Ubiquity and uniqueness: everyday mathematics from a model-theoretic perspective

Borovik, Alexandre

2008

MIMS EPrint: **2008.34**

Manchester Institute for Mathematical Sciences
School of Mathematics

The University of Manchester

Reports available from: http://eprints.maths.manchester.ac.uk/
And by contacting: The MIMS Secretary
School of Mathematics
The University of Manchester
Manchester, M13 9PL, UK

ISSN 1749-9097

Ubiquity and uniqueness: everyday mathematics from a model-theoretic perspective

Alexandre Borovik

Séminaire "Des Mathématiques"
Ecole Normale Supèrieure
Paris
16 January 2008

A philosophical introduction

There is nothing more practical than a good theory.

James C. Maxwell

There is nothing more practical than a good theory.

James C. Maxwell

There is nothing more practical than a good philosophy.

Alexandre V. Borovik

Are mathematical objects invented or discovered?

Are mathematical objects invented or discovered?

Serious legal implications: mathematical formulae are patentable in USA but not in UK.

For British lawmakers and lawyers, mathematics is discovered, for American — invented.

Are mathematical objects invented or discovered?

Serious legal implications: mathematical formulae are patentable in USA but not in UK.

For British lawmakers and lawyers, mathematics is discovered, for American — invented.

I have seen a patent application for use of the formula

$$x^a \cdot x^b = x^{a+b}$$

in cryptography.

Pythagoreans vs. Formalists

- Do mathematical objects exist?
- Might it happen that we tend to confuse existence with uniqueness and ubiquity?
- Why does most of Mathematics deal with such a limited range of objects?
- Why could the same objects be studied by bizarrely different methods?

First-order Logic

$\forall$, $\exists$, $\wedge$, $\vee$, $\neg$, $\rightarrow$, algebraic operations, $=$, ...

Theory is a set of formulae (without free variables)

A theory is **consistent** if no contradiction can be derived.

Löwenheim-Skolem: If a theory is consistent, it has a countable model.

Elementary theory of an algebraic structure

Let G be a group (ring, field, etc.)

$Th(G)$ the set of first order formulae true in G

Elementary equivalence:

$$G \equiv H \iff Th(G) = Th(H)$$

Example

$\mathbb{Q}^+$ is torsion-free divisible abelian:

$$\left.\begin{array}{l} \forall x \forall y\ xy = yx \\ \forall x\ (x^2 = 1 \to x = 1) \\ \forall x\ (x^3 = 1 \to x = 1) \\ \quad \vdots \\ \forall x \exists y\ y^2 = x \\ \forall x \exists y\ y^3 = x \\ \quad \vdots \end{array}\right\} \text{ infinite list of axioms}$$

Groups elementary equivalent to $\mathbb{Q}^+$ are torsion-free divisible abelian and are therefore vector spaces over $\mathbb{Q}$.

$$H \equiv \mathbb{Q}^+ \Longrightarrow H \simeq \bigoplus \mathbb{Q}^+$$

Uncountable categoricity.

G is **uncountably categorical**

$$\Longleftrightarrow \exists! \text{ group } \widetilde{G} \equiv G \text{ of cardinality continuum } 2^{\aleph_0}$$

$\mathbb{Q}^+$ is uncountably categorical because there is just one $\mathbb{Q}$-vector space of cardinality continuum.

In countable domain situation is different:

$\mathbb{Q}^+$ and $\mathbb{Q}^+ \oplus \mathbb{Q}^+$

are elementary equivalent, but not isomorphic.

Algebraically closed fields

$$\forall a_1 \forall a_0 (a_1 \neq 0 \rightarrow \exists x (a_1 x + a_0 = 0))$$

$$\forall a_2 \forall a_1 \forall a_0 (a_2 \neq 0 \rightarrow \exists x (a_2 x^2 + a_1 x + a_0 = 0))$$

$$\vdots$$

$$\forall a_n \cdots \forall a_1 \forall a_0 (a_n \neq 0 \rightarrow \exists x (a_n x^n + \cdots + a_1 x + a_0 = 0))$$

$$\vdots$$

It can be shown that any two a.c. fields of the same characteristic are elementary equivalent.

Algebraically closed fields

$$\overline{\mathbb{Q}} < \overline{\mathbb{Q}}(t_1, t_2, \dots) < \overline{\overline{\mathbb{Q}}(t_1, t_2, \dots)}$$

$$\overline{\mathbb{F}_p} < \overline{\mathbb{F}_p}(t_1, t_2, \dots) < \overline{\overline{\mathbb{F}_p}(t_1, t_2, \dots)}$$

For every characteristic, there is only one a.c. field of cardinality continuum.

In characteristic 0 this field is, of course, $\mathbb{C}$.

Algebraically closed fields are uncountably categorical.

