Pop's conjecture on the elementary theory of finitely generated fields

Thomas Scanlon

University of California, Berkeley

Paris VII
8 June 2006

Theories of finitely generated fields

Conjecture (Pop)

If K and L are finitely generated fields, then $K \equiv L$ if and only if $K \cong L$.

Theories of finitely generated fields

Conjecture (Pop)

If K and L are finitely generated fields, then $K \equiv L$ if and only if $K \cong L$.

Theorem

If K is a finitely generated field, then there is a sentence ϕ_K in the language of rings for which for any finitely generated field L, $L \models \phi_K$ if and only if $L \cong K$. In particular, Pop's conjecture holds.

Quasifinite axiomatizability

The issues raised by Pop are very close in character to those studied by Khelif, Nies, Oger and Sabbagh around theories of finitely generated groups.

Quasifinite axiomatizability

The issues raised by Pop are very close in character to those studied by Khelif, Nies, Oger and Sabbagh around theories of finitely generated groups.

Definition (Nies)

A finitely generated group is quasiaxiomatizable if it is isomorphic to any elementarily equivalent finitely generated group. It is quasifinitely axiomatizable (QFA) if relative to the class of finitely generated groups its isomorphism class is isolated by a single sentence.

Quasifinite axiomatizability

The issues raised by Pop are very close in character to those studied by Khelif, Nies, Oger and Sabbagh around theories of finitely generated groups.

Definition (Nies)

A finitely generated group is quasiaxiomatizable if it is isomorphic to any elementarily equivalent finitely generated group. It is quasifinitely axiomatizable (QFA) if relative to the class of finitely generated groups its isomorphism class is isolated by a single sentence.

The phrase quasifinitely axiomatizable already appears in Zilber's work on totally categorical structures with a different meaning.

Logic and Pop's conjecture

Most of the work to date on Pop's conjecture has been performed by algebraists and involves converting deep theorems of arithmetic algebraic geometry to a first-order form, but the conjecture visibly concerns logic and methods from logic should be useful.

Logic and Pop's conjecture

Most of the work to date on Pop's conjecture has been performed by algebraists and involves converting deep theorems of arithmetic algebraic geometry to a first-order form, but the conjecture visibly concerns logic and methods from logic should be useful.

Indeed, we resolve the conjecture by showing that every infinite finitely generated field is parametrically biïnterpretable with $\mathbb{Z}$.

Logic and Pop's conjecture

Most of the work to date on Pop's conjecture has been performed by algebraists and involves converting deep theorems of arithmetic algebraic geometry to a first-order form, but the conjecture visibly concerns logic and methods from logic should be useful.

Indeed, we resolve the conjecture by showing that every infinite finitely generated field is parametrically biïnterpretable with $\mathbb{Z}$.

As the corresponding question for groups has been studied by logicians, it should come as no surprise that biïnterpretation with $\mathbb{Z}$ is one of their main tools as well.

Transcendence degree

Theorem (Pop)

If K and L are elementarily equivalent finitely generated fields, then L may be realized as a finite extension of K and vice versa.

Transcendence degree

Theorem (Pop)

If K and L are elementarily equivalent finitely generated fields, then L may be realized as a finite extension of K and vice versa.

Theorem (Poonen)

For each positive integer n there is a formula $\psi_n(x_1, \ldots, x_n)$ in the language of rings such that if K is a finitely generated field and $\mathbf{a} = (a_1, \ldots, a_n) \in K^n$, then $K \models \psi_n(\mathbf{a})$ if and only if $a_1, \ldots, a_n$ are algebraically dependent over the prime field.

From algebraic dependence to Pop's theorem

Pop's theorem follows from Poonen's (and was, in fact, proven using a weaker version of the definability of algebraic dependence).

- Suppose K and L are elementarily equivalent finitely generated fields.
- Find $a_1, \ldots, a_n \in K$ a transcendence basis and $a_{n+1}, \ldots, a_m \in K$ so that K is generated by $a_1, \ldots, a_m$.
- $L \equiv K \models (\exists \mathbf{x}, \mathbf{y}) \neg \psi_n(\mathbf{x}) \& \bigwedge_{i=1}^{\ell} P_i(\mathbf{x}, \mathbf{y}) = 0$ where $\{P \in \mathbb{Z}[X_1, \ldots, X_m] \mid P(a_1, \ldots, a_m) = 0\} = (P_1, \ldots, P_\ell)$.
- Let $b_1, \ldots, b_m$ witness the truth of this sentence in L. Then the association $a_i \mapsto b_i$ defines an embedding of K into L.
- L and K have the same transcendence degree as they both satisfy $(\exists \mathbf{x})(\forall y) \neg \psi_n(\mathbf{x}) \& \psi_{n+1}(\mathbf{x}, y)$. Thus, L is a finite extension of K.

