Mathematisches Forschungsinstitut Oberwolfach

Report No. 49/2016

DOI: 10.4171/OWR/2016/49

Definability and Decidability Problems in Number Theory

Organised by
Jochen Koenigsmann, Oxford
Hector Pasten, Cambridge MA
Alexandra Shlapentokh, Greenville
Xavier Vidaux, Concepción

23 October – 29 October 2016

Abstract. This workshop brought together experts working on variations of Hilbert's Tenth Problem and more general decidability issues for structures other than the ring of integers arising naturally in number theory and algebraic geometry.

Mathematics Subject Classification (2010): 03XX, 11XX, 12E30, 12JXX, 13A18, 14XX.

Introduction by the Organisers

This highly interdisciplinary workshop brought together 51 Mathematicians from Number Theory, Logic, Algebraic Geometry, Computability, Model Theory, Arithmetic of Fields, Valuation Theory, and some other related areas. Many contributions and discussions were inspired and driven by the big open decidability questions such as Hilbert's Tenth Problem over $\mathbb{Q}$, the decidability of the first-order theory of $\mathbb{F}_p((t))$ or of $\mathbb{C}(t)$, variations of Büchi's Problem and other weak forms of arithmetic, as well as associated questions of definability and logical complexity in various rings of number theoretic interest, and in analogous rings of functions. Several of these issues are closely related to major conjectures in Arithmetic Geometry, thus faring in deep waters. However, what was most remarkable about the workshop was the immense and effective effort the participants made in being understood, in getting across their key points, and in promoting the common understanding. There was an open, friendly yet well-focused atmosphere, a high spirit of joint venture, possibly propelled by the dynamics between the large numbers of both excellent young researchers on the one hand, and the rather matured

experts on the other. And, of course, the wonderful setting of MFO, and the extreme degree of professionality it is run by on all levels, have played a crucial part in making this workshop such a success.

Let us briefly mention some of the scientific highlights (not including the more survey-like contributions by Colliot-Thélène, Fehm and Derakhshan). One of them was Philip Dittmann's theorem that irreducibility is diophantine, i.e. definable by an existential first-order formula, in global fields. This vastly generalises partial earlier results in this direction by Poonen, Koenigsmann, Park, Colliot-Thélène and Van Geel. In the case of $\mathbb{Q}$, this theorem (which now holds unconditionally) would follow if $\mathbb{Z}$ was diophantine in $\mathbb{Q}$ (which is one of the big open problems in the field, and which would imply that Hilbert's Tenth Problem for $\mathbb{Q}$ is unsolvable).

Another breakthrough towards proving that $\mathbb{Z}$ is *not* diophantine in $\mathbb{Q}$ (and $\mathbb{F}_p[t]$ not in $\mathbb{F}_p(t)$ etc.) is Hector Pasten's theorem that these negative results follow from a new conjecture of his on the behavior of proximity functions in diophantine approximation – a conjecture that he has verified in a number of cases. He also discussed recent work with Ram Murty showing that standard analytic conjectures on L-functions imply that $\mathbb{Z}$ is diophantine in $\mathcal{O}_K$ for all number fields K, nicely complementing similar results of Mazur and Rubin which assume conjectures on Ш.

Natalia Garcia-Fritz developed a powerful machinery generalising Vojta's approach for solving Büchi's problem (modulo Bombieri-Lang) by finding all curves of low genus in surfaces with unconditional arithmetic applications à la Büchi for function fields of characteristic zero.

There were two undecidability results for certain infinite extensions of global fields, one by Kirsten Eisenträger for the perfect closure of a global field of positive characteristic, and one by Martin Widmer for sufficiently ramified extensions of $\mathbb{Q}$ following the track set out by Videla and Vidaux along the lines of Julia Robinson's classical undecidability result for the ring of totally real integers.

By contrast, we had one contribution in the opposite direction (towards decidability) in Győry's talk, where he described his work (and of his collaborators) on effective finiteness results for certain diophantine equations over $\mathbb{Z}$ and over finitely generated domains, vastly extending Baker's results from the 1960s on integral points on certain curves.

There were two major contributions from Model Theory: Itay Kaplan showed that the structure $(\mathbb{Z}, +, \mathbb{P}')$ is decidable (where $\mathbb{P}' = \{\pm p \mid p \in \mathbb{P}\}$ with $\mathbb{P}$ denoting the set of rational primes) and is of U-rank 1, while $(\mathbb{N}, +, \mathbb{P})$ is known to be undecidable (both under Dickson's conjecture). And Thomas Scanlon answered two questions about the logical complexity of finitely generated commutative rings proving, firstly, that for any such ring R, there is a first-order sentence in the language of rings that determines R (among the f.g. comm. rings) up to isomorphism and, secondly, characterising those infinite f.g. rings that are biinterpretable with

$\mathbb{Z}$ (e.g. all infinite finitely generated integral domains are). This nicely complemented Florian Pop's talk addressing the long-standing question of whether all f.g. *fields* are, up to isomorphism, determined by their first-order theory.

Finally, let us highlight two important valuation theoretic inputs which were similar to each other in providing a new conceptual framework for dealing with decidability issues for valued fields, one by Raf Cluckers about "Resplendent Minimality", a notion analogous to o-minimality but tailored towards the analysis of henselian valued fields, the idea being that definable subsets of the line are controlled by a finite set of points (like the end points of intervals in the o-minimal setting). The other was Franz-Viktor Kuhlmann's report on his and others' research on the new notion of *extremal* valued fields, that is, valued fields in which for each polynomial (in several variables) the set of values obtained by plugging in elements of the valuation ring always attains a maximum. It is easy to check that $\mathbb{F}_p((t))$ is extremal, and the hope is that this property (together with residue field $\mathbb{F}_p$ and value group elementarily equivalent to $\mathbb{Z}$) suffices to axiomatise $\mathbb{F}_p((t))$ (thus proving its decidability).

Thursday afternoon was almost entirely devoted to a very interesting "Open Problems" session, chaired by Jeroen Demeyer, for which we give a separate "extended abstract".

Acknowledgement: The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-1049268, "US Junior Oberwolfach Fellows". Moreover, the MFO and the workshop organizers would like to thank the Simons Foundation for supporting Natalia Garcia-Fritz in the "Simons Visiting Professors" program at the MFO.

Workshop: Definability and Decidability Problems in Number Theory

Table of Contents

Abstracts

Torsion of Abelian Varieties Over Large Algebraic Fields

Moshe Jarden
(joint work with Sebastian Petersen)

Wulf-Dieter Geyer and Moshe Jarden published the following result in the Israel Journal of Mathematics (1978):

Theorem 1 (cf. [GeJ78, p. 259, Prop. 1.2]). *Let K be a finitely generated field, E an elliptic curve over K, and e a positive integer. Then, the following statements hold for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$:*

(a) *If $e = 1$, then $E_l(K_s(\sigma)) \neq 0$ for infinitely many prime numbers l.*
(b) *If $e \geq 2$, then $E_l(K_s(\boldsymbol{\sigma})) \neq 0$ only for finitely many prime numbers l.*
(c) *If $e \geq 2$ and l is a prime number, then $E_{l^\infty}(K_s(\boldsymbol{\sigma}))$ is finite.*

Statements (b) and (c) on $\boldsymbol{\sigma}$ are equivalent to "$E_{\mathrm{tor}}(K_{\mathbf{s}}(\boldsymbol{\sigma}))$ is finite".

Here "K **is finitely generated**" means that K is finitely generated over its prime field. We write

- $\tilde{K}$ for a fixed algebraic closure of K,
- K_s for the separable algebraic closure of K in $\tilde{K}$,
- $\mathrm{Gal}(K) = \mathrm{Gal}(K_s/K)$ for the absolute Galois group of K,
- $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$,
- $K_s(\boldsymbol{\sigma})$ for the fixed field of $\sigma_1, \ldots, \sigma_e$ in K_s,
- E_m for the kernel of multiplication of E with a positive integer m, and
- $E_{l^\infty} = \bigcup_{i=1}^{\infty} E_{l^i}$ for every prime number l.

Finally we equip the group $\mathrm{Gal}(K)$ and its powers $\mathrm{Gal}(K)^e$ with their unique Haar measure μ_K such that $\mu_K(\mathrm{Gal}(K)^e) = 1$. Then we say "a statement holds for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$", when the statement holds for all $\boldsymbol{\sigma}$ in a set of measure 1.

Geyer and Jarden conjectured in the above cited work that Theorem 1 holds also for abelian varieties.

Conjecture 2 ([GeJ78, p. 260, Conjecture]). *Let K be a finitely generated field, A a non-trivial abelian variety over K, and e a positive integer. Then, the following statements hold for almost all $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$:*

(a) *If $e = 1$, then $A_l(K_s(\sigma)) \neq 0$ for infinitely many l.*
(b) *If $e \geq 2$, then $A_l(K_s(\boldsymbol{\sigma})) \neq 0$ only for finitely many l.*
(c) *If $e \geq 2$, then $A_{l^\infty}(K_s(\boldsymbol{\sigma}))$ is finite for each l.*

Previous Results:

- Conjecture 2 is proved for finite fields K in [JaJ84, p. 114, Prop. 4.2]. Part (c) of the conjecture in general and part (b) of the conjecture in characteristic 0 are proved in [JaJ01, Main Theorem].
- The main result of [GeJ05] considers a non-trivial variety A over a number field K and proves the existence of a finite Galois extension L of K such that for almost all $\sigma \in \mathrm{Gal}(L)$ there exist infinitely many prime numbers l with $A_l(\tilde{K}(\sigma)) \neq 0$.
- David Zywina [Zyw10] improves the result of [GeJ05] and proves Part (a) of the conjecture for a number field K not anly for almost all $\sigma \in \mathrm{Gal}(L)$, as in [GeJ05], but for almost all $\sigma \in \mathrm{Gal}(K)$.

We report here about a proof of Part (a) of the conjecture for every finitely generated field K of characteristic 0.

Main Theorem. *Let K be a finitely generated extension of $\mathbb{Q}$ and let A be a non-trivial abelian variety over K. Then, for almost all $\sigma \in \mathrm{Gal}(K)$ there exist infinitely many prime numbers l with $A_l(\tilde{K}(\sigma)) \neq 0$.*

This completes the proof of Part (a) of the conjecture in characteristic 0, 38 years after it was made. Parts (a) and (b) of the conjecture in positive characteristic are, up to spacial cases, still open.

In the rest of the extended abstract we highlight the main ingredients of the proof. Throughout A denotes an abelian variety of dimension g over a finitely generated extension K of $\mathbb{Q}$. For each prime number l we consider the l-ic representation $\rho_{A,l}\colon \mathrm{Gal}(K) \to \mathrm{GL}_{2g}(\mathbb{F}_l)$ of $\mathrm{Gal}(K)$ given by the action of $\mathrm{Gal}(K)$ on the $\mathbb{F}_l$-vector-space A_l of dimension $2g$.

Theorem of Serre. The proof of [GeJ05] as well as the proof of [Zyw10] depends on the main result of [Ser86]. That result is concerned with the case, where K is a number field. Among others, that result gives a finite Galois extension L of K, a positive integer n, and for each l a connected reductive subgroup H_l of $\mathrm{GL}_{2g,\mathbb{F}_l}$ of a fixed rank r, such that $\rho_{A,l}(\mathrm{Gal}(L)) \leq H_l(\mathbb{F}_l)$ and $(H_l(\mathbb{F}_l) : \rho_{A,l}(\mathrm{Gal}(L)))$ divides n. In addition, the fields $L(A_l)$, with l ranges over all prime numbers, are linearly disjoint over L. Moreover, Serre's theorem supplies a set Λ of prime numbers of positive Dirichlet density, such that H_l splits over $\mathbb{F}_l$ for each $l \in \Lambda$. The proof of Serre depends on the renown results of Faltings from 1983 (The Tate Conjecture) and on class field theory. The latter makes the generalization of Serre's proof to finitely generated transcendental extensions of $\mathbb{Q}$ unclear.

Borel-Cantelli Lemma. For each l we set

$$\begin{aligned} S_l &= \{\sigma \in \mathrm{Gal}(L) \mid 1 \text{ is an eigenvalue of } \rho_{A,l}(\sigma)\} \\ &= \{\sigma \in \mathrm{Gal}(L) \mid \exists \mathbf{a} \in A_l(\tilde{K}) \mid \mathbf{a} \neq 0 \text{ and } \sigma\mathbf{a} = \mathbf{a}\} \\ &= \{\sigma \in \mathrm{Gal}(L) \mid A_l(\tilde{K}(\sigma)) \neq 0\} \end{aligned}$$

The work [GeJ05] proves the existence of a positive constant c and a set Λ of prime numbers of positive Dirichlet density, such that $\mu_L(S_l) > \frac{c}{l}$ for each $l \in \Lambda$. Hence, $\sum_{l\in\Lambda} \mu_L(S_l) = \infty$. By the theorem of Serre, the sets S_l with $l \in \Lambda$ are μ_L-independent. It follows from a lemma of Borel-Cantelli, that almost all $\sigma \in \mathrm{Gal}(L)$ lie in infinitely many sets S_l with $l \in \Lambda$. Therefore, for almost all $\sigma \in \mathrm{Gal}(L)$ there are infinitely many l with $A_l(\sigma) \neq 0$. This is the desired result over L.

The combinatorial approach of Zywina. Zywina uses the lemma of Borel-Cantelli in a finer way. In his work [Zyw10] he chooses a system of representatives B for $\mathrm{Gal}(K)$ modulo $\mathrm{Gal}(L)$. For each l and every $\beta \in B$ he considers the set

$$U_{\beta,l} = \{\sigma \in \beta\mathrm{Gal}(L) \mid 1 \text{ is an eigenvalue of } \rho_{A,l}(\sigma)\}.$$

Then, Zywina computes a positive constant c and find a set Λ_β of prime numbers of positive Dirichlet density such that

$$\mu_K(U_{\beta,l}) \geq \frac{c}{l} \text{ for all } l \in \Lambda_\beta. \tag{1}$$

Let U_β be the set of all σ that belong to infinitely many of the sets $U_{\beta,l}$ with $l \in \Lambda_\beta$. Again, by Borel-Cantelli, we have that $\mu_K(U_\beta) = \frac{1}{[L:K]}$. Since the U_β's with $\beta \in B$ are disjoint, it follows that for almost all $\sigma \in \mathrm{Gal}(K)$ there exist infinitely many l with $A_l(\tilde{K}(\sigma)) \neq 0$.

Function fields. From now on we assume that K is a finitely generated transcendental extension of $\mathbb{Q}$ and choose a subfield E of K, such that K/E is a regular transcendental extension of transcendence degree 1. We look for a prime divisor $\mathfrak{p}$ of K/E with residue field $\bar{K}$, at which A has a good reduction to an abelian variety $\bar{A}$ over $\bar{K}$, such that

$$\mathrm{Gal}(K(A_l)/K) \cong \mathrm{Gal}(\bar{K}(\bar{A}_l)/\bar{K}) \tag{2}$$

at least for every l in a set of positive Dirichlet density. Unfortunately, Hilbert irreducibility theorem supplies prime divisors $\mathfrak{p}$ that have the above mentioned property only for finitely many l's.

An openness theorem. Instead, we choose a smooth curve S over E with function field K, such that A has a good reduction along S and set $\hat{K} = \prod_l K(A_l)$. Then, we use a combination of results of Anna Cadoret and Akio Tamagawa in [CaT12], [CaT13], and [Cad15], in order to find a point $\mathbf{s} \in S(\tilde{E})$ with an open decomposition group in $\mathrm{Gal}(\hat{K}/K)$. The fixed field K' in $\tilde{K}$ of that decomposition group is a finite extension K' of K. Reduction modulo $\mathbf{s}$ gives an isomorphism

$$\mathrm{Gal}(\hat{K}/K') \to \mathrm{Gal}(\hat{K}_{\mathbf{s}}/\bar{K}_{\mathbf{s}}),$$

where $\bar{K}_{\mathbf{s}}$ is the residue field of K at $\mathbf{s}$ and $\hat{K}_{\mathbf{s}} = \prod_l \bar{K}_{\mathbf{s}}(\bar{A}_l)$. Then, the desired isomorphism (2) follows for all prime number l, with K' replacing K.

The theorem of Serre over K. Now we use a result of [GaP13] that gives a finite Galois extension L of K that contains K' and satisfies the same reduction condition as K'. Moreover, the fields $L(A_l)$, with l ranges over all prime numbers, are linearly disjoint over L. Observe that $\bar{K}_{\mathbf{s}}$ is again finitely generated over $\mathbb{Q}$, however with a transcendence degree over $\mathbb{Q}$ smaller by 1. Starting from the theorem of Serre for number fields, we may use induction in order to prove an analogous theorem for K.

Strongly regular points. Now that we have the theorem of Serre for K, we follow the proof in [Zyw10] in order to achieve the estimates (1) for our abelian variety A/K. The proof uses a careful analysis of regular points of the reductive groups H_l mentioned in Serre's theorem with $l \in \Lambda$. It applies the following crucial observation of Zywina: If $\mathbf{t} \in H_l(\mathbb{F}_l)$, then $\mathbf{t}^{n!} \in \rho_{A,l}(\mathrm{Gal}(L))$. Moreover, if $\mathbf{t}'$ is an $\mathbb{F}_l$-rational regular point of H_l, T is the unique maximal torus of H_l that contains $\mathbf{t}'$, and $r = \mathrm{rank}(H_l) = \dim(T)$, then $T(\mathbb{F}_l)$ contains at most $(n!)^r$ points $\mathbf{t}$ with $\mathbf{t}^{n!} = \mathbf{t}'$. Finally, still following Zywina, we use the Lang-Weil estimates in order to prove that "almost all points" of $\rho_{A,l}(\mathrm{Gal}(K))$ are regular in H_l and their characteristic polynomials have "maximal number of of roots in $\mathbb{F}_l$" (we call such points "strongly regular").

Serre's density theorem. At one point of its proof, [Zyw10] applies the Chebotarev density theorem for number fields in order to choose a prime of K whose Artin class is a given conjugacy class of $\mathrm{Gal}(L(A_l)/K)$ (where L is the finite Galois extension of K mentioned in Serre's theorem). Instead, we find an appropriate integrally closed domain R which is finitely generated over $\mathbb{Z}$ such that $\mathrm{Quot}(R) = K$ and use a generalization of the Chebotarev density theorem to our function field (that goes back to [Ser65]) in order to find a maximal prime ideal of K with the corresponding properties.

References

[Cad15] A. Cadoret, *An open adelic image theorem for abelian schemes*, International Mathematics Research Notices, (2015).

[CaT12] A. Cadoret and A. Tamagawa, *A uniform open image theorem for l-adic representations, I*, Duke Mathematical Journal **161** (2012), 2605–2634.

[CaT13] A. Cadoret and A. Tamagawa, *A uniform open image theorem for l-adic representations, II*, Duke Mathematical Journal **162** (2013), 2301–2344.

[GeJ78] W.-D. Geyer and M. Jarden, *Torsion points of elliptic curves over large algebraic extensions of finitely generated fields*, Israel Journal of Mathematics **31** (1978), 157–197.

[GaP13] W. Gajda and S. Petersen, *Independence of l-adic Galois representations over function fields*, Compositio Mathematica **149** (2013), 1091–1107.

[GeJ05] W.-D. Geyer and M. Jarden, *Torsion of Abelian varieties over large algebraic fields*, Finite Field Theory and its Applications **11** (2005), 123–150.

[JaJ84] M. Jacobson and M. Jarden, *On torsion of abelian varieties over large algebraic extensions of finitely generated fields*, Mathematika **31** (1984), 110–116.

[JaJ01] M. Jacobson and M. Jarden, *Finiteness theorems for torsion of abelian varieties over large algebraic fields*, Acta Arithmetica **98** (2001), 15–31.

[Ser65] J.-P. Serre, *Zeta and L-functions*, in Arithmetical Algebraic Geometry (Schilling, ed.), Harper and Row, New York (1965), 82–92.

[Ser86] J.-P. Serre, *Groupes linéaires modulo p et points d'ordre fini des variétés abéliennes*, Cours au Collège de France, Unpublished notes of Eva Bayer-Flukiger, 1986.
[Zyw10] D. Zywina, *Abelian varieties over large algebraic fields with infinite torsion*, Israel Journal of Mathematics **211** (2016), 493–508.

L'obstruction de Brauer–Manin et ses raffinements

Jean-Louis Colliot-Thélène

J'ai donné un exposé de synthèse. Ceci en est un court résumé, qui ne prétend à aucune originalité. Je renvoie le lecteur aux rapports récents [3, 5, 1] pour plus de détails et de références.

Sauf mention du contraire, par variété lisse sur un corps on entend ici une variété lisse géométriquement intègre.

1. Solutions locales, solutions globales

Soit k un corps de nombres. Pour v une place de k, on note k_v le complété.

Étant donnée une k-variété X, on aimerait décider si l'ensemble $X(k)$ des points k-rationnels de X est non vide. On a l'inclusion $X(k) \hookrightarrow \prod_v X(k_v)$, où v parcourt toutes les places de k. On sait décider si $\prod_v X(k_v) \neq \emptyset$. *Si X est géométriquement intègre, alors $X(k_v) \neq \emptyset$ pour presque toute place v.*

Si pour toute X dans une classe de variétés, la condition $\prod_v X(k_v) \neq \emptyset$ implique $X(k) \neq \emptyset$, alors on dit que le principe de Hasse vaut pour (les variétés dans) cette classe. Il en est ainsi pour les quadriques (Minkowski, Hasse) et pour les variétés projectives lisses connexes espaces homogènes de groupes algébriques linéaires (Harder). Il en est aussi ainsi pour les équations $\mathrm{Norm}_{K/k}(\Xi) = c$ pour K/k une extension cyclique de corps de nombres et $c \in k^\times$.

Supposons X lisse, connexe. Si $X(k)$ est non vide et dense dans le produit topologique $\prod_v X(k_v)$, on dit que X satisfait l'approximation faible. Ceci implique que $X(k)$ est dense dans X pour la topologie de Zariski.

On peut généraliser ces questions pour un morphisme. Si $f : X \to Y$ est un morphisme de k-variétés, on demande de décrire $f(X(k)) \subset Y(k)$. Le cas $Y = \mathrm{Spec}(k)$ correspond à la question : $X(k)$ est-il vide?

Pour $Y = \mathbf{A}^1_k$, la droite affine, on se demande quels sous-ensembles de $k = \mathbf{A}^1(k)$ peuvent être obtenus comme une telle image $f(X(k))$: c'est la question de la description des ensembles diophantiens dans k. Pour $k = \mathbf{Q}$, Mazur a demandé si $\mathbf{Z} \subset \mathbf{Q}$ est diophantien. Königsmann a démontré que le complémentaire de $\mathbf{Z}$ dans $\mathbf{Q}$ est diophantien. Poonen a montré que le complémentaire des carrés dans un corps de nombres k est diophantien, ceci a été étendu au complémentaire des puissances n-ièmes par J. Van Geel et l'orateur. Un résultat plus général a été obtenu par P. Dittmann (voir son exposé).

Si $f : X \to Y$ est un k-morphisme de k-variétés géométriquement intègres, de base Y projective et à fibres géométriquement intègres, alors *pour presque toute place v, on a $f(X(k_v)) = Y(k_v)$*. J'avais proposé un critère plus général sur f

assurant cette dernière propriété. Ce critère a été établi par J. Denef, voir l'exposé de Skorobogatov.

2. Obstruction de Brauer–Manin

On trouve dans la littérature de nombreux contre-exemples au principe de Hasse et à l'approximation faible. On en trouve en particulier parmi:

- les équations normes $\mathrm{Norm}_{K/k}(\Xi) = c$, avec $c \in k^\times$, pour certaines extensions K/k non cycliques (Hasse).
- les courbes de genre 1 (Lind, Reichardt, Selmer)
- les surfaces cubiques lisses (Swinnerton-Dyer, Cassels et Guy)
- les surfaces intersections lisses de deux quadriques dans $\mathbf{P}^4_k$ (Birch et Swinnerton-Dyer)
- les surfaces fibrées en coniques sur la droite projective (Iskovskikh)

En 1970, Manin décrivit un formalisme qui permit d'expliquer les divers contre-exemples au principe de Hasse alors connus. Ce formalisme utilise le groupe de Brauer $\mathrm{Br}(X)$ d'une variété X.

Pour toute variété X sur un corps k, et F un surcorps de k, on dispose d'une application d'évaluation

$$X(F) \times \mathrm{Br}(X) \to \mathrm{Br}(F).$$

Pour k un corps de nombres, la théorie du corps de classes fournit des injections $\mathrm{Br}(k_v) \hookrightarrow \mathbf{Q}/\mathbf{Z}$ qui s'insèrent dans une suite exacte fondamentale

$$0 \to \mathrm{Br}(k) \to \oplus_v \mathrm{Br}(k_v) \to \mathbf{Q}/\mathbf{Z} \to 0.$$

Le fait que cette suite est un complexe généralise en particulier la loi de réciprocité quadratique de Gauss.

Pour X une k-variété projective et lisse, notant $X(\mathbb{A}_k) = \prod_v X(k_v)$, en faisant la somme des évaluations locales, on obtient un accouplement

$$X(\mathbb{A}_k) \times \mathrm{Br}(X) \to \mathbf{Q}/\mathbf{Z}$$

$$(\{P_v\}, \alpha) \mapsto \sum_v \alpha(P_v).$$

On note $X(\mathbb{A}_k)^{\mathrm{Br}}$ le noyau à gauche de cet accouplement. C'est un fermé dans $X(\mathbb{A}_k)$, appelé ensemble de Brauer-Manin de X. De la suite exacte ci-dessus on déduit que l'adhérence de $X(k)$ dans $X(\mathbb{A}_k)$ est contenue dans $X(\mathbb{A}_k)^{\mathrm{Br}}$.

On dit que l'obstruction de Brauer–Manin au principe de Hasse est la seule pour une classe $\mathcal{C}$ de variétés projectives et lisses si, pour toute variété X dans $\mathcal{C}$ avec $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$, on a $X(k) \neq \emptyset$.

Une courbe elliptique E sur le corps de nombres k a son groupe de Tate-Shafarevich fini si et seulement si, pour toute courbe X de genre 1 de jacobienne E, si l'on a $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$, alors on a $X(k) \neq \emptyset$.

3. L'obstruction de Brauer-Manin n'est pas toujours la seule

En 1999, Skorobogatov a donné le premier exemple inconditionnel de variété X projective et lisse sur un corps de nombres k avec $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$ mais $X(k) = \emptyset$.

L'exemple de Skorobogatov est une surface bielliptique. Son groupe fondamental géométrique est non commutatif.

