Abstract isomorphisms, coordinatization, and bi-interpretability

Alexei Miasnikov
(Stevens Institute)

Vavilov Memorial 2024
Saint Petersburg State University
September 17th, 2024

Outline

In this talk I will show that quite often behind various "rigidity phenomena" one can find a bi-interpretation of algebraic structures.

- "Coordinatization"
- "Rigidity"
- "Abstract isomorphisms"
- "Equivalence of categories"

This bi-interpretation typically gives the most precise and robust description of the phenomenon.

Examples

- Fundamental theorems of geometry
- Malcev correspondence between nilpotent k-groups groups and nilpotent Lie k-algebras over a field k of characteristic zero.
- Abstract isomorphisms of unipotent k-groups.

Projective spaces

Let V be a vector space over a field k.

The projective space

$$P(V) = \langle P(V); \subseteq \rangle$$

of V is the set $P(V)$ of all linear subspaces of V equipped with just one binary relation, the inclusion $\subseteq$.

A projectivity is an isomorphism $P(V_1) \to P(V_2)$.

A semilinear isomorphism $f : V_1 \to V_2$ relative to a field isomorphism $\lambda : k_1 \to k_2$ is a bijection $f : V_1 \to V_2$ such that for all $x, y \in V_1, \alpha \in k_1$ the following holds:

- $f(x + y) = f(x) + f(y)$,
- $f(\alpha x) = \lambda(\alpha) f(x)$.

The fundamental theorem of projective geometry

The fundamental theorem of projective geometry

Let V_1 and V_2 be vector spaces over fields k_1 and k_2 of dimension ≥ 3. Then:

- if $P(V_1)$ is isomorphic to $P(V_2)$ then $k_1 \simeq k_2$ and $dim_{k_1} V_1 = dim_{k_2} V_2$.
- Every projectivity $P(V_1) \rightarrow P(V_2)$ is induced by some semilinear isomorphism $V_1 \rightarrow V_2$.

The fundamental theorem of projective geometry

Theorem [Burger-M.]

Let F be an arbitrary field and V a vector space over F of finite dimension $n \geq 3$. Then F is regularly bi-interpretable in $P(V)$.

Decidability of the first-order theory

Corollary

Let V be a vector space of dimension $n \geq 3$ over a field F. Then the theory $Th(P(V))$ is decidable if and only if the theory $Th(F)$ is decidable.

First-order classification

Corollary

For vector spaces V_1, V_2 of dimension ≥ 3 over fields F_1 and F_2, respectively, we have

$$P(V_1) \equiv P(V_2) \iff F_1 \equiv F_2 \text{ and } dim_{F_1} V_1 = \dim_{F_2} V_2.$$

Theorem

Let V be a vector space of dimension $n \geq 3$ over a field F. Then for any algebraic structure $\mathcal{P} = \langle P; \subseteq \rangle$ one has $P(V) \equiv \mathcal{P}$ if and only if $\mathcal{P}$ is isomorphic to $P(\bar{V})$, where $\bar{V}$ is a vector space of dimension n over a field $\bar{F}$ such that $F \equiv \bar{F}$.

First-order classification

Corollary

For vector spaces V_1, V_2 of dimension ≥ 3 over fields F_1 and F_2, respectively, we have

$$P(V_1) \equiv P(V_2) \iff F_1 \equiv F_2 \text{ and } dim_{F_1} V_1 = \dim_{F_2} V_2.$$

Theorem

Let V be a vector space of dimension $n \geq 3$ over a field F. Then for any algebraic structure $\mathcal{P} = \langle P; \subseteq \rangle$ one has $P(V) \equiv \mathcal{P}$ if and only if $\mathcal{P}$ is isomorphic to $P(\bar{V})$, where $\bar{V}$ is a vector space of dimension n over a field $\bar{F}$ such that $F \equiv \bar{F}$.

Richness

Theorem

Let V be a finite dimensional vector space over a field F of dimension $n \geq 3$. Then $P(V)$ is rich if and only if F is rich.

It is known that the field of rational numbers $\mathbb{Q}$, as well all number fields, are rich.

Corollary

Let F be the field of rational numbers $\mathbb{Q}$ or a number field and V a vector space of a finite dimension ≥ 3 over F. Then $P(V)$ is rich.

Other properties

More general: let S be a property which is preserved under regular bi-interpretation.

Metatheorem

Let S be a property which is preserved under regular bi-interpretation. If V is a vector space of a finite dimension $n \geq 3$ over a field F then $P(V)$ satisfies S if and only if F satisfies S.

