Defining the integers in the rationals

NYWIMN Conference

May 2, 2008

Carol Wood

Department of Mathematics and Computer Science
Wesleyan University

Defining $\mathbb{Z}$ in $\mathbb{Q}$: Outline

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Gödelian phenomena

Several results concerning undecidability of the first order theory of an algebraic structure M have been obtained via a link to Gödel's Incompleteness Theorem.
Gödel showed that the first order theory of the natural numbers $\mathbb{N}$ is undecidable.
For example, suppose we can show that (a copy of) $\mathbb{N}$, including its addition and multiplication, is definable in M.
A decision procedure for the theory of M would then relativize to a decision procedure for the first order theory of $< \mathbb{N}, +, \cdot >$. But Gödel showed this to be impossible.
Thus no decision procedure exists for the theory of M.

Definability

What do we mean by "first order definable"? Logicians know; for others, examples can help.
Start with the ring of integers $\mathbb{Z}$.
Let's see that $\mathbb{N}$ is definable in $\mathbb{Z}$.
First, a way *NOT* to do it:
$x \in \mathbb{N} \leftrightarrow x = 0 \vee x = 1 \vee x = 2 \vee \ldots$

No infinite disjunctions!

The first-order definition we give involves some basic number theory.
Lagrange's Theorem to the rescue:
$x \in \mathbb{N} \leftrightarrow \exists a \exists b \exists c \exists d (x = a^2 + b^2 + c^2 + d^2)$

Continuing, with a minor rewrite

$$x \in \mathbb{N} \leftrightarrow \exists a \exists b \exists c \exists d (0 = x - (a^2 + b^2 + c^2 + d^2))$$

Note also that this definition is of a particularly nice form, involving only existential quantifiers.
Thus we have an equation in four variables such that an integer x is a natural number exactly when the equation has a solution in $\mathbb{Z}$ for those four variables.
This says that $\mathbb{N}$ is Diophantine in $\mathbb{Z}$.

Squares

As a second example, we define the set of squares in $\mathbb{Z}$.
x is a square $\leftrightarrow \exists a(a^2 = x))$.
Thus the set of squares is also Diophantine.

Examples of definable subsets of $\mathbb{N}$:

- the set of numbers x which are not powers of 2:
  $\exists a \exists b(x = (2a + 3)b)$
- the set of all composite x
  $\exists a \exists b(x = (a + 2)(b + 2))$

Nonsquares

The set of nonsquares is definable in $\mathbb{Z}$:
x is a nonsquare $\leftrightarrow \forall a(a^2 \neq x)$.
This definition is not optimal, in that it is not Diophantine.

H10

Related to the question of definability is the matter of the complexity of the definition.

In 1900 Hilbert asked whether one could decide whether a Diophantine equation over the integers has an integral solution.

The first order assertion that a given equation has a solution is an existential formula.

Gödel's Incompleteness Theorem does not settle this question. It may be possible to decide the existential part of an undecidable theory; an example of this behavior would be interesting!

We will return to H10 later...

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Representing integers

Theorem (Julia Robinson, 1948). The ring of integers $\mathbb{Z}$ is definable in the field of rationals $\mathbb{Q}$.

The proof uses facts about which rationals can be represented by certain quadratic forms.

Recall that a quadratic form $f = a_1X_1^2 + a_2X_2^2 + \cdots + a_sX_s^2$ with coefficients in a field K is said to *represent* 0 *in* K just in case the equation $f(X) = 0$ has a solution $X \in K^s, X \neq 0$.

Underlying the ingredients of JR's proof is a fundamental local-global principle:

Hasse-Minkowski Theorem. A quadratic form f with integer coefficients represents zero in $\mathbb{Q}$ if and only if f represents 0 mod n for every positive integer n and f represents 0 in $\mathbb{R}$.

We take $r \in \mathbb{Q}$ and write $r = \frac{n}{d}$ with $d \geq 1$ and such that n and d have no common divisors > 1.
Using forms which can only represent r when d is not divisible by certain primes, JR was able to pick out those r for which d must equal 1.

- $f = X^2 + Y^2 - pZ^2$, where p is a prime integer, $p \equiv 3 \bmod 4$.
  FACT. f represents $2 + pr^2$ in $\mathbb{Q} \leftrightarrow 2 \nmid d$ and $p \nmid d$
- $g = X^2 + qY^2 - pZ^2$, where p and q are odd primes with $p \equiv 1 \bmod 4$ and q *not* a square mod p.
  FACT. g represents $2 + pqr^2$ in $\mathbb{Q} \leftrightarrow p \nmid d$ and $q \nmid d$.

  The proof of both facts relies on the Hasse-Minkowski Theorem.

