Transfert d'imaginaires

Comment éliminer les imaginaires dans les corps p-adiques

Silvain Rideau
(avec E. Hrushovski et B. Martin)

Paris 11, École Normale Supérieure

19 septembre, 2013

Table des matières

Codes et Quotients

Définition (Code)

Soit X un ensemble définissable (avec paramètres) dans une structure M. On dit que $a \in M$ est un code de X s'il existe une formule $\phi[x, y]$ telle que

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

Définition (Quotient représenté)

Soit M une structure, D un ensemble $\varnothing$-définissable et $E \subseteq D^2$ une relation d'équivalence $\varnothing$-définissable. Le quotient D/E est dit représenté dans M s'il existe une fonction $\varnothing$-définissable f de domaine D telle que

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

Élimination des imaginaires

Proposition

Soit M une structure avec aux moins deux constantes, les énoncés suivants sont équivalentes :

(i) Tout ensemble définissable de M (avec paramètres) est codé ;

(ii) Tout quotient définissable dans M est représenté.

Une théorie T élimine les imaginaires si dans tout modèle de T l'un des énoncé précédent est vérifié.

Exemple

- Un non-exemple : les ensembles infinis ;
- Un exemple : les corps algébriquement clos.

La construction de Shelah

Définition

Soit M une $\mathcal{L}$-structure, on définit ainsi un nouveau langage $\mathcal{L}^{\mathrm{eq}} \supseteq \mathcal{L}$ et une $\mathcal{L}^{\mathrm{eq}}$-structure M^{eq} :

- Pour toute relation d'équivalence E $\varnothing$-définissable sur un produit de $\mathcal{L}$-sortes $\prod_i S_i$, on ajoute une nouvelle sorte S_E et une fonction $f_E : \prod_i S_i \to S_E$;
- Dans M^{eq}, on interprète S_E par $\prod_i S_i(M)/E(M)$ et f_E par la projection canonique.

Proposition

Soit T une théorie complète. Le langage $\mathcal{L}^{\mathrm{eq}}$ et la théorie $T^{\mathrm{eq}} = \mathrm{Th}(M^{\mathrm{eq}})$ ne dépend pas du choix de $M \vDash T$.

Proposition

Soit T une théorie complète. La théorie T^{eq} élimine les imaginaires.

La construction de Shelah

Définition

Soit M une $\mathcal{L}$-structure, on définit ainsi un nouveau langage $\mathcal{L}^{\mathrm{eq}} \supseteq \mathcal{L}$ et une $\mathcal{L}^{\mathrm{eq}}$-structure M^{eq} :

- Pour toute relation d'équivalence E $\varnothing$-définissable sur un produit de $\mathcal{L}$-sortes $\prod_i S_i$, on ajoute une nouvelle sorte S_E et une fonction $f_E : \prod_i S_i \to S_E$;
- Dans M^{eq}, on interprète S_E par $\prod_i S_i(M)/E(M)$ et f_E par la projection canonique.

Proposition

Soit T une théorie complète. Les énoncés suivants sont équivalents :

(i) T élimine les imaginaires ;

(ii) Pour tout $M \vDash T$ et $e \in M^{\mathrm{eq}}$, il existe un uple $d \in M$ tel que :

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

Ensembles finis

Définition (Élimination faible des imaginaires)

Une théorie complète T élimine faiblement les imaginaires si pour tout $M \vDash T$ et $e \in M^{\mathrm{eq}}$, il existe un uple $d \in M$ tel que :

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

Exemple

Les ensembles infinis éliminent faiblement les imaginaires.

Proposition

Si T élimine faiblement les imaginaires et tout ensemble fini dans tout modèle de T a un code, alors T élimine les imaginaires.

Imaginaires finis

Définition (EI/UFI)

Une théorie complète T élimine les imaginaires aux imaginaires finis uniformes près si pour tout $M \models T$ et $e \in M^{\mathrm{eq}}$, il existe un uple $d \in M$ tel que :

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

Proposition

Si T a EI/UFI et que tout quotient fini définissable (avec paramètres) dans tout modèle de T est représenté (en utilisant les même paramètres), alors T élimine les imaginaires.