Nilpotent k-groups

Definition

A nilpotent group G admits exponents in a characteristic zero field k if it is equipped with an exponentiation function:

$$G \times k \to G, \quad (x, a) \mapsto x^a,$$

satisfying the following axioms for all $x, y, x_1, \ldots, x_n \in G$ and $a, b \in k$:

1) $x^1 = x, \;\; x^a x^b = x^{(a+b)}, \;\; (x^a)^b = x^{(ab)}$,
2) $(y^{-1}xy)^a = y^{-1}x^a y$,
3) $x_1^a x_2^a \cdots x_n^a = (x_1 x_2 \cdots x_n)^a \tau_2(\bar{x})^{\binom{a}{2}} \cdots \tau_c(\bar{x})^{\binom{a}{c}}$,

where τ_i are the Petresco words, c is the nilpotency class of G, and $\binom{a}{i}$ are binomial coefficients.

Let G and H be two k-groups. A group homomorphism $\phi : G \to H$ is called

- a k-homomorphism if
$$\phi(g^a) = (\phi(g))^a$$
for all $g \in G$ and $a \in k$.
- a semilinear (semialgebraic) if there is an automorphism $\sigma : k \to K$ such that
$$\phi(g^a) = (\phi(g))^{\sigma(a)}$$
for all $g \in G$ and $a \in k$.

Malcev basis and coordinates

Let G be a nilpotent k-group finitely generated over k.

Elements $u_1, \ldots, u_n \in G$ form a Malcev basis of G if the k-subgroups $H_i = \langle u_i, \ldots, u_n \rangle_k$ form a central series in G:

$$G = H_1 > \ldots > H_n > H_{n+1} = 1$$

that is $[H_1, H_i] \leq H_{i+1}$ for all i.

In this case every element $g \in G$ can be uniquely presented as a product

$$g = u_1^{a_1} \ldots u_n^{a_n}$$

for some $a_i \in k$.

The tuple $t(g) = (a_1, \ldots, a_n)$ termed Malcev coordinates of g in the basis $(u_1, \ldots, u_n)$.

Algebraicity

Malcev theorem: there are polynomials $f_i(\bar{x}, \bar{y}) \in k[\bar{x}, \bar{y}]$ such that for any $g, h \in G$

$$t(gh) = (f_1(t(g), t(h)), \ldots, f_n(t(g), t(h)).$$

so multiplication is defined by polynomials.

The same for inversion $g \to g^{-1}$ and k-exponentiation $(g, a) \to g^a$.

The coordinates $t([u_i, u_j])$, $1 \leq i, j \leq n$ are the structural constants of the base $\bar{u} = (u_1, \ldots, u_n)$.

The coefficients of the polynomials f_i are completely defined by the structural constants of the base $\bar{u}$ (they generate the field of definition for G).

Malcev correspondence

The following theorem, termed the Malcev correspondence, was proved first in the case where $k = \mathbb{Q}, \mathbb{R}$ by A. Malcev in the finite dimensional case.

Later it was noticed by M. Lazard (in an unpublished paper) that finite-dimensionality condition can be removed.

D. Quillen extended these results to the pro-nilpotent case using the theory of complete Hopf-algebras.

Finally R. B. Warfield sketched, using Quillen's approach, a generalization to the case of arbitrary k-groups, where k is a field of characteristic zero.

Malcev correspondence

Let k be a field of characteristic zero, $\mathcal{G}$ be the category of k-groups and $\mathcal{L}$ be the category of nilpotent Lie k-algebras. Then there is a category equivalence

$$\rho : \mathcal{L} \to \mathcal{G}, \quad \rho : L \to G(L)$$

such that for any $L \in \mathcal{L}$ the group $G(L)$ is the set L equipped with a multiplication given by the Campbell-Baker-Hausdorf formula:

$$x * y = x + y + \frac{1}{2}(x, y) + \cdots$$

where $\cdots$ is a linear combination of Lie brackets of weight greater than 2 with rational coefficients.

Malcev correspondence

Theorem [Amaglobeli, Bokelavadze, M.]

Let L be a nilpotent Lie algebra over a field k of characteristic zero and $G = G(L)$. Then L and the nilpotent k-group $G(L)$ are absolutely injectively bi-interpretable in each other by equations.

Generalized algebraic groups

The classical algebraic groups are defined via algebraic sets from the classical algebraic geometry.

Intuitively, a classical algebraic group G is an algebraic set $A \subset \mathbb{C}^n$ equipped with the multiplication $\cdot$ and inversion $^{-1}$ whose graphs are also algebraic sets over $\mathbb{C}$.

Think about $SL(n, \mathbb{C})$, $GL(n, \mathbb{C})$, or $T(n, \mathbb{C})$, or $UT(n, \mathbb{C})$.

