UNIFORMLY RECURSIVELY ENUMERABLE SETS OF POLYNOMIALS OVER FINITE FIELDS

Jeroen Demeyer
Ghent University (Ghent, Belgium)

Define an algebraic set over a ring R as the zero set of a system of polynomial equations. Define a diophantine set as the projection (onto some of the coordinates) of an algebraic set. Equivalently, a diophantine set is a set defined by a positive existential formula in the language of rings. It is easy to see that diophantine sets are always recursively enumerable.

It was shown in 1970 by Davis, Putnam, Robinson and Matiyasevich that recursively enumerable subsets of $\mathbb{Z}$ are diophantine over $\mathbb{Z}$. As an immediate consequence, one gets the undecidability of diophantine equations over $\mathbb{Z}$, i.e. a negative answer to Hilbert's Tenth Problem.

This equivalence of recursively enumerable and diophantine has been generalized to various other rings. In this talk, we present this equivalence for $\mathbb{F}_p[t]$, uniformly in p. One particular consequence of this result is that, for every recursively enumerable subset S of the prime numbers, there exists a polynomial with coefficients in $\mathbb{Z}[t]$ such that this polynomial has a zero modulo p (in $\mathbb{F}_p[t]$) if and only if $p \in S$.

This is joint work with Joseph Flenner, Alexandra Shlapentokh, Xavier Vidaux