Transferring imaginaries

How to eliminate imaginaries in p-adic fields

Silvain Rideau
(joint work with E. Hrushovski and B. Martin)

Paris 11, École Normale Supérieure

April 3, 2013

Contents

Codes and Quotients

Definition (Code)

In some structure M, a set X definable (with parameters) is said to be coded by some tuple a if there is a formula $\phi[x,y]$ such that

$$\phi[M,a'] = X(M) \iff a' = a.$$

Definition (Representable quotient)

Let M be some structure, D be a definable set and E be a definable equivalence relation on D. The quotient D/E is said to be representable in M if there exists a definable function f with domain D such that

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

Eliminating imaginaries

Proposition

Let M be some structure with at least two constants, the following are equivalent:

(i) Any subset of M definable (with parameters) is coded,

(ii) Every quotient definable in M is representable.

A theory is said to eliminate imaginaries if every model of T verifies any of the two statements in the previous proposition.

Example

- A non-example : infinite sets,
- An example : algebraically closed fields.

Shelah's construction

Definition

Let M be a $\mathcal{L}$-structure, we define a new language $\mathcal{L}^{\mathrm{eq}}$ and a $\mathcal{L}^{\mathrm{eq}}$-structure M^{eq} as follows:

- For any definable equivalence relation E on a product of $\mathcal{L}$-sorts $\prod_i S_i$, we add to $\mathcal{L}$ a sort S_E and a function $f_E : \prod_i S_i \to S_E$,
- In M^{eq}, S_E is interpreted as $\prod_i S_i(M)/E(M)$ and f_E as the canonical projection.

Proposition

Let T be a complete theory. The language $\mathcal{L}^{\mathrm{eq}}$ and the theory $T^{\mathrm{eq}} = \mathrm{Th}(M^{\mathrm{eq}})$ does not depend on the choice of $M \models T$.

Proposition

Let T be a complete theory. The theory T^{eq} eliminates imaginaries.

Shelah's construction

Definition

Let M be a $\mathcal{L}$-structure, we define a new language $\mathcal{L}^{\text{eq}}$ and a $\mathcal{L}^{\text{eq}}$-structure M^{eq} as follows:

- For any definable equivalence relation E on a product of $\mathcal{L}$-sorts $\prod_i S_i$, we add to $\mathcal{L}$ a sort S_E and a function $f_E : \prod_i S_i \to S_E$,
- In M^{eq}, S_E is interpreted as $\prod_i S_i(M)/E(M)$ and f_E as the canonical projection.

Proposition

Let T be a complete theory. The following are equivalent:

(i) T eliminates imaginaries,

(ii) For all, $M \vDash T$ and $e \in M^{\text{eq}}$, there exists a tuple $d \in M$ such that:

$$d \in \text{dcl}^{\text{eq}}(e) \text{ and } e \in \text{dcl}^{\text{eq}}(d).$$

Finite sets

Definition (Weak elimination of imaginaries)

A complete theory T weakly eliminates imaginaries if for all $M \models T$ and $e \in M^{\mathrm{eq}}$, there exists a tuple $d \in M$ such that:

$$d \in \mathrm{acl}^{\mathrm{eq}}(e) \text{ and } e \in \mathrm{dcl}^{\mathrm{eq}}(d).$$

Example

Infinite sets weakly eliminate imaginaries.

Proposition

Suppose T has weak elimination of imaginaries and every finite set in every model of T is coded, then T eliminates imaginaries.

Finite imaginaries

Definition (EI/UFI)

A complete theory T eliminates imaginaries up to uniform finite imaginaries if for all $M \models T$ and $e \in M^{eq}$, there exists a tuple $d \in M$ such that:

$$d \in \mathrm{dcl}^{eq}(e) \text{ and } e \in \mathrm{acl}^{eq}(d).$$

Proposition

Suppose T has EI/UFI and any finite quotient definable (with parameters) in any model of T is representable, then T eliminates imaginaries.

Contents

Some definitions

Definition

Let K be a field, a valuation on K is a map v from $K^\star$ to some abelian ordered group Γ that satisfies the following axioms:

(i) $\mathrm{v}(xy) = \mathrm{v}(x) + \mathrm{v}(y)$,

(ii) $\mathrm{v}(x+y) \geq \min\{\mathrm{v}(x), \mathrm{v}(y)\}$

- We usually add a point ∞ to Γ to denote $v(0)$, greater than any other point in Γ.
- The set $\mathcal{O} = \{x \in K \mid \mathrm{v}(x) \geq 0\}$ is a ring, called the valuation ring of K.
- 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.
- We will also be considering the group $\mathrm{RV} := K^\star/(1+\mathfrak{M})$.