In this case G is defined via three polynomial systems of equations with coefficients in $\mathbb{C}$:

$$\Gamma = \{U(\bar{x}), M(\bar{x}, \bar{y}, \bar{z}), In(\bar{x}, \bar{z})\},$$

where $\bar{x}, \bar{y}$, and $\bar{z}$ are n-tuples of variables, and $U(\bar{x})$ defines the algebraic set A, and $M(\bar{x}, \bar{y}, \bar{z}), In(\bar{x}, \bar{z})$ define the multiplication and the inversion on A.

Generalized algebraic schemes and groups

We generalize the notion of algebraic group by allowing arbitrary FO formulas in place of equations.

This leads to algebraic schemes via interpretaions.

Interpretations of groups

We consider groups in the standard group theory language $\{\cdot, ^{-1}, 1\}$.

A group G is interpretable in a structure $\mathbb{B}$ if

- there is a definable in $\mathbb{B}$ subset $A \subseteq \mathbb{B}^n$,
- there is a definable in $\mathbb{B}$ equivalence relation $\sim$ on A,
- the quotient set $A/\sim$ is equipped with group multiplication $\cdot$ and inversion $^{-1}$, which are also definable in $\mathbb{B}$,
- the group $\langle A/\sim, \cdot, ^{-1} \rangle$ is isomorphic to G.

In this case G is interpreted in $\mathbb{B}$ by a set

$$\Gamma = \{U(\bar{x}), E(\bar{x}, \bar{y}), M(\bar{x}, \bar{y}, \bar{z}), In(\bar{x}, \bar{z})\},$$

where $E(\bar{x}, \bar{y})$ is a FO formula that defines $\sim$ on A, while $M(\bar{x}, \bar{y}, \bar{z})$ and $In(\bar{x}, \bar{z})$ define the multiplication and inversion on $A/\sim$.

We write in this case $G = \Gamma(\mathbb{B})$.

Definition

Let $G = \Gamma(\mathbb{B})$ as above.

In this case we say that Γ is the first order group scheme in the language of $\mathbb{B}$ and G is a generalized algebraic group over $\mathbb{B}$ defined by the scheme Γ.

To study $\Gamma(\mathbb{B})$ one needs to know a lot about $\mathbb{B}$.

Like in the classical algebraic groups we may consider generalized algebraic groups over $\mathbb{C}$ and $\mathbb{R}$.

We will also consider $\mathbb{Z}$ for $\mathbb{B}$.

Some facts:

- $\mathbb{C}$ and $\mathbb{R}$ admit elimination of quantifiers, so every formula is equivalent to a quantifire-free one.
- in integral domains $a = 0 \vee b = 0 \iff ab = 0$, so disjunctions of equations are equivalent to an equation,
- in fields $a \neq 0 \iff \exists x(ax = 1)$, so equalities can be replaced by Diophantine formulas.
- in $\mathbb{R}$ one has $a \geq 0 \iff \exists y(x = y^2)$

This implies that definable sets in $\mathbb{C}$ and $\mathbb{R}$ are precisely the constructible sets from algebraic geometry (intersections of algebraic sets and projections of algebraic sets).

Elimination of imaginaries

But there is an equivalence relation $\sim$ in the notion of interpretaion, that do not occur in the definition of the standard algebraic groups.

Derfinition

A structure $\mathbb{A}$ has elimination of imaginaries if for any definable subset $A \subseteq \mathbb{A}^n$ and every definable in $\mathbb{A}$ equivalence relation $\sim$ on A there is a definable in $\mathbb{A}$ function $f : A \to \mathbb{A}^m$ such that $a \sim b \iff f(a) = f(b)$.

If $\mathbb{A}$ has elimination of imaginaries then in the definition of interpretaion in $\mathbb{A}$ one can replace the quotient set $A/\sim$ by a definable set $f(A)$.

Elimination of imaginaries

Theorem [Poizat]

$\mathbb{R}$ and $\mathbb{C}$ have elimination of imaginaries.

- Thus generalized algebraic groups over $\mathbb{C}$ and $\mathbb{R}$ are almost the classical algebraic groups, but over $\mathbb{Z}$ they are very different.
- Note that $\mathbb{Z}$ admits elimination of imaginaries, but there is no elimination of quantifiers (to the contrary, Π_n and Σ_n hierarchies are proper). There is a lot of interesting generalized algebraic groups over $\mathbb{Z}$, which are not $\mathbb{Z}$-points of the classical algebraic groups.