Table des matières

- Imaginaires
- Corps valués
- Transfert d'imaginaires
- Les imaginaires p-adiques

Quelques définitions

Définition

Soit K un corps, une valuation sur K est une fonction v de $K^\star$ dans un groupe abélien ordonné Γ qui satisfait les conditions suivantes :

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

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

- On ajoute habituellement un point ∞ à Γ, plus grand que tout point de Γ, pour représenter $v(0)$;
- L'ensemble $\mathcal{O} = \{x \in K \mid \mathrm{v}(x) \geq 0\}$ est un anneau et c'est l'anneau de valuation de K ;
- Il a un unique idéal maximal $\mathfrak{M} = \{x \in K \mid \mathrm{v}(x) > 0\}$;
- Le corps résiduel $\mathcal{O} / \mathfrak{M}$ sera appelé k.
- On considérera aussi le groupe $\mathrm{RV} := K^\star/(1+\mathfrak{M})$.

Quelques exemples

- Soit p un nombre premier, on définit la valuation p-adique sur $\mathbb{Q}$ en posant $\mathrm{v}_p(p^n a/b) = n$ quand $a \wedge b = a \wedge p = b \wedge p = 1$;
- On notera $\mathbb{Q}_p$, le corps des nombres p-adiques. C'est le complété de $\mathbb{Q}$ pour la valuation p-adique ;
- Soit $\mathcal{L}_{\mathrm{div}}$ le langage des anneaux augmenté d'un prédicat $\leq$. Tout corps valué peut être muni d'une $\mathcal{L}_{\mathrm{div}}$-structure en interprétant $x \leq y$ par $\mathrm{v}(x) \leq \mathrm{v}(y)$. On notera ACVF la théorie des corps valués algébriquement clos (dans le langage $\mathcal{L}_{\mathrm{div}}$).

Remarque

Dans le langage $\mathcal{L}_{\text{div}}$, le quotient $\Gamma = K^\star / \mathcal{O}^\star$ n'est représentable dans aucun corps algébriquement clos ni dans $\mathbb{Q}_p$.

Cependant, dans le cas de ACVF, Haskell, Hrushovski et Macpherson ont montré quelles sortes il suffisait de rajouter.

Les sortes géométriques

Définition (Les sortes S_n)

Les éléments de S_n sont les $\mathcal{O}$-modules libres de K^n de rang n.

Définition (Les sortes T_n)

Les éléments de T_n sont de la forme $a + \mathfrak{M}s$ où $s \in \mathrm{S}_n$ et $a \in s$.

- On peut donner une définition alternative de ces sortes, par exemple $\mathrm{S}_n = \mathrm{GL}_n(K)/\mathrm{GL}_n(\mathcal{O})$;
- Le langage géométrique $\mathcal{L}^{\mathcal{G}}$ est composé des sortes K, S_n et T_n pour tout n, munies du langage des anneaux sur K et de fonctions $\rho_n : \mathrm{GL}_n(K) \to \mathrm{S}_n$ et $\tau_n : \mathrm{S}_n \times K^n \to \mathrm{T}_n$.
- On peut identifier Γ à S_1 de façon canonique et ρ_1 est alors identifié avec v ;
- T_1 peut être identifié (de façon canonique) avec RV ;
- L'ensemble des boules (ouvertes ou fermées, de rayon potentiellement infini) $\mathcal{B}$ peut être identifié de façon canonique avec un sous-ensemble de $K \cup \mathrm{S}_2 \cup \mathrm{T}_2$.

Les sortes géométriques

Définition (Les sortes S_n)

Les éléments de S_n sont les $\mathcal{O}$-modules libres de K^n de rang n.

Définition (Les sortes T_n)

Les éléments de T_n sont de la forme $a + \mathfrak{M}s$ où $s \in S_n$ et $a \in s$.

