Transferring imaginaries

How to eliminate imaginaries in p-adic fields

Silvain Rideau

joint work with E. Hrushovski and B. Martin
in “Definable equivalence relations and zeta functions of groups”
with an appendix by R. Cluckers

Orsay Paris-Sud 11, École Normale Supérieure

May 12, 2014

Some notations

Let (K, v) be a valued field.

- We will denote by $\mathcal{O} = \{x \in K \mid \mathrm{v}(x) \geq 0\}$ the valuation ring;
- It has a unique maximal ideal $\mathfrak{M} = \{x \in K \mid \mathrm{v}(x) > 0\}$;
- The residue field $\mathcal{O} / \mathfrak{M}$ will be denoted k;
- The value group will be denoted by Γ;
- Let also $\mathrm{RV} := K^\star/(1 + \mathfrak{M}) \supseteq k^\star$.

First model theory results

Let $\mathcal{L}_{\mathrm{div}} = \{\mathbf{K}; 0, 1, +, -, \cdot, |\}$ where $x|y$ is interpreted by $\mathrm{v}(x) \leq \mathrm{v}(y)$.

Theorem (A. Robinson, 1956)

The $\mathcal{L}_{\mathrm{div}}$-theory ACVF of algebraically closed valued fields eliminates quantifiers.

Let $\mathcal{L}_{\mathrm{P}} = \mathcal{L}_{\mathrm{div}} \cup \{P_n \mid n \in \mathbb{N}_{>0}\}$ where $x \in P_n$ if and only if $\exists y, y^n = x$.

Theorem (Macintyre, 1976)

The $\mathcal{L}_{\mathrm{P}}$-theory of $\mathbb{Q}_p$ eliminates quantifiers.

Imaginaries

Let T be a theory

- For all definable equivalence relation E, does there exist a definable function f — a representation — such that

$$\forall x, y,\ xEy \iff f(x) = f(y).$$

- For all definable (with parameters) set X, is there a tuple $\bar{c}$ — a code — such that automorphisms fix $\bar{c}$ if and only if they stabilize X set-wise?

Positive answers to these two questions are equivalent and is called elimination of imaginaries.

Theorem (Poizat, 1983)

The theory ACF of algebraically closed fields in the language $\mathcal{L}_{\mathrm{rg}} = \{\mathbf{K}; 0, 1, +, -, \cdot\}$ eliminates imaginaries.

Remark

To any $\mathcal{L}$-structure M we can associate the $\mathcal{L}^{\mathrm{eq}}$-structure M^{eq} where we add a point for each imaginary.

Imaginaries in valued fields

Remark

In the language $\mathcal{L}_{\mathrm{div}}$, the quotient $\Gamma = \mathbf{K}^\star / \mathcal{O}^\star$ is not representable in algebraically closed valued field nor in $\mathbb{Q}_p$.

However, in the case of ACVF — the theory of algebraically closed valued fields — Haskell, Hrushovski and Macpherson have shown what imaginary sorts it suffices to add.

The geometric sorts

Definition

- The elements of $\mathbf{S}_n$ are the free $\mathcal{O}$-module in $\mathbf{K}^n$ of rank n.
- The elements of $\mathbf{T}_n$ are of the form $a + \mathfrak{M}s$ where $s \in \mathbf{S}_n$ and $a \in s$.

We can give an alternative definition of these sorts, for example $\mathbf{S}_n \simeq \mathrm{GL}_n(\mathbf{K})/\mathrm{GL}_n(\mathcal{O})$.

Definition

The geometric language $\mathcal{L}_{\mathcal{G}}$ is composed of the sorts $\mathbf{K}$, $\mathbf{S}_n$ and $\mathbf{T}_n$ for all n, with $\mathcal{L}_{\mathrm{rg}}$ on $\mathbf{K}$ and functions $\rho_n : \mathrm{GL}_n(\mathbf{K}) \to \mathbf{S}_n$ and $\tau_n : \mathbf{S}_n \times \mathbf{K}^n \to \mathbf{T}_n$.