Picking out the integers

Let $\phi(r, y, z) = \exists a \exists b \exists c(2 + yzr^2 = a^2 + yb^2 - zc^2)$.

Think of $\phi(r, y, z)$ as saying that r can be represented in both ways described in the previous FACTS.

Let $\theta(r) = (\phi(0, y, z) \wedge \forall w(\phi(w, y, z) \rightarrow \phi(w + 1, y, z)) \rightarrow \phi(r, y, z))$.

Think of $\theta(r)$ as saying that induction applies to r.

Claim: a rational r is an integer $\leftrightarrow \forall y \forall z \theta(r)$.

By defining $\mathbb{Z}$ in $\mathbb{Q}$, JR proved that the theory of the rationals is undecidable.
This formula is complicated, involving several alternations of quantifiers, $\forall\exists\forall$
It was the best available until quite recently.

Defining $\mathbb{Z}$ in $\mathbb{Q}$

H10 was solved in the negative in the late 1960's by Matijasevich, building on previous work of Martin Davis, Hilary Putnam and Julia Robinson.

Theorem (DPRM). There is no algorithm for deciding, given a polynomial f in n variables with integer coefficients, whether $f = 0$ has an integral solution.

An auxiliary question remains open: whether one can decide solvability for any third degree polynomial. Second degree: decidable. Fourth degree: undecidable.

Note that we can formulate H10 for any ring R, simply by replacing "integer coefficients" by "coefficients in R" and "integral solution" by "solution in R".

To transfer this negative result for $\mathbb{Z}$ to another ring, it is not enough to be able to define $\mathbb{Z}$ in the ring, but it does suffice if one can define $\mathbb{Z}$ via an *existential* formula.

This has been achieved in some instances. H10 is a more subtle question than decidability of the full theory, and H10 remains open for several undecidable rings, including $\mathbb{Q}$ and finite extensions of $\mathbb{Q}$ (i.e., number fields).

Also, there are no number fields for which it is known that H10 has a positive solution for its ring of integers.

Many researchers have been involved in this fascinating enterprise, and I cannot list them all here, but will give references at the end.

Ok, one name for this crowd: Alexandra Shlapentokh, PhD NYU 1988.

Defining $\mathbb{Z}$ in $\mathbb{Q}$

In her thesis (also at Berkeley), Kirsten Eisenträger worked on various questions around H10. She gave a new proof that, given a global field k and a nonarchimedean prime $\mathfrak{p}$, the set of elements of k integral at $\mathfrak{p}$ is Diophantine.
She did this in order to provide one of two key pieces needed to settle H10 for positive characteristic cases, i.e., finite extensions of $\mathbb{F}_q(t)$.
Of note for us today is her use of division algebras, specifically quaternion algebras, which take the place of quadratic forms in earlier results along the same lines.

Quaternion algebras

Let K be a field of characteristic $\neq 2$, and let $a, b \in K^\times$.
The *quaternion algebra* over K, $H_{a,b} = H_{a,b}(K)$ is the K-algebra generated by i and j, where $i^2 = a, j^2 = b$, and $ij = k = -ji$. $H_{a,b}$ is four dimensional over K, with basis $\{1, i, j, k\}$.
most familiar case is the division algebra of real quaternions, with $K = \mathbb{R}$ and $a = b = -1$.
In general, $H_{a,b}(K)$ is either a division algebra or it is isomorphic to $M_2(K)$, all two-by-two matrices over K.

We will be interested in $H_{a,b}$ for $K = \mathbb{Q}$ and, for p prime, in $K = \mathbb{Q}_p$, the field of p-adics .

For an element $\alpha = x_1 + x_2 i + x_3 j + x_4 k$, the *reduced norm* $n(\alpha) = x_1^2 - a x_2^2 - b x_3^2 + ab x_4^2$, and the *reduced trace* $tr(\alpha) = 2x_1$.

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Crash course in the p-adics

We will think of the p-adics as follows (although much more could be said):

$$\mathbb{Q}_p = \{\Sigma_{i=k}^{\infty} a_i p^i | k \in \mathbb{Z}, 0 \leq a_k \leq p-1\}$$

Inside $\mathbb{Q}_p$ there is a subring $\mathbb{Z}_p$ of p-adic integers, namely all elements with no non-zero coefficients for negative powers of p:

$$\mathbb{Z}_p = \{\Sigma_{i=0}^{\infty} a_i p^i | 0 \leq a_k \leq p-1\}$$

We will refer to the reduction map from $\mathbb{Z}_p$ to $\mathbb{F}_p$ given by

$$red_p : \Sigma_{i=0}^{\infty} a_k p^k \longrightarrow a_0$$

.