Some examples

- Let p be a prime number, then we can define the p-adic valuation on $\mathbb{Q}$ by taking $\mathrm{v}_p(p^n a/b) = n$ whenever $a \wedge b = a \wedge p = b \wedge p = 1$,
- We will denote by $\mathbb{Q}_p$, the field of p-adic numbers, the completion of $\mathbb{Q}$ for the p-adic valuation. It is also a valued field,
- We will denote by ACVF the theory of algebraically closed valued field (in some language to be specified).

Imaginaries in valued fields

Remark

In the language of rings enriched with a predicate for $\mathrm{v}(x) \leq \mathrm{v}(y)$, the quotient $\Gamma = K^\star / \mathcal{O}^\star$ is not representable in any algebraically closed valued field nor in $\mathbb{Q}_p$

However, in the case of *ACVF*, Haskell, Hrushovski and Macpherson have shown what imaginary sorts it suffices to add.

The geometric sorts

Definition (The sorts S_n)

The elements of S_n are the free $\mathcal{O}$-module in K^n of rank n.

Definition (The sorts T_n)

The elements of T_n are of the form $a + \mathfrak{M}s$ where $s \in S_n$ and $a \in s$.

- We can give an alternative definition of these sorts, for example $S_n = GL_n(K)/GL_n(\mathcal{O})$,
- The geometric language $\mathcal{L}^{\mathcal{G}}$ is composed of the sorts K, S_n and T_n for all n, with the ring language on K and functions $\rho_n : GL_n(K) \to S_n$ and $\tau_n : S_n \times K^n \to T_n$.

- S_1 can be identified with Γ and ρ_1 with v,
- T_1 can be identified with RV,
- The set of balls (open and closed, possibly with infinite radius) $\mathcal{B}$ can be identified with a subset of $K \cup S_2 \cup T_2$.

The geometric sorts

Definition (The sorts S_n)

The elements of S_n are the free $\mathcal{O}$-module in K^n of rank n.

Definition (The sorts T_n)

The elements of T_n are of the form $a + \mathfrak{M}s$ where $s \in S_n$ and $a \in s$.

Theorem (Haskell, Hrushovski and Macpherson, 2006)

The $\mathcal{L}^{\mathcal{G}}$-theory ACVF eliminates imaginaries.

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 imaginairies be eliminated uniformly in p.

Contents

A first example : real-closed fields

Example (Square roots)

Let K be a real closed field and $\overline{K}^{\text{alg}}$ be its algebraic closure (both fields are considered as ring language structures).

- Let $a \in K$, the function $f : x \mapsto \sqrt{x-a}$ can be defined in K but not in $\overline{K}^{\text{alg}}$,
- However, the 1-to-2 correspondance $F = \{(x,y) \mid y^2 = x - a\}$ is quantifier free definable both in K and $\overline{K}^{\text{alg}}$,
- F is the Zariski closure of the graph of f and $f(x)$ can be defined (in K) as the greatest y such that $(x,y) \in F$,
- In fact, f can be coded by the code of F in $\overline{K}^{\text{alg}}$ (which is K).

The general setting

- Let $\widetilde{\mathcal{L}} \subseteq \mathcal{L}$ be two languages,
- Let $\widetilde{T}$ be a $\widetilde{\mathcal{L}}$ theory that eliminates quantifiers and imaginaries,
- Let T be a $\mathcal{L}$-theory such that $\widetilde{T}_\forall \subseteq T$.

Question

Under what hypotheses can we deduce that T eliminates imaginaries?

Let $\widetilde{M} \vDash \widetilde{T}$ and $M \vDash T$ such that $M \subseteq \widetilde{M}$. Let us fix some notations:

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

Similarly for acl, tp and TP.

The specific cases

- The theory $\widetilde{T}$ will be either $\mathrm{ACVF}_{0,0}$ or $\mathrm{ACVF}_{0,p}$, in $\mathcal{L}^{\mathcal{G}}$.
- The theory T will be either :
  - [pC] The $\mathcal{L}^{\mathcal{G}}$-theory of L a finite extension of $\mathbb{Q}_p$, with a constant added for a generator of $L \cap \overline{\mathbb{Q}}^{\mathrm{alg}}$.
  - [PL] The $\mathcal{L}^{\mathcal{G}}$-theory of $\prod L_p/\mathcal{U}$ where L_p is a finite extension of $\mathbb{Q}_p$ and $\mathcal{U}$ is a non principal ultrafilter on the set of primes, with constants added for some (2-generated) subfield F verifying certain properties.

