Tarski problems for associative algebras and group rings

Olga Kharlampovich
(based on joint results with A. Miasnikov)

Diableretes, 2016

Tarski's type problems for a given group or algebra G:

- First-order classification: Describe groups (algebras) H such that $Th(G) = Th(H)$.
- Decidability: Is the theory $Th(G)$ decidable?

General intuition:

The situation in "free-like" associative algebras is very different from the one in "free-like" groups (free or torsion-free hyperbolic) groups.

In free-like groups there is more geometry and topology, more about equations and their solutions,

In free-like associative algebras and group rings it is more about algebra, arithmetic, about describing (interpreting) some classical commutative objects sitting in algebras.

Let F be a field, X a set of variables, and $F[X]$ a ring of commutative polynomials in variables X with coefficients in F.

The following formula defines F in $F[X]$:

$$\phi(x) = (x = 0) \vee \exists y(xy = 1)$$

The operations $+$ and $\cdot$ in F are the restrictions of the ones from $F[X]$, so they are also definable in $F[X]$ by formulas.

The field F is definable in the ring $F[X]$.
Notice, that all the formulas that define F in $F[X]$ do not depend on F or X. F is definable uniformly in F and X.

Since F is definable in $F[X]$ for every first-order sentence ϕ of fields one can effectively construct a sentence ϕ^* of rings such that

$$F \models \phi \Longleftrightarrow F[X] \models \phi^*.$$

Implications:

- If $Th(F)$ is undecidable then $Th(F[X])$ is undecidable;
- for any fields F and K

$$F[X] \equiv K[Y] \Longrightarrow F \equiv K$$

Important consequences

Since F is definable in $F[X]$ for every first-order sentence ϕ of fields one can effectively construct a sentence ϕ^* of rings such that

$$F \models \phi \Longleftrightarrow F[X] \models \phi^*.$$

Implications:

- If $Th(F)$ is undecidable then $Th(F[X])$ is undecidable;
- for any fields F and K

$$F[X] \equiv K[Y] \Longrightarrow F \equiv K$$

More generally:
Let $\mathbb{B} = \langle B; L(\mathbb{B})\rangle$ be a structure.

An operation f or a predicate P on a subset $A \subseteq B^n$ is definable in $\mathbb{B}$ if its graph is definable in $\mathbb{B}$.

Definition

An algebraic structure $\mathbb{A} = \langle A; f, \ldots, P, \ldots, c, \ldots\rangle$ is definable in $\mathbb{B}$ if there is a definable subset $A^* \subseteq B^n$ and operations $f^*, \ldots,$ predicates $P^*, \ldots,$ and constants $c^*, \ldots,$ all definable in $\mathbb{B}$ such that the structure $\mathbb{A}^* = \langle A^*; f^*, \ldots, P^*, \ldots, c^*, \ldots, \rangle$ is isomorphic to $\mathbb{A}$.

For example, if Z is the center of a group G then it is definable as a group in G, the same for the center of a ring.

Let $\sim$ be a definable equivalence relation on the definable subset $A \subseteq B^n$. Then the quotient set $A^* = A/\sim$ is *interpretable* in $\mathbb{B}$.

An operation f or a predicate P on the quotient set A^* is interpretable in $\mathbb{B}$ if the full preimage of its graph in A is definable in $\mathbb{B}$.

For example, if N is a normal definable subgroup of a group G, then the equivalence relation $x \sim y$ on G given by $xN = yN$ is definable in G, so the quotient set G/N of all right cosets of N is interpretable in G.

It is easy to see that the multiplication induced from G on G/N is also interpretable in G. This show that the quotient group G/N is interpretable in G.

Interpretability

Let $\sim$ be a definable equivalence relation on the definable subset $A \subseteq B^n$. Then the quotient set $A^* = A/\sim$ is *interpretable* in $\mathbb{B}$.

An operation f or a predicate P on the quotient set A^* is interpretable in $\mathbb{B}$ if the full preimage of its graph in A is definable in $\mathbb{B}$.

For example, if N is a normal definable subgroup of a group G, then the equivalence relation $x \sim y$ on G given by $xN = yN$ is definable in G, so the quotient set G/N of all right cosets of N is interpretable in G.