From algebraic dependence to Pop's theorem

Pop's theorem follows from Poonen's (and was, in fact, proven using a weaker version of the definability of algebraic dependence).

- Suppose K and L are elementarily equivalent finitely generated fields.
- Find $a_1, \ldots, a_n \in K$ a transcendence basis and $a_{n+1}, \ldots, a_m \in K$ so that K is generated by $a_1, \ldots, a_m$.
- $L \equiv K \models (\exists \mathbf{x}, \mathbf{y}) \neg \psi_n(\mathbf{x}) \& \bigwedge_{i=1}^{\ell} P_i(\mathbf{x}, \mathbf{y}) = 0$ where $\{P \in \mathbb{Z}[X_1, \ldots, X_m] \mid P(a_1, \ldots, a_m) = 0\} = (P_1, \ldots, P_\ell)$.
- Let $b_1, \ldots, b_m$ witness the truth of this sentence in L. Then the association $a_i \mapsto b_i$ defines an embedding of K into L.
- L and K have the same transcendence degree as they both satisfy $(\exists \mathbf{x})(\forall y) \neg \psi_n(\mathbf{x}) \& \psi_{n+1}(\mathbf{x}, y)$. Thus, L is a finite extension of K.

From algebraic dependence to Pop's theorem

Pop's theorem follows from Poonen's (and was, in fact, proven using a weaker version of the definability of algebraic dependence).

- Suppose K and L are elementarily equivalent finitely generated fields.
- Find $a_1, \ldots, a_n \in K$ a transcendence basis and $a_{n+1}, \ldots, a_m \in K$ so that K is generated by $a_1, \ldots, a_m$.
- $L \equiv K \models (\exists \mathbf{x}, \mathbf{y}) \neg \psi_n(\mathbf{x}) \& \bigwedge_{i=1}^{\ell} P_i(\mathbf{x}, \mathbf{y}) = 0$ where $\{P \in \mathbb{Z}[X_1, \ldots, X_m] \mid P(a_1, \ldots, a_m) = 0\} = (P_1, \ldots, P_\ell)$.
- Let $b_1, \ldots, b_m$ witness the truth of this sentence in L. Then the association $a_i \mapsto b_i$ defines an embedding of K into L.
- L and K have the same transcendence degree as they both satisfy $(\exists \mathbf{x})(\forall y) \neg \psi_n(\mathbf{x}) \& \psi_{n+1}(\mathbf{x}, y)$. Thus, L is a finite extension of K.

From algebraic dependence to Pop's theorem

Pop's theorem follows from Poonen's (and was, in fact, proven using a weaker version of the definability of algebraic dependence).

- Suppose K and L are elementarily equivalent finitely generated fields.
- Find $a_1, \ldots, a_n \in K$ a transcendence basis and $a_{n+1}, \ldots, a_m \in K$ so that K is generated by $a_1, \ldots, a_m$.
- $L \equiv K \models (\exists \mathbf{x}, \mathbf{y}) \neg \psi_n(\mathbf{x}) \& \bigwedge_{i=1}^{\ell} P_i(\mathbf{x}, \mathbf{y}) = 0$ where $\{P \in \mathbb{Z}[X_1, \ldots, X_m] \mid P(a_1, \ldots, a_m) = 0\} = (P_1, \ldots, P_\ell)$.
- Let $b_1, \ldots, b_m$ witness the truth of this sentence in L. Then the association $a_i \mapsto b_i$ defines an embedding of K into L.
- L and K have the same transcendence degree as they both satisfy $(\exists \mathbf{x})(\forall y) \neg \psi_n(\mathbf{x}) \& \psi_{n+1}(\mathbf{x}, y)$. Thus, L is a finite extension of K.

From algebraic dependence to Pop's theorem

Pop's theorem follows from Poonen's (and was, in fact, proven using a weaker version of the definability of algebraic dependence).