Ceci a mené à la définition, pour toute k-variété projective et lisse X sur un corps de nombres k, d'un ensemble $X(\mathbb{A}_k)^{\text{ét,Br}}$ avec

$$X(k) \subset X(\mathbb{A}_k)^{\text{ét,Br}} \subset X(\mathbb{A}_k)^{\mathrm{Br}} \subset X(\mathbb{A}_k).$$

L'ensemble $X(\mathbb{A}_k)^{\text{ét,Br}}$ admet plusieurs définitions équivalentes, faisant intervenir des revêtements finis étales de X (Skorobogatov, Harari, Stoll, Demarche, Harpaz, Schlank).

Ce formalisme ne couvre pas tous les contre-exemples au principe de Hasse. On a donné des exemples de variété X projective et lisse avec $X(\mathbb{A}_k)^{\text{ét,Br}} \neq \emptyset$ mais néanmoins $X(k) = \emptyset$.

Poonen construisit de telles X en dimension 3. Ses exemples sont des solides fibrés en surfaces de Châtelet au-dessus d'une courbe C ne possédant qu'un nombre fini de points.

Puis Harpaz et Skorobogatov réussirent à construire une surface X munie d'une fibration au-dessus d'une telle courbe C, en se servant d'un contre-exemple au principe de Hasse pour une fibre singulière union de courbes de genre zéro.

Pál, Skorobogatov et l'auteur donnèrent ensuite de tels exemples avec X fibrée en quadriques de dimension au moins 1 au-dessus d'une telle courbe C.

Smeets construisit des variétés X projectives et lisses avec $X(\mathbb{A}_k)^{\text{ét,Br}} \neq \emptyset$ et $X(k) = \emptyset$ avec variété d'Albanese triviale, ce qui n'était le cas d'aucun des précédents exemples. Smeets montre aussi comment sous la conjecture *abc* on peut construire des exemples de tels X à groupe fondamental géométrique trivial.

4. L'obstruction de Brauer-Manin est parfois la seule

La conjecture suivante a été faite par Sansuc et l'auteur dans le cas des surfaces, puis énoncée par l'auteur en dimension quelconque.

Conjecture. Soit X une variété projective et lisse sur un corps de nombres k. Si X est géométriquement rationnellement connexe, alors $X(k)$ est dense dans $X(\mathbb{A}_k)^{\mathrm{Br}}$.

Rappelons qu'une variété algébrique connexe sur le corps des complexes est dite rationnellement connexe si on peut relier deux points complexes généraux par une courbe de genre zéro. Si X/k est géométriquement rationnellement connexe, alors le fermé $X(\mathbb{A}_k)^{\mathrm{Br}} \subset X(\mathbb{A}_k)$ est aussi ouvert dans $X(\mathbb{A}_k)$.

Théorème (Sansuc, Borovoi) *Soient G un k-groupe algébrique linéaire connexe et Y une k-variété espace homogène de G. On suppose que les stabilisateurs géométriques sont connexes. Alors pour toute k-variété projective et lisse X k-birationnelle à Y, l'ensemble $X(k)$ est dense dans $X(\mathbb{A}_k)^{\mathrm{Br}}$.*

On essaye d'établir la conjecture par une méthode de fibration. On est amené à la:

Question. Soit $f : X \to \mathbf{P}^1_k$ un morphisme projectif surjectif à fibre générique géométriquement rationnellement connexe. Si l'obstruction de Brauer-Manin est la seule pour les fibres lisses de f, en est-il ainsi pour l'espace total X?

Cette question a fait l'objet de nombreux travaux depuis les années 1980 (l'auteur, Sansuc, Swinnerton-Dyer, Skorobogatov, Harari). On a en particulier obtenu des résultats conditionnels sous l'hypothèse de Bouniakowsky-Dickson-Schinzel, et plus récemment sous une hypothèse nouvelle introduite par Harpaz et Wittenberg [4].

Harpaz et Wittenberg [4] ont aussi montré de façon inconditionnelle que *pour une fibration $f : X \to \mathbf{P}^1_k$ comme ci-dessus, si sur toute extension finie de k, l'obstruction de Brauer-Manin est la seule pour les fibres lisses de f, l'hypothèse $X(\mathbb{A}_k)^{\mathrm{Br}} \neq \emptyset$ implique que la k-variété X possède un zéro-cycle de degré 1* : le pgcd des extensions finies L/k avec $X(L) \neq \emptyset$ est 1. Ce théorème s'applique à toute variété fibrée sur $\mathbf{P}^1_k$ dont la fibre générique est birationnelle à un espace homogène de groupe algébrique linéaire à stabilisateurs connexes. Cela étend et recouvre un grand nombre de résultats antérieurs ayant leur source dans un article de Salberger (1988). Un point important dans [4] est l'utilisation des théorèmes de Poitou-Tate sur la cohomologie des tores, qui sont une version tordue de la suite exacte fondamentale pour le groupe de Brauer d'un corps de nombres.

Lorsque $k = \mathbf{Q}$, les résultats de Green, Tao, Ziegler en combinatoire additive, et d'autres résultats de théorie analytique des nombres, ont permis dans les dernières années d'obtenir des énoncés inconditionnels sur les points rationnels (Browning, Mathiesen, Skorobogatov, Harpaz, Wittenberg).

Un type de variété géométriquement rationnelle qui a été beaucoup étudié est donné par les modèles $f : X \to \mathbf{P}^1_k$ d'une hypersurface $Y \subset \mathbf{A}^{d+1}_k$ d'équation affine

$$\mathrm{Norm}_{K/k}(\Xi) = P(t),$$

où K/k est un corps de nombres de degré d et $P(t) \in k[t]$ un polynôme non nul, la fibration f correspondant à la projection sur la coordonnée t.

Théorème (Browning et Matthiesen [2]). *Soit $K/\mathbf{Q}$ une extension finie de degré d, et soit $P(t) = c\prod_{i=1}^{n}(t-e_i) \in \mathbf{Q}[t]$ un polynôme non nul dont toutes les racines sont dans $\mathbf{Q}$. Pour tout modèle projectif et lisse X de l'hypersurface de $\mathbf{A}^{d+1}$ d'équation $\mathrm{Norm}_{K/\mathbf{Q}(\Xi)} = P(t)$, l'ensemble $X(\mathbf{Q})$ est dense dans $X(\mathbb{A}_{\mathbf{Q}})^{\mathrm{Br}}$.*

L'énoncé implique que si $X(\mathbf{Q})$ est non vide, alors $X(\mathbf{Q})$ est dense dans X pour la topologie de Zariski, résultat nouveau pour presque tout n.

References

[1] T.D. Browning, How often does the Hasse principle hold? Notes pour l'École d'été 2015 de l'A.M.S. (Salt Lake City, Utah), disponible à l'adresse https://people.maths.bris.ac.uk/∼matdb/pubs.html

[2] T. D. Browning and L. Matthiesen, Norm forms for arbitrary number fields as products of linear polynomials, Ann. Sc. Éc. Norm. Sup., à paraître, disponible à l'adresse https://arxiv.org/abs/1604.08543

[3] J.-L. Colliot-Thélène, Local-global principle for rational points and zero-cycles, Arizona Winter School, March 2015, disponible à l'adresse http://www.math.u-psud.fr/∼colliot/AWS30MAI2015.pdf

[4] Y. Harpaz et O. Wittenberg, On the fibration method for zero-cycles and rational points, Annals of Math. **183** (2016), no. 1, 229–295.
[5] O. Wittenberg, Rational points and zero-cycles on rationally connected varieties over number fields, rapport à l'École d'été 2015 de l'A.M.S. (Salt Lake City, Utah) disponible à l'adresse https://arxiv.org/abs/1604.08543

On Arithmetic Surjectivity

Alexei N. Skorobogatov
(joint work with Dan Loughran and Arne Smeets)

Given a dominant proper morphism of smooth varieties $X \to Y$ over a number field k, how often is the induced map on k_v-points surjective? We show that the set of such primes v is Frobenian in the sense of Serre and so has a density. We give a necessary and sufficient condition for this set to contain all but finitely many primes of k. This generalises a result of Denef [5, 6] conjectured by Colliot-Thélène [4], which gives a purely algebraic-geometric proof of a celebrated theorem of Ax–Kochen [3].

Our condition is as follows: for any birational modification $X' \to Y'$ of $X \to Y$ the fibres over all points of Y' of codimension 1 must be *pseudo-split* varieties. A (not necessarily irreducible or reduced) scheme Z over a perfect field k is called pseudo-split if every element of the absolute Galois group of k fixes at least one geometrically irreducible component of the smooth locus of Z. In fact, we show that there is a birational modification $X' \to Y'$ such that it is enough to check this condition on Y'. The proof uses log geometry of Kato and Illusie, and a crucial ingredient is the toroidalisation theorem of Abramovich–Karu [1, 2].

References

[1] D. Abramovich and K. Karu. Weak semistable reduction in characteristic 0. *Invent. math.* **139** (2000) 241–273.
[2] D. Abramovich, J. Denef, and K. Karu. Weak toroidalization over non-closed fields. *Manuscripta math.* **142** (2013) 257–271.
[3] J. Ax and S. Kochen. Diophantine problems over local fields. I. *Amer. J. Math.* **87** (1965) 605–630.
[4] J.-L. Colliot-Thélène. Fibre spéciale des hypersurfaces de petit degré. *C. R. Math. Acad. Sci. Paris* **346** (2008), no. 1–2, 63–65.
[5] J. Denef. Proof of a conjecture by Colliot-Thélène. arXiv:1108.6250
[6] J. Denef. Geometric proofs of theorems of Ax–Kochen and Eršov. *Amer. J. Math.* **138** (2016) 181–199.

Analytic Maps on Elliptic Surfaces and Analogues of Hilbert's Tenth Problem for Rings of Analytic Functions

Thanases Pheidas
(joint work with Xavier Vidaux)

Introduction

Let D be any proper superset of $\{0\} \times \mathbb{C} \subseteq \mathbb{C}^2$. A function of two variables, t_1 and t_2, is *analytic* on D if, for any point (a_1, a_2) of D, there is a power series in the pair $(t_1 - a_1, t_2 - a_2)$ of variables, with positive radius of convergence (i.e. there is a positive constant M such that the power series converges for $|t_1 - a_1|, |t_2 - a_2| < M$), and such that the function coincides with the power series on D. A quotient of two analytic functions of the variables t_1 and t_2, both defined on the connected subset $D \subseteq \mathbb{C}^2$, and such that the denominator is not the zero function, is called a *meromorphic function* of the pair (t_1, t_2) on D. We denote by $\mathcal{H}_{t_1,t_2}(D)$ the ring of analytic functions of the pair of variables (t_1, t_2) on D and by $\mathcal{M}_{t_1,t_2}(D)$ the field of meromorphic functions of the pair of variables (t_1, t_2) on D. When D is $\{0\} \times \mathbb{C}$, one extends the above definitions in the usual way.

We consider $\mathcal{H}_{t_1,t_2}(D)$ and $\mathcal{M}_{t_1,t_2}(D)$ as rings and models of the language L_{t_1,t_2} which extends the language L_r of rings $L_r = \{+, \cdot, 0, 1, =\}$ (all the symbols have the usual interpretations) by constant-symbols for the independent variables t_1 and t_2. We would like to know whether the existential theories of $\mathcal{H}_{t_1,t_2}(D)$ and $\mathcal{M}_{t_1,t_2}(D)$ in L_{t_1,t_2} are decidable or undecidbale. At this point we do not know the answer to this question. But here we are announcing the proof of the following relevant result.

For $x \in \mathcal{M}_{t_1,t_2}(D)$ we write $x|_{(t_1,t_2)=(0,0)} = 0$ to indicate the following:

The meromorphic function x, considered as a power series in the variable t_1 (with coefficents in $\mathbb{C}((t_2))$), has no terms with negative exponents, and has a constant term which at $t_2 = 0$ obtains the value 0.

(In other words, x, evaluated first at $t_1 = 0$ and then at $t_2 = 0$, has the value 0).

We define a predicate-symbol Eval which, in the case of $\mathcal{M}_{t_1,t_2}(D)$, we interpret as

$$\text{Eval}(x) \text{ if and only if } x|_{(t_1,t_2)=(0,0)} = 0$$

(so Eval is a one-place predicate), and in the case of $\mathcal{H}_{t_1,t_2}(D)$, we interpret as

$$\text{Eval}(a, b) \text{ if and only if } \tfrac{a}{b}|_{(t_1,t_2)=(0,0)} = 0$$

(so Eval in the structure over $\mathcal{H}_{t_1,t_2}(D)$ is a two-place predicate).

We also define the predicate C (over each of $\mathcal{H}_{t_1,t_2}(D)$ and $\mathcal{M}_{t_1,t_2}(D)$) to stand for the constant functions (so $C(x)$ stands for $x \in \mathbb{C}$).

Let $L_{t_1,t_2,\text{Eval}}$ be the language which extends L_{t_1,t_2} by the predicate Eval and let $L_{t_1,t_2,\text{Eval},C}$ be the language which extends $L_{t_1,t_2,\text{Eval}}$ by the predicate C.

We prove:

Theorem 1.

(1) *The set $\mathbb{Z}$ of rational integers is positive-existentially definable over $\mathcal{H}_{t_1,t_2}(D)$ as an $\mathcal{L}_{t_1,t_2,\mathrm{Eval},C}$-structure. Consequently the positive existential $\mathcal{L}_{t_1,t_2,\mathrm{Eval},C}$-theory of the ring $\mathcal{H}_{t_1,t_2}(D)$ is undecidable.*

(2) *The set $\mathbb{Z}$ of rational integers is positive-existentially definable over $\mathcal{M}_{t_1,t_2}(D)$ as an $\mathcal{L}_{t_1,t_2,\mathrm{Eval},C}$-structure. Consequently the positive existential $\mathcal{L}_{t_1,t_2,\mathrm{Eval},C}$-theory of the field $\mathcal{M}_{t_1,t_2}(D)$ is undecidable.*

When $D = \mathbb{C}^2$, we can get rid of the constants in the language, so we obtain the following corollary:

Corollary 2. *Let $\mathcal{H}_{t_1,t_2}(\mathbb{C}^2)$ be the set of functions of the pair of varables (t_1, t_2) which are analytic as the pair ranges over $\mathbb{C}^2$ and let $\mathcal{M}_{t_1,t_2}(\mathbb{C}^2)$ be its field of fractions. We have:*

(1) *The set $\mathbb{Z}$ of rational integers is positive-existentially definable over $\mathcal{H}_{t_1,t_2}(\mathbb{C}^2)$ as an $\mathcal{L}_{t_1,t_2,\mathrm{Eval}}$-structure. Consequently the positive existential $\mathcal{L}_{t_1,t_2,\mathrm{Eval}}$-theory of the ring $\mathcal{H}_{t_1,t_2}(\mathbb{C}^2)$ is undecidable.*

(2) *The set $\mathbb{Z}$ of rational integers is positive-existentially definable over $\mathcal{M}_{t_1,t_2}(\mathbb{C}^2)$ as an $\mathcal{L}_{t_1,t_2,\mathrm{Eval}}$-structure. Consequently the positive existential $\mathcal{L}_{t_1,t_2,\mathrm{Eval}}$-theory of the field $\mathcal{M}_{t_1,t_2}(\mathbb{C}^2)$ is undecidable.*

The obvious questions that arise from our work are:

Question 1. Is Eval positive-existentially definable over $\mathcal{H}_{t_1,t_2}(\mathbb{C}^2)$ as an $\mathcal{L}_{t_1,t_2}$-structure?

Question 2. Is Eval positive-existentially definable over $\mathcal{M}_{t_1,t_2}(\mathbb{C}^2)$ as an $\mathcal{L}_{t_1,t_2,\mathrm{ord}}$-structure? (where ord stands for the ordinary valuation, namely: $\mathrm{ord}(x)$ if and only if x is analytic at $(0,0)$ and takes the value 0 there)

Of course one may ask the similar questions for general D instead of $\mathbb{C}$, and C in the language.

History of the problem

There should be no need to justify the following as natural questions:

Question 3. Is there an algorithm which, given an algebraic differential equation (in one or more variables), with coefficients in $\mathbb{Z}[z]$, decides whether the equation has or does not have a solution which is a) analytic at $\{0\}$ (i.e. a power series around 0, with positive radius of convergence), b) analytic on some open superset of the unit disc, c) analytic on the whole complex plane (or the proper power of it)?

Unfortunately the answer to (any of) these three questions is negative, due to the observation that for any $n \in \mathbb{C}$ the following holds:

$n \in \mathbb{Z}$ if and only if

there is a power series $x \in \mathbb{C}[[z]] \setminus \{0\}$ (z is a variable) such that $z\frac{dx}{dz} = nx$.

This allows for a definition of the integers in the structure of $\mathbb{C}[[z]]$ (and any subring of it, containing the polynomials over $\mathbb{C}$) together with differentiation - and this produces an undecidability (i.e. no existence of algorithm) result. Of course one also needs to be able to say $n \in \mathbb{C}$ (or be able to define it) and one needs to have a symbol for the independent variable z. The same is true of the existential theory of this structure. (We do not know who thought of this first; we have heard of it from L. Lipshitz as part of the folklore of the area).

Subsequently it seems natural to weaken our requirement and ask the similar question, but only for the existential theory of any of the above rings (of functions analytic, a) at a point, b) on an open or closed disk, and c) on $\mathbb{C}$), without differentiation.

Question 4. Is there an algorithm which, given an algebraic equation (in one or more variables), with coefficients in $\mathbb{Z}[z]$, decides whether the equation has or does not have a solution which is a) analytic at $\{0\}$ (i.e. a power series around 0, with positive radius of convergence), b) analytic on some open superset of the unit disc, c) analytic on the whole complex plane (or the proper power of it)?

So far this problem is open. But the following have been answered:

- The first order theory of the ring of functions of one variable, which are germs of analytic functions at the origin, is decidable ([14]).
- The first order theory of the ring of functions of the variable z, analytic as z ranges over the unit disc (open or closed), considered as a model of the language L_r, is undecidable ([24]).
  The idea of the proof may be seen in the following statement:
  For any $n \in \mathbb{C}$, we have $n \in \mathbb{N}$ if and only if
  there is a function x, analytic on the closed unit disc, such that
  $x[1] = 0 \wedge \forall \rho \in \mathbb{C}\ (x[\frac{1}{\rho}] = 0 \to (x[\frac{1}{\rho+1}] = 0 \vee \rho = n))$.
- J. Denef and M. Gromov proved (in an unpublished manuscript, made available to us by G. Cherlin) that the existential theory of the ring of functions of z, analytic on the open unit disc, in the language $L_{z,C}$, is undecidable — see also [3]. Huuskonen in [12] showed that the set of constant functions is definable over that ring, in a mild extension of the language L_r. Whether there is a positive-existential definition of $\mathbb{C}$ in the language L_r is unclear to us.
- The positive existential theory of the ring of functions of the variable z, analytic on $\mathbb{C}_p$ (the p-adic analogue of $\mathbb{C}$), in the language $L_r \cup \{z\}$, is undecidable ([17]). The similar problem for the field of quotients (i.e. the field of meromorphic functions on $\mathbb{C}_p$) has a negative answer in a language that extends L_z by a predicate for the meromorphic functions which are analytic at $z = 0$ ([27]).
- The first order theory of (possibly transcendental) meromorphic functions of characteristic $p > 2$ is undecidable ([19]).
- Let T denote the non-constant functions (in any set of functions). Consider the language $L_T = L_r \cup \{T\}$ and consider any of the rings of analytic

functions mentioned above as a model of that language. Rubel in [25] (beyond asking many of the above questions) proved that the positive existential theory of the ring of functions of the variable z, analytic on a disc (open or closed) is decidable. The similar question for functions analytic on $\mathbb{C}$ remains open. Notice that in the language L_T one can express positive-existentially the property of a complex variety being 'non-hyperbolic' in the sense of S. Lang's [16] - see [23] for some connections.

- More relevant material can be found in the bibliography below. Beware: the "proof" of the "result" of [21] is wrong. What may be recovered from it is discussed in [22].

1. The main novelty of the proof

We study the solutions $(x, y) \in \mathcal{M}_{\delta,z}(\{-2,\} \times \mathbb{C})^2$ of the Equation

$$(z^3 + \delta z^2 + z)y^2 = x^3 + \delta x^2 + x \tag{1}$$

where δ and z are variables.

Let (x, y) be a solution of Equation 1 with $y \neq 0$. Define

$$\alpha_{xy} = \frac{x-1}{(z-1)y} \ . \tag{2}$$

Our main technical result is

Theorem 3. *As (x, y) ranges over the set of solutions of Equation (1) over $\mathcal{M}_{\delta,z}(\{-2,\} \times \mathbb{C})$, with $y \neq 0$, the set of finite values of α_{xy} at $(z, \delta) = (1, -2)$ (meaning: evaluated first at $z = 1$ and then at $\delta = -2$) contains the odd rational integers and is contained in $\mathbb{Z}$.*

References

[1] M. Artin, *On the solutions of analytic equations*, Invent. Math. **5** (1968), 277–291.

[2] M. Artin, *Algebraic approximation of structures over complete local rings*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 23–58.

[3] J. Becker, C. W. Henson and L. A. Rubel, *First-order conformal invariants*, Annals of Mathematics **112** (1980), 123–178.

[4] F. Delon, *Dans les anneaux de séries formelles à plusieurs indéterminées*, Fundamenta Mathematicae **112-2** (1981), 215–229.

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

[6] J. Denef and M. Gromov, *The ring of analytic functions in the disk has undecidable theory*, 1985 (letter communication by G. Cherlin).

[7] J. Denef and L. Lipshitz, *Power Series solutions of algebraic differential equations*, Mathematische Annalen **267** (1984), 213–238

[8] J. Denef, *Decision problems for differential equations*, Journal of Symbolic Logic **54(3)** (1989), 941–950.

[9] L. van den Dries, *A specialization theorem for analytic functions on compact sets*, Proceedings Kininklijke Nederlandse Academie van Weteschappen (A), **85-4**(1988),391–396.

[10] Hej Iss'sa, *On the meromorphic function field of a Stein variety*, Annals of Mathematics, **83**(1966), 34–46.

[11] C. W. Henson and L. Rubel, *Some applicatons of Nevanlinna Theory to Mathematical Logic: Identities of exponential functions*, Transactions of American Mathematical Society, **282-1**(1984), 1–32; and *Corrections*, same journal, **294-1**(1986), 381.
[12] T. Huuskonen, *Constants are definable in rings of analytic functions*, Proceedings of the American Mathematical Society, 122-3 (1994), 697–702.
[13] K. H. Kim and F. W. Roush, *Diophantine undecidability of* $\mathbb{C}(t_1, t_2)$, Journal of Algebra, **150-1**,(1992), 35–44.
[14] S. Kochen, *The model theory of local fields*, Lecture Notes in Math., 499 (1975)(Proc. Internat. Summer Inst. and Logic Colloq., Kiel, 1974,), Springer, 384–425.
[15] J. Kollar, *Polynomials with integral coefficients equivalent to a given polynomial*, Electronic Research Announcements of AMS, **3** (1997), 17–27.
[16] S. Lang, *Hyperbolic and Diophantine Analysis*, Bulletin of the American Mathematical Society, **14-2** (1986), 159–205.
[17] L. Lipshitz and T. Pheidas, *An analogue of Hilbert's Tenth Problem for p-adic entire functions*, The Journal of Symbolic Logic, **60-4** (1995), 1301-1309
[18] Y. Matijasevich, *Enumerable sets are diophantine*, Doklady Akademii Nauka SSSR, **191** (1970), 272–282.
[19] H. Pasten, *Definability of Frobenius orbits and a result on rational distance sets*, Monatsh Math (2016), doi:10.1007/s00605-016-0973-2
[20] Th. Pheidas, *Extensions of Hilbert's tenth problem*, Journal of Symbolic Logic, **59-2** (1994),372–397.
[21] Th. Pheidas, *The diophantine theory of a ring of analytic functions*, Journal fur die reine und angewandte Mathematik, **463** (1995), 153–167.
[22] Th. Pheidas and K. Zahidi, *Undecidability of existential theories of rings and fields: A survey*, Contemporary Mathematics **270** (2000), 49–106.
[23] Th. Pheidas and K. Zahidi, *Analogues of Hilbert's tenth problem*, Model theory with Applications to Algebra and Analysis Vol. 2 (Eds. Zoe Chatzidakis, Dugald Macpherson, Anand Pillay, Alex Wilkie), London Math Soc. Lecture Note Series Nr 250, Cambridge Univ Press, 2008.
[24] R. Robinson, *Undecidable rings*, Transactions of the American Mathematical Society **70** (1951), 137.
[25] L. Rubel, *An essay on diophantine equations for analytic functions*, Expositiones Mathematicae, **14** (1995), 81–92.
[26] A. Shlapentokh, *Hilbert's Tenth Problem of algebraic functions of characteristic 0*, Journal of Number Theory, **40-2** (1992), 218–236.
[27] X. Vidaux, *An analogue of Hilbert's 10th problem for fields of meromorphic functions over non-Archimedean valued fields*, Journal of Number Theory **101** (2003), 48–73 (and Thesis, University of Angers, 2002).

Northcott Number and Undecidability of Certain Algebraic Rings

Martin Widmer

In this report we discuss the Property (N), the Northcott number, and a connection, recently observed by Vidaux and Videla, between the former and the undecidability of certain rings of algebraic numbers.

Throughout this note K denotes a subfield of the algebraic numbers $\overline{\mathbb{Q}}$, and $\mathcal{O}_K$ denotes the ring of integers of K. We write $K^{(d)}$ for the composite field of all extensions of K of degree at most d, $K_{ab}^{(d)}$ for the maximal abelian subextension of $K^{(d)}/K$, and K_{tr} for the maximal totally real subfield of K. Let $H(\cdot)$ denote the absolute multiplicative Weil height on $\overline{\mathbb{Q}}$.

1. Property (N)

Following Bombieri and Zannier, we say a subset A of $\overline{\mathbb{Q}}$ has Property (N) if for every $X \geq 1$

$$|\{\alpha \in A; H(\alpha) < X\}| < \infty.$$

Already back in 1949 Northcott showed that sets of uniformly bounded degree (over $\mathbb{Q}$), in particular number fields, have Property (N). In fact, as observed by Dvornicich and Zannier [4], a slight modification of Northcott's original argument shows that the ground field $\mathbb{Q}$ can be replaced by any field K with Property (N). In 2001 Bombieri and Zannier [1] asked which fields of infinite degree (if any) have Property (N). This is a difficult widely open problem, and all known examples stem from one of the following two criteria.

Theorem 1 (Bombieri, Zannier 2001)**.** *Let k be a number field, and let d be a positive integer. Then $k_{ab}^{(d)}$ has Property (N).*

In conjunction with work of Checcoli [2] this implies that any realisation (over $\mathbb{Q}$) of an abelian group with finite exponent has Property (N). Another criterion for Property (N) was given by the author in 2011.