We look at $\mathbb{C}$ algebraically, ignoring topology:

there are $2^{2^{\aleph_0}}$ automorphisms of $\mathbb{C}$

but only two continuous: identity and complex conjugation

Macintyre 1970:

Uncountably categorical fields are algebraically closed

Macintyre 1970:

Uncountably categorical fields are algebraically closed

Informally:

"uncountably categorical structure" means

"it has best possible description by means of logic"

Simple algebraic groups over a.c. fields are uncountably categorical.

For example, $SL_n(\mathbb{C})$ are uncountably categorical.

Zilber's Conjecture (c. 1975)

Simple $\aleph_1$-categorical groups are simple algebraic groups over a.c. fields.

Altınel, B, Cherlin:

If a simple uncountably categorical group G contains an infinite elementary abelian 2-group

then G is a Chevalley group over an a.c. field of char 2.

Altınel, B, Cherlin:

If a simple uncountably categorical group G contains an infinite elementary abelian 2-group

then G is a Chevalley group over an a.c. field of char 2.

In particular, simple algebraic groups over algebraically closed fields of characteristic 2 are Chevalley groups.

Schanuel's Conjecture:

In $\mathbb{C}$,

$$\text{tranc.deg.}(x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x^n}) \geqslant \text{rk}_{\mathbb{Q}}(x_1, \ldots, x_n)$$

Example. Take $x_1 = \ln 2$, then

$$\text{tranc.deg.}(\ln 2, e^{\ln 2}) \geqslant \text{rk}_{\mathbb{Q}}(\ln 2)$$

or

$$\text{tranc.deg.}(\ln 2, 2) \geqslant 1$$

Hence $\ln 2$ is transcendental.

Boris Zilber:

- Took language $+, \cdot, \exp$ of a field with formal exponentiation

  $\exp : K^+ \to K^\times, \quad \exp(x+y) = \exp \cdot \exp y$

- chose axioms for a.c. field of characteristic 0 with exponentiation;
- some other nice properties;
- made sure all of above holds in $\mathbb{C}$ with standard exponentiation.
- Added Schanuel's Conjecture as an axiom;
- proved that axioms are consistent and hence have a model.

Finally, proved that in cardinality continuum such model is **unique** up to isomorphism.

Let us call Boris Zilber's field $\mathbb{B}$.

Do you have any doubts that $\mathbb{B} = \mathbb{C}$?

A million dollar question

All mathematics is divided in three parts:

- *cryptography (paid for by the CIA, the KGB and the like),*
- *hydrodynamics (supported by manufacturers of atomic submarines) and*
- *celestial mechanics (financed by the military and by other institutions dealing with missiles, such as NASA).*

Cryptography has generated number theory, **algebraic geometry over finite fields***, algebra, combinatorics and computers.*

Vladimir Arnold

Indeed, why there is so much fuss around finite fields?

Why is modern cryptography based on finite fields?

Why does mathematics reuse the same objects?

More specific: why is the range of structures usable in computer-based cryptography so narrow?

This last question has very obvious practical implications.

Imagine: that the proverbial

- little green men from Mars stole a satellite from its orbit;
- they attempt to analyze a microchip for the Diffie-Hellman key exchange.
- Would they be surprised to discover that humans are using finite fields and elliptic curves?

Diffie-Hellman key exchange

- Alice and Bob choose a big finite abelian group G and an element $g \in G$.
- Alice selects her *secret* integer a, computes g^a and sends the value to Bob.
- Similarly, Bob selects his *secret* integer b and sends g^b.
- Alice raises the element g^b received from Bob to her secret exponent a and computes $(g^b)^a$.
- Similarly, Bob computes $(g^a)^b$.
- Since $(g^b)^a = g^{ab} = (g^a)^b$, the element g^{ab} is the secret shared element known only to Alice and Bob.

What do we need for the realization of this protocol?

- A cyclic group G of very large prime order p such that its elements can be presented by short (that is, of length $O(\log p)$) strings of 0s and 1s.
- The group operation has to be quick, in any case, better than in $O(\log^2 p)$ basic operations of the computer.
- The *discrete logarithm problem* of finding the secret exponent a from g and g^a has to be very difficult for all elements $g \neq 1$ in G; in any case, it should not allow a solution by a polynomial time algorithm.

- This should preferably be done for an arbitrary prime p, or for sufficiently many primes.
- The implementation of the particular instances of the algorithm, compilation of the actual executable file for the computer (or realization of the algorithm at the hardware level in a microchip, say, in a mobile phone) should be easy and done in polynomial time of small degree in $\log p$.

Two classical ways of making cyclic groups C_p of prime order p:

- the additive group of the field of residues modulo p, $\mathbb{Z}/p\mathbb{Z}$.
- Select a prime q such that p divides $q-1$ and generate G by an element g of the multiplicative order p in the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^*$.