Remark

By Ax-Kochen-Ersov, the theories of [PL] are the completions of the theory of equicharacteristic zero Henselian valued fields with a pseudo-finite residue field and a $\mathbb{Z}$-group as valuation group.

Dominant sorts

Definition

In a theory, a set of sorts $\mathbf{S}$ will be called dominant if for any other sort S of the language, there is a surjective $\varnothing$-definable function $f : \prod_i S_i \to S$ where the S_i are in $\mathbf{S}$.

Example

- The set consisting of all the sorts is dominant.
- The set of "real" sorts (i.e. the original sorts from M) are dominant in M^{eq},
- In a valued field in the geometric language, the sort K is dominant.

For any choice of theory T, we will suppose that a set of dominant sorts has been chosen, and we will write $\mathrm{dom}(M)$ for the union of the dominant sorts in any model of T.

Algebraic boundedness

Hypothesis (i)

For all $M_1 \preccurlyeq M$ and $c \in \mathrm{dom}(M)$, $\mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(M_1 c) \cap M \subseteq \mathrm{acl}_{\widetilde{\mathcal{L}}}(M_1 c)$.

Proof.

[p C] Follows immediately from the fact that for all models M and $A \subseteq K(M)$, $\mathrm{acl}_{\widetilde{\mathcal{L}}}(A) \preccurlyeq M$.

[PL] A lot more technical. □

Coping with $\mathrm{dcl}_{\widetilde{\mathcal{L}}}(M)$

Hypothesis (ii)

For all $e \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(M)$, 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'.

Proposition

Hypothesis (ii) implies that finite sets are coded in T.

Proof.

It suffices to consider $e \in S_n(\mathrm{dcl}_{\widetilde{\mathcal{L}}}(M))$. Such a lattice has a basis in some finite extension $L|K(M)$. With the added constants, $\mathcal{O}(L)$ is generated over $\mathcal{O}(M)$ by has an element a whose minimal polynomial is over the prime field. Then the image of $e(L)$ by the function $\sum x_i a^i \mapsto (x_i)$ will work. □

Unary imaginaries

Hypothesis (iii)

Any $\mathcal{L}(M)$-definable unary set $X \subseteq \mathrm{dom}(M)^1$ is coded.

Proof.

We need a precise description of unary types. □

Germs

Definition

Let $A \subseteq \widetilde{M}$, r and s be A-definable functions and $p \in \mathrm{TP}_{\widetilde{\mathcal{L}}}(A)$ that contains the domain of both r and s. The functions r and s are said to have the same p-germ if for some $c \models p$, $r(c) = s(c)$.

Remark

- If r and s have the same p-germ, then for any $c \models p$, $r(c) = s(c)$,
- "Having the same p-germ" is an equivalence relation on A-definable functions. We will write $\partial_p r$ for the class of all A-definable functions having the same p-germ as r,
- If p is a definable type and we only consider the germs of a family of uniformly defined functions r_b, $\partial_p r_b$ is an imaginary,
- In any case, if p is $\mathrm{Aut}(\widetilde{M}/A)$-invariant, then the action of $\mathrm{Aut}(\widetilde{M}/A)$ on $\widetilde{\mathcal{L}}(\widetilde{M})$-definable functions induces an action on p-germs.

Controlling germs

Hypothesis (iv)

For any $A = \mathrm{acl}^{\mathrm{eq}}_{\mathcal{L}}(A) \cap M$ and $c \in \mathrm{dom}(M)^1$, there exists an $Aut(\widetilde{M}/A)$-invariant type $\widetilde{p} \in \mathrm{TP}_{\widetilde{\mathcal{L}}}(\widetilde{M})$ such that $\widetilde{p}|M$ is consistent with $\mathrm{tp}_{\mathcal{L}}(c/A)$.
Moreover, for any $\widetilde{\mathcal{L}}(B)$-definable function r:

($\star$) There exists a sequence $(\varepsilon_i)_{i\in\kappa}$, with $\varepsilon_i \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(AB)$ such that any $\sigma \in \mathrm{Aut}(\widetilde{M}/A)$ fixes $\partial_{\widetilde{p}} r$ iff σ fixes almost every ε_i.

Proof.

