(Non)definability in finitely generated rings (ASL 2011 session on definability throughout mathematical logic in honor of Leo Harrington)

Thomas Scanlon [1]

UC Berkeley

25 March 2011

[1] Joint work with Matthias Aschenbrenner

The problem stated informally

We know from Gödel's work that the class of definable sets in $(\mathbb{N}, +, \times, 0, 1)$ is very rich.

One might expect that mathematical structures which are closely connected to arithmetic would share this feature.

We shall restrict attention to the class of finitely generated commutative rings and ask to what extent is the theory of definability in a given finitely generated ring $(R, +, \times, \{r\}_{r \in R})$ as complicated as that of arithmetic over the natural numbers.

An example to put the question into context

Theorem (Lagrange)

An integer is nonnegative if and only if it is the sum of four squares of integers.

Corollary

$\mathbb{N}$ *is definable in* $(\mathbb{Z}, +, \times, 0, 1)$

Consequently, every set $S \subseteq \mathbb{N}^m$ which is definable in arithmetic is also definable in $\mathbb{Z}$.

An easier observation

The usual presentation of $\mathbb{Z}$ as differences of natural numbers (implemented in any number of ways) shows that $\mathbb{Z}$ is interpretable in $\mathbb{N}$. Thus every $\mathbb{Z}$-definable set $S \subseteq \mathbb{Z}^n$ corresponds to an $\mathbb{N}$-definable set.

For instance, we might identify the nonnegative integers with the even natural numbers and the negative integers with the odd natural numbers and thereby transfer the ring operations to piecewise defined polynomials on $\mathbb{N}^2$.
For example, addition on $\mathbb{Z}$ may be given by the folllowing rule.

$$x +_{\mathbb{Z}} y := \begin{cases} x + y & \text{if } x \text{ and } y \text{ are both even} \\ x + y + 1 & \text{if } x \text{ and } y \text{ are both odd} \\ x - y + 1 & \text{if } x \geq y \text{ and } x \not\equiv y \pmod 2 \\ y - x & \text{if } y > x \text{ and } x \not\equiv y \pmod 2 \end{cases}$$

Hence, via this identification, a definable set $X \subseteq \mathbb{Z}^n$ may be seen as an $\mathbb{N}$-definable set in $\mathbb{N}^n$.

The problem, somewhat more formally stated

From the example, we saw that $\mathbb{N}$ and $\mathbb{Z}$ have essentially the same theory of definability because the structures are bi-interpretable. We are thus led to the following question.

Question

For which finitely generated rings R are the structures $(\mathbb{N}, +, \times, 0, 1)$ and $(R, +, \times, 0, 1)$ bi-interpretable?

A solution?

- Clearly, if a structure is to interpret $\mathbb{N}$, it had better be infinite.
- The natural numbers are rigid, but not every finitely generated ring is rigid (consider $R = \mathbb{Z}[\sqrt{2}]$ with the map $a + b\sqrt{2} \mapsto a - b\sqrt{2}$). Thus, we relax the problem allowing for parameters to be used for the interpretations.
- Using Gödel coding of sequences, it is fairly easy to see that the polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$ may be interpreted (even recursively) in $\mathbb{N}$. Likewise, since $\mathbb{Z}[x_1, \ldots, x_n]$ is noetherian, the equivalence relation on $\mathbb{Z}[x_1, \ldots, x_n]$ coming from any ideal is definable. Hence, every finitely generated ring is interpretable in $\mathbb{N}$.
- From theorems of B. Poonen (on the definability of algebraic dependence) and J. Robinson and R. Robinson on the definability/interpretability of $\mathbb{N}$ in number rings (global fields of positive characteristic, respectively), every infinite finitely generated ring interprets $\mathbb{N}$.
- A. Khelif has announced that every infinite finitely generated commutative ring is bi-interpretable with $\mathbb{N}$.

Qualifying Khelif's solution

There are some problems with Khelif's solution.

- Formally, his proof depends on a published result (due to me) whose proof is incorrect. (Though if one looks into my proof, one sees that the error can be circumvented to obtain the statement Khelif requires.)
- Khelif's use of the term "bi-interpretable" is non-standard. For the theorem he aims to prove, namely that for any finitely generated commutative ring R there is a sentence ϕ_R in the language of rings for which $R \models \phi_R$ and if S is a finitely generated ring with $S \models \phi_R$, then $R \cong S$, can be achieved using his weaker bi-interpretation notion.

Indeed, G. Sabbagh has recently announced that Khelif has produced a complete proof taking into account the two issue mentioned above. In related work, in his thesis, E. Naziazeno has implemented Khelif's strategy using simpler results from algebra to find the sentences isolating the isomorphism type of individual finitely generated rings.

Bi-interpretations

Definition

An interpretation of the $\mathscr{L}'$-structure B in the $\mathscr{L}$-structure A consists of an $\mathscr{L}$-definable set $X \subseteq A^n$ (for some natural number n) and a surjective function $I : X \to B$ so that for any $\mathscr{L}'$-definable set $Y \subseteq B^m$ the preimage $(I^{\times m})^{-1} Y$ is $\mathscr{L}$-definable. A pair of interpretations I of B in A and J of A in B is a bi-interpretation if the graph of the composite $J \circ I$ is $\mathscr{L}$-definable and the graph of $J \circ I$ is $\mathscr{L}'$-definable.

Remark

A bi-interpretation may be regarded as an equivalence of categories between the category of $\mathscr{L}$-definable sets in A and the $\mathscr{L}'$-definable sets in B. (See, Makkai and Reyes in LNM 611)

Interpretations without a bi-interpretation

Proposition

The ring $R = \mathbb{Z} \times \mathbb{Z}$ interprets $\mathbb{N}$ and is interpretable with $\mathbb{N}$, but is not bi-interpretable with $\mathbb{N}$.