- Suppose K and L are elementarily equivalent finitely generated fields.
- Find $a_1, \ldots, a_n \in K$ a transcendence basis and $a_{n+1}, \ldots, a_m \in K$ so that K is generated by $a_1, \ldots, a_m$.
- $L \equiv K \models (\exists \mathbf{x}, \mathbf{y}) \neg \psi_n(\mathbf{x}) \& \bigwedge_{i=1}^{\ell} P_i(\mathbf{x}, \mathbf{y}) = 0$ where $\{P \in \mathbb{Z}[X_1, \ldots, X_m] \mid P(a_1, \ldots, a_m) = 0\} = (P_1, \ldots, P_\ell)$.
- Let $b_1, \ldots, b_m$ witness the truth of this sentence in L. Then the association $a_i \mapsto b_i$ defines an embedding of K into L.
- L and K have the same transcendence degree as they both satisfy $(\exists \mathbf{x})(\forall y) \neg \psi_n(\mathbf{x}) \& \psi_{n+1}(\mathbf{x}, y)$. Thus, L is a finite extension of K.

From algebraic dependence to Pop's theorem

Pop's theorem follows from Poonen's (and was, in fact, proven using a weaker version of the definability of algebraic dependence).

- Suppose K and L are elementarily equivalent finitely generated fields.
- Find $a_1, \ldots, a_n \in K$ a transcendence basis and $a_{n+1}, \ldots, a_m \in K$ so that K is generated by $a_1, \ldots, a_m$.
- $L \equiv K \models (\exists \mathbf{x}, \mathbf{y}) \neg \psi_n(\mathbf{x}) \& \bigwedge_{i=1}^{\ell} P_i(\mathbf{x}, \mathbf{y}) = 0$ where $\{P \in \mathbb{Z}[X_1, \ldots, X_m] \mid P(a_1, \ldots, a_m) = 0\} = (P_1, \ldots, P_\ell)$.
- Let $b_1, \ldots, b_m$ witness the truth of this sentence in L. Then the association $a_i \mapsto b_i$ defines an embedding of K into L.
- L and K have the same transcendence degree as they both satisfy $(\exists \mathbf{x})(\forall y) \neg \psi_n(\mathbf{x}) \& \psi_{n+1}(\mathbf{x}, y)$. Thus, L is a finite extension of K.

Definitions of $\mathbb{Z}$ in global fields

Theorem (J. Robinson)

If K is a number field, then $\mathbb{Z} \subseteq K$ is definable.

Definitions of $\mathbb{Z}$ in global fields

Theorem (J. Robinson)

If K is a number field, then $\mathbb{Z} \subseteq K$ is definable.

Theorem (R. Robinson)

If K is a function field of a curve over a finite field, then $(\mathbb{Z}, +, \times)$ is interpretable in K.

Uniform definitions of $\mathbb{Z}$ in global fields

Rumely proved a uniform version of the Robinsons' theorems.

- There is a sentence ζ in the language of rings for which a global field satisfies ζ if and only if it has characteristic zero.
- There is a formula $\theta(x)$ so that for any number field K, $\mathbb{Z} = \theta(K)$.
- There is a formula $\mu(x, y, z, w)$ so that if K is a global field of positive characteristic and $t \in K$ is nonconstant, then $K \models \mu(x, y, z, t)$ if and only if there are integers m and n for which $x = t^n$, $y = t^m$ and $z = t^{mn}$.

Uniform definitions of $\mathbb{Z}$ in global fields

Rumely proved a uniform version of the Robinsons' theorems.

- There is a sentence ζ in the language of rings for which a global field satisfies ζ if and only if it has characteristic zero.
- There is a formula $\theta(x)$ so that for any number field K, $\mathbb{Z} = \theta(K)$.
- There is a formula $\mu(x, y, z, w)$ so that if K is a global field of positive characteristic and $t \in K$ is nonconstant, then $K \models \mu(x, y, z, t)$ if and only if there are integers m and n for which $x = t^n$, $y = t^m$ and $z = t^{mn}$.

Uniform definitions of $\mathbb{Z}$ in global fields

Rumely proved a uniform version of the Robinsons' theorems.

- There is a sentence ζ in the language of rings for which a global field satisfies ζ if and only if it has characteristic zero.
- There is a formula $\theta(x)$ so that for any number field K, $\mathbb{Z} = \theta(K)$.
- There is a formula $\mu(x, y, z, w)$ so that if K is a global field of positive characteristic and $t \in K$ is nonconstant, then $K \models \mu(x, y, z, t)$ if and only if there are integers m and n for which $x = t^n$, $y = t^m$ and $z = t^{mn}$.