We need a precise description of unary types. □

Rigidity of finite sets

Hypothesis (v)

For all $A = \operatorname{acl}^{eq}_{\mathcal{L}}(A) \cap M$ and $c \in \operatorname{dom}(M)$, $\operatorname{acl}^{eq}_{\mathcal{L}}(Ac) \cap M = \operatorname{dcl}^{eq}_{\mathcal{L}}(Ac) \cap M$.

Proof.

[p C] Follows from the fact that the hypothesis is true for $A \subseteq K$, and that for all $e \in M$ there is a tuple $c \in K(M)$ such that $e \in \operatorname{dcl}^{eq}_{\mathcal{L}}(c)$ and $\operatorname{tp}_{\mathcal{L}}(c/\operatorname{acl}^{eq}_{\mathcal{L}}(c))$ has an invariant extension.

[PL] False in some cases. □

The theorem

Theorem (EI/UFI Criterion)

If the hypotheses (i) to (iv) are true, then T eliminates imaginaries up to uniform finite imaginaries.

Corollary (EI Criterion)

If the hypotheses (i) to (v) are true, then T eliminates imaginaries.

Contents

Generic types

Definition

Let M be a valued field, $A \subseteq M^{\mathrm{eq}}$, $b_i \in \mathcal{B}(\mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(A))$ be a decreasing sequence of balls and $P = \bigcap_i b_i$. We define :

$$q_P|A := P(x) \cup \{x \notin b \mid b \in \mathcal{B}(\mathrm{acl}^{\mathrm{eq}}_{\mathcal{L}}(A)), b \subset P\}.$$

Any $c \vDash q_P|A$ will be said to be generic in P over A.

Remark

- If $A = \mathrm{acl}^{\mathrm{eq}}_{\mathcal{L}}(A)$, any $c \in K(M)^1$ is generic over A in

$$\bigcap P(c, A) := \{b \in \mathcal{B}(A) \mid c \in b\}.$$

- P is said to be strict if the sequence b_i does not have a smallest element. In the [pC] case, $P(c, A)$ is strict.

Relative completeness

Definition

Let p be a partial type over some parameters A and $f = (f_i)$ be a family of A-definable functions. The type p is said to be complete relative to f if the map $\mathrm{tp}_{\mathcal{L}}(c/A) \mapsto \mathrm{tp}_{\mathcal{L}}(f(c)/A)$ is injective on the set of completions of p.

Unary types in [pC]

Let r_n be the canonical surjection $K^\star \to K^\star/(K^\star)^n$.

Proposition

Let $A \subseteq M^{eq}$ and P be a strict intersection of balls in $\mathcal{B}(\mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(A))$, then :

- If there exists a ball $a \in \mathcal{B}(\mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(A))$ such that $a \subset P$, then $q_P|A$ is complete relative to $(\mathrm{v}(x-a), r_n(x-a) \mid 2 \geq n)$.
- If not, $q_P|A$ is complete.

Proof.

If $A \subseteq \mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(K(A))$ then the proposition follows from quantifier elimination. If not, find $M_0 \preccurlyeq M$ such that $A^{eq} \subseteq M_0^{\mathrm{eq}}$ and for any $c \models q_P|A$ there exists $c' \models q_P|M_0^{\mathrm{eq}}$ such that $c \equiv_A c'$.
In the first case, any M_0 works, in the second, choose M_0 that omits P. □

Remark

With the added constant, $r_n(M) \subseteq \mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(\varnothing)$.

Unary types in [PL] (strict case)

Proposition

Let $A \subseteq M^{eq}$ and P be a strict intersection of balls in $\mathcal{B}(\mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(A))$, then :

- If there exists a ball $a \in \mathcal{B}(\mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(A))$ such that $a \subset P$, then $q_P|A$ is complete relative to $\mathrm{rv}(x - a)$.
- If not, $q_P|A$ is complete.

Proof.

The same proof as previously works. □

Unary types in [PL] (closed ball case)

Let $b \in \mathcal{B}(\mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(A))$ and γ be the radius of b. We define the following map $\mathrm{res}_b : x \mapsto x + \gamma\mathcal{M}$, the maximal open subball of b containing x.

Proposition

The type $q_b|A$ is complete relative to res_b.

Proof.

The same proof as previously works (except that the omission type argument is not useful). □

Unary types in [PL] (closed ball case)

Let $b \in \mathcal{B}(\mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(A))$ and γ be the radius of b. We define the following map $\mathrm{res}_b : x \mapsto x + \gamma\mathcal{M}$, the maximal open subball of b containing x.