Interlude: $\mathbb{Z}_p$ is definable in $\mathbb{Q}_p$

For $p \neq 2, \mathbb{Z}_p = \{x | \exists y (y^2 = px^2 + 1)\}$

To see this, think about what happens when you square a Laurent series with negative terms.

$\mathbb{Q}$ to $\mathbb{Q}_p$

We consider $H_{a,b} = H_{a,b}(\mathbb{Q})$; all four-dimensional central simple algebras over $\mathbb{Q}$ arise in this form.
Next we tensor $H_{a,b}$ with $\mathbb{Q}_p$ over $\mathbb{Q}$. Here we are assuming $p \neq 2$; the case $p = 2$ can be handled similarly.
One of two things occurs:

- $H_{a,b} \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong H_{a,b}(\mathbb{Q}_p)$

  This is called the ramified case.

- $H_{a,b} \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong M_2(\mathbb{Q}_p)$

  This is called the unramified, or split, case.

Overview of Poonen's definition

To define $\mathbb{Z}$ in $\mathbb{Q}$, Poonen considers the set $S_{a,b}(K)$ of all possible reduced traces of elements n $H_{a,b}(K)$ of reduced norm 1.

- When p does not ramify, all elements become traces, so $S_{a,b}(\mathbb{Q}_p) = \mathbb{Q}_p$.
- If p ramifies, the situation is more complicated, and information can be extracted when at least one of a and b is positive.

Final steps

In case $a > 0$ or $b > 0$, Hasse-Minkowski tells us that

$$S_{a,b}(\mathbb{Q}) = \mathbb{Q} \cap \bigcap_p S_{a,b}(\mathbb{Q}_p).$$

- The set of all rationals $T_{a,b}$ of a certain form occurs as the intersection of the $\mathbb{Z}_p$'s for ramified p.
- As a, b range over the positive integers, the intersection of the $T_{a,b}$'s equals $\mathbb{Z}$.

Ingredients of proof

For q a pth power, let $U_q = \{s \in \mathbb{F}_q | x^2 - sx + 1 \text{ is irreducible over } \mathbb{F}_q\}$.

- $U_q \neq \emptyset$, and for $q > 11$, $U_q + U_q = \mathbb{F}_q$.
  This requires a geometric argument, together with information about bounds on the numbers of points on curves on finite fields.
- If p is unramified, then $red_p^{-1}(U_p) \subseteq S_{a,b}(\mathbb{Q}_p) \subseteq \mathbb{Z}_p$.
  The proof uses the fact that s is a reduced trace of an element of norm 1 just in case $x^2 - sx + 1$ is the reduced characteristic polynomial of an element of $H_{a,b} \otimes \mathbb{Q}_p$.
- Let $T_{a,b} = \mathbb{Q} \cap \{s + s' + n | s, s' \in S_{a,b}, 0 \leq n \leq 2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11\}$.
  Then $T_{a,b} = \bigcap \mathbb{Z}_p$ where the intersection is taken over p ramified.
- $\bigcap_{a,b>0} T_{a,b} = \mathbb{Z}$.
  For each p one must find pairs a, b, that ramify at p. This is not hard.

Poonen's definition of $\mathbb{Z}$ in $\mathbb{Q}$:

$\psi(x) = \forall a \forall b \exists x_1 \ldots \exists x_4 \exists y_1 \ldots \exists y_4 (a + x_1^2 + x_2^2 + x_3^2 + x_4^2)(b + y_1^2 + y_2^2 + y_3^2 + y_4^2)$
$[(x_1 - ax_2^2 - bx_3^2 + abx_4^2 - 1)^2 + \prod_{n=0}^{2309}((n - x - 2x_1)^2 - 4ay_2^2 - 4by_3^2 +$
$4aby_4^2 - 4)^2] = 0.$

Remarks

The top line has the sole function of allowing one to ignore negative values of a and b.

The two universal quantifiers come from using local-global properties and it is hard to see how this approach would allow one to get down to existential-only.

It is however the first reduction in number of alternations of quantifiers in 60 years.

Notes after talk: Marker pointed out something I should have mentioned, that Rumely gave a proof of Julia Robinson's result which is considerably less "ad hoc" than hers, using local-global properties in a systematic way.

References

- K. Eisentrager, Integrality at a prime for global fields..., J. Number Theory 114 (2005), 170-181.
- B. Poonen, Characterizing integers among rational numbers with a universal existential formula, preprint (see also his article in the March 2008 Notices of the AMS)
- J. Robinson, Definability of decision problems in arithmetic, J. S. L. 14 (1949), 98-114. (See also Flath and Wagon's Monthly article of 1991, pp 812-823.
- R. Rumely, Undecidability and Definability for the Theory of Global Fields, Trans AMS 262 (1980),pp. 195-217.
- A. Shlapentokh, Hilberts Tenth Problem, Cambridge UP 2007