Imaginaries in Model Theory

Martin Hils

Équipe de Logique Mathématique, Université Paris 7

Philosophy and Model Theory Conference
Université Paris Ouest & École normale supérieure
June 2-5, 2010, Paris

Outline

Context

- $\mathcal{L}$ is some countable **first order language** (possibly many-sorted);
- T a **complete** $\mathcal{L}$-theory;
- $\mathcal{U} \models T$ is very **saturated** and **homogeneous**;
- all models $\mathcal{M}$ we consider (and all parameter sets A) are **small**, with $\mathcal{M} \preccurlyeq \mathcal{U}$.

Imaginary Elements

Recall:

- An **equivalence relation** E on a set D is a binary relation which is **reflexive**, **symmetric** and **transitive**;
- D is partitioned into the **equivalence classes modulo** E, i.e. sets of the form $d/E := \{d' \in D \mid dEd'\}$.

Definition

An **imaginary element** in $\mathcal{U}$ is an equivalence class d/E, where E is a definable equivalence relation on a definable set $D \subseteq U^n$ and $d \in D(\mathcal{U})$.

Examples of Imaginaries I

Example (Unordered tuples)

- In any theory, the formula

$$(x = x' \wedge y = y') \vee (x = y' \wedge y = x')$$

defines an equiv. relation $(x, y)E_2(x', y')$ on pairs, with

$$(a, b)E_2(a', b') \Leftrightarrow \{a, b\} = \{a', b'\}.$$

Thus, $\{a, b\}$ may be thought of as an imaginary element.

- Similarly, for any $n \in \mathbb{N}$, the set $\{a_1, \ldots, a_n\}$ may be thought of as an imaginary.

Examples of Imaginaries II

A group $(G, \cdot)$ is a **definable group** in $\mathcal{U}$ if $G \subseteq_{def} U^k$ and $\Gamma = \{(f, g, h) \in G^3 \mid f \cdot g = h\} \subseteq_{def} U^{3k}$ for some $k \in \mathbb{N}$.

Example (Cosets)

Let $(G, \cdot)$ be definable group in $\mathcal{U}$ and H a definable subgroup of G. Then any **coset**

$$g \cdot H = \{g \cdot h \mid h \in H\}$$

is an imaginary (w.r.t. $gEg' \Leftrightarrow \exists h \in H\, g \cdot h = g'$).

Examples of Imaginaries III

Example (Vectors in Affine Space)

- Consider the **affine space** associated to the $\mathbb{Q}$-vector space $\mathbb{Q}^n$, i.e. the structure $\mathcal{M} = \langle \mathbb{Q}^n, \alpha \rangle$, where

$$\alpha(a, b, c) := a + (c - b).$$

- The **vector** $\vec{bc}$ is an imaginary $(b, c)/E$ in $\mathcal{M}$, for

$$(b, c)E(b', c') :\Leftrightarrow \alpha(b, b, c) = \alpha(b, b', c').$$

Utility of Imaginaries

Taking into account imaginary elements has several advantages:

- may talk about **quotient objects**
  (e.g. G/H, where $H \leq G$ are definable groups)
  $\Rightarrow$ category of def. objects is closed under quotients;
- right framework for **interpretations**;
- existence of **codes for definable sets**
  (will be made precise later).

Adding Imaginaries: Shelah's $\mathcal{M}^{eq}$-Construction

There is a canonical way of adding all imaginaries to $\mathcal{M}$, due to Shelah, by expanding

- $\mathcal{L}$ to a many-sorted language $\mathcal{L}^{eq}$,
- T to a (complete) $\mathcal{L}^{eq}$-theory T^{eq} and
- $\mathcal{M} \models T$ to $\mathcal{M}^{eq} \models T^{eq}$ such that
- $\mathcal{M} \mapsto \mathcal{M}^{eq}$ is an equivalence of categories between $\langle Mod(T), \preccurlyeq \rangle$ and $\langle Mod(T^{eq}), \preccurlyeq \rangle$.