- $\mathbf{S}_1$ can be identified with Γ and ρ_1 with v;
- $\mathbf{T}_1$ can be identified with RV;
- The set of balls (open and closed, possibly with infinite radius) $\mathbb{B}$ can be identified with a subset of $\mathbf{K} \cup \mathbf{S}_2 \cup \mathbf{T}_2$.

The geometric sorts

Definition

- The elements of $\mathbf{S}_n$ are the free $\mathcal{O}$-module in $\mathbf{K}^n$ of rank n.
- The elements of $\mathbf{T}_n$ are of the form $a + \mathfrak{M}s$ where $s \in \mathbf{S}_n$ and $a \in s$.

Definition

The geometric language $\mathcal{L}_{\mathcal{G}}$ is composed of the sorts $\mathbf{K}$, $\mathbf{S}_n$ and $\mathbf{T}_n$ for all n, with $\mathcal{L}_{\mathrm{rg}}$ on $\mathbf{K}$ and functions $\rho_n : \mathrm{GL}_n(\mathbf{K}) \to \mathbf{S}_n$ and $\tau_n : \mathbf{S}_n \times \mathbf{K}^n \to \mathbf{T}_n$.

Theorem (Haskell, Hrushovski and Macpherson, 2006)

- The $\mathcal{L}_{\mathcal{G}}$-theory $\mathrm{ACVF}^{\mathcal{G}}$ eliminates imaginaries.
- In particular, the imaginaries in $\mathrm{ACVF}^{\mathcal{G}}_{0,p}$ (respectively those in $\mathrm{ACVF}^{\mathcal{G}}_{p,p}$) can be eliminated uniformly in p.

The geometric sorts

Definition

- The elements of $\mathbf{S}_n$ are the free $\mathcal{O}$-module in $\mathbf{K}^n$ of rank n.
- The elements of $\mathbf{T}_n$ are of the form $a + \mathfrak{M}s$ where $s \in \mathbf{S}_n$ and $a \in s$.

Definition

The geometric language $\mathcal{L}_{\mathcal{G}}$ is composed of the sorts $\mathbf{K}$, $\mathbf{S}_n$ and $\mathbf{T}_n$ for all n, with $\mathcal{L}_{\mathrm{rg}}$ on $\mathbf{K}$ and functions $\rho_n : \mathrm{GL}_n(\mathbf{K}) \to \mathbf{S}_n$ and $\tau_n : \mathbf{S}_n \times \mathbf{K}^n \to \mathbf{T}_n$.

Question

1. Are all imaginaries in $\mathbb{Q}_p$ coded in the geometric sorts or are there new imaginaries in this theory?
2. Can these imaginaries be eliminated uniformly in p?

The general setting

In the paper, we give a more general setting, but here we will only consider substructures of ACVF.

- Let $T \supseteq \mathrm{ACVF}_\forall^{\mathcal{G}}$ be an $\mathcal{L}_{\mathcal{G}}$-theory.

Let $\widetilde{M} \models \mathrm{ACVF}^{\mathcal{G}}$ and $M \models T$ such that $M \subseteq \widetilde{M}$. Let us fix some notations:

- Let $A \subseteq \widetilde{M}$, we will write $\mathrm{dcl}_{\widetilde{M}}(A)$ for the $\mathcal{L}_{\mathcal{G}}$-definable closure in $\widetilde{M}$,
- Let $A \subseteq M^{\mathrm{eq}}$, we will write $\mathrm{dcl}_M^{\mathrm{eq}}(A)$ for the $\mathcal{L}^{\mathrm{eq}}$-definable closure in M^{eq}.

Similarly for acl, tp and TP (the space of types).