The Diophantine problem

Corollary

Let L be a nilpotent Lie algebra over a field k of characteristic zero and $G = G(L)$. Then the Diophantine problem in L is PTime equivalent to the Diophantine problem in G.

Corollary

Let L be a nilpotent Lie k-algebra with coefficients in a field k of characteristic zero and $G = G(L)$. Then:

1) G and L have isomorphic categories of algebraic sets;
2) G and L have precisely the same projective logical categories.

J. Tits (Talk at International Congress of Mathematicians, Nice, 1970):

"A natural question that arises in the case of an algebraic group $\mathcal{G}$ over a field K is whether the (abstract) group of K-points $\mathcal{G}(K)$ keeps the information about the filed K and the structure of the algebraic scheme $\mathcal{G}$".

He made it a bit more precise:

Is it true that every isomorphism $\mathcal{G}(K) \to \mathcal{G}'(K')$ is induced by some field isomorphism $\sigma : K \to K'$ and some K-isomorphism of algebraic groups $\mathcal{G} \to \mathcal{G}'$, provided K' is identified with K via σ.

Long history:

Schreier, van der Warden, Hua, Diedonne, Borel, Tits, O'Meara, Steinberg, Humphreys, ..., Petechuk, Golubchik-Mikhalev, Zelmanov, ...

Abstract isomorphisms of Chevalley groups

Theorem [Bunina, 2024]

Let $G = G_\pi(\Phi, R)$ (or $E_\pi(\Phi, R)$) be an (elementary) Chevalley group of rank > 1, R be a commutative ring with 1. Suppose that for $\Phi = A_2, B_l, C_l$ or F_4 we have $1/2 \in R$, for $\Phi = G_2$ we have $1/2, 1/3 \in R$. Then every automorphism of the group G is standard.

Recall, that an automorphism of $G_\pi(\Phi, R)$ (or $E_\pi(\Phi, R)$) is standard if it is a composition of central, ring, inner, and graph automorpisms.

Back to the Tits question:

Theorem [Bunina-Gvozdevsky]

Let G be a Chevalley group over a commutative rings R with 1, constructed by irreducible root systems of rank > 1. Assume that $1/2 \in R$ for the systems A_2, B_l, C_l or F_4 and $1/2, 1/3 \in R$ for $\Phi = G_2$. Then:

- The central quotients $G/Z(G)$ of Chevalley groups G are regularly bi-interpretable with the corresponding rings.
- The same holds for adjoint Chevalley groups and for boundedly generated Chevalley groups.
- There are examples of Chevalley group with infinite center, which is not bi-interpretable with R and is elementarily equivalent to a group that is not a Chevalley group itself.

The theorem above gives a lot on model theory of Chevalley groups G:

Bi-interpretability of $G/Z(G)$ and R effectively reduces (most of) the model theory of $G/Z(G)$ to the model theory of R.

To go from $G/Z(G)$ to G one uses abelian cohomological deformations.

To explain consider two examples.

More examples

Malcev: For any $m, n \geq 3$

$$SL(n, F) \equiv SL(m, \tilde{F}) \iff n = m \text{ and } \tilde{F} \equiv F.$$

Theorem [M.-Sohrabi, 2022; Bunina, 2022]

Let F be a field and $n \geq 3$. Then for any group H one has

$$H \equiv SL(n, F) \iff H \simeq SL(n, \tilde{F}) \text{ for some } \tilde{F} \equiv F.$$

Note, that the theorem above strengthen quite a bit Malcev's result.

I am looking for something like that but in a very general context

More examples

Malcev: For any $m, n \geq 3$

$$SL(n,F) \equiv SL(m,\tilde{F}) \Longleftrightarrow n = m \text{ and } \tilde{F} \equiv F.$$

Theorem [M.-Sohrabi, 2022; Bunina, 2022]

Let F be a field and $n \geq 3$. Then for any group H one has

$$H \equiv SL(n,F) \Longleftrightarrow H \simeq SL(n,\tilde{F}) \text{ for some } \tilde{F} \equiv F.$$

Note, that the theorem above strengthen quite a bit Malcev's result.

I am looking for something like that but in a very general context

Malcev: For any $m, n \geq 3$

$$GL(n, F) \equiv GL(m, \tilde{F}) \iff n = m \textit{ and } \tilde{F} \equiv F$$

.

Theorem [M.-Sohrabi, 2022]

Let F be a field. If H is a group such that $H \equiv GL_n(F), n \geq 3$, then $H \cong GL_n(\tilde{F}, \bar{f})$ for some field $\tilde{F} \equiv F$ and a tuple of 2-cocycles $\bar{f}$.