Theorem 2 ([11])**.** *Let k be a number field, let $k = k_0 \subsetneq k_1 \subsetneq k_2 \subsetneq \ldots$ be a nested sequence of finite extensions, and set $K = \bigcup_i k_i$. Suppose that*

$$\inf_{k_{i-1} \subsetneq M \subseteq k_i} \left(\frac{|\Delta_M|^{\frac{1}{[M:k_{i-1}]}}}{|\Delta_{k_{i-1}}|} \right)^{\frac{1}{[M:k_0]}} \longrightarrow \infty$$

as i tends to infinity where the infimum is taken over all intermediate fields M strictly larger than k_{i-1}, and Δ_{k_i} denotes the discriminant of k_i. Then the field K has Property (N).

In particular, for $d_i \in \mathbb{N}$ the field $\mathbb{Q}(2^{1/d_1}, 3^{1/d_2}, 5^{1/d_3}, 7^{1/d_4}, \ldots)$ has Property (N) if and only if the sequence $(\log 2)/d_1, (\log 3)/d_2, (\log 5)/d_3, (\log 7)/d_4, \ldots$ tends to infinity (cf. [11]). Theorem 2 also implies that if $\{G_i\}$ is a sequence of finite solvable groups then there exists a realisation of $\prod_i G_i$ (over $\mathbb{Q}$) with Property (N) (cf. [3, Theorem 4]).

A natural candidate to look at is the field $\mathbb{Q}^{(d)}$ which was explicitly addressed by Bombieri and Zannier.

Question 1 (Bombieri, Zannier 2001)**.** Let d be a positive integer. Does $\mathbb{Q}^{(d)}$ have Property (N)?

Although some progress on this question has been made (cf. [5, 11]) the question remains open for all $d \geq 3$.

2. The Northcott number

The concept of Property (N) was recently refined by Vidaux and Videla [8]. They introduced the Northcott number $N(A)$ of a subset A of $\overline{\mathbb{Q}}$ defined by

$$N(A) = \inf_{t\in\mathbb{R}}\{t; |\{\alpha \in A; H(\alpha) < t\}| = \infty\},$$

and they proposed the following question.

Question 2 (Vidaux, Videla 2016)**.** Which real numbers can be realised as Northcott numbers of ring extensions of $\mathbb{Q}$?

The arguments from the proof of Theorem 2 easily provide the following result.

Theorem 3. *For any $t \geq 1$ there exists a field $K \subset \overline{\mathbb{Q}}$ with*

$$t \leq N(K) \leq N(\mathcal{O}_K) \leq t^2.$$

3. Undecidability and connections to Property (N)

We say an enumerable ring R is decidable if its full first order theory in the language $\mathcal{L} = (\cdot, +, -, 0, 1)$ of rings is decidable. If R is not decidable we say R is undecidable. Gödel has shown that $\mathbb{Z}$ is undecidable. By showing that $\mathbb{Z}$ is definable in R by a first order formula (from now on we drop "by a first order formula") J.Robinson [6, 7] has shown that number fields, their ring of integers, $\mathcal{O}_{\mathbb{Q}_{tr}^{(2)}}$, and $\mathcal{O}_{\overline{\mathbb{Q}}_{tr}}$ are all undecidable. Interestingly $\overline{\mathbb{Q}}_{tr}$ is decidable as shown by Fried, Haran and Völklein. Other examples of decidable subrings of $\overline{\mathbb{Q}}$ are $\mathcal{O}_{\overline{\mathbb{Q}}}$ (van den Dries) and $\overline{\mathbb{Q}}$ (Tarski).

For a totally real ring $\mathcal{O} \subseteq \overline{\mathbb{Q}}$ Julia Robinson [7] considered the quantity

$$JR(\mathcal{O}) = \inf_{t\in\mathbb{R}}\{t; |\{\alpha \in \mathcal{O}; 0 \ll \alpha \ll t\}| = \infty\}$$

where $0 \ll \alpha \ll t$ means $0 < \sigma(\alpha) < t$ for all conjugates $\sigma(\alpha)$ over $\mathbb{Q}$.

Only little is known about the possible values of $JR(\cdot)$ (see, e.g., [8]). Following Vidaux and Videla [8], we say that $\mathcal{O}$ has Property (JR) if either $JR(\mathcal{O}) = \infty$ or the infimum is attained.

Theorem 4 (J. Robinson 1962)**.** *Let K be a totally real subfield of $\overline{\mathbb{Q}}$, and suppose $\mathcal{O}_K$ has Property (JR). Then $\mathbb{Z}$ is definable in $\mathcal{O}_K$, and hence $\mathcal{O}_K$ is undecidable.*

This criterion allowed her in particular to deduce that $\mathcal{O}_{\mathbb{Q}_{tr}^{(2)}}$ is undecidable. Videla [10] has shown that if $\mathcal{P}$ is a finite set of rational primes and $K/\mathbb{Q}$ is a pro-$\mathcal{P}$ Galois extension then $\mathcal{O}_K$ is definable in K. In particular, $\mathcal{O}_{\mathbb{Q}_{tr}^{(d)}}$ is definable in $\mathbb{Q}_{tr}^{(d)}$. As $\mathcal{O}_{\mathbb{Q}_{tr}^{(2)}}$ is undecidable it follows that $\mathbb{Q}_{tr}^{(2)}$ is undecidable.

Vidaux and Videla noticed a connection between Property (N) and Property (JR).

Theorem 5 (Vidaux, Videla 2016)**.** *If K is a totally real subfield of $\overline{\mathbb{Q}}$ and $\mathcal{O}_K$ has Property (N) then $\mathcal{O}_K$ has Property (JR). In particular, $\mathcal{O}_K$ is undecidable.*

The proof of this interesting observation is an immediate consequence of Theorem 4: if $t > 1$ and α is a totally real algebraic integer with $0 \ll \alpha \ll t$ then $H(\alpha) < t$. In particular, $JR(\mathcal{O}) = \infty$ whenever $\mathcal{O}$ has Property (N).

Thus, the undecidability of $\mathcal{O}_{\mathbb{Q}_{tr}^{(d)}}$ (and hence of $\mathbb{Q}_{tr}^{(d)}$) would follow from an affirmative answer to Question 1. However, the latter seems very difficult; the following question looks a bit more promising, and clearly a positive answer here would be sufficient as well.

Question 3. Does $\mathcal{O}_{\mathbb{Q}_{tr}^{(d)}}$ have Property (N)?

Recall that the house $\boxed{\cdot}$ of an algebraic number is the maximum modulus of its conjugates (over $\mathbb{Q}$). Note that for every non-zero algebraic integer α we have $\boxed{\alpha} \geq H(\alpha)$; moreover, the house is easier to control than the height. Thus, even more promising, and still sufficient for the undecidability of $\mathcal{O}_{\mathbb{Q}_{tr}^{(d)}}$ and $\mathbb{Q}_{tr}^{(d)}$, would be to establish a Property (N) (but with respect to the house) for the ring $\mathcal{O}_{\mathbb{Q}_{tr}^{(d)}}$.

Question 4. Is $|\{\alpha \in \mathcal{O}_{\mathbb{Q}_{tr}^{(d)}}; \boxed{\alpha} < X\}| < \infty$ for all $X \geq 1$?

References

[1] E. Bombieri and U. Zannier, *A Note on heights in certain infinite extensions of* $\mathbb{Q}$, Rend. Mat. Acc. Lincei, **12** (2001), 5–14.

[2] S. Checcoli, *Fields of algebraic numbers with bounded local degrees and their properties*, Trans. Amer. Math. Soc., **365** (4) (2013), 2223–2240.

[3] S. Checcoli and M. Widmer, *On the Northcott property and other properties related to polynomial mappings*, Math. Proc. Cam. Philos. Soc., **155** (1) (2013), 1–12.

[4] R. Dvornicich and U. Zannier, *On the properties of Northcott and Narkiewicz for fields of algebraic numbers*, Functiones et Approximatio, **39** (2008), 163–173.

[5] L. Pottmeyer, *Heights and totally p-adic numbers*, Acta Arith., **171** (3) (2015), 277–291.

[6] J. Robinson, *The undecidability of algebraic rings and fields*, Proc. Amer. Math. Soc. **10** (1959) 950–957.

[7] J. Robinson, *On the decision problem for algebraic rings*, in Studies in Mathematical Analysis and Related Topics, ed. by G. Szegö (Stanford University Press, Stanford, 1962), 297–304.

[8] X. Vidaux and C. R. Videla, *Definability of the natural numbers in totally real towers of nested square roots*, Proc. Amer. Math. Soc. **48** (1) (2016), 58–62.

[9] X. Vidaux and C. R. Videla, *A note on the Northcott property and undecidability*, Bull. London Math. Soc. **143** (10) (2015), 4463–4477.

[10] C. R. Videla, *Definability of the ring of integers in pro-p Galois extensions of number fields*, Israel J. Math. **118** (2000), 1–14.

[11] M. Widmer, *On certain infinite extensions of the rationals with Northcott property*, Monatsh. Math. **162** (3) (2011), 341–353.

Model Theory of the j Function

Sebastian Eterović

Our aim is to show a generic transcendence property for the j function in the spirit of Schanuel's conjecture (see conjecture (S) of [1]). Such a result is proved in Theorem 1.2 of [2] for the exponential function in the context of exponential fields. This result relies heavily on Theorem 3 of [1] (the so-called Ax-Schanuel

theorem). In [4], the authors prove an analogous Ax-Schanuel theorem for the j function, and so it was natural to wonder if a similar strategy to that used in [2] would provide a transcendence result for j. This is the subject of the talk.

First we introduce the notion of j-fields (in analogy to the way exponential fields are defined in [3]). Given a field K, for any subfield F of K there is an action of $\mathrm{GL}_2(F)$ on $\mathbb{P}^1(K) = K \cup \{\infty\}$, given by:

$$gx = \frac{ax+b}{cx+d},$$

where $g \in \mathrm{GL}_2(F)$ is represented by $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Whenever we say that $\mathrm{GL}_2(F)$ acts on K, it will be in this manner. Throughout, let $G = \mathrm{GL}_2(\mathbb{Q})$ and let $\{\Phi_N(X,Y)\}$ denote the family of modular polynomials.

Definition 1. A *j-field* is a two-sorted structure $\langle K, D, j, j', j'', j''' \rangle$, where K is a field of characteristic zero, and D is a subset of K disjoint from $\mathbb{Q}$ which is closed under the action of G. The maps $j, j', j'', j''' : D \to K$ satisfy:

- The function identity
$$\frac{j'''}{j'} - \frac{3}{2}\left(\frac{j''}{j'}\right)^2 + \left(\frac{j^2 - 1968j + 2654208}{2j^2(j-1728)^2}\right)(j')^2 = 0.$$
- The axiom scheme: for all $z_1, z_2 \in D$, if $z_1 = gz_2$, then $\Phi_N(j(z_1), j(z_2)) = 0$. Given g there is a way to obtain the value of N needed for this axiom. We also include as axioms the algebraic expressions that can be obtained by deriving the modular polynomials.
- The axiom scheme: for every $z_1, z_2 \in D$, if $\Phi_N(j(z_1), j(z_2)) = 0$, then $\bigvee_{g \in G} gz_2 = z_1$. Note that for this axiom we need to allow formulae with a countable number of disjunctions.

Traditionally, the j function is understood as a modular function defined on the upper-half plane, but we extend it to be defined on the upper and lower half planes so that $j : \mathbb{H}^+ \cup \mathbb{H}^- \to \mathbb{C}$. Given $z \in \mathbb{H}^-$ we define $j(z) := \overline{j(\overline{z})}$, where $\overline{z}$ is the complex conjugate of z (even though the symbol is the same, it should be clear from context when we use $\overline{z}$ to denote complex conjugate or a tuple of elements). Given that we are interested in transcendence properties of j, then it does not matter if we extend the domain of j in the way we have done.

One of the versions of the Ax-Schanuel theorem for j (Theorem 1.3 of [4]) is given in a differential setting, which turns out to be more helpful for our purposes. This is why we need to introduce the notion of j-derivations.

Definition 2. Let (K, D) be a j-field. A map $\partial : K \to K$ is a called a *j-derivation* if it satisfies for every $a, b \in K$ and $z \in D$:

- $\partial(a+b) = \partial(a) + \partial(b)$.
- $\partial(ab) = a\partial(b) + b\partial(a)$.
- $\partial(j(z)) = j'(z)\partial(z), \quad \partial(j'(z)) = j''(z)\partial(z), \quad \partial(j''(z)) = j'''(z)\partial(z)$.

For $C \subseteq K$, Let $j\mathrm{Der}(K/C)$ be the set of j-derivations $\partial : K \to K$ satisfying $\partial(c) = 0$ for every $c \in C$. Note that all these spaces are K-vector spaces. These derivations define a natural pregeometry as follows. Let $C \subseteq K$, and $a \in K$. We say that a belongs to the *j-closure* of C, denoted $a \in j\mathrm{cl}(C)$, if for every $\partial \in j\mathrm{Der}(K/C)$ we have that $\partial(a) = 0$.

Now we can state our main result. The notation we use is as follows: for A and B subsets of a given field of characteristic zero, we write $\mathrm{t.d.}(A/B)$ to denote the transcendence degree of the field extension $\mathbb{Q}(A)/\mathbb{Q}(B)$. Given some elements $z_1, \ldots, z_n$ in the field, we write $\overline{z}$ to denote the tuple $(z_1, \ldots, z_n)$, and if f is a function, then $f(\overline{z})$ denotes the tuple $(f(z_1), \ldots, f(z_n))$. Finally, given a subfield F of K, let $G^F := \{g \in \mathrm{GL}_2(F) : gD \subseteq D\}$.

Theorem 3 (General Main Theorem)**.** *Let (K, D) be a j-field and $C \subseteq K$ be $j\mathrm{cl}$-closed. Let $\lambda_1, \ldots, \lambda_m, z_1, \ldots, z_n \in D$ be such that they do not contain zeros of j'''. Suppose $\lambda_1, \ldots, \lambda_m$ are $j\mathrm{cl}$-independent over C, and $z_1, \ldots, z_n$ are in different G-orbits. Let $F = \mathbb{Q}(\overline{\lambda})$. Let $g \in G^F \setminus G$ be a non-scalar matrix such that $g\overline{z}$ does not include zeros of j'''. Then:*

$$\mathrm{t.d.}\,(j(\overline{z}), j'(\overline{z}), j''(\overline{z}), j(g\overline{z}), j'(g\overline{z}), j''(g\overline{z})/F, C) \geq 3n.$$

The condition on j''' not vanishing comes from the hypothesis of the Ax-Schanuel theorem for j. However, in the case of $\mathbb{C}$, using the fact that the zero of any holomorphic function have finite order, we obtain the following enhancement.

Corollary 4. *Let $\lambda_1, \ldots, \lambda_m \in \mathbb{H}^+ \cup \mathbb{H}^-$ be $j\mathrm{cl}$-independent. Let $F = \mathbb{Q}(\overline{\lambda})$ and let $z_1, \ldots, z_n \in \mathbb{H}^+ \cup \mathbb{H}^-$ be in different G-orbits. Let $g \in (\mathrm{GL}_2(\mathbb{R}) \cap \mathrm{GL}_2(F)) \setminus G$ be a non-scalar matrix. Then:*

$$\mathrm{t.d.}\,(j(\overline{z}), j'(\overline{z}), j''(\overline{z}), j(g\overline{z}), j'(g\overline{z}), j''(g\overline{z})/F) \geq 3n.$$

Loosely, this should be understood as: if the entries of g are sufficiently generic (transcendental with respect to j), then we obtain the above transcendence result for j and its derivatives. Using o-minimality, we can prove that there are uncountably many values for the λ_i that can be used, although unfortunately no explicit values are known.

We have succeeded in obtaining a transcendence property, but there are still a couple of questions that remain open and that could be the subject of future work.

- Is the inequality of Theorem 3 sharp? Some modular versions of Schanuel's conjecture say that the answer to this should be no. Of course, a proof of such a conjecture is considered to be out of reach, and so we ask whether there is a method to improve the inequality short of proving the modular Schanuel conjectures.
- Is there a more explicit description of the pregeometry $j\mathrm{cl}$? In the case of exponential fields it turns out that the pregeometry defined by exponential derivations agrees with the pregeometry defined by Khovanskii systems (which is a non-degenerate system of equations of exponential polynomials). However, this is not yet known as the strategy used for exponential

fields that relies too much on the properties of the exponential map, and so the same mehtod cannot be transfered to the j function.

References

[1] James Ax. On Schanuel's Conjecture. *Ann. of Math. (2)*, **93**, (1971), 252–268.

[2] Martin Bays, Jonathan Kirby, A.J. Wilkie. A Schanuel Property for Exponentially Transcendental Powers. *Bulletin of the London Mathematical Society*, **42**, (2010), 917–922.

[3] Jonathan Kirby. Exponential algebraicity in exponential fields. *Bulletin of the London Mathematical Society*, **42**(5), (2010), 879–890.

[4] Jonathan Pila, Jacob Tsimerman. Ax-Schanuel for the j-Function. *Duke Mathematical Journal*, DOI 10.1215/00127094-3620005, (2016).

Undecidability for the Perfect Closure of Function Fields of Positive Characteristic

Kirsten Eisenträger

Hilbert's Tenth Problem in its original form can be stated in the following form: find a uniform algorithm that determines, given a multivariate polynomial equation with integer coefficients, whether the equation has an integer solution or not.

In [3] Matiyasevich proved that no such algorithm exists, *i.e.* that Hilbert's Tenth Problem is undecidable. Since then various analogues of this problem have been studied by considering the same problem as above for polynomial equations with coefficients and solutions over some other commutative ring R. While Hilbert's Tenth Problem over $\mathbb{Q}$, and over number fields in general, is still wide open, diophantine undecidability has been proved for function fields of curves over finite fields and also for some infinite extensions of $\mathbb{F}_p(t)$ (see [4], [7], [5], [6], [1]).

To our knowledge, Hilbert's Tenth Problem is not known to be undecidable for a field that is not finitely generated over its constant field. A natural candidate for a field with this property and for which Hilbert's Tenth Problem might be undecidable is the perfect closure of a global field of positive characteristic. The perfect closure of a field k of characteristic $p > 0$ is obtained by adjoining p^n-th roots of all elements of k for all $n \geq 1$.

Our goal was to prove that Hilbert's Tenth Problem is undecidable for the perfect closure of any global field of positive characteristic. Currently, we are only able to prove the following weaker theorem.

Theorem 1. *Let K be the perfect closure of a global field k of odd characteristic. The first-order theory of K is undecidable.*

Let $q = p^m$ for some prime p and some integer $m \geq 1$. In the simplest case, namely when the global field is $\mathbb{F}_q(t)$, we obtain $\mathbb{F}_q(t, t^{1/p}, t^{1/p^2}, t^{1/p^3}, \dots)$ as the perfect closure.

A first attempt to prove that Hilbert's Tenth Problem for K is undecidable would be to follow Pheidas' approach for Hilbert's Tenth Problem over $\mathbb{F}_q(t)$ (see [4]). Several of the main theorems in Pheidas' proof for rational function fields can also be proved for the perfect closure. For example, Pheidas proved that

$\{x \in \mathbb{F}_q(t) : \mathrm{ord}_t(x) \geq 0\}$ is diophantine over $\mathbb{F}_q(t)$. Here ord_t is the discrete valuation on $\mathbb{F}_q(t)$ with uniformizer t. In [2] the analogous statement was proved for the perfect closure K of a global function field k of odd characteristic: it was shown that the set of all elements of the perfect closure K that are integral at some prime $\mathfrak{p}$ of K is diophantine over K.

One big difference in proving undecidability for the perfect closure is that the value group for the valuation on the perfect closure K is now $\mathbb{Z}[1/p] = \{a/p^m : a \in \mathbb{Z}, m \in \mathbb{Z}_{\geq 0}\}$, while the value group of the valuation ord_t on $\mathbb{F}_q(t)$ is $\mathbb{Z}$.

References

[1] Kirsten Eisenträger. Hilbert's Tenth Problem for algebraic function fields of characteristic 2. *Pacific J. Math.*, 210(2):261–281, 2003.

[2] Kirsten Eisenträger. Integrality at a prime for global fields and the perfect closure of global fields of characteristic $p > 2$. *J. Number Theory*, 114(1):170–181, 2005.

[3] Ju. V. Matiyasevich. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191:279–282, 1970.

[4] Thanases Pheidas. Hilbert's tenth problem for fields of rational functions over finite fields. *Invent. Math.*, 103(1):1–8, 1991.

[5] Alexandra Shlapentokh. Diophantine undecidability over algebraic function fields over finite fields of constants. *J. Number Theory*, 58(2):317–342, 1996.

[6] Alexandra Shlapentokh. Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic. *Pacific J. Math.*, 193(2):463–500, 2000.

[7] Carlos R. Videla. Hilbert's tenth problem for rational function fields in characteristic 2. *Proc. Amer. Math. Soc.*, 120(1):249–253, 1994.

Resplendent Minimality

Raf Cluckers

(joint work with Immanuel Halupczok, Silvain Rideau)

We introduce a new tameness notion for valued fields, tentatively called resplendent minimality, but a name like 'expansion minimality' may be more adequate. This notion resembles o-minimality for the real field in the sense that it can be easily verified from quantifier elimination, and that it has several strong consequences.

Resplendency can mean that a result is maintained after adding structure of a certain kind. Forms of minimality usually mean that unary definable sets are controlled in some way by a finite set (like a set of boundary points in o-minimality). It are these meanings that are pertained in our new notion of resplendent minimality, intended for valued fields but, mutatis mutandis, possibly interesting in other contexts as well. The goals of our notion are three-fold: easy verifiability, broad applicability, and strong consequences.

Let us explain how unary sets look like and how they are controlled by a finite set. Let K be a valued field with valuation ring $\mathcal{O}_K$ and maximal ideal $\mathcal{M}_K$. By a proper ideal of $\mathcal{O}_K$ we mean an ideal which is nonzero and which is different from $\mathcal{O}_K$. Let I be a proper ideal of $\mathcal{O}_K$, and consider the quotient group $K^\times/1+I$.

The disjoint union of this quotient with $\{0\}$ is denoted by RV_I, with natural map $rv_I : K \to RV_I$ which sends 0 to 0 and nonzero x to its image in the quotient.

Definition 1. Let X and C be subsets of K with C finite. Say that the set X is I-prepared by C if for all x and y in K such that

$$rv_I(x-c) = rv_I(y-c) \text{ for each } c \in C, \tag{1}$$

one either has $x \in X$ and $y \in X$, or, one has $x \notin X$ and $y \notin X$.

Our notion of resplendent minimality is based on the preparability of unary definable sets, even when the definability is allowed to be in expansions of certain kinds.

As some of the main results based on the notion, we develop a dimension theory, a property called Jacobian property, and we show that some classical structures like the variant of the language of valued fields known as Basarab's language [1] as well as subanalytic expansions [2] are resplendently minimal.

References

[1] Ş. Basarab, *Relative elimination of quantifiers for Henselian valued fields*, Ann. Pure Appl. Logic **53**, No. 1 (1991), 51–74.

[2] R. Cluckers, L. Lipshitz, *Fields with Analytic Structure*, J. Eur. Math. Soc. **13** (2011), 1147–1223.

Effective Finiteness Results for Diophantine Equations Over Finitely Generated Domains

Kálmán Győry

Matijasevich gave a *negative* answer for Hilbert's Tenth Problem by showing that there is no universal algorithm for deciding the solvability of any polynomial Diophantine equation over $\mathbb{Z}$. Many mathematicians investigated the possibility to provide a *positive* answer in case of important classes of diophantine equations or, more generally, give algorithms for finding, at least in principle, all the solutions over $\mathbb{Z}$ or over more general domains.

In the 1960s, A. Baker established several effective finiteness theorems over $\mathbb{Z}$ for various important classes of Diophantine equations in two unknowns, including Thue equations, hyper- and superelliptic equations and equations of genus 1. By means of his effective method concerning logarithmic forms, he gave explicit upper bounds for the solutions which made it possible, at least in principle, to determine all the solutions. Many people improved Baker's results and generalized them to equations over number fields. In the 1970s we obtained, over number fields, effective finiteness results for unit and S-unit equations as well as for discriminant form equations, index form equations and for a large class of norm form equations in an arbitrary number of unknowns. In the 1980s we worked out an effective specialization method to extend the effective theory of Diophantine equations over number fields to the more general case when the ground ring belongs to a large and important class of finitely generated domains over $\mathbb{Z}$ (which may contain

transcendental elements, too). Recently, we refined with J. H. Evertse the method mentioned and generalized the effective theory to the case of *arbitrary* ground domains finitely generated over $\mathbb{Z}$.

In my talk, first I gave a brief overview of the most important effective finiteness results over number fields. Then I presented our effective generalizations with Evertse to the case of equations over finitely generated domains.

Model Theory and Zeta Functions

Jamshid Derakhshan

Let $\phi(x_1, \ldots, x_n)$ be a formula (over $\mathbb{Q}$) of the language of rings or the languages of valued fields by Basarab-Kuhlmann and Denef-Pas, let $f(\bar{x})$ be a definable function. Let dx denote a normalized Haar measure on $\mathbb{Q}_p^n$. Consider the p-adic integral $Z(p,s) := \int_{X_p} |f(\bar{x})|^s dx$, where s is a complex variable, and X_p denotes the set $\{(x_1, \ldots, x_n) \in \mathbb{Q}_p^n : \phi(x_1, \ldots, x_n) \text{ holds in } \mathbb{Q}_p\}$. These integrals are generalizations of Igusa's local zeta functions. Denef proved that they are rational functions in p^{-s}, and uniformities in the rationality as p varies was proved by several authors (see [2]). I have considered the case of an Euler product over primes of such integrals. This is a global zeta function.

Theorem 1. *Consider the integrals $Z(p,s)$ defined as above. Consider the Euler product over primes $Z(s) := \prod_p Z(p,s)$. Assume that $Z(s)$ converges in some half-plane in $\mathbb{C}$. Then the abscissa of convergence of $Z(s)$ is a rational number α, and $Z(s)$ admits meromorphic continuation to the half-plane $\{s \in \mathbb{C} : Re(s) > \alpha - \delta\}$ for some $\delta > 0$. The extended function has only a pole at $s = \alpha$ on the line $Re(s) = \alpha$.*

As a corollary we obtain:

Corollary 2. *Suppose that a Dirichlet series $Z(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ can be represented as an Euler product as in Theorem 1. Then there is $c \in \mathbb{R}$ such that*

$$a_1 + \cdots + a_N \sim N^{\alpha} (logN)^{w-1}$$

as $N \to \infty$, where w is the order of the pole of $Z(s)$ at α.

Theorem 1 generalizes work of du Sautoy-Grunewald [3] on zeta functions counting subgroups of finite index in finitely generated nilpotent groups.