It is easy to see that the multiplication induced from G on G/N is also interpretable in G. This show that the quotient group G/N is interpretable in G.

Interpretability

Definition

An algebraic structure $\mathbb{A} = \langle A; f, \ldots, P, \ldots, c, \ldots \rangle$ is interpretable in a structure $\mathbb{B}$ if there is a subset $A^* \subseteq B^n$ definable in $\mathbb{B}$, an equivalence relation $\sim$ on A^* definable in $\mathbb{B}$, operations $f^*, \ldots,$ predicates $P^*, \ldots,$ and constants $c^*, \ldots,$ on the quotient set $A^*/\sim$ all interpretable in $\mathbb{B}$ such that the structure $\mathbb{A}^* = \langle A^*/\sim; f^*, \ldots, P^*, \ldots, c^*, \ldots, \rangle$ is isomorphic to $\mathbb{A}$.

Interpretation is uniformly in a class of structures C if the defining formulas are the same for every structure B from C.

Interpretability

Definition

An algebraic structure $\mathbb{A} = \langle A; f, \ldots, P, \ldots, c, \ldots \rangle$ is interpretable in a structure $\mathbb{B}$ if there is a subset $A^* \subseteq B^n$ definable in $\mathbb{B}$, an equivalence relation $\sim$ on A^* definable in $\mathbb{B}$, operations $f^*, \ldots,$ predicates $P^*, \ldots,$ and constants $c^*, \ldots,$ on the quotient set $A^*/\sim$ all interpretable in $\mathbb{B}$ such that the structure $\mathbb{A}^* = \langle A^*/\sim; f^*, \ldots, P^*, \ldots, c^*, \ldots, \rangle$ is isomorphic to $\mathbb{A}$.

Interpretation is uniformly in a class of structures C if the defining formulas are the same for every structure B from C.

Theorem

Let F be an arbitrary field and X an arbitrary non-empty set. Then the following hold:

1) For any irreducible polynomial $a \in F[X]$ the arithmetic $\mathbb{N} = \langle N; +, \cdot, 0, 1 \rangle$ is interpretable with the parameter a in $F[X]$ uniformly in F, X, and a (i.e., the interpretation formulas are the same for all fields F, sets X, and irreducible polynomials a). We denote this interpretation by $\mathbb{N}_a$.
2) For any irreducible polynomials $a, b \in F[X]$ the canonical (unique) isomorphism of interpretations $\mathbb{N}_a \to \mathbb{N}_b$ is definable in $F[X]$ uniformly in F, X, and a, b.
3) The arithmetic $\mathbb{N}$ is 0-interpretable in $F[X]$.

Let $a \in F[X]$ be irreducible. Then the formula

$$\forall u (u \mid x \to (u \in F \vee a \mid u))$$

defines in $F[X]$ a set $\{\alpha a^n \mid \alpha \in F, n \in \mathbb{N}\}$.
A formula

$$a - 1 \mid x - 1$$

defines in this set the subset

$$N_a = \{a^n \mid n \in \mathbb{N}\}.$$

For any $n, m, k \in \mathbb{N}$ one has

$$n + m = k \iff a^n \cdot a^m = a^k,$$

$$n \mid m \iff (a^n - 1) \mid (a^m - 1).$$

which defines addition and division (hence multiplication) on $\mathbb{N}_a \simeq \mathbb{N}$.

Important implications

If A is interpretable in B then for every first-order sentence ϕ in the language of A one can effectively construct a sentence ϕ^* in the language of B such that

$$A \models \phi \Longleftrightarrow B \models \phi^*.$$

Undecidability of $Th(F[X])$

Since the arithmetic $\mathbb{N}$ is interpretable in $F[X]$ and $Th(\mathbb{N})$ is undecidable the following result holds.

Theorem [Robinson, ...]

For any field F the elementary theory of $F[X]$ is undecidable.

This is typical use of interpretability.

It solves the Tarski's problem on decidability of the theory for polynomial rings $F[X]$.

Theorem [Denef]

For any field F of zero characteristic, the Diophantine problem for $F[X]$ is undecidable.

Theorem

$$F[X] \equiv K[Y] \Longrightarrow |X| = |Y| \text{ and } F \equiv K.$$

Sketch of the proof: If $F[X] \equiv K[Y]$, then they have the same Krull dimension, hence $|Y| = |X|$.