Théorème (Haskell, Hrushovski et Macpherson, 2006)

La $\mathcal{L}^{\mathcal{G}}$-théorie ACVF élimine les imaginaires.

Question

1. Est-ce que tout les imaginaires de $\mathbb{Q}_p$ sont aussi codés dans les sortes géométriques ou est-ce qu'il y a de nouveaux imaginaires dans cette théorie ?
2. Est-ce que ces imaginaires peuvent être éliminés uniformément en p.

Table des matières

Un premier exemple : les corps réels clos

Exemple (Racine carrée)

Soit K un corps réel clos et $\overline{K}^{\mathrm{alg}}$ sa clôture algébrique (les deux corps sont considérés dans le langage des anneaux).

- Soit $a \in K$, la fonction $f : x \mapsto \sqrt{x-a}$ peut être définie dans K mais pas dans $\overline{K}^{\mathrm{alg}}$;
- Cependant la correspondance $F = \{(x,y) \mid y^2 = x - a\}$ est définissable sans quantificateurs à la fois dans K et dans $\overline{K}^{\mathrm{alg}}$;
- F est la clôture de Zariski du graphe de f et $f(x)$ peut être défini (dans K) comme le plus grand y tel que $(x,y) \in F$;
- En fait, f peut être codé dans K par le code de F dans $\overline{K}^{\mathrm{alg}}$ (qui se trouve être dans K).

Le cas général

- Soient $\widetilde{\mathcal{L}} \subseteq \mathcal{L}$ deux langages ;
- Soit $\widetilde{T}$ une $\widetilde{\mathcal{L}}$ théorie qui élimine les quantificateurs et les imaginaires ;
- Soit T une $\mathcal{L}$-théorie telle que $\widetilde{T}_\forall \subseteq T$.

Question

Sous quelles hypothèses peut-on déduire que T élimine les imaginaires ?

Soit $\widetilde{M} \models \widetilde{T}$ et $M \models T$ tel $M \subseteq \widetilde{M}$. Fixons quelques notations :

- Soit $A \subseteq \widetilde{M}$, on écrira $\mathrm{dcl}_{\widetilde{\mathcal{L}}}(A)$ pour la clôture $\widetilde{\mathcal{L}}$-définissable (sans quantificateur) dans $\widetilde{M}$;
- Soit $A \subseteq M^{\mathrm{eq}}$, on écrira $\mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(A)$ pour la clôture $\mathcal{L}^{\mathrm{eq}}$-définissable dans M^{eq}.

De même pour acl, tp et TP.

Les cas particuliers

- En pratique la théorie $\widetilde{T}$ sera soit $\mathrm{ACVF}_{0,0}$ ou $\mathrm{ACVF}_{0,p}$, dans $\mathcal{L}^{\mathcal{G}}$.
- La théorie T sera :

[p C] La $\mathcal{L}^{\mathcal{G}}$-théorie de L une extension finie de $\mathbb{Q}_p$, enrichie avec une constante pour un générateur de $L \cap \overline{\mathbb{Q}}^{\mathrm{alg}}$.

[PL] La $\mathcal{L}^{\mathcal{G}}$-théorie de $\prod L_p/\mathcal{U}$ où L_p est une extension finie de $\mathbb{Q}_p$ et $\mathcal{U}$ est un ultrafiltre non principal sur l'ensemble des nombre premiers, avec des constantes rajoutées pour un sous-corps F (généré par deux éléments) qui vérifie certaines propriétés.

Remarque

Par Ax-Kochen-Ersov, les théories du cas [PL] sont les complétions de la théorie des corps d'équicaractéristique zéro henséliens avec un corps résiduel pseudo-fini et un groupe de valeur un $\mathbb{Z}$-groupe.

Sortes dominantes

Définition

Dans une théorie, un ensemble de sortes $\mathbf{S}$ est dit dominant si pour toute sorte S du langage, il y a une surjection $\varnothing$-définissable $f : \prod_i S_i \to S$ où les S_i sont toutes dans $\mathbf{S}$.