Shelah's $\mathcal{M}^{eq}$-Construction (continued)

For any $\emptyset$-definable equivalence relation E on M^n we add

- a new **imaginary sort** S_E
  (the intitial sort of M is called the **real sort** S_{real}),
  a new function symbol $\pi_E : S_{real}^n \to S_E$
  $\Rightarrow$ obtain $\mathcal{L}^{eq}$;
- axioms stating that π_E is surjective, with

$$\pi_E(\bar{a}) = \pi_E(\bar{a}') \Leftrightarrow \bar{a} E \bar{a}'$$

  $\Rightarrow$ obtain T^{eq};
- expand $\mathcal{M} \models T$, interpreting π_E and S_E accordingly
  $\Rightarrow$ obtain $\mathcal{M}^{eq} = \langle M, M^n/E, \ldots ; R^{\mathcal{M}}, f^{\mathcal{M}}, \ldots, \pi_E^{\mathcal{M}^{eq}}, \ldots \rangle$.

Definable and algebraic closure

Definition

Let $B \subseteq \mathcal{U}$ be a set of parameters and $a \in \mathcal{U}$.

- a is **definable over** B if $\{a\}$ is a B-definable set;
- a is **algebraic over** B if there is a finite B-definable set containing a.
- The **definable closure of** B is given by

$$\mathrm{dcl}(B) = \{a \in \mathcal{U} \mid a \text{ definable over } B\}.$$

- Similarly define $\mathrm{acl}(B)$, the **algebraic closure of** B.

These definitions make sense in $\mathcal{U}^{eq}$;
may write dcl^{eq} or acl^{eq} to stress that we work in $\mathcal{U}^{eq}$.

Galois Characterisation of Algebraic Elements

Fact

Let $\mathrm{Aut}_B(\mathcal{U}) = \{\sigma \in \mathrm{Aut}(\mathcal{U}) \mid \sigma(b) = b \ \forall\, b \in B\}$.

1. $a \in \mathrm{dcl}(B)$ *if and only if* $\sigma(a) = a$ *for all* $\sigma \in \mathrm{Aut}_B(\mathcal{U})$
2. $a \in \mathrm{acl}(B)$ *if and only if there is a* **finite set** A_0 *containing* a *which is* **fixed set-wise** *by every* $\sigma \in \mathrm{Aut}_B(\mathcal{U})$.

Existence of codes for definable sets in $\mathcal{U}^{eq}$

Fact

For any definable set $D \subseteq \mathcal{U}^n$ there exists $c \in \mathcal{U}^{eq}$ (unique up to interdefinability) such that $\sigma \in \mathrm{Aut}(\mathcal{U})$ fixes D setwise if and only if it fixes c.

Proof.

Suppose D is defined by $\varphi(\overline{x}, \overline{d})$. Define the equivalence relation $E(\overline{z}, \overline{z}')$ as

$$\forall \overline{x}(\varphi(\overline{x}, \overline{z}) \Leftrightarrow \varphi(\overline{x}, \overline{z}')).$$

Then $c := \overline{d}/E$ serves as a code for D. □

The Galois Group

- Any $\sigma \in \mathrm{Aut}_B(\mathcal{U})$ fixes $\mathrm{acl}^{eq}(B)$ setwise.
- Define the **Galois group** of B as

$$\mathrm{Gal}(B) := \{\sigma\restriction_{\mathrm{acl}^{eq}(B)} \mid \sigma \in \mathrm{Aut}_B(\mathcal{U})\}.$$

Example

- Let $b_1 \neq b_2$ be in an **infinite set without structure**, $b := (b_1, b_2)/E_2$ (think of b as $\{b_1, b_2\}$) and $B = \{b\}$. Then $b_i \in \mathrm{acl}^{eq}(B)$ and $\mathrm{Gal}(B) = \{\mathrm{id}, \sigma\} \simeq \mathbb{Z}/2$, where σ permutes b_1 and b_2.
- Let $M \models$ **ACF** $= T$ and $K \subseteq M$ a subfield. Then $\mathrm{Gal}(K) = \mathrm{Gal}(K^{alg}/K)$, where
  - K^{alg} = (field theoretic) algebraic closure of K,
  - $\mathrm{Gal}(K^{alg}/K)$ = (field theoretic) Galois group of K.

Galois Correspondence in T^{eq}

$\mathrm{Gal}(B)$ is a **profinite group**: a clopen subgroup is given by

$$\{\sigma \mid \sigma(a_i) = a_i \forall i\}$$

for some finite subset $\{a_1, \ldots, a_n\}$ of $\mathrm{acl}^{eq}(B)$.

Theorem (Poizat)

There is a 1:1 correspondence between

- **closed subgroups** *of* $\mathrm{Gal}(B)$ *and*
- dcl^{eq}**-closed sets** A *with* $B \subseteq A \subseteq \mathrm{acl}^{eq}(B)$.