Since F is definable in $F[X]$ uniformly in F and X it follows that $F \equiv K$.

But the converse is not true! Take as F and K algebraic closures of transcendental extensions of $\mathbb{Q}$ of different finite transcendence degrees. Then $F \equiv K$ but $F[X] \not\equiv K[X]$.

Theorem

$$F[X] \equiv K[Y] \Longrightarrow |X| = |Y| \textit{ and } F \equiv K.$$

Sketch of the proof: If $F[X] \equiv K[Y]$, then they have the same Krull dimension, hence $|Y| = |X|$.

Since F is definable in $F[X]$ uniformly in F and X it follows that $F \equiv K$.

But the converse is not true! Take as F and K algebraic closures of transcendental extensions of $\mathbb{Q}$ of different finite transcendence degrees. Then $F \equiv K$ but $F[X] \not\equiv K[X]$.

Theorem

$$F[X] \equiv K[Y] \Longrightarrow |X| = |Y| \text{ and } F \equiv K.$$

Sketch of the proof: If $F[X] \equiv K[Y]$, then they have the same Krull dimension, hence $|Y| = |X|$.

Since F is definable in $F[X]$ uniformly in F and X it follows that $F \equiv K$.

But the converse is not true! Take as F and K algebraic closures of transcendental extensions of $\mathbb{Q}$ of different finite transcendence degrees. Then $F \equiv K$ but $F[X] \not\equiv K[X]$.

For a set A let $Pf(A)$ be the set of all finite subsets of A.

Definition of hereditary finite sets over A

- $HF_0(A) = A$,
- $HF_{n+1}(A) = HF_n(A) \cup Pf(HF_n(A))$,
- $HF(A) = \bigcup_{n \in \omega} HF_n(A)$.

For a ring $R = (A; +, \times, 0, 1)$ define a new structure

$$HF(R) = \langle HF(A); P_A, +, \times, 0, 1, \in \rangle,$$

where P_A is the predicate defining A in $HF(A)$, $+, \times, 0, 1$ are defined on A as before and $\in$ is the membership predicate on $HF(A)$.

For a set A let $Pf(A)$ be the set of all finite subsets of A.

Definition of hereditary finite sets over A

- $HF_0(A) = A$,
- $HF_{n+1}(A) = HF_n(A) \cup Pf(HF_n(A))$,
- $HF(A) = \bigcup_{n\in\omega} HF_n(A)$.

For a ring $R = (A; +, \times, 0, 1)$ define a new structure

$$HF(R) = \langle HF(A); P_A, +, \times, 0, 1, \in \rangle,$$

where P_A is the predicate defining A in $HF(A)$, $+, \times, 0, 1$ are defined on A as before and $\in$ is the membership predicate on $HF(A)$.

The main point:

The first-order theory of $HF(R)$ has the same expressiveness as the *weak second order theory* of R.

For example: one can use arithmetic in $HF(R)$, finite sequences of of elements from R, define the lengths of the sequences by formulas, take their components, concatenations, etc. - extremely powerful language.

Theorem (Bauval)

Rings of polynomials of finite number of variables over infinite fields $F[X]$ and $K[Y]$ are elementarily equivalent if and only if $|X| = |Y|$ and $HF(F) \equiv HF(K)$.

Corollary

If F and K are computable (for instance, $\mathbb{Q}$, and f.g. extensions of $\mathbb{Q}$, or algebraic closure of $\mathbb{Q}$), then the polynomial rings $F[X]$ and $K[Y]$ are elementarily equivalent iff they are isomorphic.

Theorem (Bauval)

Rings of polynomials of finite number of variables over infinite fields $F[X]$ and $K[Y]$ are elementarily equivalent if and only if $|X| = |Y|$ and $HF(F) \equiv HF(K)$.

Corollary

If F and K are computable (for instance, $\mathbb{Q}$, and f.g. extensions of $\mathbb{Q}$, or algebraic closure of $\mathbb{Q}$), then the polynomial rings $F[X]$ and $K[Y]$ are elementarily equivalent iff they are isomorphic.

