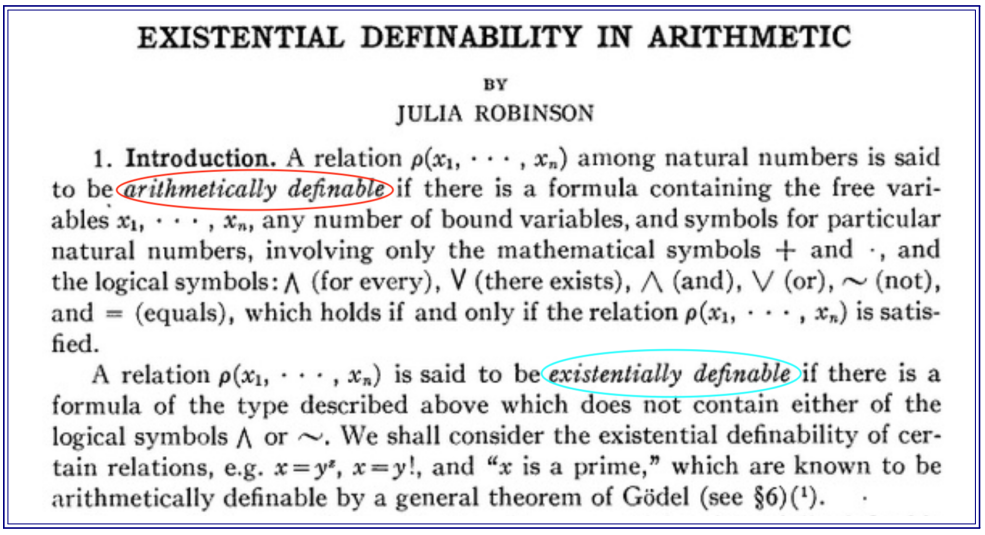
Chapter 3

Arithmetical definability

3.1 Introduction



EXISTENTIAL DEFINABILITY IN ARITHMETIC

BY

JULIA ROBINSON

1. **Introduction.** A relation $\rho(x_1, \cdots, x_n)$ among natural numbers is said to be *arithmetically definable* if there is a formula containing the free variables $x_1, \cdots, x_n$, any number of bound variables, and symbols for particular natural numbers, involving only the mathematical symbols $+$ and $\cdot$, and the logical symbols: $\bigwedge$ (for every), $\bigvee$ (there exists), $\wedge$ (and), $\vee$ (or), $\sim$ (not), and $=$ (equals), which holds if and only if the relation $\rho(x_1, \cdots, x_n)$ is satisfied.

A relation $\rho(x_1, \cdots, x_n)$ is said to be *existentially definable* if there is a formula of the type described above which does not contain either of the logical symbols $\bigwedge$ or $\sim$. We shall consider the existential definability of certain relations, e.g. $x = y^z$, $x = y!$, and "x is a prime," which are known to be arithmetically definable by a general theorem of Gödel (see §6)(1).

Figure 3.1: Arithmetical definability, as presented by Julia Robinson in 1952

3.2 The history of arithmetical definability

3.2.1 Specification of the notion "being an integer" in the arithmetic of rationals

In 1949, in her abstract "Undecidability in the arithmetic of integers and rationals and in the theory of fields" [14], Julia Robinson captures the property "being an integer" in the following manner (see also [13]):

$$\begin{aligned}\zeta \in \mathbb{Z} \quad \Longleftrightarrow \quad \zeta \in \mathbb{Q} \ \ \& \ \ \forall\, a\, \forall\, b \Big(\quad & a \in \mathbb{Q} \ \& \ b \in \mathbb{Q} \ \& \\ & \eta(a,b,0) \ \& \\ & \forall\, u \big(u \in \mathbb{Q} \ \& \ \eta(a,b,u) \implies \eta(a,b,u+1) \big) \\ \implies \quad & \\ & \eta(a,b,\zeta) \\ \Big)\,, \quad &\end{aligned}$$

where

$$\begin{aligned}\eta(a,b,w) \quad \Leftrightarrow_{\text{Def}} \quad \exists\, r\, \exists\, s\, \exists\, t \Big(\quad & r \in \mathbb{Q} \ \& \ s \in \mathbb{Q} \ \& \ \mathbb{Q}(t) \\ \& \quad & \\ & 2 + a \cdot b \cdot w^2 + b \cdot r^2 \ = \ s^2 + a \cdot t^2 \\ \Big)\,. \quad &\end{aligned}$$

An alternative characterization of integers among rational numbers is put forward by Bjorn Poonen in 2008: his specification

$$\begin{aligned}\zeta \in \mathbb{Z} \quad \Longleftrightarrow \quad & \\ \forall\, a\, \forall\, b\, \exists\, x_1\, \exists\, x_2\, \exists\, x_3\, \exists\, x_4\, \exists\, y_1\, \exists\, y_2\, \exists\, y_3 \quad & \\ (a + x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot (b + x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot \quad & \\ \Big((x_1^2 - a\, x_2^2 - b\, x_3^2 + a\, b\, x_4^2 - 1)^2 \ + \quad & \\ \textstyle\prod_{n=0}^{2309} \big((n - \zeta - 2\, x_1)^2 - 4\, a\, y_1^2 - 4\, b\, y_2^2 + 4\, a\, b\, y_3^2 - 4 \big)^2 \Big) \quad = \quad 0\,, \quad &\end{aligned}$$