Uniform definitions of $\mathbb{Z}$ in global fields

Rumely proved a uniform version of the Robinsons' theorems.

- There is a sentence ζ in the language of rings for which a global field satisfies ζ if and only if it has characteristic zero.
- There is a formula $\theta(x)$ so that for any number field K, $\mathbb{Z} = \theta(K)$.
- There is a formula $\mu(x, y, z, w)$ so that if K is a global field of positive characteristic and $t \in K$ is nonconstant, then $K \models \mu(x, y, z, t)$ if and only if there are integers m and n for which $x = t^n$, $y = t^m$ and $z = t^{mn}$.

Uniform interpretations of and in $\mathbb{Z}$

It follows from the theorems of Poonen and Rumely that $\mathbb{Z}$ is uniformly interpreted in the class of infinite finitely generated fields.

Uniform interpretations of and in $\mathbb{Z}$

It follows from the theorems of Poonen and Rumely that $\mathbb{Z}$ is uniformly interpreted in the class of infinite finitely generated fields.

It follows from Gödel coding that the class of infinite finitely generated fields is uniformly interpreted in $\mathbb{Z}$.

Uniform interpretations of and in $\mathbb{Z}$

It follows from the theorems of Poonen and Rumely that $\mathbb{Z}$ is uniformly interpreted in the class of infinite finitely generated fields.

It follows from Gödel coding that the class of infinite finitely generated fields is uniformly interpreted in $\mathbb{Z}$.

Theorem

There are formulas $A(x, y, z, w)$ and $M(x, y, z, w)$ in the language of rings so that for each integer n, $A(\mathbb{Z}, n)$ is the graph of a function $\oplus_n : \mathbb{Z}^2 \to \mathbb{Z}$ and $M(\mathbb{Z}, n)$ is the graph of a function $\otimes_n$ for which $(\mathbb{Z}, \oplus_n, \otimes_n)$ is a finitely generated field. Moreover, for any infinite finitely generated field K there is some integer $[K]$ for which $(\mathbb{Z}, \oplus_{[K]}, \otimes_{[K]}) =: \widetilde{K} \cong K$.

Biïnterpretation with $\mathbb{Z}$

Theorem

If K is an infinite finitely generated field, then K is parametrically biïnterpretable with $\mathbb{Z}$.

- If K is a finitely generated field of characteristic zero and $[K] \in \mathbb{Z}$ is a code for the interpretation of K in $\mathbb{Z}$, then there is a parametrically definable isomorphism between $(K, +, \times)$ and $(\mathbb{Z}, \oplus_{[K]}, \otimes_{[K]})$.
- If K is an infinite finitely generated field of positive characteristic, $t \in K$ is nonconstant, and $[K] \in \mathbb{Z}$ is a code for K, then there is a parametrically definable isomorphism between $(K, +, \times)$ and $(\{t^n \mid n \in \mathbb{Z}\}, \oplus_{t[K]}, \otimes_{t[K]})$ where the formulas M and A are interpreted relative to the the interpretation of $\mathbb{Z}$.

Biïnterpretation with $\mathbb{Z}$

Theorem

If K is an infinite finitely generated field, then K is parametrically biïnterpretable with $\mathbb{Z}$.

In fact, we can say more.

- If K is a finitely generated field of characteristic zero and $[K] \in \mathbb{Z}$ is a code for the interpretation of K in $\mathbb{Z}$, then there is a parametrically definable isomorphism between $(K, +, \times)$ and $(\mathbb{Z}, \oplus_{[K]}, \otimes_{[K]})$.
- If K is an infinite finitely generated field of positive characteristic, $t \in K$ is nonconstant, and $[K] \in \mathbb{Z}$ is a code for K, then there is a parametrically definable isomorphism between $(K, +, \times)$ and $(\{t^n \mid n \in \mathbb{Z}\}, \oplus_{t[K]}, \otimes_{t[K]})$ where the formulas M and A are interpreted relative to the the interpretation of $\mathbb{Z}$.

Biïnterpretation with $\mathbb{Z}$

Theorem

If K is an infinite finitely generated field, then K is parametrically biïnterpretable with $\mathbb{Z}$.