The specific cases of interest

The theory T will be either :

[pCF] The $\mathcal{L}_{\mathcal{G}}$-theory of K a finite extension of $\mathbb{Q}_p$, with a constant added for a generator of $K \cap \overline{\mathbb{Q}}^{\mathrm{alg}}$ over $\mathbb{Q}_p \cap \overline{\mathbb{Q}}^{\mathrm{alg}}$;

[PLF] The $\mathcal{L}_{\mathcal{G}}$-theory of equicharacteristic zero Henselian valued fields with a pseudo-finite residue field, a $\mathbb{Z}$-group as valuation group and 2 constants added:

- A uniformizer, i.e. $\pi \in \mathbf{K}$ with minimal positive valuation;
- An unramified Galois-unifomizer. i.e an element $c \in \mathbf{K}$ such that $\mathrm{res}(c)$ generates $k^\star/(\bigcap_n P_n(k^\star))$.

Remark

Every $\prod K_p/\mathcal{U}$ where K_p is a finite extension of $\mathbb{Q}_p$ and $\mathcal{U}$ is a non principal ultrafilter on the set of primes is a model of PLF. In fact, By the Ax-Kochen-Eršov principle any model of PLF is equivalent to one of these ultraproducts.

A first example: extracting square roots in $\mathbb{Q}_3$

- Let $a \in \mathbb{Q}_3$ and $f : P_2(\mathbb{Q}_3^\star) + a \to \mathbb{Q}_3$, where P_2 is the set of squares, defined by:
$$f(x)^2 = x - a \text{ and } \mathrm{ac}(f(x)) = 1.$$
- This function can be defined in $\mathbb{Q}_3$ but not in $\overline{\mathbb{Q}_3}^{\mathrm{alg}} \vDash \mathrm{ACVF}_{0,3}$.
- However, the 1-to-2 correspondence
$$F = \{(x, y) \mid y^2 = x - a\}$$
is quantifier free definable both in $\mathbb{Q}_3$ and $\overline{\mathbb{Q}_3}^{\mathrm{alg}}$.
- F is the Zariski closure of the graph of f and $f(x)$ can be defined (in $\mathbb{Q}_3$) as the y such that $(x, y) \in F$ and $\mathrm{ac}(y) = 1$.
- F is coded in $\overline{\mathbb{Q}_3}^{\mathrm{alg}}$ and this code is in $\mathrm{dcl}_{\widetilde{M}}(\mathbb{Q}_3) = \mathbb{Q}_3$.
- The graph of f is coded by the code of F.

An abstract criterion

Theorem

Assume the following holds:

(i) Any $\mathcal{L}(M)$-definable unary set $X \subseteq \mathbf{K}(M)$ is coded;

(ii) For all $M_1 \preccurlyeq M$ and $c \in \mathbf{K}(M)$, $\mathrm{dcl}^{\mathrm{eq}}_M(M_1 c) \cap M \subseteq \mathrm{acl}_{\widetilde{M}}(M_1 c)$;

(iii) For all $e \in \mathrm{dcl}_{\widetilde{M}}(M)$, there exists a tuple $e' \in M$ such that for all $\sigma \in \mathrm{Aut}(\widetilde{M})$ with $\sigma(M) = M$, σ fixes e if and only if it fixes e';

(iv) For any $A = \mathrm{acl}^{\mathrm{eq}}_M(A) \cap M$ and $c \in \mathbf{K}(M)$, there exists an $\mathrm{Aut}(\widetilde{M}/A)$-invariant type $\widetilde{p} \in \mathrm{TP}_{\widetilde{M}}(\widetilde{M})$ such that $\widetilde{p}|M$ is consistent with $\mathrm{tp}_{\mathcal{L}}(c/A)$;

(v) For all $A = \mathrm{acl}^{\mathrm{eq}}_M(A) \cap M$ and $c \in \mathbf{K}(M)$, $\mathrm{acl}^{\mathrm{eq}}_M(Ac) \cap M = \mathrm{dcl}^{\mathrm{eq}}_M(Ac) \cap M$.

