\alpha_0, \alpha_1, \ldots, \alpha_N \in \mathbb{C} \setminus \{0\}$ and $\mu_i \in \mathbb{C} \setminus \{0\}$; and μ_i are pairwise distinct.

Note: EXP($\mathbb{C}$) is a ring under the usual operations.

Undecidability of the existential theory of the ring of exponential sums

We consider the following language

$$L = \{+, \cdot, 0, 1, e^z\}$$

L contains symbols for the ring operations on EXP($\mathbb{C}$) and constant-symbols for its elements 0, 1 and e^z. The only relation symbol of L is the usual one for equality ($=$). We consider EXP($\mathbb{C}$) as a model of L, with the usual interpretation of the symbols. We ask

Question 1 *Is the positive existential first order theory of EXP($\mathbb{C}$), as a structure of the language L, decidable or undecidable?*

In other words, we ask whether there is an algorithm, which, given a finite set of polynomial equations, in many variables and with coefficients in $\mathbb{Z}[e^z]$, the algorithm replies (always correctly) to the question whether the equations have or do not have a common solution over EXP($\mathbb{C}$).

In a recent unpublished paper P. D Aquino, Th. Pheidas and G. Terzo have had partial results in the direction of proving a negative answer (actually, a considerably more general statement) but they do it only pending on a number theoretic hypothesis. We provide a new proof, based partially on theirs, but using different tools ('Pell Equations' instead of Elliptic Curves). Our approach has been suggested by A. Macintyre. Our result may be considered as an analogue of Hilbert's Tenth Problem for this structure and as a step to answering the similar problem for the ring of exponential polynomials, which is still open. We prove:

Theorem 5 *The ring of gaussian integers $\mathbb{Z}[i]$ is positive existentially definable over EXP($\mathbb{C}$), as an L-structure. Hence the positive existential theory of this structure is undecidable.*

In order to prove Theorem 5 we adapt techniques of [2] and we show the following Theorem

We consider the equation

$$(e^{2z} - 1)y^2 = x^2 - 1 \tag{1}$$

where $x, y \in$ EXP($\mathbb{C}$).

Let (a_1, b_1) and (a_2, b_2) be solutions of (1). We define the law $\oplus$ by

$$(a_1, b_1) \oplus (a_2, b_2) = (a_1 a_2 + (e^{2z} - 1) b_1 b_2, a_1 b_2 + a_2 b_1)$$

The pair $(a, b) = (a_1, b_1) \oplus (a_2, b_2)$ is also a solution of (1).

It is easy to see that the law $\oplus$ makes the set of solutions of (1) into a commutative group. This follows from the observation that $\oplus$ corresponds to multiplication in EXP[$\mathbb{C}$][$\sqrt{e^{2z} - 1}$] as follows: (with notation as above)

$$(a_1 + \sqrt{e^{2z} - 1} b_1) \cdot (a_2 + \sqrt{e^{2z} - 1} b_2) = a + \sqrt{e^{2z} - 1} b\ .$$

The 'negative' of the point (a, b) denoted $\ominus(a, b)$ is $(a, -b)$ and the identity element of the group is $(1, 0)$.

We denote by $\kappa \odot (a, b) = (a, b) \oplus \cdots \oplus (a, b)$. ($(a, b)$ added to itself by $\oplus$ κ times.)

Theorem 6 *The solutions of the equation (1) are given by*

$$(x, y) = \kappa \odot (\pm e^z, 1) \oplus \lambda \odot (\pm e^{-z}, \mathrm{i}e^{-z}).$$

The proof uses techniques of [5], [1] and [4].

Important points of the proof

We would like to characterise all the solutions of Equation (1) over EXP($\mathbb{C}$). Observe that, by the definition of EXP($\mathbb{C}$), x and y lay in some ring of the form $R = \mathbb{C}[e^{\mu_1 z}, e^{-\mu_1 z}, \ldots, e^{\mu_k z}, e^{-\mu_k z}]$, where k is a natural number and each $\mu_i \in \mathbb{C}$. In [1] it is shown that one can choose the μ_i in such a way that $\mu_1 = \frac{1}{N}$, for some natural number N, and the set $\{1, \mu_2, \cdots, \mu_k\}$ is linearly independent over the field $\mathbb{Q}$. By results of [5] it follows that the set $\{e^{\mu_1 z}, \ldots, e^{\mu_k z}\}$ is algebraically independent over $\mathbb{C}$. So the question about solutions of (1) becomes

Given a natural number N, find the solutions of

$$(Z^{2N} - 1)y^2 = x^2 - 1 \tag{2}$$

over the ring

$$\mathbb{C}[Z, Z^{-1}, t_2, t_2^{-1}, \ldots, t_\ell, t_\ell^{-1}],$$

where $Z = e^{\frac{1}{N}}$ and the elements $t_2, \ldots t_\ell$ may be considered as variables over $\mathbb{C}[Z, Z^{-1}]$. At a first stage we show that any solution of (2) does not depend on the varables t_j, i.e. is over $\mathbb{C}[Z, Z^{-1}]$. Then, extending techniques of [4] we show that any solution is over the ring $\mathbb{C}[Z^N, Z^{-N}]$. Finally we give the characterization of solutions as in Theorem 2. Subsequently the set of integers is positive existentially definable, by techniques of [3] and [2].

Forthcoming Research

One may view this problem as an effort towards answering the following question. We consider the ring of functions $\mathcal{H}$ of the independent variable z, analytic on $\mathbb{C}$. Let L_z be the language of arithmetic, augmented by a constant-symbol for z: $L_z = \{+, \cdot; 0, 1, z\}$. We ask:

Question 2 *Is the positive existential theory of $\mathcal{H}$ in L_z decidable?*

This work is based on my Master Thesis entitled "An analogue of Hilbert' s Tenth Problem for the ring of exponential sums" presented in September 2016 at the University of Crete. The research part of this Thesis is based on the paper with title "An analogue of Hilbert' s Tenth Problem for the ring of exponential sums" which is a joint work with Thanases Pheidas.

References

[1] T. Pheidas and P. D'Aquino and G. Terzo, *Undecidability of the diophantine theory of exponential sums*, manuscript.

[2] J. Denef, *Hilbert's Tenth Problem for Quadratic Rings*, Transactions of the American Mathematical Society, **48**(1975), 214–220

[3] J. Denef, *The diophantine problem for polynomial rings and fields of rational functions*, Transactions of the American Mathematical Society, **242**(1978), 391–399

[4] Th. Pheidas and K. Zahidi *Undecidable existential theories of polynomial rings and function fields*, Communications in Algebra, **27**(**10**)(1999), 4993–5010

[5] L. van den Dries, *Exponential rings, exponential polynomials and exponential functions*, Pacific Journal of Mathematics, (1) **113**(1984), 51–66.