In fact, we can say more.

- If K is a finitely generated field of characteristic zero and $[K] \in \mathbb{Z}$ is a code for the interpretation of K in $\mathbb{Z}$, then there is a parametrically definable isomorphism between $(K, +, \times)$ and $(\mathbb{Z}, \oplus_{[K]}, \otimes_{[K]})$.
- If K is an infinite finitely generated field of positive characteristic, $t \in K$ is nonconstant, and $[K] \in \mathbb{Z}$ is a code for K, then there is a parametrically definable isomorphism between $(K, +, \times)$ and $(\{t^n \mid n \in \mathbb{Z}\}, \oplus_{t[K]}, \otimes_{t[K]})$ where the formulas M and A are interpreted relative to the the interpretation of $\mathbb{Z}$.

Biïnterpretation with $\mathbb{Z}$

Theorem

If K is an infinite finitely generated field, then K is parametrically biïnterpretable with $\mathbb{Z}$.

In fact, we can say more.

- If K is a finitely generated field of characteristic zero and $[K] \in \mathbb{Z}$ is a code for the interpretation of K in $\mathbb{Z}$, then there is a parametrically definable isomorphism between $(K, +, \times)$ and $(\mathbb{Z}, \oplus_{[K]}, \otimes_{[K]})$.
- If K is an infinite finitely generated field of positive characteristic, $t \in K$ is nonconstant, and $[K] \in \mathbb{Z}$ is a code for K, then there is a parametrically definable isomorphism between $(K, +, \times)$ and $(\{t^n \mid n \in \mathbb{Z}\}, \oplus_{t[K]}, \otimes_{t[K]})$ where the formulas M and A are interpreted relative to the the interpretation of $\mathbb{Z}$.

QFA from biïnterpretation

For each formula $\eta(x, y; \mathbf{z}, u, v)$, there is another formula $\varphi_\eta(\mathbf{z}, u, v)$ which naturally expresses

$\eta(K; \mathbf{z}, u, v)$ is the graph of an isomorphism between $(K, +, \times)$ and $(\mathbb{Z}, \oplus_v, \otimes_v)$ where by "$\mathbb{Z}$" we mean $\mathbb{Z}$ itself if K has characteristic zero and $\{u^n \mid n \in \mathbb{Z}\}$ in positive characteristic.

QFA from biïnterpretation

For each formula $\eta(x, y; \mathbf{z}, u, v)$, there is another formula $\varphi_\eta(\mathbf{z}, u, v)$ which naturally expresses

$\eta(K; \mathbf{z}, u, v)$ is the graph of an isomorphism between $(K, +, \times)$ and $(\mathbb{Z}, \oplus_v, \otimes_v)$ where by "$\mathbb{Z}$" we mean $\mathbb{Z}$ itself if K has characteristic zero and $\{u^n \mid n \in \mathbb{Z}\}$ in positive characteristic.

If K is parametrically biïnterpretable with $\mathbb{Z}$, then it is so via some $\eta(x, y; \mathbf{a}, 1, [K])$ (if $\mathrm{char}(K) = 0$) or $\eta(x, y; \mathbf{a}, t, t^{[K]})$ (if $\mathrm{char}(K) > 0$).

QFA from biïnterpretation

For each formula $\eta(x, y; \mathbf{z}, u, v)$, there is another formula $\varphi_\eta(\mathbf{z}, u, v)$ which naturally expresses

$\eta(K; \mathbf{z}, u, v)$ is the graph of an isomorphism between $(K, +, \times)$ and $(\mathbb{Z}, \oplus_v, \otimes_v)$ where by "$\mathbb{Z}$" we mean $\mathbb{Z}$ itself if K has characteristic zero and $\{u^n \mid n \in \mathbb{Z}\}$ in positive characteristic.

If K is parametrically biïnterpretable with $\mathbb{Z}$, then it is so via some $\eta(x, y; \mathbf{a}, 1, [K])$ (if $\mathrm{char}(K) = 0$) or $\eta(x, y; \mathbf{a}, t, t^{[K]})$ (if $\mathrm{char}(K) > 0$).
The isomorphism type of K is then specified by $\phi_K := (\exists \mathbf{z})\varphi_\eta(\mathbf{z}, 1, [K])$ (or $\phi_K := (\exists \mathbf{z})(\exists t)\varphi_\eta(\mathbf{z}, t, t^{[K]})$).