Given an algebraic group G defined over $\mathbb{Q}$, let c_m denote the number of conjugacy classes in the group $G(\mathbb{Z}/m\mathbb{Z})$. Consider the series $\sum_{n=1}^{\infty} c_m m^{-s}$. It turns out to have an Euler product representation as in Theorem 1 for some formulas of the Denef-Pas language. Theorem 1 yields an asymptotic formula for the growth of the partial sums of the c_m. This solves a problem of U. Onn. There are other applications of Theorem 1 to questions on subgroup growth and representation growth (studying the number of irreducible complex representations) of groups.

Turning to number-theoretic applications, Manin has conjectured similar asymptotic formulas for the number of rational points of bounded height on algebraic

varieties. There are many proved cases of Manin's conjecture, and one powerful method, introduced by Rudnick and Sarnak, and followed by Gorodnick and Oh uses integration on the adele space of the variety and ergodic theory to reduce the conjecture to the meromorphic continuation of the adelic height zeta function on the adelic space of the variety. In this way, Theorem 1 can be used to count rational points of bounded height in orbits of group actions, answering a question in [1].

The proof of Theorem 1 uses motivic integration and results on the model theory of finite and pseudo-finite fields by Ax and Chatzidakis-van den Dries-Macintyre, together with some algebraic geometry and number theory.

References

[1] Oh, H. Orbital counting via mixing and unipotent flows. In *Homogeneous flows, moduli spaces and arithmetic*, vol. 10 of *Clay Math. Proc.* Amer. Math. Soc., Providence, RI, 2010, pp. 339–375.

[2] Denef, J., and Loeser, F. Definable sets, motives, and p-adic integrals. *J. Amer. Math. Soc. 14*, 2 (2001), 429–469.

[3] du Sautoy, M. P. F., and Grunewald, F. Analytic properties of zeta functions and subgroup growth. *Ann. of Math. 152* (2000), 793 – 833.

Hilbert's Tenth Problem on Subrings of $\mathbb{Q}$

Russell Miller

Each subring of the field $\mathbb{Q}$ of rational numbers is characterized by the set of prime numbers which have inverses in the subring. We write R_W for the subring $\mathbb{Z}[\frac{1}{p} : p \in W]$, where W can be any subset of the set $\mathbb{P}$ of all primes. Therefore we can endow it with the usual topology on the power set $\mathcal{P}(\mathbb{P})$, making the set of all subrings of $\mathbb{Q}$ into a topological space, which we now describe.

An element W of $\mathcal{P}(\mathbb{P})$ can be viewed either as a subset of $\mathbb{P}$, or as a *path* through the complete binary tree, or as a countable infinite binary sequence. For example, the subset W_3 containing all primes congruent to 3 mod 4 corresponds to the sequence $01011001101\cdots$, indicating that $p_0 \notin W_3$, $p_1 \in W_3$, $p_2 \notin W_3$, and so on. (Here, of course, $2 = p_0 < p_1 < p_2 < \cdots$ lists all primes in order.) The standard basis for the usual topology on $\mathcal{P}(\mathbb{P})$ contains the sets

$$\mathcal{U}_\sigma = \{W \in \mathcal{P}(\mathbb{P}) : \sigma \text{ is an initial segment of } W\},$$

where σ ranges over all finite binary sequences. Thus $\mathcal{U}_{010}$ contains exactly those $W \subseteq \mathbb{P}$ with $2 \notin W$, $3 \in W$, and $5 \notin W$, for instance, and so $W_3 \in \mathcal{U}_{010}$. Under this topology, $\mathcal{P}(\mathbb{P})$ is homeomorphic to the *Cantor set*, the well-known subset of the unit interval with "middle thirds" omitted. Thus our topology on the space of all subrings of $\mathbb{Q}$ makes it a compact, totally disconnected space which has the property of Baire: no nonempty open set is meager. It is also naturally endowed with a measure: one defines $\mu(U_\sigma) = 2^{-|\sigma|}$, and extends to get the *Lebesgue measure* on the space. Under this measure, $\mu(\mathcal{U})$ represents the probability that a subring R_W lies in $\mathcal{U}$ if the set W is chosen by flipping independent coins to decide

which primes lie in W. Notice that this is *not* equal to Lebesgue measure on the middle-thirds set as a subset of $\mathbb{R}$; indeed the Cantor set has measure 0 within $\mathbb{R}$.

We wish to use this topology to study Hilbert's Tenth Problem on subrings of $\mathbb{Q}$, defining $\mathrm{HTP}(R) = \{i \in \mathbb{N} : f_i = 0 \text{ has a solution in } R\}$ under a fixed enumeration $f_0, f_1, \ldots$ of $\mathbb{Z}[X_0, X_1, \ldots]$. For each f_i, we set $\mathcal{A}(f_i) = \{W \subseteq \mathbb{P} : f_i \in \mathrm{HTP}(R_W)\}$. Notice that $\mathcal{A}(f_i)$ must be open: if $W \in \mathcal{A}(f_i)$, then $\mathcal{U}_\sigma \subseteq \mathcal{A}(f_i)$, provided we choose an initial segment $\sigma \subseteq W$ long enough to ensure that each prime used in the solution to f_i in R_W lies in every $V \in \mathcal{U}_\sigma$.

We will also consider $\mathcal{C}(f_i)$, the interior of the complement of $\mathcal{A}(f_i)$, and $\mathcal{B}(f_i) = \mathcal{P}(\mathbb{P}) - \mathcal{A}(f_i) - \mathcal{C}(f_i)$, the *boundary* of $\mathcal{A}(f_i)$. $\mathcal{C}(f_i)$, being open, is also given by finitary conditions: if $W \in \mathcal{C}(f_i)$, then $\mathcal{U}_\sigma \cap \mathcal{A}(f_i) = \emptyset$ for some $\sigma \subseteq W$, and so the semilocal ring $R_{\mathbb{P}-\sigma^{-1}(0)}$ has no solution to f_i, since it belongs to U_σ. This means that some finite subset of the complement $\overline{W}$ (namely $\sigma^{-1}(0)$) is sufficient to rule out all possible rational solutions to f_i.

It follows that, for every i, the set $\mathrm{HTP}(\mathbb{Q})$ contains enough information to decide, for each σ, whether $\mathcal{U}_\sigma \subseteq \mathcal{C}(f_i)$ or not. Indeed, it is a result going back to Julia Robinson that $\mathrm{HTP}(\mathbb{Q}) \equiv_T \mathrm{HTP}(R)$ for every semilocal subring R of $\mathbb{Q}$. Moreover, the computation of $\mathrm{HTP}(R)$ from $\mathrm{HTP}(\mathbb{Q})$ is uniform in the finite set of primes which are not inverted in R.

Now, being the boundary of the open set $\mathcal{A}(f_i)$, the set $\mathcal{B}(f_i)$ must be nowhere dense in $\mathcal{P}(\mathbb{P})$. It follows that the *entire boundary set*

$$\mathcal{B} = \cup_{i \in \mathbb{N}} \mathcal{B}(f_i)$$

is meager, and we refer to subrings in its (comeager) complement $\overline{\mathcal{B}}$ as *HTP-generic* subrings of $\mathbb{Q}$, as this reflects the notion of genericity in set theory.

Proposition 1. *If $W \in \overline{\mathcal{B}}$, then $HTP(R_W) \equiv_T W \oplus HTP(\mathbb{Q})$.*

Indeed, with an $\mathrm{HTP}(\mathbb{Q})$-oracle, we can enumerate (for any i) the strings σ with $\mathcal{U}_\sigma \subseteq \mathcal{C}(f_i)$, and also the strings σ with $\mathcal{U}_\sigma \subseteq \mathcal{A}(f_i)$. But W must lie in one of these sets, since $W \notin \mathcal{B}(f_i)$, so eventually we will find that some initial segment of W is one of these types of strings, and then we will know whether $W \in \mathcal{A}(f_i)$.

We give a quick example of a set in $\mathcal{B}$. Let f be a polynomial which holds exactly when the conjunction of the following three conditions is true:

$$X^2 + Y^2 = 1 \ \ \& \ \ X > 0 \ \ \& \ \ Y > 0.$$

The reader may show that f has a solution in $\mathbb{Z}[\frac{1}{p}]$ whenever $p \equiv 1 \bmod 4$, but no solution in R_{W_3}, with W_3 as above. In fact, $\mathcal{B}(f)$ is the power set of $\{2\} \cup W_3$.

Now we turn to computability theory. The discussion above, along with standard computability arguments, yields the following results.

Theorem 2. *For every set C (e.g., for $C = \emptyset'$, the Halting Problem), we have:*

- *$HTP(\mathbb{Q}) \geq_T C \iff \{W : HTP(R_W) \geq_T C\}$ is non-meager.*
- *$HTP(\mathbb{Q}) \geq_1 C \iff \{W : HTP(R_W) \geq_1 C\}$ is non-meager.*

- $(\mathbb{Z}, +, \cdot)$ *has a Diophantine definition in* $\mathbb{Q} \iff$
  it has a Diophantine definition in non-meager-many subrings R_W*.*
- $\mathbb{Z}$ *is existentially definable in* $\mathbb{Q} \iff$
  $\mathbb{Z}$ *is existentially definable in non-meager-many subrings* R_W*.*

The optimistic view of this theorem is that it opens a route for proving undecidability of HTP($\mathbb{Q}$), without requiring that we address $\mathbb{Q}$ itself: it would suffice to prove that a not-too-small set of subrings R all have HTP(R) $\geq_T C$ for some undecidable C. (Indeed, it is a corollary of Prop. 1 that if HTP($\mathbb{Q}$) is decidable, then every HTP-generic W can itself compute HTP(R_W).) Likewise, a diophantine model of $(\mathbb{Z}, +, \cdot)$ in $\mathbb{Q}$, and $\exists$-definability of $\mathbb{Z}$ there, would follow if these properties held for anything more than a meager set of subrings.

The pessimistic view is that Theorem 2 suggests that there is much more to do. Specifically, we conjecture that the many impressive results in such works as [1, 4], which give diophantine models of the integers within various subrings of $\mathbb{Q}$, may only have used subrings from the entire boundary set $\mathcal{B}$.

Question 1. Does there exist an HTP-generic subring of $\mathbb{Q}$ within which there is a diophantine model of $(\mathbb{Z}, +, \cdot)$?

Measure theory (cf. [3]). It is natural to ask whether results analogous to the above hold when one uses measure theory in place of Baire category. Broadly speaking, the answer is that everything still goes through, except that we do not know whether boundary sets $\mathcal{B}(f_i)$ must have measure 0 (which of course is the analogue of being meager). In light of Theorem 3 below, this is a crucial question.

Question 2. Does there exist a polynomial f with $\mu(\mathcal{B}(f)) > 0$?

If not, then we can prove the measure-theoretic analogues of Theorem 2. Moreover, a negative answer would allow us to apply the following theorem.

Theorem 3 (Miller)**.** *If there is an existential definition of* $\mathbb{Z}$ *within the field* $\mathbb{Q}$*, then* $\mu(\mathcal{B}) = 1$*.*

A stronger version of this theorem says that if $\mathbb{Z}$ is $\exists$-definable within $\mathbb{Q}$, then every pair of positive real numbers (r, s) with $r + s < 1$ and with appropriate complexity can be realized as $r = \mu(\mathcal{A}(f))$ and $s = \mu(\mathcal{C}(f))$ for some f. As a partial converse, if every pair (r, s) can be realized this way, then HTP($\mathbb{Q}$) must be Turing-equivalent to the Halting Problem.

Other results. We make note here of certain other computability-theoretic results and questions about Hilbert's Tenth Problem, which may be of use for number theory. The first involves the *jump* W', which is essentially the Halting Problem relativized to the base set W, and which always computes HTP(R_W).

Theorem 4 (Miller)**.** *The set of those* W *such that the jump* W' *is diophantine in* R_W *is meager and has measure* 0*.*

This shows that $\mathbb{Z}$ is an unusual subring of $\mathbb{Q}$, as $\emptyset'$ is diophantine in $\mathbb{Z}$.

Theorem 5 (Miller)**.** *If HTP($\mathbb{Q}$) is decidable, then there must exist a decidable subset of $\mathbb{N}$ which is not diophantine in $\mathbb{Q}$. (Equivalently, if all decidable sets are diophantine in $\mathbb{Q}$, then HTP($\mathbb{Q}$) is undecidable.)*

Say that a polynomial $h \in \mathbb{Q}[X, Y, \vec{Z}]$ is *HTP-complete* for a subring R_W of $\mathbb{Q}$ if, for every $f \in \mathbb{Q}[T, \vec{U}]$, there exists some $x \in \mathbb{Q}$ such that

$$(\forall q \in \mathbb{Q})\ [f(q, \vec{U}) \in \mathrm{HTP}(R_W) \iff h(x, q, \vec{Z}) \in \mathrm{HTP}(R_W)].$$

h is *effectively HTP-complete* for R_W if there is a computable function mapping each f to a corresponding x. The point here is mainly that, if the jump W' is diophantine in R_W, then R_W must have an effectively HTP-complete polynomial.

Question 3. Which subrings of $\mathbb{Q}$ have (effectively) HTP-complete polynomials?

References

[1] Kirsten Eisenträger and Graham Everest. Descent on elliptic curves and Hilbert's tenth problem. *Proc. Amer. Math. Soc.*, 137(6):1951–1959, 2009.

[2] Russell Miller. Baire category theory and Hilbert's Tenth Problem inside $\mathbb{Q}$. in *Pursuit of the Universal: 12th Conference on Computability in Europe, CiE 2016*, eds. A. Beckmann, L. Bienvenu & N. Jonoska, **LNCS 9709** (Berlin: Springer-Verlag, 2016), 343–352.

[3] Russell Miller. Measure theory and Hilbert's Tenth Problem inside $\mathbb{Q}$, to appear in the *Proceedings of the IMS Workshop on Sets and Computations*.

[4] Bjorn Poonen. Hilbert's Tenth Problem and Mazur's conjecture for large subrings of $\mathbb{Q}$. *Journal of the AMS*, 16(4):981–990, 2003.

On a Weak Form of Divisibility

Alla Sirokofskich

In what follows $\mathbb{F}_q$ is a finite field, with $q = p^n$, p a prime; $\mathbb{F}_q[t]$ is the ring of polynomials over $\mathbb{F}_q$, while $\mathbb{F}_q^*$ stands for $\mathbb{F}_q - \{0\}$ and $(\mathbb{F}_q[t])^*$ stands for $\mathbb{F}_q[t] - \{0\}$. By $\mathbb{N}$ we denote the set of positive integers and let $\mathbb{N}_0$ be $\mathbb{N} \cup \{0\}$.

L. Lipshitz in [3] and A. Beltyukov independently in [1] showed that the existential theory of $\mathbb{Z}$ in the language of addition and divisibility is decidable. A. Semenov in [5] showed that the elementary theory of $\mathbb{Z}$ in the language of addition and the predicate for powers of 2 is decidable. J. Robinson asked in a personal communication with L. Lipshitz whether the existential theory of $\mathbb{Z}$ in the language of addition, divisibility and the predicate for powers of 2 is decidable.

In an effort to attack problems over the integers, some researchers examine the analogous problems over polynomials in one variable over finite fields. T. Pheidas in [4] showed that the existential theory of $\mathbb{F}_q[t]$ is decidable in the language of addition and divisibility. Also in [6] it was proved that the theory of $\mathbb{F}_q[t]$ is decidable in the language of addition and the predicate for powers of t. Therefore the natural question is to ask

Open Problem 1. *Is the existential theory of $\mathbb{F}_q[t]$ in the language of addition, divisibility and the predicate for powers of t decidable?*

Motivated by work of L. Lipshitz [3] and Th. Pheidas, we study the decidability of the existential theory of the structure with universe the set of polynomials of one variable, t, over a finite field $\mathbb{F}_q$, in the language consisting of addition, inequality of degrees of polynomials and weak form of divisibility. Namely, we are interested in the restriction of regular divisibility of linear polynomials over $\mathbb{F}_q[t]$, in several variables which take values in the set of powers of t. Polynomials over finite fields have been extensively studied because of their many important applications. We proceed with the definition of an important class of polynomials.

Definition 2. Let $f \in \mathbb{F}_q[t]$ with $deg(f) = m \neq 0$. Then f is called primitive polynomial over F_q if it is the minimal polynomial over F_q of a primitive element a of F_{q^m}, i.e., it is a monic polynomial, irreducible over F_q and has a root a in F_{q^m}, such that $\langle a \rangle = F_{q^m}^{\times}$. Where by $F_{q^m}^{\times}$ we mean the multiplicative group of F_{q^m}.

Next we state a property of polynomials over a finite field which will lead us to the notion of order of a polynomial.

Lemma 3. *Let $f \in \mathbb{F}_q[t]$ be a polynomial of degree $m \geq 1$ with non zero valuation at $t = 0$, i.e., $f(0) \neq 0$. Then there exists $e \in \mathbb{N}$ such that $e \leq q^m - 1$ and f divides $t^e - 1$.*

Given the existence of an exponent in Lemma 3, it is natural to consider the smallest non-zero exponent and name it order, i.e.,

Definition 4. Let $f \in \mathbb{F}_q[t]$ with $f(0) \neq 0$. The least $e \in \mathbb{N}$ such that $f | t^e - 1$ is called the order of f. We denote the order of f by $ord(f)$.

Some authors call $ord(f)$ the period of f or the exponent of f. The notion of the order can be extended for f, with $f(0) = 0$, as follows: since f can be written uniquely as $t^k g(t)$, where $g(0) \neq 0$, $ord(f)$ is defined to be equal to $ord(g)$.

More details about the properties of an order of a polynomial and also a proof of Lemma 3 can be found in [2].

We proved the following fact:

Proposition 5. *Let $f \in \mathbb{F}_q[t]$ with $t \nmid f$ and $deg(f) = m$. Then*

1. *If $ord(f) = q^m - 1$, then for every $g \in \mathbb{F}_q[t]$ with $f \nmid g$ there is $n < q^m - 1$ such that $f | t^n + g$.*
2. *If $ord(f) < q^m - 1$, then there is $g \in \mathbb{F}_q[t]$ with $f \nmid g$ such that for all $n \in \mathbb{N}$ $f \nmid t^n + g$.*

We recall a known characterisation of primitive polynomials by means of their order. Namely,

Theorem 6. *A polynomial $f \in F_q[t]$ of degree m is a primitive polynomial over F_q if and only if f is monic, $t \nmid f$ and $ord(f) = q^m - 1$.*

Let $\mathbf{P} = \{t^n : n \in \mathbb{N}_0\}$. Then, Proposition 5 actually gives a different characterisation of primitive polynomials, i.e.,

Theorem 7. *A polynomial $f \in F_q[t]$ of degree m is a primitive polynomial over F_q if and only if f is monic and for all $g \in F_q[t]$ with $g \not| f$ there is some $y \in \mathbf{P}$ such that $f|y+g$.*

Definition 8. Let $f \in \mathbb{F}_q[t][x_1, ..., x_n]$. We say that f satisfies the $\mathbf{ND_t}$-property, if for all evaluations at $(x_1, ..., x_n) = (t^{k_1}, ..., t^{k_n})$, with each $k_i \in \mathbb{N}_0$, we have that with $t \not| f(t^{k_1}, ..., t^{k_n})$.

We proved that there is a finite procedure which given an $f \in \mathbb{F}_q[t][x_1, ..., x_n]$ checks the $\mathbf{ND_t}$-property for f.

Now we proceed to the solution of a system of linear equations in one variable over $F_q[t]$ where the unknown variable takes values in $\mathbf{P}$. Namely we proved

Theorem 9. *Let $f_1, ..., f_s, g_1, ..., g_s \in \mathbb{F}_q[t]$ such that $t \not| f_i$ for all i and $e_i = ord(f_i)$. Assume that for every $i = 1, ..., s$ there is $\lambda_i \in \mathbb{N}$ such that $f_i | t^{\lambda_i} + g_i$ and let λ_{0i} be the smallest such power for every i. Then*

$$\exists y \in \mathbf{P}[\bigwedge_{i=1}^{s} f_i|(y+g_i)] \iff \exists \lambda \in \mathbb{N} \bigwedge_{i=1}^{s} e_i|(\lambda - \lambda_{0i})).$$

As a corollary we obtain a partial answer to Open Problem 1, namely when the number of existential quantifiers is one. In other words we proved that the $\exists_1$-theory of $\mathbb{F}_q[t]$ in the language of addition, divisibility and the predicate for powers of t is decidable.

References

[1] A. Beltyukov, *Decidability of the universal theory of natural numbers with addition and divisibility*, Zapiski Nauchnykh Seminarov Leningradskogo Otdeleniya Matematicheskogo Instituta im. V, A. Steklova AN SSSR (LOMI) **60** (1976), 15–28.

[2] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press (1994).

[3] L. Lipshitz, *The diophantine problem for addition and divisibility*, Transactions of the American Mathematical Society **235** (1978), 271–283.

[4] T. Pheidas, *The diophantine problem for addition and divisibility in polynomial rings*, Thesis, Purdue University, (1985).

[5] A. Semenov, *On the definability of arithmetic in its fragments*, Soviet Math. Dokl., **25** (1982), 300–303.

[6] A. Sirokofskich, *On an exponential predicate in polynomials over finite fields*, Proceedings of the American Mathematical Society **138** (2010), 2569–2583.

An Analogue of Hilbert's Tenth Problem for the Ring of Exponential Sums

Dimitra Chompitaki
(joint work with Thanases Pheidas)

At a glance: We prove that the positive existential theory of the ring of exponential sums is undecidable.

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

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

where $\alpha_i, \mu_j \in \mathbb{C}$. We ask whether the positive existential first order theory of $\mathrm{EXP}(\mathbb{C})$, as a structure of the language

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

is decidable or undecidable. 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 1. *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 1 we adapt techniques of [3] and we show Theorem 2:

We consider the equation

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

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

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

Theorem 2. *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 $t_2, \ldots t_\ell$ are variables over 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].

The results of Theorem 2 may be stated as

The set of solutions of

$$(T^2 - 1)y^2 = x^2 - 1$$

over the tower of rings

$$\cup_N \mathbb{C}[T^{\frac{1}{N!}}, T^{-\frac{1}{N!}}]$$

stabilizes at the level of $\mathbb{C}[T, T^{-1}]$.

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.

On Stabilizers of Algebraic Function Fields of One Variable

Aharon Razon
(joint work with Wulf-Dieter Geyer, Moshe Jarden)

We consider an infinite field K and write $\tilde{K}$ for a fixed algebraic closure of K. We also consider an absolutely integral curve Γ in $\mathbb{P}^n_K$ with $n > 2$. The curve $\Gamma_{\tilde{K}}$ should have only finitely many inflection points, finitely many double tangents, and there exists no point in $\mathbb{P}^n_{\tilde{K}}$ through which infinitely many tangents to $\Gamma_{\tilde{K}}$ go. In addition there exists a prime number q such that $\Gamma_{\tilde{K}}$ has a cusp of multiplicity q and the multiplicities of all other points of $\Gamma_{\tilde{K}}$ are at most q. Under these assumptions, we construct a nonempty Zariski-open subset O of $\mathbb{P}^n_{\tilde{K}}$ such that if $n \geq 3$, the projection from each point $\mathbf{o} \in O(K)$ birationally maps Γ onto an absolutely integral curve Γ' in $\mathbb{P}^{n-1}_K$ with the same properties as Γ (keeping q unchanged). If $n = 2$, then the projection from each $\mathbf{o} \in O(K)$ maps Γ onto $\mathbb{P}^1_K$ and leads to a stabilizing element t of the function field F of Γ over K. The latter means that $F/K(t)$ is a finite separable extension whose Galois closure $\hat{F}$ is regular over K.

References

[1] W.D. Geyer, M. Jarden, and A. Razon, *On stabilizers of algebraic function fieldsof one variable*, Adv. Geom (2016).

Irreducibility of Polynomials Over Number Fields is Diophantine

Philip Dittmann

In this talk I introduced the following result and sketched a proof of it.

Theorem 1 ([2])**.** *Let K be a number field. Then the set of polynomials in $K[X]$ with no root in K is diophantine, in the sense that for every $n > 0$ the set $\{(a_0, \dots, a_{n-1}) \in K^n \colon X^n + a_{n-1}X^{n-1} + \cdots + a_0$ has no root in $K\}$ is diophantine.*

This is a generalisation of a result by Colliot-Thélène and Van Geel [1] proving that the set of non-n-th powers is diophantine in any number field.

As a corollary to the theorem we obtain:

Corollary 2. *Let K be a number field and $K^{**} \supseteq K^*$ with $K^{**} \equiv K^* \equiv K$. Then K^* is relatively algebraically closed in K^{**}.*

This answers [3, Question 25] positively.

Using the standard model-theoretic machinery of the Łoś-Tarski Preservation Theorem, we also obtain a result on irreducibility of polynomials in an arbitrary number of variables:

Corollary 3. *Let K be a number field. Then irreducibility of polynomials over K in an arbitrary number of variables is diophantine. More formally, fix $r, d \geq 0$. Then the set*

$$\{\overline{a} \in K^{(d+1)^r} : \sum_{0 \leq i_1, \ldots, i_r \leq d} a_{i_1,\ldots,i_r} X_1^{i_1} \cdots X_r^{i_r} \in K[X_1, \ldots, X_r] \text{ is irreducible}\}$$

is diophantine.

The proof of Theorem 1 is based on Brauer groups, generalising the use of quaternion algebras in [5], [4] and [3]. Specifically, for every prime number l we find a diophantine predicate T_K such that when L/K is a finite extension and A/L is a central simple algebra of degree l, then

$$T_K(A/L) \cap K = \bigcap_{v \in \Delta(A/L)} \mathcal{O}_v \cap K,$$

where $\Delta(A/L)$ is the set of places of L at which A does not split.

We then use the predicate T_K to express that certain central simple algebras locally split in the field extension $\big(K[X]/(f)\big)/K$ when f is an irreducible polynomial of degree > 1 over K.

References

[1] Jean-Louis Colliot-Thélène and Jan Van Geel, *Le complémentaire des puissances n-ièmes dans un corps de nombres est un ensemble diophantien*, Compositio Math. **151** (2015), 1965–1980.

[2] Philip Dittmann, *Irreducibility of polynomials over number fields is diophantine*, submitted, available as arXiv:1601.07829 [math.NT], 2016.

[3] Jochen Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, Ann. Math. **183** (2016), 73–93.

[4] Jennifer Park, *A universal first order formula defining the ring of integers in a number field*, Math. Res. Lett. **20** (2013), 961–980.

[5] Bjorn Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131** (2009), no. 3, 675–682.

Diophantine Subsets of Henselian Fields

Arno Fehm

(joint work with Sylvy Anscombe, Philip Dittmann)

In this talk I reported on recent work concerning diophantine henselian valuation rings and valuation ideals. Here, a subset of a field F is *diophantine* if it is the projection of the common zero set of a family of polynomials with integer coefficients.