Exemple

- L'ensemble de toutes les sortes est dominant ;
- L'ensemble des sortes « réelles » (i.e. les sortes originelles de M) sont dominantes dans M^{eq}.
- Dans un corps valué dans le langage géométrique, la sorte K est dominante.

Dans toute théorie T, on suppose qu'on a choisi un ensemble dominant de sortes et on écrira $\mathrm{dom}(M)$ pour l'union des sortes dominantes dans $M \models T$.

Algébriquement borné

Hypothèse (i)

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

Démonstration.

[p C] C'est une conséquence immédiate du fait que pour tout $M \vDash T$ et $A \subseteq K(M)$, $\mathrm{acl}_{\widetilde{\mathcal{L}}}(A) \cap M \preccurlyeq M$.

[PL] Beaucoup plus technique. $\square$

Prendre en compte $\mathrm{dcl}_{\widetilde{\mathcal{L}}}(M)$

Hypothèse (ii)

Pour tout $e \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(M)$, il existe un uple $e' \in M$ tel que pour tout $\sigma \in \mathrm{Aut}(\widetilde{M})$ tel que $\sigma(M) = M$, σ fixe e si et seulement s'il fixe e'.

Proposition

L'hypothèse (ii) implique que les ensembles finis sont codés dans T.

Démonstration.

Il suffit de considérer $e \in S_n(\mathrm{dcl}_{\widetilde{\mathcal{L}}}(M))$. Un tel réseau a une base dans une extension finie $L|K(M)$. Comme le groupe de Galois est borné, on peut remplacer L par l'union de toutes les extension de même degré que L. Avec les constantes que l'on a ajouté, $\mathcal{O}(L)$ est généré en temps que $\mathcal{O}(M)$-algèbre par un élément a dont le polynôme minimal est à paramètres dans le corps premier. Alors l'image de $e(L)$ par la fonction $\sum x_i a^i \mapsto (x_i)$ marche. $\square$

Imaginaires unaires

Hypothèse (iii)

Tout ensemble $\mathcal{L}(M)$-définissable unaire $X \subseteq \mathrm{dom}(M)$ est codé.

Démonstration.

On a besoin d'une description précise des types unaires. $\square$

Germes

Définition

Soit $A \subseteq \widetilde{M}$, r et s des fonctions $\widetilde{\mathcal{L}}(A)$-définissable et $p \in \mathrm{TP}_{\widetilde{\mathcal{L}}}(A)$ qui contient le domaine de r et s. Les fonctions r et s ont le même p-germe si $r(x) = s(x) \in p$.

Remarque

- « Avoir le même p-germe » est une relation d'équivalence sur les fonctions A-définissables. On écrira $\partial_p r$ la classe r pour cette équivalence ;
- Si p est un type définissable et qu'on ne considère que les germes d'une famille de fonctions uniformément définies r_b, alors $\partial_p r_b$ est un imaginaire ;
- Dans tous les cas, si p est $\mathrm{Aut}(\widetilde{M}/A)$-invariant, alors l'action de $\mathrm{Aut}(\widetilde{M}/A)$ sur les fonctions $\widetilde{\mathcal{L}}(\widetilde{M})$-définissables induit une action sur les p-germes.

Contrôler les germes

Hypothèse (iv)

Pour tout $A = \mathrm{acl}^{\mathrm{eq}}_{\mathcal{L}}(A) \cap M$ et $c \in \mathrm{dom}(M)$, il existe un type $Aut(\widetilde{M}/A)$-invariant $\widetilde{p} \in \mathrm{TP}_{\widetilde{\mathcal{L}}}(\widetilde{M})$ tel que $(\widetilde{p}|M) \cup \mathrm{tp}_{\mathcal{L}}(c/A)$ est consistant.
De plus, pour toute fonctions $\widetilde{\mathcal{L}}(B)$-définissable r :

($\star$) Il existe une séquence $(\varepsilon_i)_{i \in \kappa}$, avec $\varepsilon_i \in \mathrm{dcl}_{\widetilde{\mathcal{L}}}(AB)$ tel que tout $\sigma \in \mathrm{Aut}(\widetilde{M}/A)$ fixe $\partial_{\widetilde{p}} r$ si et seulement si σ fixe presque tous les ε_i.