Isomorphisms via comparison of evaluation

If k is a field, C is an algebraic curve of k, $K = k(C)$ is the function field of C, and K' is a copy of K, then if $C(k)$ were infinite and the evaluation functions $\text{ev} : K \times C(k) \to \mathbb{P}^1(k)$ and $\text{ev}' : K' \times C(k) \to \mathbb{P}^1(k)$ given by $(f, P) \mapsto f(P)$ were definable, then we could define an isomorphism between K and K' by $f \mapsto f' \Leftrightarrow (\forall P \in C(k))\, \text{ev}(f, P) = \text{ev}'(f', P)$.

Isomorphisms via comparison of evaluation

If k is a field, C is an algebraic curve of k, $K = k(C)$ is the function field of C, and K' is a copy of K, then if $C(k)$ were infinite and the evaluation functions $\text{ev} : K \times C(k) \to \mathbb{P}^1(k)$ and $\text{ev}' : K' \times C(k) \to \mathbb{P}^1(k)$ given by $(f, P) \mapsto f(P)$ were definable, then we could define an isomorphism between K and K' by $f \mapsto f' \Leftrightarrow (\forall P \in C(k))\, \text{ev}(f, P) = \text{ev}'(f', P)$.

If $C(k)$ is finite, then one needs to uniformly define evaluation for points $P \in C(k')$ where k' ranges over some definable set of fields for which there are infinitely many points on C.

Isomorphisms via comparison of evaluation

If k is a field, C is an algebraic curve of k, $K = k(C)$ is the function field of C, and K' is a copy of K, then if $C(k)$ were infinite and the evaluation functions $\mathrm{ev} : K \times C(k) \to \mathbb{P}^1(k)$ and $\mathrm{ev}' : K' \times C(k) \to \mathbb{P}^1(k)$ given by $(f, P) \mapsto f(P)$ were definable, then we could define an isomorphism between K and K' by $f \mapsto f' \Leftrightarrow (\forall P \in C(k))\, \mathrm{ev}(f, P) = \mathrm{ev}'(f', P)$.

If $C(k)$ is finite, then one needs to uniformly define evaluation for points $P \in C(k')$ where k' ranges over some definable set of fields for which there are infinitely many points on C.

Defining evaluation at P is equivalent to defining the valuation ord_P.

Isomorphisms via comparison of evaluation

If k is a field, C is an algebraic curve of k, $K = k(C)$ is the function field of C, and K' is a copy of K, then if $C(k)$ were infinite and the evaluation functions $\mathrm{ev} : K \times C(k) \to \mathbb{P}^1(k)$ and $\mathrm{ev}' : K' \times C(k) \to \mathbb{P}^1(k)$ given by $(f, P) \mapsto f(P)$ were definable, then we could define an isomorphism between K and K' by $f \mapsto f' \Leftrightarrow (\forall P \in C(k))\, \mathrm{ev}(f, P) = \mathrm{ev}'(f', P)$.

If $C(k)$ is finite, then one needs to uniformly define evaluation for points $P \in C(k')$ where k' ranges over some definable set of fields for which there are infinitely many points on C.

Defining evaluation at P is equivalent to defining the valuation ord_P. By the usual tricks, defining the valuation ord_P is equivalent to defining the relation $\mathrm{ord}_P(f) \equiv 0 \pmod{\ell}$ for any integer ℓ greater than one.

Defining evaluation

Theorem

Suppose that (k, v) is a discretely valued field with $\pi \in k$ a uniformizer. Let $K = k(t)$ and consider K in the language of rings augmented by a predicate for $\mathscr{O}_{k,v} = \{x \in k \mid v(x) \geq 0\}$ and constants for π and t. Then the evaluation function $(f, P) \mapsto f(P)$ is definable.

Defining evaluation

Theorem

Suppose that (k, v) is a discretely valued field with $\pi \in k$ a uniformizer. Let $K = k(t)$ and consider K in the language of rings augmented by a predicate for $\mathscr{O}_{k,v} = \{x \in k \mid v(x) \geq 0\}$ and constants for π and t. Then the evaluation function $(f, P) \mapsto f(P)$ is definable.

The corresponding result for $K = k(C)$, the function field of a curve, holds at least as long as one avoids ramified points and is uniform in the sense that one can consider $P \in C(k')$ where k' ranges over some definable family of fields.