It is given by

$$H \mapsto \{a \in \mathrm{acl}^{eq}(B) \mid h(a) = a \;\forall\, h \in H\}.$$

Elimination of Imaginaries

Definition

The theory T **eliminates imaginaries** if every imaginary element $a \in \mathcal{U}^{eq}$ is interdefinable with a real tuple $\overline{b} \in \mathcal{U}^n$.

Fact

- *Suppose that for every $\emptyset$-definable equivalence relation E on $\mathcal{U}^n$ there is an $\emptyset$-definable function*

  $$f : \mathcal{U}^n \to \mathcal{U}^m \text{ (for some } m \in \mathbb{N}\text{)}$$

  such that $\overline{a} E \overline{a}'$ if and only if $f(\overline{a}) = f(\overline{a}')$.

  Then T eliminates imaginaries.
- *The converse is (almost) true.*

Examples of theories which eliminate imaginaries

Example

- The theory T^{eq} eliminates imaginaries. (By construction.)
- The theory of an infinite set does not eliminate imaginaries. (The two element set $\{a, b\}$ cannot be coded.)
- $Th(\langle \mathbb{N}, +, \times \rangle)$ eliminates imaginaries.
- **Algebraically closed fields** eliminate imaginaries (Poizat).
- Many other theories of fields eliminate imaginaries.

Illustration: how to **code finite sets** in fields?

Use **symmetric functions**: $D = \{a, b\}$ is coded by the tuple $(a + b, ab)$, as a and b are the roots of $X^2 - (a + b)X + ab$.

Utility of Elimination of Imaginaries

T has **e.i.** $\Rightarrow$ many constructions may be done in T:

- **quotient objects** are present in $\mathcal{U}$;
- **codes** for definable sets exist in $\mathcal{U}$;
- get a **Galois correspondence in** T (replacing dcl^{eq}, acl^{eq} by dcl and acl, respectively);
- may replace T^{eq} by T in the **group constructions** we will present in the next section.

Main Theorem of Galois Theory

Corollary

Let K be a (perfect) field and $\mathrm{Gal}(K^{alg}/K)$ its Galois group. Then the map

$$H \mapsto \{a \in K^{alg} \mid h(a) = a \; \forall \, h \in H\}$$

is a 1:1 correspondence between the set of **closed subgroups** *of $\mathrm{Gal}(K)$ and the set of* **intermediate fields** $K \subseteq L \subseteq K^{alg}$.

Uncountably Categorical Theories

Definition

Let κ be a cardinal. A theory T is κ-**categorical** if, up to isomorphism, T has only one model of cardinality κ.

Theorem (Morley's Categoricity Theorem)

If T is κ-categorical for some uncoutable cardinal κ, then it is λ-categorical for all uncountable λ.

This result marks the beginning of modern model theory!

Strongly Minimal Theories

Definition

- A definable set D is **strongly minimal** if for every definable subset $X \subseteq D$ either X or $D \setminus X$ is finite.
- A theory T is **strongly minimal** if $x = x$ defines a strongly minimal set.

Example (strongly minimal theories)

1. Infinite sets without structure.
2. Infinite vector spaces over some fixed field K.
3. Algebraically closed fields.

Relation to Uncountable Categoricity

Fact

1. *Strongly minimal theories are uncountably categorical.*
2. *Let T be an uncountably categorical theory. Then there is a strongly minimal set D definable in T such that T is largely controlled by D.*

Linear dependence in vector spaces

- V a vector space over the field K
- For $A \subseteq V$ consider the **linear span**

$$Span(A) = \left\{ \sum_{i=1}^{n} k_i \cdot a_i \mid k_i \in K,\ a_i \in A \right\}$$

- $X \subseteq V$ is **linearly independent** if $x \notin Span(X \setminus \{x\})$ for all $x \in X$
- X is a **basis** if it is maximal indep. ($\Leftrightarrow$ minimal generating)
- The **dimension of** V is the cardinality of a basis of V (well-defined)

acl-dependence in strongly minimal sets

Fact

Infinite vector spaces are strongly minimal, with $\mathrm{acl}(A) = Span(A)$*.*

In any strongly minimal theory, we get

- a **dependence relation** (and a combinatorial geometry), using acl instead of *Span*;
- corresponding notions of **basis** and **dimension**.

Geometries in strongly minimal theories

1. **Infinite set** without structure, has a **trivial** geometry, i.e. pairwise independence ⇒ independence.

