Definability and decidability problems in number theory

organized by
Kirsten Eisentraeger, Valentina Harizanov, Jennifer Park, and Alexandra Shlapentokh

Workshop Summary

Workshop summary

The goal of this workshop was to explore generalizations and re-formulations of Hilbert's tenth problem and related conjectures. Hilbert's tenth problem asks whether there is an algorithm that decides, given a multivariate polynomial equation with integer coefficients, whether it has an integer solution. Although the original problem was resolved in 1970 by Matiyasevich (building on the works of Davis, Putnam, and Robinson), many natural extensions, including the analogue over the rational numbers, remain open. The aim of this workshop was to explore these extensions from various points of view, and to encourage collaborations between mathematicians of different backgrounds. In particular, this workshop brought together mathematicians working in number theory, arithmetic geometry, computability theory, and model theory.

Each morning began with two talks. The speakers of the first three days were given instructions to provide a broad overview of their respective fields, in addition to introducing their own results. The last two days' talks were more specialized as the participants became more familiar with each other's areas as the workshop progressed. The talks were given by

- Alexandra Shlapentokh and Russell Miller,
- Kirsten Eisentraeger and Tom Scanlon,
- Florian Pop and Karl Rubin,
- Julia Knight and Arno Fehm,
- Philip Dittmann and Hector Pasten.

On Monday afternoon, all participants gathered to collect open problems in the field, and we compiled a list of thirteen problems. Many of these problems stemmed from attempts to reduce extensions of Hilbert's tenth problem over various rings and fields to Hilbert's tenth problem over $\mathbb{Z}$.

On Tuesday, the organizers chose seven problems to be worked on, and the participants organized themselves into working groups. Each afternoon was then devoted to group work on these chosen problems.

Working groups

The working groups worked on the following problems:

- Density of the sets of boundary polynomials. This problem considered the existence of roots of polynomials in a monotonically increasing sequence of subrings of $\mathbb{Q}$ (in the sense that we start with $\mathbb{Z}$ and systematically invert larger and larger sets of primes). A boundary polynomial is a polynomial without a root at any finite stage of the process but potentially with a root, if certain primes are inverted at a later stage.

One of the methods for solving the problem led to a question concerning elliptic curves. More precisely, given a model of an elliptic curve of rank 1 corresponding to an equation of the form $y^2 = x^3 + ax + b$, and prime multiples of a generator of the group, can one prove that the number of distinct primes in the denominator of the coordinates of the points grows at a certain rate. There are some conjectures related to this question, but in general the problem seems very hard at the moment. The group made some calculations that seem to confirm that the rate of growth of the number of primes in the denominator supports the conjecture that the density of the set of boundary polynomials can be positive. The group plans to continue to work on the problem. (K. Eisenträger, B. Kadets, R. Miller, J. Park, K. Rubin, M. Soskova, A. Shlapentokh, C. Springer)

- Defining $k[x_1, \ldots, x_n]$ inside the rational function field $k(x_1, \ldots, x_n)$. The group first worked on the special case where the partial derivatives $\frac{\partial}{\partial x_i}$ are included in the language for all $1 \leq i \leq n$, and solved this problem completely; this problem will be written up and submitted for publication. They then worked on achieving the same goal via defining the valuations of $k(x_1, ..., x_n)$ with $n > 1$, and reported some progress on this problem as well. The group plans to continue working on this problem. (M. Barone, B. Castle, D. Haskell, T. Morrison, E. Naziazeno, F. Pop, T. Scanlon)
- Understanding the automorphisms of cohesive powers $\prod_C F$ for finite algebraic extensions F of $\mathbb{Q}$, and whether there are any that do not arise from automorphisms of F. Cohesive products of computable structures can be viewed as effective ultraproducts over cohesive sets. A set is cohesive if it is infinite and indecomposable with respect to computably enumerable sets. It is known that any cohesive power of $\mathbb{Q}$ is rigid. The group began by assuming that there is a Diophantine definition of $\mathbb{Z}$ over the ring of integers of the number field F. The group then established that the answer to the second part of the problem is negative. The group would like to collect all results that establish such definitions and plan to continue their research collaboration. (P. Dittman, R. Dimitrov, V. Harizanov)
- Measuring the complexity of the root-taking process of polynomials defined over the Hahn field $K((G))$. Assuming that K is an algebraically closed field of characteristic 0 and let G a divisible ordered Abelian group, Knight, Lange, and Solomon have partial results on measuring the complexity of the root-taking process; some related problems were discussed at the workshop.