Defining evaluation

Theorem

Suppose that (k, v) is a discretely valued field with $\pi \in k$ a uniformizer. Let $K = k(t)$ and consider K in the language of rings augmented by a predicate for $\mathscr{O}_{k,v} = \{x \in k \mid v(x) \geq 0\}$ and constants for π and t. Then the evaluation function $(f, P) \mapsto f(P)$ is definable.

The corresponding result for $K = k(C)$, the function field of a curve, holds at least as long as one avoids ramified points and is uniform in the sense that one can consider $P \in C(k')$ where k' ranges over some definable family of fields.

We use a local-global principle for the Brauer group and a concrete criterion for the splitting of cyclic algebras to prove these theorems.

Cyclic algebras

Let K be a field containing a primitive ℓ^{th} root of unity ω for some prime ℓ. For $A, B \in K$ we define $D(A, B, \omega; K)$ to be the noncommutative associative K-algebra generated by α and β subject to the relations $\alpha^\ell = A$, $\beta^\ell = B$, and $\beta\alpha = \omega\alpha\beta$.

Cyclic algebras

Let K be a field containing a primitive ℓ^{th} root of unity ω for some prime ℓ. For $A, B \in K$ we define $D(A, B, \omega; K)$ to be the noncommutative associative K-algebra generated by α and β subject to the relations $\alpha^\ell = A$, $\beta^\ell = B$, and $\beta\alpha = \omega\alpha\beta$.

Proposition (see Lam's book on Noncommutative Algebra)

$D(A, B, \omega; K)$ is a division algebra if and only if A is not an ℓ^{th} power in K and B is not a norm from the field extension $K(\alpha)/K$.

Local-global principle

Theorem (Auslander-Brumer)

Let k be a field and D is a central simple algebra over $k(t)$ with $\dim_{k(t)} D$ prime to the characteristic of k. Then D is a division algebra if and only if there is some irreducible polynomial $P \in k[t]$ for which $D \otimes_{k(t)} K$ is a division algebra where K is the completion of $k(t)$ at P.

Proving biïnterpretability with $\mathbb{Z}$

- Working by induction on the transcendence degree of the infinite finitely generated field K we show that K is parametrically biïnterpretable with $\mathbb{Z}$.

Proving biïnterpretability with $\mathbb{Z}$

- Working by induction on the transcendence degree of the infinite finitely generated field K we show that K is parametrically biïnterpretable with $\mathbb{Z}$.
- The case of K a global field was solved by Rumely.

Proving biïnterpretability with $\mathbb{Z}$

- Working by induction on the transcendence degree of the infinite finitely generated field K we show that K is parametrically biïnterpretable with $\mathbb{Z}$.
- The case of K a global field was solved by Rumely.
- In the inductive case with $\operatorname{tr.deg}(K) = n + 1$, choose $a_1, \ldots, a_n \in K$ algebraically independent and set $k := \{x \in K \mid K \models \psi_{n+1}(x, a_1, \ldots, a_n)\}$, the relative algebraic closure of the subfield generated by $a_1, \ldots, a_n$. Express $K = k(C)$.

Proving biïnterpretability with $\mathbb{Z}$

- The case of K a global field was solved by Rumely.
- In the inductive case with $\operatorname{tr.deg}(K) = n + 1$, choose $a_1, \ldots, a_n \in K$ algebraically independent and set $k := \{x \in K \mid K \models \psi_{n+1}(x, a_1, \ldots, a_n)\}$, the relative algebraic closure of the subfield generated by $a_1, \ldots, a_n$. Express $K = k(C)$.
- By induction, k is biïnterpretable with $\mathbb{Z}$. Hence, for any recursive family $\mathscr{F}$ of field extensions of k, the evaluation function which takes $f \in \widetilde{K}$ (the copy of K in $\mathbb{Z}$), $F \in \mathscr{F}$, and $P \in C(F)$ and returns $f(P)$ is definable in K.