By Bauval's theorem the model $HF(F)$ of hereditary finite sets over F is uniformly definable in the ring $F[x]$.
Hence $F[X] \equiv K[Y] \implies HF(F) \equiv HF(K)$, and

$$HF(F) \equiv HF(K) \iff F \equiv_{w.s.o.l.} K.$$

Conversely, we can enumerate all the monomials in $F[X]$ and represent each element in $F[X]$ as a finite set of coefficients in F. Multiplication in $F[X]$ is interpretable in the weak second order logic of F. Therefore the theory of $F[X]$ is interpretable in the weak second order theory of F uniformly on $F[X]$.

Theorem (Bauval)

A noetherian ring R is first-order equivalent to $F[X]$ if and only if it is isomorphic to a polynomial ring $K[Y]$ where $|X| = |Y|$ and $HF(F) \equiv HF(K)$.

In applications it is convenient to use the list superstructure of $\mathbb{A}$:

$$S(\mathbb{A},\mathbb{N}) = \langle \mathbb{A}, S(A), \mathbb{N}; t(s,i), l(s), \frown, \rangle,$$

where

- $S(A) =$ all finite sequences of elements from A.
- $\frown$ is the operation of concatenation of two sequences
- $\mathbb{N} = \langle N \mid +, \cdot, 0, 1\rangle$ is the standard arithmetic,
- $l : S(A) \to N$ is the length function on sequences
- $t : S(A) \times \mathbb{N} \to A$ is the coordinate function: $t(s,i)$ is the i's component of s.

Fact: $HF(\mathbb{A})$ and $S(\mathbb{A},\mathbb{N})$ are bi-interpretable in one another.

The weak second-order theory

In applications it is convenient to use the list superstructure of $\mathbb{A}$:

$$S(\mathbb{A},\mathbb{N}) = \langle \mathbb{A}, S(A), \mathbb{N}; t(s,i), l(s), \frown, \rangle,$$

where

- $S(A)$ = all finite sequences of elements from A.
- $\frown$ is the operation of concatenation of two sequences
- $\mathbb{N} = \langle N \mid +, \cdot, 0, 1\rangle$ is the standard arithmetic,
- $l : S(A) \to N$ is the length function on sequences
- $t : S(A) \times \mathbb{N} \to A$ is the coordinate function: $t(s,i)$ is the i's component of s.

Fact: $HF(\mathbb{A})$ and $S(\mathbb{A},\mathbb{N})$ are bi-interpretable in one another.

Theorem

Let F be an infinite field and X an arbitrary non-empty set. Then the following hold:

1) *for a given non-invertible polynomial $P \in F[X]$ one can interpret $S(F,\mathbb{N})$ in $F[X]$ using the parameter P uniformly in F, X, and P.*
2) *for any non-invertible polynomials $P, Q \in F[X]$ the canonical (unique) isomorphism of the interpretations above $S(F,\mathbb{N})_P \to S(F,\mathbb{N})_Q$ is definable in $F[X]$ uniformly in F, X, P, and Q.*

Interpretation of $S(F,\mathbb{N})$ in $F[t]$

$$(\alpha_0,\ldots,\alpha_n) \Longleftrightarrow (\alpha_0+\alpha_1 t+\ldots+\alpha_n t^n, t^n)$$

.

Definability of such pairs:

$$degf(t) \leq n \Longleftrightarrow t^n f(\frac{1}{t}) \in F[t]$$

.

Hence the formula: $\phi(f,t,t^n) =$

$$\exists g \forall \alpha \in F^* \exists \beta,\gamma \in F \Big(t - \frac{1}{\alpha} \mid f-\beta \wedge t-\alpha \mid t^n - \gamma \wedge t-\alpha \mid g - \beta\gamma \Big).$$

Denote by $\mathbb{A} = \mathbb{A}_F(X)$ a free associative unital algebra over a field F with basis X.

Approach to Tarski's problems for $\mathbb{A}_F(X)$:

Do the same as for commutative polynomials

Definability of $F[t]$

Theorem [Bergman]

The centralizer in $\mathbb{A}_F(X)$ of a non-scalar polynomial is isomorphic to $F[t]$.

Corollary

The ring $F[t]$ is definable in $\mathbb{A}_F(X)$ uniformly in F and X.