After partial results [4, 5, 6, 12] by various authors we used our work on the existential theory of equicharacteristic henselian fields [2] to obtain the following characterization:

Theorem 1 ([3, Cor. 5.3])**.** *For a field F the following are equivalent:*

(1) *$F[[t]]$ (resp. $tF[[t]]$) is diophantine in $F((t))$.*

(2) *$\mathcal{O}_v$ (resp. $\mathfrak{m}_v$) is diophantine in K for some equicharacteristic henselian nontrivially valued field (K, v) with $Kv \equiv F$.*
(3) *$\mathcal{O}_v$ (resp. $\mathfrak{m}_v$) is uniformly diophantine in K for the class of equicharacteristic henselian nontrivially valued fields (K, v) with $Kv \equiv F$.*
(4) *$\mathcal{O}_v$ (resp. $\mathfrak{m}_v$) is uniformly diophantine in K for the class of henselian valued fields (K, v) with $Kv \equiv F$.*
(5) *There is no elementary extension $F \preceq F^*$ with a nontrivial valuation u on F^* such that F^*u is isomorphic to a subfield of F^* (resp. with a nontrivial henselian valuation u on a subfield E of F^* such that $Eu \cong F^*$).*

The aim of this talk was to investigate condition (5) for the maximal ideal and for the valuation ring.

1. Valuation ideals

Condition (5) for the maximal ideal is best explained when considering a version that allows the polynomials to have coefficients in a subfield C of F, in which case we speak of *C-diophantine* instead of diophantine:

Proposition 2 ([3, Prop. 6.10])**.** *For perfect fields $C \subseteq F$ the following are equivalent:*

(i) *$tF[[t]]$ is not C-diophantine in $F((t))$.*
(ii) *There exists a subfield $C \subseteq E \subseteq F^* \succeq F$ and a nontrivial henselian valuation u on E which is trivial on C and satisfies $Eu \cong_C F^*$.*
(iii) *For every smooth integral C-variety X, the set of F-rational points $X(F)$ is empty or C-Zariski dense in X.*

Note that in the case $C = F$, (iii) is the definition of a large field in [11].

Corollary 3. *For a field F, $tF[[t]]$ is F-diophantine in $F((t))$ iff F is not large.*

Example 4. If F is a finitely generated field, then one can find a counterexample X to (iii) defined over the prime field, so $tF[[t]]$ is even diophantine in $F((t))$.

Thus, the abstract condition (5) in the case of the valuation ideal turns out to be a well-studied purely arithmetic-geometric property of F.

2. Valuation rings

We do not have a similarly nice description for (5) in the case of the valuation ring, but we can verify it in several examples:

Example 5. (5) is trivially satisfied if F is finite.

Example 6. By a theorem of Frey–Prestel, (5) is satisfied if F is PAC, PRC or PpC without a separably, real or p-adically closed subfield, e.g. $F = \mathbb{Q}^{\mathrm{tr}}$, the field of totally real algebraic numbers.

Example 7. (5) is satisfied for $F = \mathbb{Q}$: Indeed, by Lagrange's Four Squares Theorem, $\mathbb{Q}^*$ has a unique ordering and is dense in its real closure. So, if $\mathbb{Q}^*u$ embeds

into $\mathbb{Q}^*$, then $\mathbb{Q}^*u$ is formally real and the Baer–Krull theorem implies that u is convex. This compatibility of ordering and valuation gives that $\mathbb{Q}^*$ is dense in its real closure also with respect to u, and therefore $\mathbb{Q}^*u$ is real closed, contradicting that it is isomorphic to a subfield of $\mathbb{Q}^*$.

In order to generalize this last example to arbitrary not necessarily real number fields, we recall the definition of the Kochen ring:

Definition 8. For a prime number p,

$$\gamma_p(x) = \frac{1}{p} \cdot \frac{x^p - x}{(x^p - x)^2 - 1}$$

is the *p-adic Kochen operator* and

$$\Gamma_p(F) = \left\{ a(1+pb)^{-1} : a, b \in \mathbb{Z}_{(p)}[\gamma_p(F)] \right\}$$

is the *p-adic Kochen ring*.

The p-adic Kochen ring of F is a suitable analogue of the set of sums of squares in that it is the intersection of all the p-valuation rings of F, cf. [13]. So in order to generalize the above proof, one would want to have a p-adic analogue of the Four Squares Theorem:

Question 1. Is there some n_p such that

$$\Gamma_p(\mathbb{Q}) = \left\{ a(1+pb)^{-1} : a, b \in \sum_{i=1}^{n_p} \gamma_p(\mathbb{Q}) \right\} \ ?$$

Note that this is in fact a special case of Poonen's question [9, Question 5.3]. What we can prove, building on the diophantine predicates developed in [10, 7, 8], is a slightly weaker form that takes into account that $\gamma_p(\mathbb{Q})$, as opposed to $\mathbb{Q}^{\times 2}$, is not closed under products:

Theorem 9 ([1])**.** *There exists n_p and $f_p \in \mathbb{Z}_{(p)}[X_1, \ldots, X_{n_p}]$ such that for all number fields F,*

$$\Gamma_p(F) = \left\{ a(1+pb)^{-1} : a, b \in f_p(\gamma_p(F), \ldots, \gamma_p(F)) \right\}.$$

With this, the p-adic analogue of the above proof goes through and we obtain:

Corollary 10. *$\mathbb{Q}^*$ has a unique p-valuation ring, and if u is a nontrivial valuation on $\mathbb{Q}^*$ with $\mathbb{Q}^*u$ formally p-adic, then $\mathbb{Q}^*u$ is p-adically closed.*

Corollary 11. *If $F \subsetneqq \mathbb{Q}_p \cap \mathbb{Q}^{\mathrm{alg}}$ for some p (e.g. if F is any number field), then $F[[t]]$ is diophantine in $F((t))$.*

Note that Theorem 9 is uniform over all number fields but does not give an explicit bound on the number of variables, the degree or the height of f_p, and so it would be very interesting to see a direct and explicit proof of it.

References

[1] S. Anscombe, P. Dittmann and A. Fehm, *Residue fields of valuations on nonstandard number fields*, manuscript (2016).
[2] S. Anscombe and A. Fehm, *The existential theory of equicharacteristic henselian valued fields*, Algebra and Number Theory **10** (2016), 665–683.
[3] S. Anscombe and A. Fehm, *Characterizing diophantine henselian valuation rings and valuation ideals*, arXiv:1602.01233 [math.LO] (2016).
[4] W. Anscombe and J. Koenigsmann, *An existential $\emptyset$-definition of $\mathbb{F}_q[[t]]$ in $\mathbb{F}_q((t))$*, J. Symbolic Logic **79** (2014), 1336–1343.
[5] R. Cluckers, J. Derakhshan, E. Leenknegt and A. Macintyre, *Uniformly defining valuation rings in henselian valued fields with finite or pseudo-finite residue fields*, Annals Pure Appl. Logic **164** (2013), 1236–1246.
[6] A. Fehm, *Existential $\emptyset$-definability of henselian valuation rings*, J. Symbolic Logic **80** (2015), 301–307.
[7] J. Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, Annals Math. **183** (2016), 73–93.
[8] J. Park, *A universal first order formula defining the ring of integers in a number field*, Math. Res. Lett. **20** (2013), 961–980.
[9] B. Poonen, *Sums of values of a rational function*, Acta Arithmetica **112** (2004), 333-343.
[10] B. Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, American Journal of Mathematics **131** (2009), 675–682.
[11] F. Pop, *Embedding problems over large fields*, Annals Math. **144** (1996), 1–34.
[12] A. Prestel, *Definable henselian valuation rings*, J. Symbolic Logic **80** (2015), 1260–1267.
[13] A. Prestel and P. Roquette, *Formally p-adic fields*, Springer (1984).

L-functions, Proximity Functions, and Diophantine Sets

Hector Pasten

The goal of this note (and my talk) is to discuss descriptions of the Diophantine sets of global fields and their rings of integers. By [4] and [10], a set in $\mathbb{Z}$ is Diophantine if and only if it is listable in the sense of recursion theory; I'll refer to this result as the DPRM theorem. This gives a complete description of the Diophantine sets of $\mathbb{Z}$, implying that Hilbert's tenth problem is unsolvable.

Rings of integers. The analogue of DPRM for rings of S-integers in a global function field (S a non-empty finite set of places) follows from [5] and [23].

The analogue of the DPRM for the rings of integers O_K of a number field K is known for: CM fields and certain degree 4 extensions [7, 6]; K with exactly one complex place [16, 21, 24]; K contained in one of the previous fields [20].

Towards the general case, the series of papers [18, 2, 22] culminated in the following elliptic curve criterion by Poonen and Shlapentokh: *Suppose that for every cyclic extension of prime degree L/F of number fields there is an elliptic curve E defined over F such that* $\mathrm{rk}(E(L)) = \mathrm{rk}(E(F)) > 0$. *Then for every number field K, the Diophantine sets and the listable sets of O_K are the same.*

Mazur and Rubin [13] verified the elliptic curve criterion conditionally on a conjecture on Shafarevich-Tate groups. Alternatively, using non-vanishing theorems for L-functions [8, 14], Ram Murty and I proved [15] that the criterion is satisfied under the rank part of Birch and Swinnerton-Dyer conjecture:

Theorem 1 (Murty-Pasten)**.** *Suppose that (certain) elliptic curves over number fields E/F satisfy that the L-function $L(s,E)$ is automorphic and:*

- *(Parity conjecture)* $\mathrm{ord}_{s=1}L(s,E) \equiv \mathrm{rk}(E(F)) \mod 2$
- *(Analytic rank 0 BSD) If χ is a Hecke character of F corresponding to a finite extension L/F and if $L(1,E/F,\chi) \neq 0$, then $E(L)^{\chi}_{\mathbb{C}} = 0$.*

Then the Poonen-Shlapentokh elliptic curve criterion is satisfied, and for every number field K, the analogue of DPRM for O_K holds.

Global fields. Hilbert's tenth problem for $\mathbb{F}_q(z)$ is undecidable [17, 25], while it is open for $\mathbb{Q}$. Nevertheless, the question of whether in a global field K Diophantine sets and listable sets are the same, remains open in all cases.

The analogue of DPRM holds for $\mathbb{Q}$ if and only if $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$. In the direction of the latter, Koenigsmann proved [9] that $\mathbb{Z}$ admits a $\forall\exists\exists...\exists$-positive definition in $\mathbb{Q}$, so that it only remains to eliminate one universal quantifier.

However, Mazur conjectured that if $X/\mathbb{Q}$ is a projective variety then the topological closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ has only finitely many connected components [11, 1]. This would imply that $\mathbb{Z}$ is not Diophantine in $\mathbb{Q}$. There is a lesser known version of Mazur's topological conjecture over number fields (including non-Archimedean places) with analogous non-Diophantineness implications [12, 19]:

Conjecture 2 (Mazur)**.** *Let K be a number field, $v \in M_K$, and X/K a projective variety. For $x \in X(K_v)$, let $Z_x \subseteq X$ be the limit of the Zariski closure of $X(K) \cap U$ in X, as U varies over v-neighborhoods of x. Then $\{Z_x : x \in X(K_v)\}$ is finite.*

Mazur's conjecture is specific to the number field case and the analogue for global function fields is *false*, as the following example shows:

Example 3 (cf. [17, 3]). Let $p > 2$ be prime. The sets $A = \{z^{p^n} : n \geq 0\}$ and $B = \{\lambda + z + z^p ... + z^{p^n} : n \geq 0 \text{ and } \lambda \in \mathbb{F}_p\}$ are Diophantine in $K = \mathbb{F}_p(z)$. (They are images of K-rational points of certain curve X defined over K.)

Proximity functions and heights. Let K be a global field. Let X/K be a projective variety with $\mathrm{CD}^+(X/K)$ its set of effective Cartier divisors. Fix a choice of Weil functions $\lambda_{D,v} : X(\bar{K}) - D \to \mathbb{R}$ for $D \in \mathrm{CD}^+(X/K)$ and $v \in M_K$.

Let $S \subseteq M_K$ be a finite set of places and let $D \in \mathrm{CD}^+(X/K)$. The *proximity function* to D relative to S is $m_{X,S}(D,-) := \sum_{v\in S} \lambda_{D,v}(-)$, and the *height* relative to D is $h_{X,D}(-) := \sum_{v\in M_K} \lambda_{D,v}(-)$. Both are functions $X(\bar{K}) - D \to \mathbb{R}$. One has the *trivial inequality* $m_{X,S}(D,x) \leq h_{X,D}(x) + O(1)$ for $x \in X(\bar{K}) - D$, and the central problem in Diophantine approximation is to establish non-trivial inequalities between the proximity function and the height of rational points. Let me formulate a conjecture trying to formalize the hope that the proximity function contributes non-trivially to the height. Details will appear elsewhere.

Conjecture 4. *Let K be a global field and let S be a finite set of places of K. Let X, Y be projective varieties over K. Let $D \in \mathrm{CD}^+(X/K)$ and let $f : X \to Y$ be a K-morphism. Suppose that for all $E \in \mathrm{CD}^+(Y/K)$, the height h_{X,f^*E} is unbounded on $X(K) - (D + f^*E)$. Then there exists $E_0 \in \mathrm{CD}^+(Y/K)$ such that $m_{X,S}(f^*E_0,-)$ is unbounded on $X(K) - (D + f^*E_0)$.*

Here is a summary of some results:

Theorem 5. *The case $Y = \mathbb{P}^1$ implies the general case in Conjecture 4, and in the number field setting Conjecture 2 implies Conjecture 4. In addition, Conjecture 4 holds unconditionally if X is a curve or an abelian variety.*

The relevance of Conjecture 4 in our setting is justified by the following.

Theorem 6. *Assume Conjecture 4. Then:*

(i) *$\mathbb{Z}$ is not Diophantine in $\mathbb{Q}$.*
(ii) *$\mathbb{F}_p[z]$ is not Diophantine in $\mathbb{F}_p(z)$.*
(iii) *$\{z^n : n \geq 1\}$ is not Diophantine in $\mathbb{F}_p(z)$.*

Observe that Example 3 is consistent with Conjecture 4: The curve X has maps $f, g : X \to \mathbb{P}^1$ defined over $K = \mathbb{F}_p(z)$ such that $f(X(K)) = A$ and $g(X(K)) = B$. Take $S = \{v_z\}$ the z-adic place. Let Y_0, Y_1 be the homogeneous coordinates in $\mathbb{P}^1$. For f we take the divisor $E_0 = \{Y_1 = 0\}$ and for g we take $E_0 = \{Y_1^p - Y_1 + z = 0\}$.

References

[1] J.-L. Colliot-Thélène, A. N. Skorobogatov, P. Swinnerton-Dyer, *Double fibres and double covers: paucity of rational points*, Acta Arith. 79 (1997), no. 2, 113–135.

[2] G. Cornelissen, T. Pheidas, K. Zahidi, *Division-ample sets and the Diophantine problem for rings of integers*. J. Théor. Nombres Bordeaux 17 (2005), no. 3, 727–735.

[3] G. Cornelissen, K. Zahidi, *Topology of Diophantine sets: remarks on Mazur's conjectures*. Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), 253–260, Contemp. Math., 270, Amer. Math. Soc., Providence, RI, 2000.

[4] M. Davis, H. Putnam, J. Robinson, *The decision problem for exponential diophantine equations*. Ann. of Math. (2) 74 1961 425–436.

[5] J. Demeyer, *Recursively enumerable sets of polynomials over a finite field are Diophantine*. Invent. Math. 170 (2007), no. 3, 655–670.

[6] J. Denef, *Diophantine sets over algebraic integer rings. II*. Trans. Amer. Math. Soc. 257 (1980), no. 1, 227–236.

[7] J. Denef, L. Lipshitz, *Diophantine sets over some rings of algebraic integers*. J. London Math. Soc. (2) 18 (1978), no. 3, 385–391.

[8] S. Friedberg, J. Hoffstein, *Nonvanishing theorems for automorphic L-functions on $GL(2)$*. Ann. of Math. (2) 142 (1995), no. 2, 385–423.

[9] J. Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*. Ann. of Math. (2) 183 (2016), no. 1, 73–93.

[10] J. Matijasevich, *The Diophantineness of enumerable sets*. (Russian) Dokl. Akad. Nauk SSSR 191 1970 279–282.

[11] B. Mazur, *The topology of rational points*, Exper. Math. 1 (1992), no. 1, 35–45.

[12] B. Mazur, *Open problems regarding rational points on curves and varieties*, Galois representations in arithmetic algebraic geometry (Durham 1996), London Math. Soc. Lect. Note Ser. 254 (1998), 239–265.

[13] B. Mazur, K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*. Invent. Math. 181 (2010), no. 3, 541–575.

[14] K. Murty, R. Murty, *Non-vanishing of L-functions and applications*. (English summary) Progress in Mathematics, 157. Birkhäuser Verlag, Basel, 1997. xii+196 pp. ISBN: 3-7643-5801-7

[15] R. Murty, H. Pasten, *Elliptic curves, L-functions, and Hilbert's tenth problem*. Submitted (2016).

[16] T. Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*. Proc. Amer. Math. Soc. 104 (1988), no. 2, 611–620.

[17] T. Pheidas *Hilbert's tenth problem for fields of rational functions over finite fields*. Invent. Math. 103 (1991), no. 1, 1–8.
[18] B. Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers*. Algorithmic number theory (Sydney, 2002), 33-42, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002.
[19] B. Poonen, A. Shlapentokh, *Diophantine definability of infinite discrete nonarchimedean sets and Diophantine models over large subrings of number fields*. J. Reine Angew. Math. 588 (2005), 27–47.
[20] H. Shapiro, A. Shlapentokh, *Diophantine relationships between algebraic number fields*. Comm. Pure Appl. Math. 42 (1989), no. 8, 1113–1122.
[21] A. Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields*. Comm. Pure Appl. Math. 42 (1989), no. 7, 939-962.
[22] A. Shlapentokh, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers*. Trans. Amer. Math. Soc. 360 (2008), no. 7, 3541–3555.
[23] A. Shlapentokh, *Diophantine relations between rings of S-integers of fields of algebraic functions in one variable over constant fields of positive characteristic*. J. Symbolic Logic 58 (1993), no. 1, 158–192.
[24] C. Videla *On Hilbert's Tenth Problem*, Atas da Xa Escola de Algebra, Vitoria, ES, Brasil Colecao Atas 16 p. 95–108, Sociedade Brasileira de Matematica (1989).
[25] C. Videla *Hilbert's tenth problem for rational function fields in characteristic 2*. Proc. Amer. Math. Soc. 120 (1994), no. 1, 249–253.

Decidability and Classification of the Theory of Integers with Primes

Itay Kaplan
(joint work with Saharon Shelah)

It is well known that Presburger arithmetic $T_{+,<} = Th(\mathbb{Z}, +, 0, <)$ is decidable and enjoys quantifier elimination after introducing predicates for divisibility by n for every natural number $n > 1$ (see e.g., [Mar02, Corollary 3.1.21]). The same is true for $T_+ = Th(\mathbb{Z}, +, 0)$. This is, of course, in contrast to the situation with the theory of Peano arithmetics or $Th(\mathbb{Z}, +, \cdot, 0)$ which is not decidable.

In terms of classification theory, quantifier elimination gives us that T_+ is superstable of U-rank 1, while $T_{+,<}$ is dp-minimal (a subclass of NIP theories, see e.g., [DGL11, Sim11, OU11]).

Over the years there has been much research on structures with universe $\mathbb{Z}$ or $\mathbb{N}$ and some extra structure definable from Peano. A very good survey regarding questions of decidability is [Bès01] and a list of such structures defining addition and multiplication is available in [Kor01].

Some research was also done on classifying these structures stability-theoretically. For instance, by [Poi14, Theorem 25] and also [PS14], $Th(\mathbb{Z}, +, 0, P_q)$ is superstable of U-rank ω, where P_q is the set of powers of q.

Let Pr be a predicate for the primes and their negations and consider $T_{+,Pr} = Th(\mathbb{Z}, +, 0, 1, Pr)$ and $T_{+,Pr,<} = Th(\mathbb{Z}, +, 0, 1, Pr, <)$. The language $\{+, 0, 1, Pr\}$ allows us to express famous number-theoretic conjectures such as the twin prime conjecture (for every n, there are at least n pairs of primes/negation of primes of distance 2).

By works of Jockusch, Bateman and Woods [BJW93, Woo13], assuming Dickson's conjecture (D) (see below), $Th(\mathbb{N}, +, 0, Pr^+)$ is undecidable and even defines multiplication (here, $Pr^+ = Pr \cap \mathbb{N}$). This implies that $T_{+,Pr,<}$ is undecidable as well. Dickson's conjecture states as follows.

Conjecture 1 (**(D)**(Dickson, 1904 [Dic04]))**.** *Let $k \geq 1$ and $\bar{f} = \langle f_i \mid i < k \rangle$ where $f_i(x) = a_i x + b_i$ with a_i, b_i non-negative integers, $a_i \geq 1$ for all $i < k$. Assume that the following condition holds:*

- $\star_{\bar{f}}$ *There does not exist any integer $n > 1$ dividing all the products $\prod_{i<k} f_i(s)$ for every (non-negative) integer s.*

Then there exist infinitely many natural numbers m such that $f_i(m)$ is prime for all $i < k$.

For a discussion of this conjecture see [Rib89].

Our main result is the following.

Theorem 2. *Assuming (D), the theory $T_{+,Pr}$ is decidable, unstable and supersimple of U-rank 1.*

In essence (D) implies that the set of primes is generic up to congruence conditions (while it is not generic in the sense of [CP98]), and this allows us to get quantifier elimination in a suitable language.

The main lemma used in quantifier elimination is the following.

Lemma 3. *Assuming (D), given $f_i(x) = a_i x + b_i$ with a_i, b_i non-negative integers, $a_i \geq 1$ for all $i < k$ and $g_j(x) = c_j x + d_j$ with c_j, d_j non-negative integers, $c_j \geq 1$ for all $j < k'$, if $\star_{\bar{f}}$ holds for $\bar{f} = \langle f_i \mid i < k \rangle$ and $(a_i, b_i) \neq (c_j, d_j)$ for all i, j then there are infinitely many natural numbers m for which $f_i(m)$ is prime and $g_j(m)$ is composite for all $i < k, j < k'$.*

This allows us to extract the existential quantifier from formulas of the form $\exists x \bigwedge_i Pr(a_i x + y_i) \wedge \bigwedge_j \neg Pr(c_j x + z_j)$ for integers a_i, c_j.

The proof of quantifier elimination also shows that $T_{+,Pr}$ is decidable and allows us to identify forking formulas and prove that $T_{+,Pr}$ is supersimple of U-rank 1.

To show that $T_{+,Pr}$ is unstable we show that $Pr(x + y)$ has the independence property (i.e., we show that for all n, there are $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ and $b_s \in \mathbb{Z}$ for $s \subseteq n$ such that $Pr(a_i + b_s)$ iff $i \in s$ for all $i < n$ and $s \subseteq n$). This turns out to follow from a slight generalization of the Green-Tao theorem about arithmetic progressions in the primes [GT08] (i.e., without using (D)), stating that for any $n < \omega$ and $s \subseteq n$ there is an arithmetic progression $\langle a_i \mid i < n \rangle$ of natural numbers such that a_i is prime iff $i \in s$. This fact follows from the proof of the Green-Tao theorem as was explained to us in a private communication by Tamar Ziegler, and also follows from (D).

References

[Bès01] Alexis Bès. A survey of arithmetical definability. *Bull. Belg. Math. Soc. Simon Stevin*, (suppl.):1–54, 2001. A tribute to Maurice Boffa.

[BJW93] P. T. Bateman, C. G. Jockusch, and A. R. Woods. Decidability and undecidability of theories with a predicate for the primes. *J. Symbolic Logic*, 58(2):672–687, 1993.

[CP98] Z. Chatzidakis and A. Pillay. Generic structures and simple theories. *Ann. Pure Appl. Logic*, 95(1-3):71–92, 1998.

[DGL11] Alfred Dolich, John Goodrick, and David Lippel. Dp-minimality: basic facts and examples. *Notre Dame J. Form. Log.*, 52(3):267–288, 2011.

[Dic04] L. E. Dickson. A new extension of Dirichlet's theorem on prime numbers. *Messenger of mathematics*, 33:155—161, 1904.

[GT08] Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions. *Ann. of Math. (2)*, 167(2):481–547, 2008.

[Kor01] Ivan Korec. A list of arithmetical structures complete with respect to the first-order definability. *Theoret. Comput. Sci.*, 257(1-2):115–151, 2001. Weak arithmetics.

[Mar02] David Marker. *Model Theory: An Introduction*. Springer, 2002.

[OU11] Alf Onshuus and Alexander Usvyatsov. On dp-minimality, strong dependence and weight. *Journal of symbolic logic*, 76(3):737–758, 2011.

[Poi14] Bruno Poizat. Supergénérix. *J. Algebra*, 404:240–270, 2014. À la mémoire d'Éric Jaligot. [In memoriam Éric Jaligot].

[PS14] Daniel Palacin and Rizos Sklinos. On superstable expansions of free abelian groups. *preprint, arXiv: 1405. 0568*, 2014.

[Rib89] Paulo Ribenboim. *The book of prime number records*. Springer-Verlag, New York, second edition, 1989.

[Sim11] Pierre Simon. On dp-minimal ordered structures. *Journal of Symbolic Logic*, 76(2):448–460, 2011.

[Woo13] Alan Robert Woods. Some problems in logic and number theory, and their connections. In *New studies in weak arithmetics*, volume 211 of *CSLI Lecture Notes*, pages 271–388. CSLI Publ., Stanford, CA, 2013. Dissertation, University of Manchester, Manchester, 1981, With an obituary by Costas Dimitracopoulos.

Curves of Low Genus on Surfaces and Some Extensions of Büchi's Problem

Natalia Garcia-Fritz

A sequence $a_1, \ldots, a_n$ has *second differences equal to* 2 if for all $3 \leq j \leq n$ we have $a_i - 2a_{j-1} + a_{j-2} = 2$. Büchi's problem [7] says the following:

Problem 1 (Büchi, 1970)**.** *Does there exist a positive integer M such that every sequence of M integer squares with second differences equal to* 2 *is necessarily of the form $(x+i)^2$, for $x \in \mathbb{Z}$ and $1 \leq i \leq M$?*

We will call sequences of the form $(x+i)^2$ *trivial*. As of today, the longest known non-trivial sequence of squares with second differences equal to 2 has length four, although this problem is still open.

This question also makes sense for any ring with a multiplicative unit, for example Hensley [6] in the eighties solved Büchi's problem on $\mathbb{F}_p$. A positive solution of Büchi's problem over a ring A with undecidable positive existential theory over a language $\mathcal{L}$ that contains the language of rings $\mathcal{L}_R = \{0, 1, =, +, \cdot\}$,

gives undecidability for the existential theory of A over the language $\mathcal{L}_2 = \{P_2\} \cup \mathcal{L} \setminus \{\cdot\}$, where $P_2(x)$ means "x is a square", by allowing us to define multiplication in a positive existential way using this new language (cf. [8] pp. 779-770).