Malcev: For any $m, n \geq 3$

$$GL(n, F) \equiv GL(m, \tilde{F}) \iff n = m \text{ and } \tilde{F} \equiv F$$

.

Theorem [M.-Sohrabi, 2022]

Let F be a field. If H is a group such that $H \equiv GL_n(F), n \geq 3$, then $H \cong GL_n(\tilde{F}, \bar{f})$ for some field $\tilde{F} \equiv F$ and a tuple of 2-cocycles $\bar{f}$.

If H is any group such that $H \equiv GL_n(F), n > 2$, then H fits into the short exact sequence

$$1 \to H' \cdot Z(H) \to H \to \frac{L^\times}{(L^\times)^n} \to 1$$

where $H' \cong SL_n(L)$, $L \equiv F$, as fields, and $Z(H) \equiv F^\times$.

Triangular matrix groups

Let $T_n(F)$ be the triangular matrix group over a field F.

Theorem [M.-Sohrabi, 2020]

Let F be a field. If H is a group such that $H \equiv T_n(F)$, $n \geq 3$, then $H \simeq T_n(R, \bar{f})$ for some field $R \equiv F$ and a tuple of 2-cocycles $\bar{f}$.

Tits also introduced non-commutative generalizations of the fundamental theorems of geometry

Let G be an algebraic group over a field K and $P(G)$ a set S of some K-defined algebraic subgroups of G equipped with inclusion $\subset$.

For example, for an absolutely simple adjoint algebraic group G over a field K Tits considered $P(G) = \langle S; \subset \rangle$, where S is the set of parabolic (containing Borel subgroups) K-subgroups of G.

He proved an analog of the fundamental theorem of projective geometry for such $P(G)$.

Unipotent affine algebraic groups

Now I will consider unipotent affine K-groups over a field K of chracteristic zero.

These are precisely the nilpotent K-groups discussed above.

I will look at the abstract isomorphisms and model theory of such groups.

Two discouraging examples

Let $\mathbb{Q} < K < L$ be finite algebraic field extensions.

$UT_3(L)$ is a nilpotent L-group. It can be also viewed as nilpotent K-group $\mathcal{G}(K)$.

Then an abstract isomorphism

$$UT_3(L) \to \mathcal{G}(K)$$

does not imply an isomorphism $L \to K$.

Fix: L is a "natural" field (the maximal filed of sclaras) of $UT_3(L)$, but K is not.

Two discouraging examples

Let $\mathbb{Q} < K < L$ be finite algebraic field extensions.

$UT_3(L)$ is a nilpotent L-group. It can be also viewed as nilpotent K-group $\mathcal{G}(K)$.

Then an abstract isomorphism

$$UT_3(L) \to \mathcal{G}(K)$$

does not imply an isomorphism $L \to K$.

Fix: L is a "natural" field (the maximal filed of sclaras) of $UT_3(L)$, but K is not.

The second discouraging example

There are k-nilpotent groups over a field k which have two non-isomorphic maximal fields of scalars.

Moreover, how do we approach the following group

$$G = UT_3(K_1) \times UT_3(K_2)$$

where K_1 and K_2 are finite algebraic non-isomorphic extensions of $\mathbb{Q}$?

Reduction to components

Let G be a finitely generated nilpotent k group over a field k of characteristic zero.

Then:

- G is a finite direct product of uniquely defined directly indecomposable k-subgroups

$$G = G_1 \times \ldots \times G_n \times G_0,$$

where G_0 is abelian, G_i is non-abelian and $Z(G_i) \leq [G_i, G_i]$ for every i, termed the components of G.

- every component G_i has uniquely defined maximal field of scalars $L_i = L(G_i)$.

Tits question for unipotent groups

- Every quasi-component $G_i \cdot Z(G)$ is interpretable in the group G;
- the maximal field L_i is absolutely interpretable in the quasi-component $G_i \cdot Z(G)$;
- In every component G_i there is a central series of L_i-subgroups

$$G_i > H_1 > \ldots > H_c > 1$$

  such that:
  - each H_i is definable in G_i,
  - H_i/H_{i+1} are finite dimensional L_i-vector spaces,
  - the action of L_i on H_i/H_{i+1} is definable in G_i.
- The type of the minimal structural constants of G is defined in G by first-order formulas.

This answer to Tits question allows one to describe abstract isomorphisms of unipotent k-groups and study their model theory.

There are no non-trivial abelian deformations over fields here, but they appear for nilpotent algebraic groups over rings.

Proofs are quite technical, it is convenient to go to nilpotent Lie k-algebras (using Malcev correspondence).

The non-commutative analog of the fundamental theorem of the projective geometry holds for unipotent k-groups.