Decidability

Theorem

The first-order theory of $\mathbb{A}_F(X)$ is undecidable for any F and X.

First-order classification

Theorem

Free associative algebras $\mathbb{A}_{F_1}(X)$ and $\mathbb{A}_{F_2}(Y)$ of finite rank over infinite fields F_1, F_2 are elementarily equivalent if and only if their ranks are the same and $HF(F_1) \equiv HF(F_2)$.

This implies the answer to B. Plotkin's question showing that the variety of associative algebras is logically perfect, i.e. if a f.g. algebra is isotypic to a free algebra over the same field, then they are isomorphic.

Corollary

If F_1 and F_2 are computable (for instance, $\mathbb{Q}$, and f.g. extensions of $\mathbb{Q}$, or algebraic closure of $\mathbb{Q}$), then the algebras $\mathbb{A}_{F_1}(X)$ and $\mathbb{A}_{F_2}(Y)$ are elementarily equivalent iff they are isomorphic.

Bi-interpretability

Theorem

$S(K, \mathbb{N})$ and $\mathbb{A}_K(X)$ are bi-interpretable, $HF(K)$ and $\mathbb{A}_K(X)$ are bi-interpretable.

Theorem

The set of all free bases of $\mathbb{A}_K(X)$ is 0-definable in $\mathbb{A}_K(X)$.

Theorem

There is no quantifire elimination in the theory of $\mathbb{A}_F(X)$.

Theorem

Let $\mathbb{A}_F(X)$ be a free associative algebra of finite rank over an infinite field F. Assume that B is an arbitrary ring with at least one Noetherian centralizer. Then $\mathbb{A}_F(X) \equiv B$ if and only if $B \simeq \mathbb{A}_K(Y)$ where K is a field such that $HF(F) \equiv HF(K)$ and $|X| = |Y|$.

Theorem

Let K be an infinite field and X an arbitrary non-empty set. Then for any non-invertible polynomials $P, Q \in \mathbb{A}_K(X)$ the canonical isomorphism of the centralizers $C_{\mathbb{A}}(P) \to C_{\mathbb{A}}(Q)$ is definable in $\mathbb{A}_K(X)$ uniformly in K, X, P and Q.

Non-unitary free associative algebras

Let $\mathbb{A}_F^0(X)$ be a free associative algebra with basis X without unity (non-commutative monomials on X without constant terms).

Main Problem: there is no subfield F in $\mathbb{A}_F^0(X)$!

Non-unitary free associative algebras

Theorem

The field F and its action on $\mathbb{A}_F^0(X)$ are interpretable in $\mathbb{A}_F^0(X)$ uniformly in F.

Corollary

Algebra $\mathbb{A}_F(X)$ is definable in $\mathbb{A}_F^0(X)$.

Indeed, $\mathbb{A}_F(X) = 1 \cdot F \oplus \mathbb{A}_F^0(X)$.

Theorem

Free associative algebras $\mathbb{A}_{F_1}^0(X)$ and $\mathbb{A}_{F_2}^0(Y)$ of finite rank over infinite fields F_1, F_2 are elementarily equivalent if and only if their ranks are the same and $HF(F_1) \equiv HF(F_2)$.

Theorem

The field F and its action on $\mathbb{A}_F^0(X)$ are interpretable in $\mathbb{A}_F^0(X)$ uniformly in F.

Corollary

Algebra $\mathbb{A}_F(X)$ is definable in $\mathbb{A}_F^0(X)$.

Indeed, $\mathbb{A}_F(X) = 1 \cdot F \oplus \mathbb{A}_F^0(X)$.

Theorem

Free associative algebras $\mathbb{A}_{F_1}^0(X)$ and $\mathbb{A}_{F_2}^0(Y)$ of finite rank over infinite fields F_1, F_2 are elementarily equivalent if and only if their ranks are the same and $HF(F_1) \equiv HF(F_2)$.

A group G is called Left Orderable (LO) if there is a linear ordering on G which respects left multiplication in G.

Free groups, special groups, etc., are LO.

It is not known if every torsion-free hyperbolic group is LO or not.

Fact

Every LO group satisfies the Kaplansky unit conjecture, i.e., the group of units in the group algebra $K(G)$ is precisely $K \cdot G$.