In 2000, Vojta [12] solved Büchi's problem over number fields under the Bombieri-Lang conjecture, by showing that all the curves of genus 0 or 1 on the surfaces

$$B_n := \begin{cases} x_3^2 - 2x_2^2 + x_1^2 = 2x_0^2 \\ \vdots \\ x_n^2 - 2x_{n-1}^2 + x_{n-2}^2 = 2x_0^2. \end{cases} \subseteq \mathbb{P}^n$$

with $n \geq 8$ satisfy that their rational points correspond to trivial sequences. For doing this, he finds *all* curves of genus 0 or 1 on these surfaces, building on previous work of Bogomolov [1]. He also solved this unconditionally for function fields of characteristic zero by finding all curves of genus g on these surfaces, for n large enough depending on g. Moreover, using Nevanlinna theory, he solves Büchi's problem in the context of complex meromorphic functions. My talk focused on the method appearing in his work and the extensions obtained in my thesis [5].

Let us mention that in 2006 Pheidas and Vidaux [10], by using an elementary method solved Büchi's problem for $F(z)$ in characteristic zero and also for characteristic $p \geq 19$ (which cannot be obtained from Vojta's work), and in 2009 Vidaux and Shlapentokh [11] extended this method to solve Büchi's problem for any algebraic function field of characteristic zero or of large enough characteristic with the expected applications in Logic. See [8] for more details on Büchi's problem.

One can generalize Büchi's problem by considering sequences of k-th powers with *constant second differences* (cf. [4]). This gives the following surfaces:

$$X_{n,k} := \begin{cases} x_3^k - 3x_2^k + 3x_1^k - x_0^k = 0 \\ \vdots \\ x_n^k - 3x_{n-1}^k + 3x_{n-2}^k - x_{n-3}^k = 0. \end{cases} \subseteq \mathbb{P}^n$$

For $k = 2$, defined by Browkin and Brzezinski at the H10 meeting in Ghent, 2010.

One can prove, by finding all the curves of genus less than or equal to g on the surface $X_{n,k}$ with n large enough (depending on k and g), the following:

Theorem 2 (G-F [4])**.** *Assume the Bombieri-Lang conjecture for the surfaces $X_{n,k}$. For any $k \geq 3$, there exists $M_k > 0$ such that there are no sequences of M_k k-th powers with second differences equal to 2.*

One can unconditionally prove the analogue of this arithmetic result for function fields of characteristic zero (see also [4]). Defining $\mathcal{L}_P = \{0, 1, =, +, P\}$ where $P(x)$ means "x is a power" as in [2], from Theorem 2 one obtains the following result:

Theorem 3. *Under the Bombieri-Lang conjecture and the ABC conjecture for four terms, the positive existential theory of $\mathbb{Z}$ over the language $\mathcal{L}_P$ is undecidable.*

In my talk I explained how Vojta's method for finding all curves of low genus on surfaces works, and how to obtain new arithmetic applications (under the Bombieri-Lang conjecture for number fields, and unconditionally for function fields).

He uses the following notion:

Definition 4. Let X be a smooth variety over $\mathbb{C}$, let $\mathcal{L}$ be an invertible sheaf on X and let $\omega \in H^0(X, \mathcal{L} \otimes S^r\Omega^1_{X/\mathbb{C}})$, where r is an integer. An irreducible curve C on X is said to be **ω-integral** if the image of the section $\varphi_C^*\omega$ in $H^0(\tilde{C}, \varphi_C^*\mathcal{L} \otimes S^r\Omega^1_{\tilde{C}/\mathbb{C}})$ is zero, where $\varphi_C : \tilde{C} \to X$ is the normalization of $C \subset X$.

After choosing a fixed $\omega \in H^0(X, \mathcal{L} \otimes S^r\Omega^1_{X/\mathbb{C}})$, one finds *all* ω-integral curves in X, by translating the condition of being ω-integral into solutions of differential equations. One finds solutions and using a local analysis one shows that there are no other solutions. Using cohomological arguments regarding degrees of sheaves over curves of X, one proves that every curve of genus 0 or 1 must be ω-integral.

To find such an ω, one first chooses a morphism $\pi : X \to \mathbb{P}^2$ satisfying that all irreducible components of its branch divisor are ω'-integral, for some global section $\omega' \in H^0(\mathbb{P}^2, \mathcal{L}' \otimes S^r\Omega^1_{\mathbb{P}^2/\mathbb{C}})$. If this branch divisor is "large" related to the ω' chosen, then one is able to find an $\omega \in H^0(X, \mathcal{L} \otimes S^r\Omega^1_{X/\mathbb{C}})$ satisfying the cohomological conditions we needed.

Another interesting application of this method concerns Mohanty's problem [4].

Theorem 5. *Assume the Bombieri-Lang conjecture for surfaces. There is an absolute constant M such that there is no y-arithmetic progression of rational points of length M on any Mordell's elliptic curve over $\mathbb{Q}$.*

Some open problems related to this method are the following:

Question 1. Which hypothesis must the surface $X/\mathbb{C}$ satisfy to make sure that there exists an ω that makes the method work?

It should be a condition on the relation between the branch divisor $B \subset \mathbb{P}^2$ of a morphism $\pi : X \to \mathbb{P}^2$ and the invertible sheaf $\mathcal{L}$ with the smallest degree possible (over curves in X of geometric genus less than or equal to a fixed number g) such that there exists an $\omega \in H^0(\mathbb{P}^2, \mathcal{L} \otimes S^r\Omega^1_{\mathbb{P}^2/\mathbb{C}})$ making all irreducible components of B to be ω-integral.

Another problem is to extend this method to higher dimensional varieties. Most steps of this method can be extended to this case, however one needs the following:

Question 2. Given a smooth projective variety $X/\mathbb{C}$ of dimension greater than two, and a section $\omega \in H^0(X, \mathcal{L} \otimes S^r\Omega^1_{X/\mathbb{C}})$, how can we check that a list of ω-integral curves (resp. hypersurfaces) consists of *all* ω-integral curves (resp. hypersurfaces) of X?

References

[1] M. Deschamps, *Courbes de genre géométrique borné sur une surface de type général* [d'après F. A. Bogomolov]. Séminaire Bourbaki, 30e année (1977/78), Exp. No. 519, pp. 233–247, Lecture Notes in Math., **710**, Springer, Berlin, 1979.

[2] N. Garcia-Fritz, *Representation of Powers by Polynomials and the Language of Powers.* J. Lond. Math. Soc. (2) **87** (2013), no. 2, 347–364.

[3] N. Garcia-Fritz, *Sequences of powers with second differences equal to two and hyperbolicity.* Accepted for publication in Transactions of the American Mathematical Society.

[4] N. Garcia-Fritz, *Quadratic sequences of powers and Mohanty's conjecture.* Submitted.

[5] N. Garcia-Fritz, *Curves of low genus on surfaces and applications to Diophantine problems.* PhD Thesis, Queen's University, (2015).

[6] D. Hensley, *Sequences of squares with second difference of two and a problem of logic.* Unpublished (1980-1983).

[7] L. Lipshitz, *Quadratic forms, the five square problem, and diophantine equations, The collected works of J. Richard Büchi* (S. MacLane and Dirk Siefkes, eds.) Springer, (1990), 677–680.

[8] H. Pasten, T. Pheidas, X. Vidaux, *A survey on Büchi's problem: new presentations and open problems*, Zapiski Nauchn. Sem. POMI, **377**, (2010), 111–140.

[9] T. Pheidas, X. Vidaux, *Extensions of Büchi's problem: questions of decidability for addition and kth powers.* Fund. Math. **185** (2005), no. 2, 171–194.

[10] T. Pheidas, X. Vidaux, *The analogue of Büchi's problem for rational functions.* J. London Math. Soc., **74**, No. 3 (2006), 545–565.

[11] A. Shlapentokh, X. Vidaux, *The analogue of Büchi's problem for function fields.* J. Algebra **330** (2011), 482–506.

[12] P. Vojta, *Diagonal quadratic forms and Hilbert's tenth problem*, Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Contemp. Math., **270**, Amer. Math. Soc., Providence, RI, (2000), 261–274.

On the Elementary Equivalence vs Isomorphism Problem

Florian Pop

The EEvIP (Elementary Equivalence vs Isomorphism Problem) is the question of whether the elementary theory $Th(K)$ of a finitely generated field K determines the isomorphism type of K (as a field); that is, given K, L finitely generated, does one have

$$Th(K) = Th(L) \quad \Rightarrow \quad K \cong L?$$

A much stronger variant of this question (called by some the conjecture of Pop) asks the following: Given a finitely generated field K, is there a sentence φ_K such that for all finitely generated fields L one has

$$\varphi_K \text{ holds in } L \quad \Leftrightarrow \quad K \cong L?$$

The first result of this type was proved by Rumely [1] for global fields, and geometric variants (for function fields of curve over algebraically closed base fields) were proven by, among others, Duret [2, 3] and Pierce [4]. A major breakthrough came with the introduction of the quadratic forms (Pfister forms) method, and that allowed partial results for higher dimensional finitely generated fields and function fields. We presented a proof of the fact that for finitely generated fields K with $\mathtt{Kr.dim}(K) < 3$ there exists a sentence φ_K characterising the isomorphism

type of K among all finitely generated fields. Further, we provided hints about how these methods would lead to showing the existence of such sentences φ_K for all finitely generated fields K.

The main tools for these kind of results are the following:

- Milnor Conjecture (Vojevodsky, Rost cf. [5])
- Hasse Higher Local Global Principles for Galois Cohomology (Kato [8])

The problem of finding φ_K is thus reduced to giving formulae which uniformly define the prime divisors of finitely generated fields. We can then conclude by applying the (first part of the) method of Scanlon [9].

References

[1] Rumely, R., *Undecidability and Definability for the Theory of Global Fields*. Transactions AMS **262** No. 1, (1980), 195–217.

[2] Duret, J.-L., *Sur la théorie élémentaire des corps de fonctions*. J. Symbolic Logic **51** (1986), 948–956.

[3] Duret, J.-L., *Équivalence élémentaire et isomorphisme des corps de courbe sur un corps algébriquement clos*. J. Symbolic Logic **57** (1992), 808–923.

[4] Pierce, D., *Function fields and elementary equivalence*, Bull. London Math. Soc. **31** (1999), 431–440.

[5] Kahn, E., *La conjecture de Milnor (d'après Voevodsky)*. Séminaire Bourbaki, Asterisque **245** (1997), 379–418.

[6] Rost, M., see References in [5] above.

[7] Vojevodsky, V., see References in [5] above.

[8] Kato, K., *A Hasse principle for two dimensional global fields*. J. reine angew. Math. **366** (1986), 142–180.

[9] Scanlon, T., *Infinite finitely generated fields are biinterpretable with* $\mathbb{N}$. J. Amer. Math. Soc. **21** (2008), 893–908.

Non-norms of Quadratic Extensions of Global Fields are Diophantine

Travis Morrison

(joint work with Kirsten Eisenträger)

J. Robinson [Rob49] gave a $\forall\exists\forall$ definition of $\mathbb{Z}$ in $\mathbb{Q}$. Her result was improved by Poonen [Poo09a] who gave a $\forall\exists$ definition of $\mathbb{Z}$ in $\mathbb{Q}$. Koenigsmann [Koe16] further improved on Poonen's result by removing the existential quantifier, giving a definition of the integers inside $\mathbb{Q}$ that uses only universal quantifiers. Park generalized this and showed that for any number field K, the ring of integers $\mathcal{O}_K$ is universally definable in K [8].

We can ask for similar definitions for global fields of positive characteristic. Let q be a power of a prime. While Hilbert's Tenth Problem for both $\mathbb{F}_q[t]$ and $\mathbb{F}_q(t)$ is undecidable ([Den79], [Phe91], [Vid94]), it is not known whether $\mathbb{F}_q[t]$ is diophantine over $\mathbb{F}_q(t)$. Showing this still seems out of reach, but it is possible to give a universal definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ which we do in [EM16]. More generally, we prove the natural generalization of Park's result for defining rings of integers to global function fields K.

For a finite set S of primes of K we denote by $\mathcal{O}_S$ the ring

$$\mathcal{O}_S := \{x \in K : v_{\mathfrak{p}}(x) \geq 0 \quad \forall \text{ primes } \mathfrak{p} \notin S\}.$$

This is the ring of S-integers of K.

Theorem 1. *Let K be a global function field of odd characteristic and let S be a finite, nonempty set of primes of K. Then $\mathcal{O}_S$ is first-order universally definable in K. Equivalently, $K \setminus \mathcal{O}_S$ is diophantine over K.*

Using the machinery developed by Park and its extension to global function fields, we also prove the following theorem, which generalizes a result of Koenigsmann.

Theorem 2. *Let K be a global field with char$(K) \neq 2$. Then*

$$\{(x, y) \in K^\times \times K^\times | x \notin N_y(K(\sqrt{y}))\}$$

is diophantine over K.

We will discuss the case that K is a global function field of characteristic not 2. To prove the second theorem, first we use ideas originally due to Eisenträger to prescribe integrality at a prime of K.

(1) Given a prime $\mathfrak{p} \in S_K$, let $v := v_{\mathfrak{p}}$ be its associated valuation, normalized so that it takes values in $\mathbb{Z} \cup \{\infty\}$. Define $K_{\mathfrak{p}}$ to be the completion of K at $\mathfrak{p}$, $R_{\mathfrak{p}}$ the ring of integers in $K_{\mathfrak{p}}$, the maximal ideal of $R_{\mathfrak{p}}$ by $\hat{\mathfrak{p}}$, and $\mathbb{F}_{\mathfrak{p}}$ the residue field of $\mathfrak{p}$. Let $\mathcal{O}_{\mathfrak{p}} := R_{\mathfrak{p}} \cap K$; this is the local ring of the prime $\mathfrak{p}$ in K.
(2) $H_{a,b} = K \oplus \alpha K \oplus \beta K \oplus \alpha\beta K$, the quaternion algebra over K with multiplication given by $\alpha^2 = a, \beta^2 = b, \alpha\beta = -\beta\alpha$.
(3) $\Delta_{a,b} = \{\mathfrak{p} \in S_K : H_{a,b} \otimes_K K_{\mathfrak{p}} \ncong M_2(K_{\mathfrak{p}})\}$, that is, the set of primes where $H_{a,b}$ ramifies.
(4) $(a, b)_{\mathfrak{p}} = \begin{cases} 1 & : \mathfrak{p} \notin \Delta_{a,b} \\ -1 & : \mathfrak{p} \in \Delta_{a,b} \end{cases}$, the Hilbert symbol of $K_{\mathfrak{p}}$.
(5) $S_{a,b} = \{2x_1 \in K : \exists x_2, x_3, x_4$ such that $x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1\}$. This is the set of traces of norm one elements of $H_{a,b}$.
(6) $T_{a,b} = S_{a,b} + S_{a,b}$.

Then one can show (see [Par13]) that

$$T_{a,b} := \bigcap_{\mathfrak{p} \in \Delta_{a,b}} \mathcal{O}_{\mathfrak{p}}.$$

This is a diophantine definition of the semi-local ring $\bigcap_{\mathfrak{p} \in \Delta_{a,b}} \mathcal{O}_{\mathfrak{p}}$.

Park's idea is to fix $a, b \in K^\times$ satisfying some technical conditions so that the splitting behavior of a prime $\mathfrak{p}$ of K in $L := K(\sqrt{a}, \sqrt{b})$ corresponds to certain quaternion algebras ramifying at $\mathfrak{p}$. This allows one to encode integrality at some prime $\mathfrak{p}$ with some fixed Frobenius element without referring to the prime $\mathfrak{p}$. Next, one defines a family of semi-local rings parametrized by $K^\times$.

For $p, q \in K^\times$, let

$$R_p^{(-1,-1)} = \bigcap_{\mathfrak{p} \in \Delta_{a,p} \cap \Delta_{b,p}} \mathcal{O}_\mathfrak{p},$$
$$R_p^{(1,-1)} = \bigcap_{\mathfrak{p} \in \Delta_{ab,p} \cap \Delta_{b,p}} \mathcal{O}_\mathfrak{p},$$
$$R_p^{(-1,1)} = \bigcap_{\mathfrak{p} \in \Delta_{a,p} \cap \Delta_{ab,p}} \mathcal{O}_\mathfrak{p},$$
$$R_{p,q}^{(1,1)} = \bigcap_{\mathfrak{p} \in \Delta_{ap,q} \cap \Delta_{bp,q}} \mathcal{O}_\mathfrak{p}.$$

These are all diophantine over K. The idea is that, for example, the ring $R_p^{(-1,-1)}$ will be a semi-local subring of K such that its prime ideals all split completely in L. Let $\phi_{L/K}$ denote the Artin symbol for L/K and identify $\mathrm{Gal}(L/K) \simeq \{\pm 1\} \times \{\pm 1\}$. Let $\mathfrak{m}$ be an admissible modulus of K for L/K.

For $p \in K^\times$, define the following subsets of primes of K:

$$\mathbb{P}(p) := \{\mathfrak{p} \in S_K : v_\mathfrak{p}(p) \text{ is odd.}\}.$$

Also, for $(i,j) \in \mathrm{Gal}(L/K)$, $i, j \in \{\pm 1\}$, set

$$\mathbb{P}^{(i,j)} = \{\mathfrak{p} \in S_K : \mathfrak{p} \in I_\mathfrak{m} \text{ and } \psi_{L/K}(\mathfrak{p}) = (i,j)\}$$

and set

$$\mathbb{P}^{(i,j)}(p) = \mathbb{P}(p) \cap \mathbb{P}^{(i,j)}.$$

We will need that the Jacobson radicals of the semi-local rings $R_\mathfrak{p}^\sigma$ for $\sigma \neq (1,1) \in \mathrm{Gal}(L/K)$ and $R_{p,q}^{(1,1)}$ are diophantine. This will hold when we parametrize these rings by the following:

$$\Phi_\sigma = \{p \in K^\times : (p) \in I_\mathfrak{m}, \psi_{L/K}((p)) = \sigma, \text{ and } \mathbb{P}(p) \subseteq \mathbb{P}^{(1,1)} \cup \mathbb{P}^\sigma\}.$$

$$\widetilde{\Phi_\sigma} := K^{\times 2} \cdot \Phi_\sigma;$$

$$\Psi_K := \left\{ (p,q) \in \widetilde{\Phi_{(1,1)}} \times \widetilde{\Phi_{(-1,-1)}} \mid \prod_{\mathfrak{p} \mid \mathfrak{m}} (ap, q)_\mathfrak{p} = -1 \right.$$
$$\left. \text{and } p \in a \cdot K^{\times 2} \cdot (1 + J(R_q^{(-1,-1)})) \right\}.$$

With these definitions, given $p \in K^\times$, we have

$$\mathbb{P}^{(-1,-1)}(p) = \Delta_{a,p} \cap \Delta_{b,p},$$
$$\mathbb{P}^{(-1,1)}(p) = \Delta_{a,p} \cap \Delta_{ab,p},$$
$$\mathbb{P}^{(1,-1)}(p) = \Delta_{b,p} \cap \Delta_{ab,p}.$$

Then one shows that for a prime $\mathfrak{p}$ with $\phi_{L/K}(\mathfrak{p}) = \sigma \neq (1,1)$, there is a $p \in \Phi_\sigma$ such that $\mathbb{P}^\sigma(p) = \{\mathfrak{p}\}$. Additionally, if $p \in \Phi_\sigma$, then $\mathbb{P}^\sigma(p)$ is nonempty, and

its Jacobson radical is diophantine over K. Finally, Φ_σ is diophantine over K. Similar statements hold for Ψ_K and $R_{p,q}^{(1,1)}$.

Now we use the following local-global principle, originally due to Hilbert: for $x, y \in K^\times$, x is a norm of $K(\sqrt{y})$ if and only if it is a norm in $K_\mathfrak{p}(\sqrt{y})$ for every prime $\mathfrak{p}$ of K. Then the following list of conditions gives a diophantine description of the pairs (x, y) such that x is not a norm of $K(\sqrt{y})$:

- $\exists\, \mathfrak{p}|\mathfrak{m}$ such that $(x, y)_\mathfrak{p} = -1$,
- $\bigvee_{\sigma\neq(1,1)} \exists p \in \Phi_\sigma$ such that

$$\big((x \in p \cdot K^{\times 2} \cdot (R_p^\sigma)^\times) \wedge (y \text{ or } -xy \in s_\sigma \cdot K^{\times 2} \cdot (1 + J(R_p^\sigma)))\big)$$
$$\vee\big((y \in p \cdot K^{\times 2} \cdot (R_p^\sigma)^\times) \wedge (x \text{ or } -xy \in s_\sigma \cdot K^{\times 2} \cdot (1 + J(R_p^\sigma)))\big),$$

- $\exists (p, q) \in \Psi_K$ such that $q \in (R_{p,q}^{(1,1)})^\times$ and

$$\big((x \in p \cdot K^{\times 2} \cdot (R_{p,q}^{(1,1)})^\times) \wedge (y \text{ or } -xy \in q \cdot K^{\times 2} \cdot (1 + J(R_{p,q}^{(1,1)})))\big)$$
$$\vee\big((y \in p \cdot K^{\times 2} \cdot (R_{p,q}^{(1,1)})^\times) \wedge (x \text{ or } -xy \in q \cdot K^{\times 2} \cdot (1 + J(R_{p,q}^{(1,1)})))\big).$$

To prove this, we make use of the facts about Φ_σ and Ψ_K along with the following formula for the Hilbert symbol:

$$(a, b)_\mathfrak{p} = \left[(-1)^{v_\mathfrak{p}(a)v_\mathfrak{p}(b)} \left(\frac{a^{v_\mathfrak{p}(b)}}{b^{v_\mathfrak{p}(a)}}\right)\right]^{(|\mathbb{F}_\mathfrak{p}|-1)/2}.$$

For details of this argument, along with a proof of the theorem on the universal definition of S-integers in a global field, see [EM16].

References

[AT68] E. Artin and J. Tate. *Class field theory*. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[Den79] J. Denef. The Diophantine problem for polynomial rings of positive characteristic. In *Logic Colloquium '78 (Mons, 1978)*, volume 97 of *Stud. Logic Foundations Math.*, pages 131–145. North-Holland, Amsterdam-New York, 1979.

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson. The decision problem for exponential diophantine equations. *Ann. of Math. (2)*, 74:425–436, 1961.

[Eis03] Kirsten Eisenträger. Hilbert's Tenth Problem for algebraic function fields of characteristic 2. *Pacific J. Math.*, 210(2):261–281, 2003.

[Koe16] Jochen Koenigsmann. Defining $\mathbb{Z}$ in $\mathbb{Q}$. *Ann. of Math. (2)*, 183(1):73–93, 2016.

[Mat70] Yu. V. Matiyasevich. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191:279–282, 1970.

[Maz92] Barry Mazur. The topology of rational points. *Experiment. Math.*, 1(1):35–45, 1992.

[Mil11] J.S. Milne. Class field theory (v4.01), 2011. Available at www.jmilne.org/math/.

[Par13] Jennifer Park. A universal first-order formula defining the ring of integers in a number field. *Math. Res. Lett.*, 20(5):961–980, 2013.

[Phe91] Thanases Pheidas. Hilbert's tenth problem for fields of rational functions over finite fields. *Invent. Math.*, 103(1):1–8, 1991.

[Poo09a] Bjorn Poonen. Characterizing integers among rational numbers with a universal-existential formula. *Amer. J. Math.*, 131(3):675–682, 2009.

[Poo09b] Bjorn Poonen. The set of nonsquares in a number field is Diophantine. *Math. Res. Lett.*, 16(1):165–170, 2009.

[Rob49] Julia Robinson. Definability and decision problems in arithmetic. *J. Symbolic Logic*, 14:98–114, 1949.
[Ros87] Michael Rosen. The Hilbert class field in function fields. *Exposition. Math.*, 5(4):365–378, 1987.
[Ros02] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.
[Rum80] R. S. Rumely. Undecidability and definability for the theory of global fields. *Trans. Amer. Math. Soc.*, 262(1):195–217, 1980.
[Ser79] Jean Pierre Serre. *Local Fields*. Springer-Verlag New York, Inc, New York, 1979.
[Shl94] Alexandra Shlapentokh. Diophantine classes of holomorphy rings of global fields. *J. Algebra*, 169(1):139–175, 1994.
[Shl96] Alexandra Shlapentokh. Diophantine undecidability over algebraic function fields over finite fields of constants. *J. Number Theory*, 58(2):317–342, 1996.
[EM16] Kirsten Eisenträger and Travis Morrison. Universally and existentially definable subsets of global fields. *arXiv:1609.09787*, 2016. Preprint.
[Shl15] Alexandra Shlapentokh. On definitions of polynomials over function fields of positive characteristic. *arXiv:1502.02714*, 2015. Preprint.
[Vid94] Carlos R. Videla. Hilbert's tenth problem for rational function fields in characteristic 2. *Proc. Amer. Math. Soc.*, 120(1):249–253, 1994.

Extremal Fields

Franz-Viktor Kuhlmann
(joint work with Sylvy Anscombe, Salih Azgin, Florian Pop)

I was introduced to the notion of "extremal field" by Yuri Ershov in a conference at the IPM, Teheran, in 2003. He gave the following definition: a valued field (K, v) with value group vK is called *extremal* if for all $n \in \mathbb{N}$ and every polynomial $f \in K[X_1, \ldots, X_n]$ the set

$$\{vf(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in K\} \subseteq vK \cup \{\infty\} \tag{1}$$

has a maximum. Ershov "proved" (see [1]):

Theorem 1. *If (K, v) is henselian and defectless with value group isomorphic to $\mathbb{Z}$, then it is extremal.*

In 2009 at the Fields Institute I worked with Salih Azgin (now Durhan) and Florian Pop on the characterization of extremal fields. Sergej Starchenko gave us the following counterexample to Ershov's theorem. Take $K = \mathbb{R}((t))$ with the t-adic valuation v_t, $f(X, Y) = X^2 + (XY - 1)^2$, and observe that the values $v_t f(t^k, t^{-k}) = v_t t^{2k} = 2k$, $k \in \mathbb{N}$, are unbounded in the value group $\mathbb{Z}$. But if $f(a, b) = 0$ for $a, b \in K$, then since K is orderable, we must have that $a = 0$ and $ab - 1 = 0$, which is impossible.