Proving biïnterpretability with $\mathbb{Z}$

- In the inductive case with $\operatorname{tr.deg}(K) = n + 1$, choose $a_1, \ldots, a_n \in K$ algebraically independent and set $k := \{x \in K \mid K \models \psi_{n+1}(x, a_1, \ldots, a_n)\}$, the relative algebraic closure of the subfield generated by $a_1, \ldots, a_n$. Express $K = k(C)$.
- By induction, k is biïnterpretable with $\mathbb{Z}$. Hence, for any recursive family $\mathscr{F}$ of field extensions of k, the evaluation function which takes $f \in \widetilde{K}$ (the copy of K in $\mathbb{Z}$), $F \in \mathscr{F}$, and $P \in C(F)$ and returns $f(P)$ is definable in K.
- Choosing an appropriate recursive discrete valuation on k, we see that the hypotheses for the theorem on definability of evaluation in K hold so that we may definably identify K with $\widetilde{K}$ by testing evaluation on $\mathscr{F}$-rational points.

Which classes of finitely generated fields are QFA?

If ϖ is a sentence in the language of rings, then the set $\{n \in \mathbb{Z} \mid (\mathbb{Z}, \oplus_n, \otimes_n) \models \varpi\}$ is definable in arithmetic.

Which classes of finitely generated fields are QFA?

If ϖ is a sentence in the language of rings, then the set $\{n \in \mathbb{Z} \mid (\mathbb{Z}, \oplus_n, \otimes_n) \models \varpi\}$ is definable in arithmetic.

Question (Poonen)

If $X \subseteq \mathbb{Z}$ is a definable set which is closed under isomorphism in the sense that $(n \in X \& (\mathbb{Z}, \oplus_n, \otimes_n) \cong (\mathbb{Z}, \oplus_m, \otimes_m)) \Rightarrow m \in X$, must there be a sentence ϖ_X for which $(\mathbb{Z}, \oplus_n, \otimes_n) \models \varpi_X$ if and only if $n \in X$?

Which classes of finitely generated fields are QFA?

If ϖ is a sentence in the language of rings, then the set $\{n \in \mathbb{Z} \mid (\mathbb{Z}, \oplus_n, \otimes_n) \models \varpi\}$ is definable in arithmetic.

Question (Poonen)

If $X \subseteq \mathbb{Z}$ is a definable set which is closed under isomorphism in the sense that $(n \in X \& (\mathbb{Z}, \oplus_n, \otimes_n) \cong (\mathbb{Z}, \oplus_m, \otimes_m)) \Rightarrow m \in X$, must there be a sentence ϖ_X for which $(\mathbb{Z}, \oplus_n, \otimes_n) \models \varpi_X$ if and only if $n \in X$?

Our results imply that X is elementary relative to the class of infinite finitely generated fields.

Geometric case

Question

If K and L are elementarily equivalent finitely generated extensions of $\mathbb{C}$, must they be isomorphic?

- It is unknown whether $\mathrm{Th}(\mathbb{C}(t))$ is decidable.
- Much work on this question has already been completed by Duret, Pheidas, Pierce, Poonen, and Pop amongst others.
- For trivial reasons of cardinality, K cannot be biïnterpretable with $\mathbb{Z}$.

Geometric case

Question

If K and L are elementarily equivalent finitely generated extensions of $\mathbb{C}$, must they be isomorphic?

- It is unknown whether $\mathrm{Th}(\mathbb{C}(t))$ is decidable.
- Much work on this question has already been completed by Duret, Pheidas, Pierce, Poonen, and Pop amongst others.
- For trivial reasons of cardinality, K cannot be biïnterpretable with $\mathbb{Z}$.

Geometric case

Question

If K and L are elementarily equivalent finitely generated extensions of $\mathbb{C}$, must they be isomorphic?

- It is unknown whether $\mathrm{Th}(\mathbb{C}(t))$ is decidable.
- Much work on this question has already been completed by Duret, Pheidas, Pierce, Poonen, and Pop amongst others.
- For trivial reasons of cardinality, K cannot be biïnterpretable with $\mathbb{Z}$.

Geometric case

Question

If K and L are elementarily equivalent finitely generated extensions of $\mathbb{C}$, must they be isomorphic?

- It is unknown whether $\mathrm{Th}(\mathbb{C}(t))$ is decidable.
- Much work on this question has already been completed by Duret, Pheidas, Pierce, Poonen, and Pop amongst others.
- For trivial reasons of cardinality, K cannot be biïnterpretable with $\mathbb{Z}$.

Geometric problems over $\mathbb{Q}^{\mathrm{alg}}$

Question

$\mathbb{Q}^{\mathrm{alg}}(t, s)$ and $\mathbb{Z}$ interpret each other. Are they biïnterpretable?