Corollary

If G is LO then G is definable in $K(G)$.

Centralizers

Let G be a commutative transitive and torsion free group and $g \in G$ such that $C_G(g) = \mathbb{Z}^n$. Then $C_{K(G)}(g) = K(\mathbb{Z}^n) = K[t_1, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1}]$.

Corollary

If G is torsion-free hyperbolic, then for any $g \in G$ the centralizer $C_{K(G)}(x) = K[t, t^{-1}]$ is the ring of Laurent polynomials in one variable.

Centralizers

Let G be a commutative transitive and torsion free group and $g \in G$ such that $C_G(g) = \mathbb{Z}^n$. Then $C_{K(G)}(g) = K(\mathbb{Z}^n) = K[t_1, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1}]$.

Corollary

If G is torsion-free hyperbolic, then for any $g \in G$ the centralizer $C_{K(G)}(x) = K[t, t^{-1}]$ is the ring of Laurent polynomials in one variable.

Theorem

The following holds for every ring of Laurent polynomials $K[x, x^{-1}]$ over a field K of characteristic 0:

- The arithmetic $\mathbb{N} = \langle N \mid +, \cdot, 0, 1 \rangle$ is interpretable in $K[x, x^{-1}]$ uniformly in K.
- $HF(K)$ is interpretable in $K[x, x^{-1}]$ uniformly in K.

Theorem

Let G be torsion free hyperbolic or toral relatively hyperbolic and K be an infinite field, then $Th(K(G))$ is undecidable.

Left orderable groups

Theorem

Let G, H be groups and K, L fields such that $K(G) \equiv L(H)$. If G is LO then the following hold:

1) *H is LO.*
2) *$K \equiv L$ and $G \equiv H$.*

Theorem

Let G be LO and hyperbolic and H a group such that there is an element in H with a finitely generated centralizer. Then for any fields K and L, if $K(G) \equiv L(H)$ then

- $G \equiv H$
- $HF(K) \equiv HF(L)$.

Algebras over free groups

Theorem

Let F be a finitely generated free group and K an infinite field. Let H be a group such that there is an element in H with finitely generated centralizer and L be a field. Then $K(F) \equiv L(H)$ if and only if

- *H is isomorphic to F,*
- *$HF(K) \equiv HF(L)$.*

Theorem

Let F be a finitely generated free group and K an infinite field. Let B be a ring that has an invertible element x with finitely generated centralizer, such that $x+1$ is not invertible. If $K(F) \equiv B$ then

- *B is isomorphic to a group algebra $L(H)$,*
- *H is isomorphic to F,*
- *$HF(K) \equiv HF(L)$.*

Theorem

Let K be an infinite field and F_n a free non-abelian group of rank n. Then:

- $Th(K(F_n))$ *is undecidable.*
- $K(F_n) \not\equiv K(F_m)$ *for* $n \neq m$.

Theorem

The set of all free bases of F is 0-definable in $K(F)$.

Let $L_F(X)$ be a free Lie algebra with basis X with coefficients in F.

Theorem

The field F and its action on $L_F(X)$ are definable in $L_F(X)$ uniformly in F.

Corollary

The theory of $L_F(X)$ over $\mathbb{Q}$ (any field with undecidable theory) is undecidable.

Theorem

If two free Lie algebras of finite rank over fields are elementarily equivalent, then the ranks are the same and the fields are elementarily equivalent.

Theorem

If a ring B is elementarily equivalent to a free lie algebra $\mathbb{L}_F(X)$ of rank n , then B is a Lie algebra over a field F_1, such that:

- *F_1 is elementarily equivalent to F,*
- *$B/B^n \equiv C_n$, where C_n is a free n-nilpotent Lie algebra with basis X over the field F_1.*

In particular, if B is residually nilpotent, then B is para-free.

Open problems

Problem

- *Describe para-free Lie (associative) algebras which are elementarily equivalent to a free Lie (associative) algebra.*
- *Are free associative or Lie algebras equationally Noetherian?*

Open problems

Problem

- *Describe para-free Lie (associative) algebras which are elementarily equivalent to a free Lie (associative) algebra.*
- *Are free associative or Lie algebras equationally Noetherian?*