We changed the above definition, replacing "$a_1, \ldots, a_n \in K$" by "$a_1, \ldots, a_n$ in the valuation ring of K". With this new definition, Theorem 1 holds. We proved in [3]:

Theorem 2. *If the valued field (K, v) is extremal, then it is henselian and defectless, and either*
I) vK is a $\mathbb{Z}$-group (i.e., $vK \equiv \mathbb{Z}$), or

II) vK is divisible and the residue field Kv is large.
The converse holds if
- $\mathrm{char}Kv = 0$ *(giving us a full characterization of extremal fields in this case), or*
- $vK \simeq \mathbb{Z}$ *(by Theorem 1), or*
- $\mathrm{char}K > 0$, *vK is divisible and Kv is large and perfect.*

The proof of the converse uses the model theory of tame valued fields (see [2]), in particular an Ax-Kochen-Ershov Principle in positive characteristic which is not available in mixed characteristic; this led us to the assumption "$\mathrm{char}K > 0$" for the converse in case II). Later I was able to substitute the AKE Principle by a weaker principle in order to drop the unwanted assumption. In this way I obtained a complete characterization of tame fields of positive residue characteristic that are extremal:

Theorem 3. *A tame valued field (K, v) with $\mathrm{char}Kv > 0$ is extremal if and only if its value group is divisible and its residue field is large.*

However, the characterization of all extremal fields of positive residue characteristic is still not complete. At the time of paper [3] it was not clear whether there are any extremal fields with divisible value group and imperfect residue field. Apart from Theorem 3, the new paper [4] also contains the following theorem, which is based on a construction suggested by a referee and worked out with the help of Sylvy Anscombe:

Theorem 4. *Take an $\aleph_1$-saturated valued field (K, v). If $v = v_1 \circ v_2 \circ v_3$ with v_2 of rank 1 (i.e., $v_2(Kv_1)$ is archimedean ordered), then (Kv_1, v_2) is extremal with value group $\mathbb{Z}$ or $\mathbb{R}$, and it is maximal (i.e., does not admit proper extensions that do not change value group or residue field).*

This result is quite surprising as there are no assumptions on (K, v) other than the saturation. If one takes (K, v) to have imperfect residue field, then one obtains extremal fields (Kv_1, v_2) with imperfect residue field. If one takes vK to be divisible, then also the value group of (Kv_1, v_2) is divisible. The following questions about extremal fields are still open:

Open problems:
1) Take a valued field (K, v) of positive residue characteristic. Assume that vK is a $\mathbb{Z}$-group, or that vK is divisible and Kv is an imperfect large field. Is there a simple (and useful) additional assumption which ensures that (K, v) is extremal?
2) If $v = v_1 \circ v_2$ with (K, v_1) and (Kv_1, v_2) extremal and v_1 having divisible value group, does it follow that v is extremal?
3) We know that if $v = v_1 \circ v_2$ is extremal, then so is (Kv_1, v_2) (see [4]). But we do not know whether also (K, v_1) is extremal.
4) It is not true that every maximal valued field is extremal. But is it true that every maximal valued field with value group a $\mathbb{Z}$-group or with divisible value group and large residue field is extremal?
5) Theorem 1 is particularly interesting because it implies that the Laurent series field $\mathbb{F}_p((t))$ with the t-adic valuation v_t is extremal. As it is unknown whether its elementary theory is decidable, it is an important task to determine whether

the following is a complete axiomatization: "extremal valued field of characteristic $p > 0$ with residue field $\mathbb{F}_p$ and value group elementarily equivalent to $\mathbb{Z}$".

References

[1] Yu. L. Ershov, *Extremal valued fields*, Algebra Logika **43** (2004), 582–588, 631. Translation in Algebra Logic **43** (2004), 327–330.

[2] F.-V. Kuhlmann, *The algebra and model theory of tame valued fields*, J. reine angew. Math. **719** (2016), 1–43.

[3] S. Azgin, F.-V. Kuhlmann, F. Pop, *Characterization of Extremal Valued Fields*, Proc. Amer. Math. Soc. **140** (2012), 1535–1547.

[4] S. Anscombe, F.-V. Kuhlmann, *Notes on extremal and tame valued fields*, J. Symb. Logic **81** (2016), 400–416.

(Un)Decidable Additive Expansions of Certain Euclidean Rings.

Françoise Point

Using finite automata theory, one can give similar proofs for proving either decidability (or undecidability) results on one hand for certain expansions of $(\mathbb{Z}, +, 0, <)$ and on the other hand of $(\mathbb{F}_p[X], +, 0)$, $(\mathbb{F}_p[X, X^{-1}], +, 0)$, $(\mathbb{F}_p[[X]], +, 0)$...

In the first part of the talk, we recalled the notion for a first-order structure to be finite automaton presentable (FA-presentable) which implies the decidability of the structure [2]. Then we described a class of Euclidean rings for which we can identify decidable/ undecidable expansions of their additive groups. This is a joint work with Michel Rigo and Laurent Waxweiler [5].

Then in order to handle expansions of the additive group of power series rings (over finite fields), we have to use finite automata accepting infinite words. In this case, we only considered expansions of $(\mathbb{F}_{p^n}[[X]], +, 0)$ for which we obtained similar (un)decidability results in a joint work with Luc Bélair and Maxime Gélinas [1].

In the last part of the talk, we compared certain expansions of the ordered group of the integers, namely $(\mathbb{Z}, +, 0, <, R)$ with the ones obtained when forgetting about the order, namely $(\mathbb{Z}, +, 0, R)$, where R is an strictly increasing *sparse* sequence as defined by A. I. Semenov [8].

We assume throughout that $(R, +, \cdot, 0, 1, \delta)$ is an Euclidean ring equipped with an Euclidean function $\delta : R^\star \to \mathbb{N}$ [7], where $R^\star := R \setminus \{0\}$ and we fix a non-invertible element $r \in R^\star$. This function δ induces a (total) pre-ordering $\preceq$ on R as follows: for $u,\ v \in R^\star$, we write $u \preceq v$, if $\delta(u) \leq \delta(v)$; note that $1 \preceq u$, for all $u \in R^\star$. Let $P_r := \{r^n :\ n \in \mathbb{N}\}$. We define two functions $\lambda_r,\ V_r$ from $R^\star$ to P_r as follows: The function $\lambda_r : R^\star \to P_r$ maps u to the highest power r^n of r with the property that $r^n \preceq u \prec r^{n+1}$. The function $V_r : R^\star \to P_r$ sends u to the highest power of r dividing u.

Under some natural hypothesis on the representability of the elements of R (or of a subring R_0 such that R is interpretable with R_0) by a finite automaton, we obtain the following decidability result. Suppose that R satisfies hypothesis $(\mathbf{Rep})_{r,fin}$. Then, if the graph of $+$ is r-recognizable, the structure $(R, +, -, 0, \lambda_r, V_r, \preceq, \cdot r)$ is

FA-presentable and so decidable [5, Proposition 3.1]. (Note that using the same ideas than the ones recalled in [1], one can show that the definable subsets are exactly the recognizable ones.)

Recall that any element $u \in R^\star$ can be written in a unique way, up to permutation of factors, as a product of prime elements times an invertible element, we define its *support* as the set of prime elements appearing in such decomposition.

Assume that R satisfies $(\mathbf{Rep})_{r,fin}$, and some compatibility conditions $(\mathbf{C}+)_r$ of $+$ with the representation in base r and compatibility condition $(\mathbf{C}\times)$ of $\cdot$ with the δ function. Let $r, s \in R^\star$ be two non-invertible elements which are multiplicatively independent with $s \preceq r$. Then we can define the graph of multiplication in the structure $(R, +, -, 0, \preceq, V_r, V_s, .u; u \in R)$ [5, Theorem 2.25], which implies the undecidability of its theory.

Question 1 ([5])**.** Is the structure $(R, +, -, 0, \preceq, V_r, P_s, .u; u \in R)$ undecidable?

When $R = \mathbb{Z}$, undecidability was proven by A. Bès.

Question 2. Let $r, s \in R^\star$ be two non-invertible elements which are multiplicatively independent. Can one get a characterisation of subsets of R which are definable both in $(R, +, -, 0, \preceq, V_r, .r)$ and in $(R, +, -, 0, \preceq, V_s, .s)$?

When $R = \mathbb{Z}$, the answer is given by Cobham's theorem and when R is a polynomial ring, M. Rigo and L. Waxweiler proved that one gets other subsets than those definable in $(R, +, 0)$ [6, section 2.1]. (Note that recently there was another proof of Cobham's theorem by Schäfke and Singer [9] analysing common power series solutions of two Mahler equations.)

When $r, s \in R^\star$ are two non-invertible elements which are multiplicatively dependent, then $(R, +, -, 0, \preceq, V_r, .r)$ and $(R, +, -, 0, \preceq, V_s, .s)$ are interdefinable.

Finally let us mention the following undecidability result. Assume in addition that no sum of at least two powers of r is invertible, except when this sum is equal to 1. Let f be the partial multiplication restricted to $R \times P_r$, namely $f(u, r^n) := u.r^n$, where $u \in R$ and $r^n \in P_r$. Then the theory of $(R, +, 0, 1, P_r, f)$ is undecidable [5, Corollary 2.4]. The corresponding expansion with $\mathbb{Q}$ instead of R and 2 for r has been shown to be decidable by F. Delon (the case $R = \mathbb{Z}$ is a former undecidability result of Y. Penzin).

Let $\mathcal{F} := (\mathbb{F}_p[[X]], +, 0, V_X, \lambda_X, \prec, .C; C \in \mathbb{F}_q[X])$. Using finite automata working on infinite words, we showed [1] that the theory of $\mathcal{F}$ is decidable and that the definable subsets were exactly the recognisable ones. Moreover the complexity of the definable subsets is bounded by $\exists\forall\exists\forall$. However $(\mathcal{F}, Frob_p)$ is undecidable, where $Frob_p$ denotes the Frobenius map [1].

Question 3 (H. Pasten)**.** Let $\mathcal{F}_0$ be the substructure of $\mathcal{F}$ consisting of the power series which are algebraic over $\mathbb{F}_p(X)$. Is $\mathcal{F}_0$ decidable?

Recently, there were a number of works on expansions of $(\mathbb{Z}, +, 0)$ of the form $(\mathbb{Z}, +, 0, R)$ where R is a unary predicate, some of which prompted by a question of A. Pillay on the structure induced on non-trivial centralisers in the free group on two generators. Assume $R := (r_n)$ is a strictly increasing sequence of natural

numbers. When R is the set of powers of 2 or when R has the property that the limit of its successive quotients converges to $+\infty$, R. Sklinos and D. Palacin showed that the theory of $(\mathbb{Z}, +, R)$ is superstable of U-rank ω [3], proving first a model-completeness result. Such sequences are instances of sparse sequences [4], and A. I. Semenov [8] showed model-completeness of the structure $(\mathbb{Z}, +, 0, <, R)$. One can generalise Sklinos and Palacin result to other sparse sequences for instance to sequences R given by a linear recurrence relation whose characteristic polynomial is the minimal polynomial of θ where $lim_n \frac{r_n}{\theta^n}$ exists and is strictly bigger than 1 (a preprint should be available soon).

References

[1] L. Bélair, M. Gélinas, F. Point, *Ensembles reconnaissables de séries formelles sur un corps fini*, C.R.Acad. Sci. Paris, Ser.I. **354**, Issue 3, March 2016, 225-229.

[2] B.R. Hodgson, *Théories décidables par automate fini*, Ph.D. Thesis, Université de Montréal, 1976.

[3] D. Palacin, R. Sklinos, *On superstable expansions of free abelian groups*, ArXiv:1405.0568v4, 3 Nov 2016.

[4] F. Point, *On decidable extensions of Presburger arithmetic: from A. Bertrand numeration systems to Pisot numbers*, J. Symbolic Logic **65**, no. 3, 1347- 1374, 2000.

[5] F. Point, M. Rigo and L. Waxweiler, *Defining multiplication in some additive ex- pansions of polynomial rings*, Communications in Algebra, **44:5**, 2075-2099, 2016.

[6] M. Rigo, L. Waxweiler, Logical characterization of recognizable sets of polynomials over a finite field, *Int. J. Found. Comput. Sci.* **22**, 1549–1563, 2011.

[7] P. Samuel, About Euclidean Rings, *Journal of Algebra* **19**, 282–301, 1971.

[8] A.L. Semenov, *On certain extensions of the arithmetic of natural numbers with addition*, Math. USSR Izvestiya **15**, no. 2, 401-418, 1980.

[9] R. Schäfke, M.F. Singer, *Consistent systems of linear differential and difference equations*, arXiv:1605.02616v1, 9 May 2016.

The Logical Complexity of Finitely Generated Commutative Rings

Thomas Scanlon

(joint work with Matthias Aschenbrenner, Anatole Khélif, Eudes Naziazeno)

We answer two questions about the logical complexity of finitely generated commutative rings. We say that a finitely generated commutative ring R is quasi-finitely axiomatisable (QFA) if there is a sentence $\varphi_R \in Th(R, +, \cdot, -, 0, 1)$ such that for any finitely generated commutative ring S, if $S \models \varphi_R$, then $S \cong R$. We prove:

Theorem 1. *Every finitely generated commutative ring is QFA.*

A natural way to prove Theorem 1 would be to establish that every finitely generated ring is (parametrically) bi-interpretable with $\mathbb{N}$. Second, we prove:

Theorem 2. *If R is an infinite finitely generated integral domain, then R is bi-interpretable with $\mathbb{N}$.*

However, it is easy to see as a consequence of the Feferman-Vaught Theorem (cf. [1, Corollary 9.6.4]) that

Proposition 3. *$\mathbb{Z} \times \mathbb{Z}$ is not bi-interpretable with $\mathbb{Z}$.*

Less obviously, we show by constructing a nontrivial derivation on a nonstandard model of arithmetic that the ring of dual numbers over $\mathbb{Z}$ is not bi-interpretable with $\mathbb{N}$.

Proposition 4. *The ring $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$ of dual numbers over $\mathbb{Z}$ is not bi-interpretable with $\mathbb{N}$.*

From these two results we find an algebraic characterisation of those finitely generated commutative rings which are (parametrically) bi-interpretable with $\mathbb{N}$. For a commutative ring R, we write $\mathrm{Spec}(R)$ for the spectrum of R, i.e., the set of prime ideals of R equipped with the Zariski topology, and $\mathrm{Max}(R)$ for the subset of $\mathrm{Spec}(R)$ consisting of the maximal ideals of R. We define

$$\mathrm{Spec}^\circ(R) := \mathrm{Spec}(R) \backslash \mathrm{Max}(R),$$

equipped with the subspace topology. Note that $\mathrm{Spec}^\circ(R)$ is a subspace of $\mathrm{Spec}(R)$. We write

$$N(R) := \{x \in R \mid \exists n \in \mathbb{Z}_{>0} \text{ such that } x^n = 0\}$$

for the nilradical of R, i.e. it is the ideal consisting of all the nilpotent elements of the commutative ring R. With these two notations, we have

Theorem 5. *A finitely generated commutative ring R is (parametrically) bi-interpretable with $(\mathbb{N}, +, \times)$ if and only if $Spec^\circ(R)$ is nonempty and connected in the Zariski topology, and the nilradical of R has a nontrivial annihilator in $\mathbb{Z}$, $ann_{\mathbb{Z}}(N(R)) \neq 0$.*

References

[1] W. Hodges, Model Theory, Encyclopedia of Mathematics and its Applications, vol. 42, Cambridge University Press, Cambridge, 1993.

On Diophantine Subsets of $\mathbb{Z}$

Mihai Prunescu

We handle only two subsets of $\mathbb{Z}$: $\mathbb{Z} \setminus \{0\}$ and $\mathbb{N}$. Both of them are important in translating the undecidability of Hilbert's Tenth Problem from $\mathbb{N}$ to $\mathbb{Z}$. The best result of this translation can be got only if those subsets are diophantinely defined using the smallest possible number of existential quantifiers.

In his cited article *Arithmetical definitions in the ring of integers*, Raphael Robinson proves properties of the sets which are first order definable in $\mathbb{Z}$ using only one quantifier and concludes that the set $\mathbb{N}$ of natural numbers has no such definition in $\mathbb{Z}$. This characterisation can little say about diophantine definitions. A two quantifier definition for $\mathbb{N}$ in $\mathbb{Z}$ given by Robinson is not diophantine because it contains a negation, and as we will see here, it can be repaired only with the cost of introducing another existential quantifier. Also, Robinson's characterisation cannot be used to prove that the complement of zero has no diophantine definition

with less than two quantifiers. Some new three-quantifier diophantine definitions of $\mathbb{N}$ in $\mathbb{Z}$ are constructed, but the problem to find a two-quantifier diophantine definition is let open.

Shih-Ping Tung proved in [11] that the statements of the form

$$\forall x_1, \ldots, x_n \, \exists y \; f(x_1, \ldots, x_n, y) = 0,$$

where $f \in \mathbb{Z}[x_1, \ldots, x_n, y]$, are decidable.

Theorem 1. *There does not exist any $g \in \mathbb{Z}[x, y]$ such that $x \neq 0 \leftrightarrow \exists y \; g(x, y) = 0$ holds in $\mathbb{Z}$.*

Proof: Let $g \in \mathbb{Z}[x, y]$ be such a polynomial. Then the following holds:

$$\forall x_1, \ldots, x_n \; f(x_1, \ldots, x_n) \neq 0 \longleftrightarrow \forall x_1, \ldots, x_n \, \exists y \; g(f(x_1, \ldots, x_n), y) = 0.$$

By Tung's result, these sentences can be decided by a decision algorithm, and so Hilbert's Tenth Problem would be algorithmically solvable. Contradiction. □

This shows that the definition:

$$x \neq 0 \leftrightarrow \exists y \exists z \; xy = (2z - 1)(3z - 1),$$

given by Denef and Lipshitz in [1], already uses the minimal number of quantifiers. It is known that this definition works in all rings of algebraic integers.

Also, Tung used the following definition holding in the ring of rational integers:

$$a \neq 0 \leftrightarrow \exists x \exists y \; a = (2x - 1)(3y - 1).$$

The following result of Schinzel, see [9], will be used:

Lemma 2. *Let K be a field of finite dimension over $\mathbb{Q}$ and R its ring of algebraic integers. Consider $g \in K[x, t_1, \ldots, t_r]$ a polynomial such that for all arithmetic progressions $P_1, \ldots, P_r$ in R there exist $t_i \in P_i$ and $x \in R$ such that $g(x, t_1, \ldots, t_r) = 0$. Then the following hold:*

(1) *$g = g_0 \prod_{\sigma=1}^{s} (x - x_\sigma(t_1, \ldots, t_r))$ where $s \geq 1$, all $x_\sigma \in K[t_1, \ldots, t_r]$ and g_0 as polynomial in x has no solution in $K[t_1, \ldots, t_r]$.*

(2) *For all $t_1, \ldots, t_r \in R$ there is a σ such that $x_\sigma(t_1, \ldots, t_r) \in R$.*

As a consequence:

Theorem 3. *In no ring of algebraic integers of some finite extension of $\mathbb{Q}$, the relation $x \neq 0$ allows one-quantifier diophantine definitions.*

In [8] R. M. Robinson proved that there is no first order definition of $\mathbb{N}$ in $\mathbb{Z}$ using less than two quantifiers and displayed the following definition that contains two existential quantifiers:

$$x \geq 0 \leftrightarrow \exists y \exists z \; [x = y^2 \vee (y^2 = 1 + xz^2 \wedge y^3 \neq y)].$$

This definition works by the following Lemma:

Lemma 4. *Consider the formula $\varphi(x,y,z)$ given by $z \neq 0 \wedge y^2 - xz^2 = 1$. Then the formula $\exists y \exists z\, \varphi(x,y,z)$ defines in $\mathbb{Z}$ the following set:*

$$\{-1, 0\} \cup \{x > 0 \,|\, \forall k\ x \neq k^2\}.$$

Theorem 5. *In the ring $\mathbb{Z}$ the following holds:*

$$x \geq 0 \leftrightarrow \exists y \exists z\ \varphi(4x+2, y, z).$$

This leads to the definition:

$$x \geq 0 \leftrightarrow \exists y \exists v \exists u\ (4x+2)(2u-1)^2(3v-1)^2 = y^2 - 1,$$

which has three quantifiers. *The problem to find a 2-quantifier diophantine definition of $\mathbb{N}$ in $\mathbb{Z}$ remains open.*

Bjorn Poonen asked in [7] if there is a polynomial $p(x,y)$ such that $p(\mathbb{Z}\times\mathbb{Z}) = \mathbb{N}$, without specifying what kind of coefficients the polynomial should have. In the following lines we construct polynomials $h \in \mathbb{Z}[x,y,z]$ such that $h(\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}) = \mathbb{N}$. *Poonen's question remains also open.*

Each natural number is a sum of: three triangular numbers, Gauss [3]; sum of two squares and a triangular number, Euler [2]; sum of a square, an even square and a triangular number, B. J. Jones and G. Pall [4]; sum of an even square and two triangular numbers [10]. For the resulting polynomials, which have coefficients in $\mathbb{Q}$ (some of the coefficients are $1/2$) one applies the following trick:

Proposition 6. *The relation $\Delta \subset \mathbb{Z} \times \mathbb{N}$ defined by $(k,n) \in \Delta$ if and only if*

$$2k^2 + k \quad = \quad \frac{n(n+1)}{2},$$

is an implicit bijective correspondence between $k \in \mathbb{Z}$ and $n \in \mathbb{N}$. The same is true if one replaces $2k^2 + k$ with $2k^2 - k$.

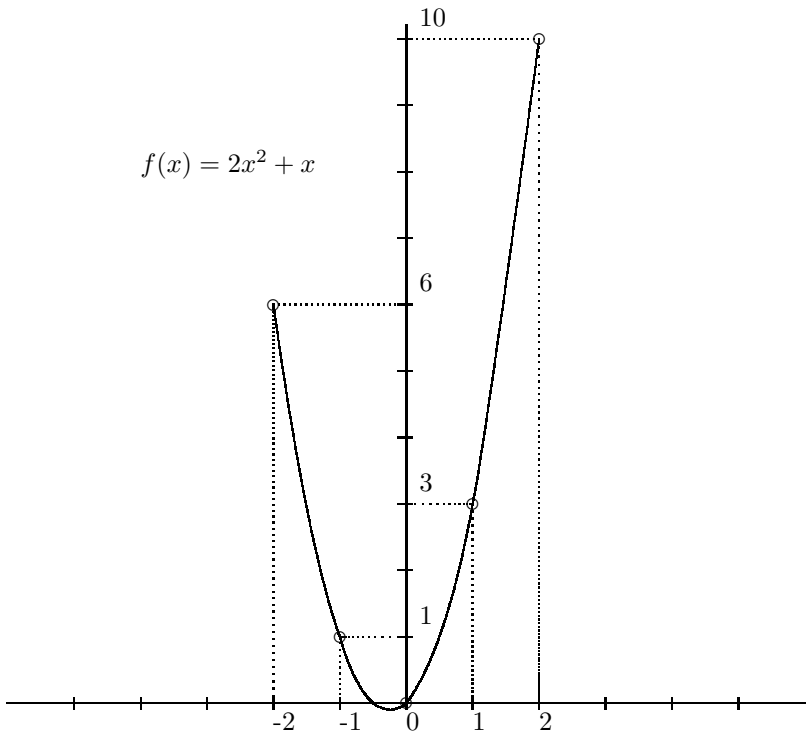
Corollary 7. *The twenty polynomials $h \in \mathbb{Z}[x,y,z]$ given by:*

$$\begin{aligned}
h(x,y,z) &= 2x^2 + 2y^2 + 2z^2 \pm x \pm y \pm z \\
h(x,y,z) &= x^2 + y^2 + 2z^2 \pm z \\
h(x,y,z) &= x^2 + 4y^2 + 2z^2 \pm z \\
h(x,y,z) &= x^2 + 2y^2 + 2z^2 \pm y \pm z \\
h(x,y,z) &= 4x^2 + 2y^2 + 2z^2 \pm y \pm z
\end{aligned}$$

have the property that $h(\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}) = \mathbb{N}$.

For the fourth line above, observe that in the fifth line $4x^2$ is itself a square.

However, we know that there are infinitely many polynomials $h \in \mathbb{Z}[x,y,z]$ with the property that $h(\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}) = \mathbb{N}$. This happens because for every univariate polynomial $p \in \mathbb{Z}[t]$, if $h_1(x,y,z) = h(x + p(y), y, z)$ and $h(\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}) = \mathbb{N}$ then $h_1(\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}) = \mathbb{N}$. Indeed $h_1(x - p(y), y, z) = h(x,y,z)$.



References

[1] **J. Denef and L. Lipshitz**: *Diophantine sets over some rings of algebraic integers.* J. London Math. Soc. (2) 18 (1978), 385–391, 1978.

[2] **L. E. Dickson**: *History of the theory of numbers.* Vol. II, A. M. S. Chelsea Pub. 1999.

[3] **Carl Friedrich Gauss**: *Disquisitiones Arithmeticae.* Yale University Press, 1966.

[4] **B. W. Jones, G. Pall**: *Regular and semi-regular positive ternary quadratic forms.* Acta Math. 70, 165–191, 1939.

[5] **Joseph-Louis Lagrange**: *Sur la solution des problèmes indéterminés du second degré.* Oeuvres, Vol. II, Gauthier-Villars, Paris, 377–535, 1868.

[6] **Yuri V. Matiyasevich**: *Hilbert's Tenth Problem is unsolvable.* The MIT Press, Cambridge, Massachusetts, 1993.

[7] **Bjorn Poonen**: http://mathoverflow.net/questions/9731/polynomial-representing-all-nonnegative-integers

[8] **Raphael M. Robinson**: *Arithmetical definitions in the ring of integers.* Proceedings of the American Mathematical Society, Vol. 2, No.2, 279–284, 1951.

[9] **A. Schinzel**: *Selected topics on polynomials.* The University of Michigan Press, Ann Arbor, 1982.

[10] **Z. W. Sun**: *Mixed sums of squares and triangular numbers.* Acta Arith. 127, 103–113, 2007.

[11] **Shih-Ping Tung**: *On weak number theories.* Japanese Journal Mathematics, 11, 203–232, 1985.

Undecidability Results Obtained from Beth's Definability Theorem

Kenji Fukuzaki

The following theorem is proved by J. Robinson [3].

Theorem 1. *Let A be a ring of totally real algebraic integers. Suppose that there is a smallest interval $(0, s)$, s real or ∞, which contains infinitely many sets of conjugates of numbers of A. The ring of all rational integers $\mathbb{Z}$ is first order definable without parameters in A, hence A is undecidable.*

We consider a proof of this theorem using Beth's definability theorem.

Let P and P' be two new n-placed relation symbols, not in the language L. Let $\Sigma(P)$ be a set of sentences of the language $L \cup \{P\}$, and let $\Sigma(P')$ be the corresponding set of sentences of $L \cup \{P'\}$ formed by replacing P everywhere by P'. We say that $\Sigma(P)$ *defines P implicitly* iff (M, S) and (M, S') are models of $\Sigma(P)$, then $S = S'$. $\Sigma(P)$ is said to *define P explicitly* iff there is a formula $\varphi(x_1 \dots x_n)$ of L such that for every model (M, S) of $\Sigma(P)$, $\varphi(x_1 \dots x_n)$ defines S in M. Beth's definability theorem states that *if $\Sigma(P)$ defines P implicitly iff $\Sigma(P)$ defines P explicitly.* ([1]).