Proof.

- Since $\mathbb{N}$ and $\mathbb{Z}$ are bi-interpretable, we may consider them interchangeably.
- Clearly, R is interpretable in $\mathbb{Z}$ as $\mathbb{Z}^2$ with coordinatewise operations.
- If we fix the parameter $e := (1, 0)$, then $\mathbb{Z} \cong R/(e)$ and the quotient of a ring by a definable ideal is clearly interpretable.
- If R were bi-interpretable with $\mathbb{N}$, then the diagonal would be definable in R.
- By the Feferman-Vaught theorem, the only definable (even with parameters) sets in R are finite Boolean combinations of boxes $A \times B$ where A and B are definable in $\mathbb{Z}$.

Products in general

The proof of non-bi-interpretability with $\mathbb{N}$ we have sketched for $\mathbb{Z} \times \mathbb{Z}$ generalizes to any commutative ring R which can be expressed as $A \times B$ with A and B both infinite.

The dual numbers

Question

Is $R := \mathbb{Z}[\epsilon]/(\epsilon^2)$ bi-interpretable with $\mathbb{N}$?

As with $\mathbb{Z} \times \mathbb{Z}$, we may interpret R in $\mathbb{Z}$ as $\mathbb{Z}^2$ with coordinatewise addition and multiplication defined by the rule

$$(x_1, x_2) \cdot (y_1, y_2) := (x_1 y_1, x_1 y_2 + y_1 x_2)$$

Likewise, $\mathbb{Z} \cong R/(\epsilon)$ so that $\mathbb{Z}$ is interpretable in R.

Proposition

R is (parametrically) bi-interpretable with $\mathbb{Z}$ if and only if $\mathbb{Z}$ is definable as a subring of R.

Definability and derivatives

Definition

Let A be a commutative ring. By a derivation on A we mean an additive map $\partial : A \to A$ which satisfies the Leibniz rule $\partial(xy) = x\partial(y) + \partial(x)y$.

Proposition

The integers are parametrically definable in $\mathbb{Z}[\epsilon]/(\epsilon^2)$ if and only if for every model ${}^*\mathbb{Z}$ of the theory of $\mathbb{Z}$ every derivation on ${}^*\mathbb{Z}$ is trivial.

Proof.

- Every ultrapower of $\mathbb{Z}[\epsilon]/(\epsilon^2)$ takes the form ${}^*\mathbb{Z}[\epsilon]/(\epsilon^2)$ where ${}^*\mathbb{Z} \succeq \mathbb{Z}$.
- For any commutative ring A the automorphisms of $A[\epsilon]/(\epsilon^2)$ fixing ϵ are exactly those of the form $a + b\epsilon \mapsto \sigma(a) + (\sigma(b) + \partial(a))\epsilon$ where $\sigma : A \to A$ is an automorphism and $\partial : A \to A$ is a derivation.
- Apply Beth Definability: Such an automorphism would preserve the interpretation of $\mathbb{Z}$ just in case ∂ is trivial.

Do derivations on nonstandard models of arithmetic exist? (Hilbert-Waring)

Theorem

For any positive integer k there is a number $B = B(k)$ for which every nonnegative integer may be expressed as a sum of at most $B(k)$ k^{th} powers of integers.

Derivatives are highly divisible

Corollary

If ${}^*\mathbb{Z} \succeq \mathbb{Z}$, $\partial : {}^*\mathbb{Z} \to {}^*\mathbb{Z}$ is a derivation and $a \in {}^*\mathbb{Z}$, then $\partial(a)$ is divisible by every positive integer.

Proof.

- Since $\partial(-a) = -\partial(a)$ we may assume that $a \geq 0$.
- Let $k \in \mathbb{Z}_+$. Then by the Hilbert-Waring theorem we may write

$$a = \sum_{i=1}^{B(k)} b_i^k$$

- Differentiating,

$$\partial(a) = \sum_{i=1}^{B(k)} k b_i^{k-1} \partial(b_i) = k\left(\sum_{i=1}^{B(k)} b_i^{k-1} \partial(b_i)\right)$$

Theorem

There is an elementary extension ${}^*\mathbb{Z} \succeq \mathbb{Z}$ possessing a nontrivial derivation $\partial : {}^*\mathbb{Z} \to {}^*\mathbb{Z}$.

Remark

The construction, which I will not describe in detail here, proceeds via an ultralimit argument. One starts with some elementary extension $Z \succeq \mathbb{Z}$, constructs nontrivial derivations $\partial_S : S \to S$ on the finitely generated subrings, and then averages these to obtain a derivation $\partial : Z \to Z^{\mathscr{U}}$ to some ultrapower. The requisite ${}^*\mathbb{Z}$ and ∂ comes as an ultralimit of this construction.

Corollary

$\mathbb{Z}[\epsilon]/(\epsilon^2)$ is not bi-interpretable with $\mathbb{Z}$, even parametrically.

Statement of full theorem

The ideas required to understand $\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z}[\epsilon]/(\epsilon^2)$ underlie the full resolution.

Theorem

Let R be a finitely generated (but infinite) commutative ring. Let $N = \{a \in R \ : \ (\exists n \in \mathbb{Z}_+) a^n = 0\}$ be the nilradical of R. Then R is bi-interpretable (parametrically) with $\mathbb{N}$ if and only if $\mathrm{ann}_{\mathbb{Z}}(N) := \{n \in \mathbb{Z} \ : \ (\forall x \in N) nx = 0\}$ is nontrivial and R has exactly one non-maximal minimal prime ideal.

The end of today's session in Leo's honor