Then T eliminates imaginaries.

Another abstract criterion

Theorem

Assume the following holds:

(i) Any $\mathcal{L}(M)$-definable unary set $X \subseteq \mathbf{K}(M)$ is coded;

(ii) For all $M_1 \preccurlyeq M$ and $c \in \mathbf{K}(M)$, $\mathrm{dcl}^{\mathrm{eq}}_M(M_1 c) \cap M \subseteq \mathrm{acl}_{\widetilde{M}}(M_1 c)$;

(iii) For all $e \in \mathrm{dcl}_{\widetilde{M}}(M)$, there exists a tuple $e' \in M$ such that for all $\sigma \in \mathrm{Aut}(\widetilde{M})$ with $\sigma(M) = M$, σ fixes e if and only if it fixes e';

(iv) For any $A = \mathrm{acl}^{\mathrm{eq}}_M(A) \cap M$ and $c \in \mathbf{K}(M)$, there exists an $\mathrm{Aut}(\widetilde{M}/A)$-invariant type $\widetilde{p} \in \mathrm{TP}_{\widetilde{M}}(\widetilde{M})$ such that $\widetilde{p}|M$ is consistent with $\mathrm{tp}_{\mathcal{L}}(c/A)$;

(v') For all $A \subseteq M$ and any $e \in \mathrm{acl}^{\mathrm{eq}}_M(A)$ there exists $e' \in M$ such that $e \in \mathrm{dcl}^{\mathrm{eq}}_M(Ae')$ and $e' \in \mathrm{dcl}^{\mathrm{eq}}_M(Ae)$.

Then T eliminates imaginaries.

p-adic imaginaries

Theorem

Let K be a finite extension of $\mathbb{Q}_p$, then the theory of K in the language $\mathcal{L}_{\mathcal{G}}$ with a constant added for a generator of $K \cap \overline{\mathbb{Q}}^{\mathrm{alg}}$ over $\mathbb{Q}_p \cap \overline{\mathbb{Q}}^{\mathrm{alg}}$ eliminates imaginaries.

Proof.

It follows from the first EI criterion. □

Ultraproducts

Theorem

Let $K = \prod K_p/\mathcal{U}$ be an ultraproduct of finite extensions K_p of $\mathbb{Q}_p$. The theory of K in the language $\mathcal{L}_{\mathcal{G}}$, with constants added for a uniformizer and an unramified Galois-uniformizer, eliminate imaginaries.

Proof.

It follows from the second EI criterion. $\square$

Remark

The sorts T_n are useless in those two cases.

Uniformity

Let $\mathcal{L}_{\mathcal{G}}^{\star}$ be $\mathcal{L}_{\mathcal{G}}$ with two constants in $\mathbf{K}$ added.

Definition

An unramified m-Galois uniformizer is a point $c \in \mathbf{K}$ such that $\mathrm{res}(c)$ generates $k^{\star}/P_m(k^{\star})$.

Corollary

For any equivalence relation E_p on a set D_p definable in K_p uniformly in p, there exists m_0 and an $\mathcal{L}_{\mathcal{G}}^{\star}$-formula $\phi(x,y)$ such that for all p, ϕ defines a function

$$f_p : D \to K_p^l \times S_m(K_p)$$

where K_p is made into a $\mathcal{L}_{\mathcal{G}}^{\star}$-structure by choosing a uniformizer and an unramified m_0-Galois uniformizer and

$$K_p \models \forall x,y,\ xE_py \iff f_p(x) = f_p(y).$$

Definable families of equivalence relations

Fix p a prime and let K_p be a finite extension of $\mathbb{Q}_p$.