A totally real number x is *totally nonnegative* ($0 \ll x$) iff x and all its conjugates are non-negative. We write $x \ll y$ to indicate that $y - x$ is totally non-negative.

Siegel [4] proved that a number in a totally real algebraic field is the sum of four squares of numbers of the field iff it is totally non-negative. Hence in a ring of totally real algebraic integers,

$$x \ll y \Leftrightarrow \exists t, u, v, w, z[t^2(y - x) = u^2 + v^2 + w^2 + z^2 \wedge t \neq 0],$$

Thus the relation $x \ll y$ is definable in the ring language. We note that $\ll$ is a partial order and that it coincides with $\leq$ in $\mathbb{Z}$.

Let A be a ring of totally real algebraic integers. Let L be the ring language and let $\Sigma(P) = \mathrm{Th}_{L\cup\{P\}}(A, \mathbb{Z})$. We easily see the following $L \cup \{P\}$-properties of $(A, \mathbb{Z})$.

Fact 2. *Let $x \in A \setminus \mathbb{Z}$. Then there exist unique $m, n \in \mathbb{Z}$ such that $m \not\ll x$, $x \not\ll m$ and $x \ll m + 1$ hold in A and $n \not\ll x$, $x \not\ll n$ and $n - 1 \ll x$ hold in A.*

We note that $(n - 1, m + 1)$ is the smallest open interval which contains x and all its conjugates and whose endpoints are rational integers.

Let (R, S) be a model of $\mathrm{Th}_{L\cup\{P\}}(A, \mathbb{Z})$. We note that S contains $\mathbb{Z}$ since S is a ring. Therefore we see that the above facts can be written as first order $L \cup \{P\}$-formulas. Hence we see that the above facts hold in R when we replace A and $\mathbb{Z}$ everywhere with R and S respectively. If (R, S') is another model of $\mathrm{Th}_{L\cup\{P\}}(A, \mathbb{Z})$, the above facts also hold in R when we replace A and $\mathbb{Z}$ everywhere with R and S' respectively.

First we consider the case where $R = A^I/\mathcal{F}$. Obviously $(A^I/\mathcal{F}, \mathbb{Z}^I/\mathcal{F})$ is a model of $\mathrm{Th}_{L\cup\{P\}}(A, \mathbb{Z})$. We put $S = \mathbb{Z}^I/\mathcal{F}$, that is, $(R, S) = (A, \mathbb{Z})^I/\mathcal{F}$. Suppose that (R, S') is also a model of $\mathrm{Th}_{L\cup\{P\}}(A, \mathbb{Z})$.

Conjecture: $S' \subseteq S$.

We discuss this conjecture. For simplicity we use representatives of the equivalence classes in $A^I/\mathcal{F}$ instead of the classes themselves. Let $x = (x_\mu) \in S'$. Then, for all $y \in S'$, $y \ll x$ or $x \ll y$ holds in R. We cannot write this sentence as an $L \cup \{P\}$-sentence. Instead, since $\mathbb{Z} \subseteq S'$, for all $n \in \mathbb{Z}$,

$$X_n = \{\mu \in I \mid n \ll x_\mu \vee x_\mu \ll n\} \in \mathcal{F}.$$

We show that for all $n \in \mathbb{Z}$, $n \ll x \vee x \ll n$ iff $n+1 \ll x \vee x \ll n+1$. Suppose that $n \ll x \vee x \ll n$. If $x \ll n$ holds in R then it follows that $x \ll n+1$. Consider the case that $n \ll x$. If $n = x$ then it follows that $x \ll n+1$, otherwise $n+1 \ll x$ follows, since S' is a model of $\mathrm{Th}_L(\mathbb{Z})$. Conversely, Suppose that $n+1 \ll x \vee x \ll n+1$. If $n+1 \ll x$ then $n \ll x$ follows. Suppose that $x \ll n+1$. If $x = n+1$ then $n \ll x$, otherwise $x \ll n$ follows. Thus,

$$Y_n = \{\mu \in I \mid [n \ll x_\mu \vee x_\mu \ll n] \leftrightarrow [n+1 \ll x_\mu \vee x_\mu \ll n+1]\} \in \mathcal{F}.$$

Then, we have $X_n \cap Y_n \subseteq X_{n+1}$. Here, we cannot go further. If we could show that all the X_n were same, the conjecture follows ; put this index set in X. Let $\mu \in X$. Suppose that $x_\mu \notin \mathbb{Z}$. Then there is an $m \in \mathbb{Z}$ such that $x_\mu \not\ll m$ and $m \not\ll x_\mu$. Hence $\mu \notin X_m = X$, a contradiction. Thus $X \subseteq \{\mu \in I \mid x_\mu \in \mathbb{Z}\}$. Hence $x \in S$. It seems that here, we need the assumption of Julia Robinson. But we don't know how to use that assumption.

If we assumed the conjecture, then we could get the following proof. We consider an arbitrary model (R, S) of $\mathrm{Th}_{L\cup\{P\}}(A, \mathbb{Z})$. It is known that there is an $L \cup \{P\}$-elementary embedding $\iota : (R, S) \to (A, \mathbb{Z})^I/\mathcal{F}$ for some set I and some ultrafilter $\mathcal{F}$ on I by Frayne's lemma([2]).

Lemma 3. $\iota(S') \subseteq \iota(S)$.

We note that although ι dose not preserve the set S', ι preserves properties of elements of S'. Hence $(\iota(R), \iota(S'))$ is also a model of $\mathrm{Th}_{L\cup\{P\}}(A, \mathbb{Z})$ and an elementary substructure of $(A, \mathbb{Z})^I/\mathcal{F})$.

Proof of the theorem assuming $S' \subseteq S$. Let (R, S) and (R, S') be models of $\mathrm{Th}_{L\cup\{P\}}(A, \mathbb{Z})$. We note that $S \cap S' \supset \mathbb{Z}$. Suppose that $S \neq S'$.

We first show $S \not\subset S'$. Suppose $S \subset S'$. Then there is a $t \in S'$ with $t \notin S$. It follows that for all $y' \in S'$ we have $t \ll y'$ or $y' \ll t$, and there is a $y \in S$ such that $t \not\ll y \wedge y \not\ll t$, a contradiction. (Symmetrically we have $S' \not\subset S$.)

Then there is a $t \in S$ with $t \notin S'$.

Since $t \notin S'$, there is an $s' \in S'$ such that $t \not\ll s' \wedge s' \not\ll t$. Then we have

$$\iota(s') \in \iota(S') \wedge \iota(t) \not\ll \iota(s') \wedge \iota(s') \not\ll \iota(t) \text{ holds in } (A, \mathbb{Z})^I/\mathcal{F}),$$

since ι is a ring embedding too.

On the other hand, since $t \in S$, we have for all $s \in S$ $t \ll s$ or $s \ll t$ holds. Then we have

$$\forall s \in \iota(S)[\iota(t) \ll s \vee s \ll t] \text{ holds in } (A, \mathbb{Z})^I/\mathcal{F}),$$

hence we get a contradiction,since $\iota(S') \subseteq \iota(S)$.

References

[1] C. C Chang and H. J. Keisler, *Model Theory*, Vol. **73** of Studies in Logic and Foundations of Mathematics, North-Holland, Amsterdam (1973), 90–91.
[2] J. L. Bell and A. B. Slomson, *Models and Ultraproducts*, North-Holland, Amsterdam, American Elsevier, New York, (1974), 161–163.
[3] J. Robinson, *On the decision problem fo algebraic rings*, In Studies in mathematical analysis and related topics, Stanford Univ. Press, Stanford, Calif., (1962), 297–304.
[4] C. Siegel, *Approximation algebraischer Zahlen*, Math. Z., **11** (1921), 173–213.

Defining Arithmetic in Polynomial Rings with Addition and Coprimes

Javier Utreras

We study the first–order theory of the structure $\langle R[t]; 1, +, \perp \rangle$, where R is a commutative integral domain with unity and $\perp$ is the binary relation of coprimality given by

$$x \perp y \text{ if and only if every common divisor of both } x \text{ and } y \text{ is a unit.}$$

We claim the following results: for R of zero characteristic, there exist

- a definable set $Z \subseteq R[t]$ containing the element t;
- a definable set $T \subseteq Z \times R[t]$ such that for every $x \in Z$ the fibre T_x is the set $\{x^n : n \in \mathbb{N}_{>0}\}$;
- a definable relation $N \subseteq T^2$ such that $\big((x, x^n), (y, y^m)\big) \in N$ if and only if $x = y$ and $|n - m| = 1$; and
- a definable relation $D \subseteq T^2$ such that $\big((x, x^n), (y, y^m)\big) \in N$ if and only if $x = y$ and n divides m.

Moreover, these sets are defined uniformly regardless of the choice of R.
For R of positive characteristic, we show that there exist

- a definable set $Z \subseteq R[t]$ containing the element t;
- a definable set $T \subseteq Z \times R[t]$ such that for every $x \in Z$ the fibre T_x is the set $\{x^{p^n} : n \in \mathbb{N}\}$;
- a definable equivalence relation $E \subseteq (\pi_2(T))^2$ (where π_2 is the projection onto the second coordinate) satisfying the following: let $x, y \in Z$, then $(x^n, y^m) \in E$ if and only if $n = m$. We shall write E_i for the class of t^{p^i};
- a definable relation $N \subseteq (\pi_2(T)/E)^2$ such that $(E_n, E_m) \in N$ if and only if $|n - m| = 1$; and
- a definable relation $D \subseteq (\pi_2(T)/E)^2$ such that $(E_n, E_m) \in N$ if and only if n divides m.

The definition of these sets depends only on the characteristic of R.
In either case, the theory of the structure $\langle \mathbb{N}; \mathrm{Neib}, | \rangle$ is interpretable within our theory, where Neib is the binary relation $|n-m| = 1$ and $|$ is the divisibility relation. By results of J. Robinson and I. Korec, this theory is identical to the first–order theory of arithmetic. In particular, we obtain that the theory of $\langle R[t]; 1, +, \perp \rangle$ is undecidable.

References

[1] I. Korec, *Definability of addition from multiplication and neighborhood relation and some related results*, Preprint 23/1996 of Math. Institute SAV Bratislava.

[2] I. Korec, *A list of arithmetical structures complete with respect to the first–order definability*, Theoretical Computer Science **257–1** (2001), 115–151.

Open Problems

Chaired by Jeroen Demeyer

Question 1 (posed by Mihai Prunescu)**.**
Consider the field $\mathbb{A} := \mathbb{R} \cap \overline{\mathbb{Q}}$ of the real algebraic numbers in the language $\mathcal{L} := \mathcal{L}_{\text{rings}} \cup \{Q\}$ where Q is a unary predicate for $\mathbb{Q}$. So $Q(\mathbb{A}) = Q(\mathbb{R}) = \mathbb{Q}$. It is clear that $\mathbb{A}$ and $\mathbb{R}$ are not $\mathcal{L}$-elementarily equivalent (for example, $\pi \in \mathbb{R}$ is $\mathcal{L}$-definable, say by an $\mathcal{L}$-formula φ, but no element of $\mathbb{A}$ satisfies φ). Do $\mathbb{A}$ and $\mathbb{R}$ have the same $\forall\exists$-$\mathcal{L}$-theory? If "yes", then $\mathbb{Z}$ is not diophantine in $\mathbb{Q}$.

Question 2 (posed by Thanases Pheidas)**.**
Find a uniform diophantine interpretation of $\mathbb{Z}$ in $\mathbb{F}_p(t)$ as p varies. Diophantine, here, means positive existentially definable over the language of rings augmented with a symbol for t. If uniformity is not required, then such an interpretation exists by a theorem of Pheidas. With the existing methods, what is missing is a uniform diophantine definition of the valuation ring $\mathbb{F}_p[t]_{(t)}$ in $\mathbb{F}_p(t)$.

Question 3 (posed by Thanases Pheidas and Jeroen Demeyer)**.**
Define (over the ring language with parameters) the valuation ring $\mathbb{C}[t]_{(t)}$ in $\mathbb{C}(t)$. This would imply that the first order theory of $\mathbb{C}(t)$ is undecidable (which is not known).

Similarly, define the place $f|_{s=0}|_{t=0} = 0$ in $\mathbb{C}(s,t)$. Is it diophantine? What about $\mathbb{F}_p(s,t)$?

Question 4 (posed by Itay Kaplan)**.**
Is there an infinite field that is finitely axiomatisable? The expectation is that there is probably no such infinite field. $\mathtt{Th}(ACF)$ is not. Similar question for groups ....

Question 5 (posed by Sylvy Anscombe and Jochen Koenigsmann)**.**
Let v be a valuation on an elementary extension $\mathbb{Q}^* \succcurlyeq \mathbb{Q}$ such that $\mathcal{O}_v$ does not contain $\mathbb{Z}^*$ nor the convex hull of $\mathbb{Z}$ (with respect to the unique ordering on $\mathbb{Q}^*$). Is the henselisation F of $\mathbb{Q}^*$ with respect to v then necessarily separably closed? The expectation is "yes" so that the only valuations that contribute to the arithmetic of $\mathbb{Q}^*$ are the ones we know. One thing we can show in this direction is, e.g., that the absolute Galois group of F is projective. The question may have a bearing on the question of whether or not $\mathbb{Z}$ is diophantine in $\mathbb{Q}$.

Question 6 (posed by Itay Kaplan)**.**
Show that there is no infinite field K with a polynomial $f \in K[X]$ such that

$f(K) \subsetneqq K$ is cofinite. This relates to the well-known conjecture that every minimal field is algebraically closed (proved in positive characteristic by Frank O. Wagner). Here K is minimal if every definable subset of K is finite or cofinite.

Question 7 (posed by Hector Pasten)**.**
Consider the binary relation E on $\mathbb{C}[t]$ defined by $E(f,g) : \deg(f) = \deg(g)$. Is E Diophantine (or definable) in $\mathbb{C}[t]$ over the ring language with parameters? It might be relevant to point out that $\mathbb{C}[t]$ is not elementarily equivalent to $\bar{\mathbb{Q}}[t]$, while $\mathbb{C}(t) \equiv \bar{\mathbb{Q}}(t)$.

Question 8 (posed by Arno Fehm)**.**
Is, for a fixed prime p, $\mathtt{Th}_\exists(\mathbb{F}_p(t), \mathcal{L}_{\text{ring}})$ decidable? It is known to be undecidable in $\mathcal{L}_{\text{ring}} \cup \{t\}$. Also, it is an observation of Pheidas that the predicate T (traditionally defined by $T(f) : f$ is non-constant) is positive existentially definable in $(\mathbb{F}_p(t), \mathcal{L}_{\text{ring}})$ and therefore the problem is equivalent to the more geometric problem of decidability of $\mathtt{Th}_\exists(\mathbb{F}_p(t), \mathcal{L}_{\text{ring}} \cup \{T\})$.

Question 9 (posed by Raf Cluckers)**.**
It is known that $\mathbb{C}[[s,t]]$ is undecidable in $\mathcal{L}_{\text{ring}} \cup \{s,t\}$ (Denef, Lipshitz, Delon). Let $0 \neq I \subsetneqq \mathbb{C}[[s,t]]$ be an ideal (e.g. $I = (s,t)$), and let $RV_I = {}^{\mathbb{C}((s,t))^*}/_{1+I}$. Is $\mathbb{C}[[s,t]]$ decidable when using $\mathtt{Th}(RV_I)$ as an oracle?

Question 10 (posed by Franz-Viktor Kuhlmann)**.**
"What are the purely inseparable extensions of a valued field in mixed characteristic?" (to put the question in a memorable form).

In characteristic (p,p):

$$K \text{ is henselian defectless } (n = e \cdot f) \iff \begin{cases} K \text{ is algebraically maximal} \\ \text{(no immediate algebraic extensions)} \\ + \\ \text{every finite purely inseparable} \\ \text{extension is defectless} \end{cases}$$

In characteristic $(0,p)$:

$$K \text{ is henselian defectless} \iff \begin{cases} K \text{ is algebraically maximal} \\ + \\ \boxed{???} \end{cases}$$

Find a nice simple criterion for $\boxed{???}$.

Question 11 (posed by Hector Pasten)**.**
Consider the binary relation S on $\mathbb{F}_p(t)$ given by $S(f,g) : f \in \mathbb{F}_p(g)$. Is S diophantine over the ring language without parameters? In particular, is $\mathbb{F}_p(t^2)$ diophantine with parameters in $\mathbb{F}_p(t)$? The problem is motivated by an approach of

Shlapentokh to the question of decidability of $\mathtt{Th}_\exists(\mathbb{F}_p(t), \mathcal{L}_{\text{ring}})$. We remark that it is a theorem of Kollar that $\mathbb{C}(t^2)$ is not diophantine (with parameters) in $\mathbb{C}(t)$.

Question 12 (posed by Hector Pasten)**.**
Let k be an algebraically closed field, complete for a non-trivial absolute value $|-|$. The ring of rigid entire functions over k is by definition the ring $\mathcal{A}_k$ of power series on the variable t with infinite radius of convergence. The field of rigid meromorphic functions $\mathcal{M}_k$ is the fraction field of $\mathcal{A}_k$. We are concerned about decidability of these rings. Three cases naturally appear:

- case I: $|-|$ is archimedean (e.g. $k = \mathbb{C}$, classical complex holomorphic and meromorphic functions);
- case II: $|-|$ is non-archimedean and k has characteristic zero;
- case III: $|-|$ is non-archimedean and k has positive characteristic.

Is $\mathtt{Th}_\exists(\mathcal{A}_k, \mathcal{L}_{\text{ring}} \cup \{t\})$ decidable? Case I remains open, while case II is undecidable by Lipshitz and Pheidas, and case III is undecidable by Garcia-Fritz and Pasten.

Is $\mathtt{Th}(\mathcal{M}_k, \mathcal{L}_{\text{ring}} \cup \{t\})$ decidable? Here, only case III is known to be undecidable by a recent result of Pasten, while cases I and II remain open. It seems that case II is the most approachable.

Note that the algebraic analogue (i.e. trivial absolute value) of case II for meromorphic functions is precisely the outstanding open question of whether $\mathtt{Th}(k(t), \mathcal{L}_{\text{ring}} \cup \{t\})$ is decidable for k an algebraically closed field of characteristic zero. Could it be that in the rigid meromorphic case one can take advantage of the topology and analysis?

Question 13 (posed by Jamshid Derakhshan)**.**
What is $\mathtt{Th}\left(\mathbb{F}_p[[t]]/(t^n)\right)$

- for all n and a fixed p?
- for almost all n and all p?
- $\cdots$

Question 14 (posed by Arno Fehm – not part of the session but was sent via email on the 28th of October 2016)**.**
Can one prove p-adic analogues of some of the undecidability results for rings of totally real algebraic integers? More precisely, can one prove for example that the ring of integers of $\mathbb{Q}_{\mathrm{t}p}^{(2)}$ is undecidable, where tp denotes the largest subfield in which p is totally split? The hope here is that maybe one can replace the (diophantine) definability of sums of squares by the (diophantine) definability of the p-adic Kochen ring. Note that it is known that for every prime number p, the ring of *all* totally p-adic integers is decidable, as opposed to the ring of all totally real integers.

Reporter: Kesavan Thanagopal

Participants

Dr. Sylvy Anscombe
Jeremiah Horrocks Institute for Mathematics,
Physics and Astronomy
University of Central Lancashire
Le7, Leighton Building
Preston PR1 2HE
UNITED KINGDOM

Prof. Dr. Zoé Chatzidakis
Département de Mathématiques et Applications
Ecole Normale Supérieure
45, Rue d'Ulm
75230 Paris Cedex 05
FRANCE

Dimitra Chompitaki
Dept. of Mathematics & Applied Mathematics
University of Crete
Voutes Campus
70013 Heraklion, Crete
GREECE

Prof. Dr. Raf Cluckers
Laboratoire Paul Painleve, UMR 8524
Université des Sciences et Technologie de Lille 1
Cité Scientifique, Bat. M2
59655 Villeneuve-d'Ascq Cedex
FRANCE

Prof. Dr. Jean-Louis Colliot-Thélène
Laboratoire de Mathématiques
Université Paris Sud (Paris XI)
Bâtiment 425
91405 Orsay Cedex
FRANCE

Prof. Dr. Paola D'Aquino
Dipartimento di Matematica
Seconda Universita degli Studi di Napoli
Viale Abramo Lincoln, 5
81100 Caserta
ITALY

Dr. Jeroen Demeyer
Department of Mathematics
Ghent University
Krijgslaan 281
9000 Gent
BELGIUM

Prof. Dr. Jamshid Derakhshan
Mathematical Institute
Radcliffe Observatory Quarter
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Philip Dittmann
Merton College Oxford
Merton Street
Oxford OX1 4JD
UNITED KINGDOM

Prof. Dr. Kirsten Eisentraeger
Department of Mathematics
Pennsylvania State University
University Park, PA 16802
UNITED STATES

Sebastian Eterovic
Mathematical Institute
Oxford University
24-29 St. Giles
Oxford OX1 3LB
UNITED KINGDOM

Prof. Dr. Arno Fehm
Fachbereich Mathematik u. Statistik
Universität Konstanz
Universitätsstrasse 10
78457 Konstanz
GERMANY

Anton Freund
School of Mathematics
University of Leeds
Leeds LS2 9JT
UNITED KINGDOM

Prof. Dr. Kenji Fukuzaki
Faculty of Intercultural Studies
The International University of Kagoshima
Kagoshima 891-0191
JAPAN

Prof. Dr. Ofer Gabber
I.H.E.S.
Le Bois Marie
35, route de Chartres
91440 Bures-sur-Yvette
FRANCE

Dr. Natalia Garcia-Fritz
Department of Mathematics
University of Toronto
40 St George Street
Toronto ON M5S 2E4
CANADA

Prof. Dr. Wulf-Dieter Geyer
Department Mathematik
FAU Erlangen-Nürnberg
Cauerstrasse 11
91058 Erlangen
GERMANY

Prof. Dr. Kalman György
Institute of Mathematics
University of Debrecen
Pf. 12
4010 Debrecen
HUNGARY

Prof. Dr. Chris Hall
Department of Mathematics
University of Wyoming
Ross Hall
Laramie WY 82071
UNITED STATES

Prof. Dr. Moshe Jarden
School of Mathematics
Tel Aviv University
Ramat Aviv
Tel Aviv 69978
ISRAEL

Dr. Itay Kaplan
Institute of Mathematics
The Hebrew University
Givat Ram
Jerusalem 91904
ISRAEL

Prof. Dr. Jochen Koenigsmann
Mathematical Institute
Radcliffe Observatory Quarter
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Prof. Dr. Franz-Viktor Kuhlmann
Institute of Mathematics
University of Silesia
Bankowa 14
40-007 Katowice
POLAND

Prof. Dr. Angus John MacIntyre
7a West Castle Road
Edinburgh EH10 5AT
UNITED KINGDOM

Prof. Dr. Russell Miller
Department of Mathematics
Queens College
CUNY
65-30 Kissena Boulevard
Flushing, NY 11367
UNITED STATES

Prof. Dr. Laurent Moret-Bailly
I. R. M. A. R.
Université de Rennes I
Campus de Beaulieu
35042 Rennes Cedex
FRANCE

Travis Morrison
Department of Mathematics
Pennsylvania State University
University Park, PA 16802
UNITED STATES

Kien Huu Nguyen
Laboratoire Paul Painleve, UMR 8524
Université des Sciences et Technologie de Lille 1
Cité Scientifique, Bat. M2
59655 Villeneuve-d'Ascq Cedex
FRANCE

Dr. Jennifer Park
Department of Mathematics
University of Michigan
2074 East Hall
530 Church Street
Ann Arbor, MI 48109-1043
UNITED STATES

Dr. Hector V. Pasten
Department of Mathematics
Harvard University
Science Center
Cambridge MA 02138-2901
UNITED STATES

Prof. Dr. Thanases Pheidas
Dept. of Mathematics & Applied Mathematics
University of Crete
Voutes Campus
70013 Heraklion, Crete
GREECE

Prof. Dr. Francoise Point
Département de Mathématique
Université de Mons
Le Pentagone
20, Place du Parc
7000 Mons
BELGIUM

Prof. Dr. Florian Pop
Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104-6395
UNITED STATES

Prof. Dr. Alexander Prestel
Fachbereich Mathematik u. Statistik
Universität Konstanz
Postfach 5560
78457 Konstanz
GERMANY

Dr. Mihai Prunescu
Institute of Mathematics "Simion Stoilow"
of the Romanian Academy
P.O. Box 1-764
014 700 București
ROMANIA

Dr. Aharon Razon
Department of Mathematics
Ben-Gurion University of the Negev
Beer-Sheva 84 105
ISRAEL

Benjamin Rigler
Mathematical Institute
Oxford University
24-29 St. Giles
Oxford OX1 3LB
UNITED KINGDOM

Prof. Dr. Thomas W. Scanlon
Department of Mathematics
University of California
Berkeley CA 94720-3840
UNITED STATES

Prof. Dr. Alexandra Shlapentokh
Department of Mathematics
East Carolina University
Greenville NC 27858-4353
UNITED STATES

Dr. Alla Sirokofskich
Dept. of Mathematics & Applied Mathematics
University of Crete
Voutes Campus
70013 Heraklion, Crete
GREECE

Prof. Dr. Alexei N. Skorobogatov
Department of Mathematics
Imperial College London
Huxley Building
180 Queen's Gate
London SW7 2AZ
UNITED KINGDOM

Dr. Giuseppina Terzo
Dipartimento di Matematica
Seconda Universita di Napoli
Via Vivaldi 43
81100 Caserta
ITALY

Kesavan Thanagopal
Mathematical Institute
Radcliffe Observatory Quarter
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Dr. Javier Utreras
Departamento de Matematica
Universidad de Concepcion
Casilla 160-C
Concepcion
CHILE

Prof. Dr. Lou van den Dries
Department of Mathematics
University of Illinois at Urbana-Champaign
273 Altgeld Hall, MC-382
1409 West Green Street
Urbana, IL 61801-2975
UNITED STATES

Prof. Dr. Jan van Geel
Vakgroep Wiskunde
Universiteit Gent
Krijgslaan 281
9000 Gent
BELGIUM

Prof. Dr. Xavier Vidaux
Departamento de Matematica
Universidad de Concepcion
Casilla 160-C
Concepcion
CHILE

Prof. Dr. Carlos R. Videla
Department of Mathematics and Computing
Mount Royal University
4825 Mount Royal Gate SW
Calgary AB T3E 6K6
CANADA

Prof. Dr. Maxim Vsemirnov
Steklov Mathematical Institute
PDMI
Fontanka 27
St. Petersburg 191 023
RUSSIAN FEDERATION

Dr. Martin Widmer
Department of Mathematics
Royal Holloway College
University of London
Egham TW20 0EX
UNITED KINGDOM