  For $s \in K((G))$, the support is well-ordered, but instead of representing s by a sequence with domain an ordinal, one uses a total function $s : G \to K$ that assigns coefficients to all elements of G to consider the following problems:
  1. For computable ordinals α, how hard is it to say that $\text{length}(s) \geq \alpha$? For finite $n \geq 1$, it is Σ^0_1 to say that $\text{length}(s) \geq n$. It is Π^0_2 to say that $\text{length}(s) \geq \omega$. At AIM, the working group was able to show that these bounds are sharp.
  2. For computable ordinals α, how hard is it for a set $S \subseteq G$ that is well-ordered, to find the α^{th} element of S, call it s_α, or to say that S has order type at most α? The working group looked at the first few ordinals. It is Δ^0_2 to compute s_n. It is Δ^0_3 to compute s_ω, or $s_{\omega \cdot n}$.

  The group plans to continue to work on the problem. (C. Hall, J. Knight)

- Decidability of the positive-existential theories of rings of complex holomorphic functions, both of one, and of several variables. Previous results were due to Lipshitz and Pheidas (defining entire functions over nonarchimedean complete algebraically closed field of characteristic 0 as L_z-structure), Garcia-Fritz and Pasten (positive characteristic version), Vidaux (meromorphic function version, as $L_{z,ord}$-structure), Pasten (positive odd characteristic version). While the standard approach using analogues of Pell's equations or Manin-Denef curves do not seem to work for all complex holomorphic functions, it may still work for analytic functions of finite order (i.e., dominated at infinity by a function of the form $e^{|z|^\alpha}$ for some real α), and the group members plan to continue their collaboration. (N. Garcia-Fritz, H. Pasten, T. Pheidas, X. Vidaux)
- Decidability of the existential theory of rational function fields over finite fields and some of their subrings, in various languages. The classical results here are the undecidability of the existential theory of $\mathbb{F}_p(t)$ in the language of rings with constant t by Pheidas for $p > 2$ from 1991, which is equivalent to the undecidability of the $\forall_1\exists$-theory of $\mathbb{F}_p(t)$ in the language of rings, and the undecidability of the existential theory of the polynomial ring $\mathbb{F}_p[t]$ in the language of rings by Pheidas-Zahidi from 1999. As the question of the undecidability of the existential theory of $\mathbb{F}_p(t)$ in the language of rings seems out of reach at this point, the group mainly focused on the decidability of the existential theory of the valuation ring $\mathbb{F}_p[t]_{(t)}$ in the language of rings, which in difficulty should lie between the question for $\mathbb{F}_p[t]$ and $\mathbb{F}_p(t)$. (S. Anscombe, P. Dittman, A. Fehm, F. Jahnke)
- Hilbert's tenth problem for henselian non-trivially valued fields of mixed characteristics. Let (K, v) be a henselian non-trivially valued field of equal characteristic, viewed as a first order structure in a suitable language. We know (Anscombe-Fehm, 2016) that the existential theory of (K, v) is axiomatized by the existential theory of the residue field k, together with the theory of henselian non-trivially valued fields of equal characteristic. It follows (still in the equal characteristic case) that the existential theory of (K, v) is decidable if and only if the existential theory of the residue field k is decidable. Framed in terms of Hilbert's tenth problem (H10), this amounts to saying that H10 has a positive solution for (K, v) if and only if it has one for k. A working group studied the possibility of extending these results to the case of mixed characteristic, both the axiomatization and the transfer of existential decidability. In the unramified case, this group has an argument that goes via the theory of Cohen rings. That is, the existential theory of an unramified henselian valued field of mixed characteristic is axiomatized by those properties together with the existential theory of its residue field. It gives a transfer principle: if H10 has a positive solution for k then it has a positive solution for (K, v). In the general case (both finitely ramified and infinitely ramified), the group felt that more work needed to be done, possibly in analogy with Thanagopal (2018), building on Ershov (2000), who constructed a field of characteristic zero, which is decidable but admits an existentially undecidable finite extension. If such a field can be constructed in positive characteristic, it follows that the residue field, pointed value group, and algebraic part, must be supplemented by something else. (S. Anscombe, P. Dittman, V. Harizanov, A. Fehm, F. Jahnke)