2. a **Vector spaces**, are **modular**:
   acl-closed sets A, B are independent over $A \cap B$, i.e.

   $$\dim(A \cup B) = \dim(A) + \dim(B) - \dim(A \cap B).$$

   (The associated geometry is **projective geometry**.)

   b **Affine spaces**, are **locally modular**, i.e.
   become modular after naming some constant.

3. **Algebraically closed fields**, are **non-locally modular**.

Zilber's Trichotomy Conjecture

Guiding principle of geometric stability theory

Geometric complexity comes from algebraic structures (e.g. infinite groups or fields) definable in the theory.

Conjecture (Zilber)

Let T be strongly minimal. Then there are three cases:

1. *T has a* **trivial geometry**.
   (This implies: $\nexists$ infinite definable groups in T^{eq}.)
2. *T is* **locally modular non-trivial**. *Then a s.m. group is definable in T^{eq}, and its geometry is projective or affine.*
3. *If T is* **not locally modular**, *an ACF is definable in T^{eq}.*

Results on the Trichotomy Conjecture

1. True for T is **totally categorical**. (Zilber, late 70's)
2. True T for **locally modular**. (Hrushovski, late 80's)
3. The conjecture is false in general. (Hrushovski 1988)
4. True for **Zariski geometries**, an important special case. (Hrushovski-Zilber 1993)

Construction of a group

Let a, b be independent elements in a strongly minimal group $(G, \cdot)$ and $c = a \cdot b$. Then

$(*)$ The set $\{a, b, c\}$ is **pairwise independent** and **dependent**.

- If T is non-trivial, adding some constants if necessary, there is a set $\{a, b, c\}$ satisfying $(*)$.
- If T is modular, any $\{a, b, c\}$ satisfying $(*)$ comes from a s.m. group $(G, \cdot)$ in T^{eq}, up to interalgebraicity:
  - There exist $a', b' \in G$ and $c' = a' \cdot b'$ such that
  - a and a' are interalgebraic, similarly b, b' and c, c'.

The Group Configuration in Stable Theories

- **Group configuration**: a configuration of (in-)dependences between tuples in $\mathcal{U}$, more complicated than $(*)$.
- (Hrushovski) Up to interalgebraicity, any group configuration comes from a definable group in $\mathcal{U}^{eq}$.
- This holds in any **stable** theory; it is a **key device** in Geometric Stability Theory.
- **Source of many applications** of model theory to other branches of mathematics.

Stable theories

- **Uncountably categorical** theories are **stable**.
- Stable theories carry a **nice notion of independence** (generalising acl-independence in s.m. theories).
- Stable = "no infinite set is ordered by a formula"
- The theory of any **module** is **stable**.
- The theory of $\langle \mathbb{N}, + \rangle$ is **unstable** ($x \leq y$ is defined by $\exists z\, x + z = y$).

Modularity in Stable Theories

Definition

T stable is called **modular**^{eq} if any acl^{eq}-closed subsets A, B of $\mathcal{U}^{eq}$ are independent over their intersection $A \cap B$.

This is the **right notion of modularity**:

Theorem

Let T be stable and modular^{eq}.

- *Non-trivial dependence $\Rightarrow \exists$ infinite def. group in T^{eq}.*
- *Def. groups in T^{eq} are* **module-like** *(Hrushovski-Pillay).*

Local modularity equals modularity^{eq}

- For T strongly minimal: **locally modular** $\Leftrightarrow$ **modular^{eq}**.

Example (Affine Space)

Let L_1, L_2 be distinct parallel lines. Put $L_i^{eq} = \mathrm{acl}^{eq}(L_i)$. Then

- $L_1 \cap L_2 = \emptyset$ and there exists a vector $0 \neq v \in L_1^{eq} \cap L_2^{eq}$
- $\dim(L_1 \cup L_2) < \dim(L_1) + \dim(L_2) - \dim(L_1 \cap L_2)$,
  car 3<2+2-0
  ($\Rightarrow$ non-modularity)
- $\dim(L_1^{eq} \cup L_2^{eq}) = \dim(L_1^{eq}) + \dim(L_2^{eq}) - \dim(L_1^{eq} \cap L_2^{eq})$,
  car $3 = 2 + 2 - 1$
  ($\Rightarrow$ modularity^{eq})

The notion of a hyperimaginary

Definition

- An equivalence relation $E(x, y)$ (where x, y are tuples of the same length) is said to be **type-definable** if

$$xEy \Leftrightarrow \bigwedge_{i \in \mathbb{N}} \varphi_i(x, y)$$

  for some sequence of $\mathcal{L}$-formulas $(\varphi_i)_{i \in \mathbb{N}}$.
- A **hyperimaginary element** is an equivalence class a/E, for some type-definable equivalence relation E.