Démonstration.

Nous avons besoin d'une description plus précise des types unaires. □

Rigidité des ensembles finis

Hypothèse (v)

Pour tout $A = \mathrm{acl}^{\mathrm{eq}}_{\mathcal{L}}(A) \cap M$ et $c \in \mathrm{dom}(M)$, $\mathrm{acl}^{\mathrm{eq}}_{\mathcal{L}}(Ac) \cap M = \mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(Ac) \cap M$.

Démonstration.

[p C] C'est une conséquence du fait que cette hypothèse est vraie quand $A \subseteq K$, et que pour tout $e \in M$ il existe un uple $c \in K(M)$ tel que $e \in \mathrm{dcl}^{\mathrm{eq}}_{\mathcal{L}}(c)$ et $\mathrm{tp}_{\mathcal{L}}(c/\,\mathrm{acl}^{\mathrm{eq}}_{\mathcal{L}}(e))$ a une extension invariante.

[PL] C'est faux dans certains cas. □

Le théorème abstrait

Théorème (Critère d'EI/UFI)

Si les hypothèses (i) à (iv) sont vérifiées, alors T élimine les imaginaires aux imaginaires finis uniformes près.

Corollaire (Critère d'EI)

Si les hypothèses (i) à (v) sont vérifiées, alors T élimine les imaginaires.

Table des matières

imaginaires p-adiques

Théorème

Soit F une extension finie de $\mathbb{Q}_p$. La théorie de F dans le langage $\mathcal{L}^{\mathcal{G}}$, avec une constante ajoutée pour un générateur de $F \cap \overline{\mathbb{Q}}^{\mathrm{alg}}$ au dessus de $\mathbb{Q}$, élimine les imaginaires.

Démonstration.

C'est une conséquence du critère d'EI. $\square$

Soit $\mathcal{L}^{\mathcal{G}^-}$ le langage $\mathcal{L}^{\mathcal{G}}$ restreint aux sortes K et S_n.

Corollaire

Soit F une extension finie de $\mathbb{Q}_p$, alors la théorie de F dans le langage $\mathcal{L}^{\mathcal{G}^-}$, avec une constante ajoutée pour un générateur de $F \cap \overline{\mathbb{Q}}^{\mathrm{alg}}$ au dessus de $\mathbb{Q}$, élimine les imaginaires.

Uniformité

Théorème

Soit $L = \prod L_p/\mathcal{U}$ un ultraproduit d'extensions finies L_p de $\mathbb{Q}_p$. La théorie de L dans le langage $\mathcal{L}^{\mathcal{G}^-}$, enrichie de certaines constantes, élimine les imaginaires.

Démonstration.

Le critère d'EI/UFI s'applique dans $\mathcal{L}^{\mathcal{G}}$ (et on se réduit à $\mathcal{L}^{\mathcal{G}^-}$ comme précédemment). Il reste à montrer que les quotients finis définissables (avec paramètres) sont représentables (avec les même paramètres). Mais on peut montrer que ces quotient sont internes à RV et de montrer que la théorie induite sur RV élimine les imaginaires. $\square$

Uniformité

Théorème

Soit $L = \prod L_p/\mathcal{U}$ un ultraproduit d'extensions finies L_p de $\mathbb{Q}_p$. La théorie de L dans le langage $\mathcal{L}^{\mathcal{G}^-}$, enrichie de certaines constantes, élimine les imaginaires.

Corollaire

Soit E une relation d'équivalence sur un ensemble définissable D dans L_p uniformément en p. Il existe alors un ensemble non vide X et une fonction $f : X \times D \to S_m \times K^l$, $\varnothing$-définissables uniformément en p, tels que pour tout nombre premier p, tout $a \in X(L_p)$ et tout $x, y \in D(L_p)$, on : $f(a,x) = f(a,y)$ si et seulement si xEy.