- In the additive group $\mathbb{Z}/p\mathbb{Z}$, the exponentiation $g \mapsto g^n$ is just multiplication by n, $g \mapsto n \cdot g$, and the Euclidean algorithm instantly solves the discrete logarithm problem.
- In $(\mathbb{Z}/q\mathbb{Z})^*$, the discrete logarithm problem is apparently hard.
- It is also conjectured to be hard in the group of points of an elliptic curve over a finite field, thus giving rise to elliptic curve cryptography.

But the group, as an abstract algebraic object, is exactly the same, the cyclic group of order p;

it is the computational realisation that matters.

How can we compare different realisations C_p?

Look at $C_p \simeq \mathbb{Z}/p\mathbb{Z}$ and $C_p \hookrightarrow (\mathbb{Z}/q\mathbb{Z})^*$.

Elements of $\mathbb{Z}/p\mathbb{Z}$ can be written as integers $0, 1, 2, \ldots, p-1$.

Given an element $g \in (\mathbb{Z}/q\mathbb{Z})^*$ of order p, we can use square-and-multiply to raise g to the power of n in $O(\log n)$ time.

$$\begin{aligned} \mathbb{Z}/p\mathbb{Z} &\to (\mathbb{Z}/q\mathbb{Z})^* \\ n &\mapsto g^n \end{aligned}$$

is an morphism of the two realisations of C_p computable in time linear in $\log p$.

We shall say that the realisation of C_p as $\mathbb{Z}/p\mathbb{Z}$ is *reducible* to its realisation as $C_p \hookrightarrow (\mathbb{Z}/q\mathbb{Z})^*$.

To compute the inverse isomorphism means to solve the discrete logarithm problem.

Therefore *morphisms* of computational realisations for C_p are homomorphisms computable in polynomial time.

Three principal classes of commutative algebraic groups over finite fields:

- unipotent—$\mathbb{Z}/p\mathbb{Z}$,
- tori —$(\mathbb{Z}/q\mathbb{Z})^*$, and
- abelian varieties—elliptic curves.

They can all be built from finite fields, by simple constructions with fast computer implementations.

My million dollar question is

> *Are there polynomial time computational ralisations for cyclic groups of prime order* $($*which therefore have a chance to meet memory and speed requirements of computer-based cryptography*$)$ *and which cannot be reduced, within polynomial space/time constraints, to one of the known types?*

Notice that non-reducibility to $\mathbb{Z}/p\mathbb{Z}$ would mean that the discrete logarithm problem cannot be solved in polynomial time, giving a chance to meet security requirements as well.

I accept that this question is likely to be out of reach of modern mathematics.

The answer will definitely involve some serious advances in complexity theory.

If the answer is “yes”,

(especially if you invent something which is quicker than elliptic curve systems)

you can patent your invention and make your million dollars.

But I expect the answer “no”.

Indeed, why are finite fields so special?

Any hints?

Consider arbitrary finite algebras:

finite sets with some operations of arbitrary nature.

Associate with every algebra $\mathbb{A}$ with ground set A the set of *all* **verbal functions** on A:

all functions from A to A expressible by combination of basic algebraic operations of $\mathbb{A}$, with elements from A used as constant "coefficients".

Verbal equivalence:

Two algebras are **verbally equivalent** if they have the same ground set and the same sets of verbal functions.

In particular, every basic algebraic operation of the first algebra is expressed in terms of the operations of the second algebra, and vice versa.

If we ignore the computational complexity, verbally equivalent algebras are in a sense mutually interchangeable.

Given a finite algebra $\mathbb{A}$, a verbal function $f(x)$ in a single variable induces a map from A to A.

Since A is finite, either $f(x)$ is a permutation of A, or it maps A to a strictly smaller subset $B \subset A$.

In the second case, some iteration

$$g(x) = f(f(\cdots f(x) \cdots))$$

is an idempotent map:

$$g(g(x)) = g(x)$$

for all x.

The idempotency of g allows us to "deform" and squeeze the basic operations of $\mathbb{A}$ to the set $C = g[A]$.

If, for example, $T(\cdot, \cdot, \cdot)$ was an operation of $\mathbb{A}$, $T' = g(T(\cdot, \cdot, \cdot))$ becomes an operation on C.

Adding all verbal operations of $\mathbb{A}$ which preserve C, we get a new algebra $\mathbb{C}$, a *retract* of $\mathbb{A}$.

What happens if $\mathbb{A}$ has no proper retracts and is therefore unsimplifiable?

Peter Pálfy: If $\mathbb{A}$ has at least three elements we have a dichotomy:

1. Every verbal function defined in terms of $\mathbb{A}$ effectively depends on just one variable.

   Then all verbal functions on A are permutations, and

   $\mathbb{A}$ is verbally equivalent to a set A with an action of a finite group G, where action of each element $g \in G$ is being treated as an unary operation.

2. But if $\mathbb{A}$ is sufficiently rich and has verbal functions which really depend on at least two variables,

   the result is astonishing:

   $\mathbb{A}$ *is verbally equivalent to a vector space over a finite field!*