An example: monads

Example

- $\mathcal{R} = \langle \mathbb{R}, +, \times, 0, 1, < \rangle$ (the **ordered field of the reals**)
- $D = S^1 = \{(x_1, x_2) \mid x_1^2 + x_2^2 = 1\}$ (the **unit cercle**)
- S^1, together with complex multiplication (adding angles) is a definable group in $\mathcal{R}$.
- $xEy :\Leftrightarrow \bigwedge_{n \in \mathbb{N}} \mathrm{dist}(x, y) < \frac{1}{n}$ is **type-definable**.
- In $\mathcal{R}^* = \langle \mathbb{R}^*, +, \times, 0, 1, < \rangle \succcurlyeq \mathcal{R}$, the equivalence class a^*/E corresponds to the **monad** of $St(a^*)$.
- $\mu := 0/E \leq S^1(\mathbb{R}^*)$ is a **subgroup**, with quotient $S^1(\mathbb{R})$.

Group Configuration in Simple Theories

- **Simple theories** generalise stable theories;
- have a **good independence notion**;
- simple unstable: **random graph**, **pseudofinite fields** (idea: simple = stable + some random noise).

Theorem (Ben Yaacov–Tomašić–Wagner 2004)

- *The group configuration theorem holds in simple theories.*
- *The corresponding group may be found in (almost) hyperimaginaries.*

Intrinsic Infinitesimals

The example S^1 is not an accident... Indeed

Theorem (2006, involves many people)

Let G be a definable compact group in $\mathcal{R}^* \succcurlyeq \mathcal{R}$ (or more generally in an o-minimal expansion of $\mathcal{R}^*$).

1. *There is a* **type-definable subgroup** $\mu \leq G$ $\Rightarrow$ *cosets $g \cdot \mu$ are hyperimaginaries.*
2. *The group $(G/\mu)(\mathbb{R}^*)$ is isomorphic to a group over the standard real numbers $\mathbb{R}$ and shares many properties with G (e.g. has the same dimension).*
3. *μ gives rise to an* **intrinsic notion of monad**.

Losing Compactness on Hyperimaginary Sorts

One would like to **add sorts for hyperimaginaries** to $\mathcal{L}$.

Example (back to the unit circle)

- S^1 in $\mathcal{R}$, with $xEy \Leftrightarrow \bigwedge_{n\in\mathbb{N}} \text{dist}(x,y) < \frac{1}{n}$;
- S^1/E is **infinite**, but **bounded**, since it does not grow in elementary extensions $\mathcal{R}^* \succcurlyeq \mathcal{R}$;
- $\Rightarrow$ Compactness is violated if a sort for S^1/E is added in first order logic:

$$\{x/E \neq a/E \mid a \in \mathrm{S}^1(\mathbb{R})\}$$

is finitely satisfiabe but unsatisfiable.

Adding Hyperimaginary Sorts in Positive Logic

In fact, **negation is the only obstacle**:

Theorem (Ben Yaacov)

One may add sorts for hyperimaginaries in positive logic without losing compactness.

- This is similar to Shelah's $\mathcal{M}^{eq}$-construction.
- On a hyperimaginary sort D/E, add predicates for any subset $X \subseteq D/E$ such that

$$\pi^{-1}(X) = \{d \in D \mid d/E \in X\}$$

is type-definable without parameters.

Where to look

Imaginaries are needed in order to

1. **understand independence, modularity** etc.;
2. **get a decent Galois correspondence**;
3. **find algebraic structures** like infinite groups or fields, explaining a complicated geometric behaviour.

$\Rightarrow$ Need to **classify imaginaries** to fully understand T.

Beyond (ordinary) imaginaries

In **more general contexts** one might have to

1. go even **beyond imaginaries**;
2. consider **hyperimaginaries** or more complicated objects;
3. adapt the logical framework ($\Rightarrow$ **positive logic**).

Important left outs

1. The use of imaginaries to **analyse types** (or groups) by **breaking them down** into **irreducible** ones (e.g. rank 1).
2. **Groupoid imaginaries**.
3. The recent **classification of imaginaries in algebraically closed valued fields** (Haskell–Hrushovski–Macpherson).