Definition

A family $(R_l)_{l\in\mathbb{N}^r} \subseteq K_p^n$ is said to be uniformly definable if there is an $\mathcal{L}_{\mathcal{G}}$ formula $\phi(x, y)$ such that for all $l \in \mathbb{N}^r$,

$$\phi(K_p, l) = R_l.$$

We say that $E \subseteq R^2$ is a definable family of equivalence relations on R if E is an equivalence relation on R and

$$\forall x, y \in R,\ xEy \Rightarrow \exists l \in \mathbb{N}^r,\ x, y \in R_l.$$

In particular, for all $l \in \mathbb{N}^r$, E induces an equivalence relation E_l on R_l.

Definable families of equivalence relations

For all prime p, let K_p be a finite extension of $\mathbb{Q}_p$.

Definition

A family $(R_{p,l})_{l\in\mathbb{N}^r} \subseteq K_p^n$ is said to be definable uniformly in p if there is an $\mathcal{L}_{\mathcal{G}}$ formula $\phi(x,y)$ such that for all prime p and $l \in \mathbb{N}^r$,

$$\phi(K_p, l) = R_{p,l}.$$

We say that $E_p \subseteq R_p^2$ is a family of equivalence relations on R_p definable uniformly in p if E_p is an equivalence relation on R_p and

$$\forall p \forall x, y \in R_p,\ xE_py \Rightarrow \exists l \in \mathbb{N}^r,\ x, y \in R_{p,l}.$$

In particular, for all $l \in \mathbb{N}^r$, E_p induces an equivalence relation $E_{p,l}$ on $R_{p,l}$.

Rationality

Theorem

Fix p a prime. Let $(R_\nu)_{\nu\in\mathbb{N}^r} \subseteq K_p^n$ be uniformly definable and E a family of definable equivalence relations on R such that for all $l \in \mathbb{N}^r$, $a_\nu = |R_\nu/E_\nu|$ is finite. Then

$$\sum_\nu a_\nu t^\nu \text{ is rational.}$$

Rationality

Theorem

Let $(R_{p,\nu})_{\nu\in\mathbb{N}^r} \subseteq K_p^n$ be definable uniformly in p and E_p a family of equivalence relations on R definable uniformly in p such that for all prime p and $\nu \in \mathbb{N}^r$, $a_{p,\nu} = |R_\nu/E_\nu|$ is finite. Then for all p,

$$\sum_\nu a_{p,\nu} t^\nu \text{ is rational.}$$

Moreover, there exists m_0 and $d \in \mathbb{N}$ such that for all choice of m_0-Galois uniformizer $c_p \in K_p$, for all $\nu \in \mathbb{N}^r$ with $|\nu| \leq d$, there exists $q_\nu \in \mathbb{Q}$ and varieties V_ν and W_ν over $\mathbb{Z}[X]$ such that for all $p \gg 0$,

$$\sum_\nu a_{p,\nu} t^\nu = \frac{\sum_{|\nu|\leq d} q_\nu |V_\nu(\mathrm{res}(K_p))| t^\nu}{\sum_{|\nu|\leq d} |W_\nu(\mathrm{res}(K_p))| t^\nu}$$

where X is specialized to $\mathrm{res}(c_p)$ in $\mathrm{res}(K_p)$.

Some remarks

- The proof proceeds by:
  1. Using uniform elimination of imaginaries to reduce to counting cosets of $\mathrm{GL}_n(\mathcal{O}(K_p))$ in $\mathrm{GL}_n(K_p)$;
  2. Using the Haar measure μ_p on $\mathrm{GL}_n(K_p)$ normalized such that $\mu_p(\mathrm{GL}_n(\mathcal{O}(K_p))) = 1$, rewrite the sum as an integral;
  3. Use Denef's result on p-adic integrals (and its uniform version given by Pas or even motivic integration).
- In the appendix, Raf Cluckers gives an alternative proof of the counting theorem for fixed p that does not use elimination of imaginaries and generalizes to the analytic setting.
- The denominator of the rational function can described more precisely.
- These results are used to show that some zeta functions that appear in the theory of subgroup growth and representation growth are rational uniformly in p.

Thank you