Proposition

The type $q_b|A$ is complete relative to res_b.

Corollary

- If there exists a ball $a \in \mathcal{B}(\mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(A))$ such that $a \subset b$, then $q_b|A$ is complete relative to $\mathrm{rv}(x - a)$.

Proof.

If $c, c' \vDash q_b|A$, $\mathrm{res}_b(c) = \mathrm{res}_b(c')$ if and only if $\mathrm{rv}(c - a) = \mathrm{rv}(c' - a)$. □

Unary types in [PL] (closed ball case)

Let $b \in \mathcal{B}(\mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(A))$ and γ be the radius of b. We define the following map $\mathrm{res}_b : x \mapsto x + \gamma\mathcal{M}$, the maximal open subball of b containing x.

Proposition

The type $q_b|A$ is complete relative to res_b.

Corollary

- If there exists a ball $a \in \mathcal{B}(\mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(A))$ such that $a \subset b$, then $q_b|A$ is complete relative to $\mathrm{rv}(x - a)$.
- If not, $q_b|A$ is complete.

Proof.

It suffices to show that a A-definable 1-dimensional affine space over k with no $\mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(A)$-points is a complete type, but that is surprisingly difficult. □

Unary Imaginaries

Proposition

In both cases, we have elimination of unary imaginaries.

Proof.

In the [PL] case we first have to show that the theory of the structure induced on RV eliminates imaginaries. It then follows (in both cases) from the description of unary types that for all $A = \mathrm{acl}^{\mathrm{eq}}_{\mathcal{L}}(A)$ and $c \in K(M)$[1]:

$$\mathrm{tp}_{\mathcal{L}}(c/B) \vdash \mathrm{tp}_{\mathcal{L}}(c/A)$$

where $B = \mathcal{B}(A)$. □

Controlling germs

Hypothesis (iv)

For any $A = \mathrm{acl}^{\mathrm{eq}}_{\mathcal{L}}(A) \cap M$ and $c \in \mathrm{dom}(M)^1$, there exists an $Aut(\widetilde{M}/A)$-invariant type $\widetilde{p} \in \mathrm{TP}_{\widetilde{\mathcal{L}}}(\widetilde{M})$ such that $\widetilde{p}|M$ is consistent with $\mathrm{tp}_{\mathcal{L}}(c/A)$.
Moreover, for any $\widetilde{\mathcal{L}}(B)$-definable function r:

($\star$) There exists a sequence $(\varepsilon_i)_{i\in\kappa}$, with $\varepsilon_i \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(AB)$ such that any $\sigma \in \mathrm{Aut}(\widetilde{M}/A)$ fixes $\partial_{\widetilde{p}} r$ iff σ fixes almost every ε_i.

Proof.

Suppose c is generic in some $P = \bigcap b_i$ over A, then take $\widetilde{p}$ to be the ACVF-generic of P over $\widetilde{M}$.

- If P is a closed ball, then $\widetilde{p}$ is A-definable and hence the germs of function on $\widetilde{p}$ are imaginaries (which can be eliminated in ACVF).
- If P is strict, take ε_i to be the germ of r on the ACVF-generic of b_i. □

Contents

p-adic imaginaries

Theorem

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

Proof.

It follows from the EI criterion. □

Let $\mathcal{L}^{\mathcal{G}^-}$ be the language $\mathcal{L}^{\mathcal{G}}$ restricted to the sorts K and S_n.

Corollary

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

Uniformity

Theorem

Let $L = \prod L_p/\mathcal{U}$ be an ultraproduct of finite extensions L_p of $\mathbb{Q}_p$. The theory of L in the language $\mathcal{L}^{\mathcal{G}^-}$ with some added constants eliminates imaginaries.

Proof.

The EI/UFI criterion applies in $\mathcal{L}^{\mathcal{G}}$ (and we reduce to $\mathcal{L}^{\mathcal{G}^-}$ in the same manner). It remains to show that definable finite quotient are represented, but one can show that they are internal to RV and, as we already know, the induced theory on RV eliminates imaginaries. □

Corollary

For any equivalence relation E on a set D definable in L_p uniformly in p, there exists uniformly definable non-empty set X and function $f : X \times D \to S_m \times K^l$ such that for any prime p, and any $a \in X(L_p)$, for all $x, y \in D(L_p)$, we have: $f(a,x) = f(a,y)$ iff xEy.