(whose variables are supposed to range over rational numbers) looks intimidating, but it alternates quantifiers only once whereas the Robinson specification requires at least two quantifier alternations.[1]

[1] According to [6], the Robinson specification, once brought into prenex form, becomes

$$\forall\, a\, \forall\, b\, \exists\, x_1 \cdots \exists\, x_7\, \forall\, v_1 \cdots \forall\, v_6 \ D(\zeta,\, a, b,\, x_1, \ldots, x_7,\, v_1, \ldots, v_6) = 0$$

This new characterization was boiled down by Jochen Koenigsmann into the following (2016):

$$\begin{array}{c} \zeta \in \mathbb{Z} \iff \\ \forall\, a\, \forall\, b\, \exists\, x_1\, \exists\, x_2\, \exists\, x_3\, \exists\, x_4\, \exists\, y_1\, \exists\, y_2\, \exists\, y_3 \\ (a + x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot (b + x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot \\ \Big((x_1^2 - a\, x_2^2 - b\, x_3^2 + a\, b\, x_4^2 - 1)^2 + \\ \big((\zeta - 2\, x_1)^2 - 4\, a\, y_1^2 - 4\, b\, y_2^2 + 4\, a\, b\, y_3^2 - 4 \big)^2 \Big) \;=\; 0\,. \end{array}$$

In the paper where he proposes this, Koenigsmann also succeeds in reducing the number of universal quantifiers preceding the existential ones from two to one. He also finds that a characterization of integral among rational numbers can be put in the form

$$\zeta \in \mathbb{Z} \iff \forall\, y_1 \cdots \forall\, y_n\; D(\,\zeta,\, y_1, \ldots, y_n\,) \neq 0\,,$$

for some $D(\zeta,\, y_1, \ldots, y_n) \in \mathbb{Z}[\zeta,\, y_1, \ldots, y_n]$.

Key ideas in the Robinson specification of $\mathbb{Z}$ in $\mathbb{Q}$

Consider again the formulas

$$\begin{array}{lcll} \zeta \in \mathbb{Z} & \iff & \forall\, a\, \forall\, b \Big(& \eta(a,b,0) \;\&\; \\ & & & \forall\, u \big(\eta(a,b,u) \implies \eta(a,b,u+1) \big) \\ & & & \implies \\ & & & \eta(a,b,\zeta) \qquad\qquad \Big)\,, \\ \eta(a,b,w) & \Leftrightarrow_{\mathrm{Def}} & \exists\, r\, \exists\, s\, \exists\, t \Big(& 2 + a \cdot b \cdot w^2 + b \cdot r^2 \;=\; s^2 + a \cdot t^2 \quad \Big)\,, \end{array}$$

whose variables are supposed to range over the rationals. If $\boldsymbol{\zeta} \in \mathbb{N}$, then by induction it satisfies

$$\begin{array}{ll} \forall\, a\, \forall\, b \Big(& \eta(a,b,0) \;\&\; \\ & \forall\, u \big(\eta(a,b,u) \implies \eta(a,b,u+1) \big) \\ & \implies \\ & \eta(a,b,\zeta) \qquad\qquad \Big)\,; \end{array} \qquad (*)$$

for a particular $D \in \mathbb{Z}[\zeta,\, a, b,\, x_1, \ldots, x_7,\, v_1, \ldots, v_6]$. More cautiously (as recalled by [19, p. 69]), [4] states that Julia Robinson's definition of the rational integers $\mathbb{Z}$ in the rational numbers $\mathbb{Q}$ can be converted to a formula of the form $\forall\exists\forall\exists(F = 0)$, where the $\forall$–quantifiers run over a total of 8 variables, and where F is a polynomial.

consequently every negative integer satisfies (*) as well, because w occurs only squared in $\eta(a, b, w)$.

Next, the somewhat harder converse implication must be proved. Assuming that $\boldsymbol{\zeta} \in \mathbb{Q}$ satisfies (*), we will check that $\boldsymbol{\zeta} \in \mathbb{Z}$: as will turn out, in fact, the denominator of $\boldsymbol{\zeta}$—in lowest terms—is not divisible by any prime number, hence it must be ± 1.

By plugging 1 in place of a, and any prime $\boldsymbol{b} \equiv 3 \mod 4$ in place of b in (*), we find out that the denominator of $\boldsymbol{\zeta}$ (in lowest terms) is neither divisible by 2 nor by $\boldsymbol{b}$. Under such an instantiation, in fact, $\eta(1, \boldsymbol{b}, \mu)$ holds precisely for those $\mu \in \mathbb{Q}$ whose denominator is odd and prime to $\boldsymbol{b}$.[2] This is the case when $\mu = 0$ (whose denominator in lowest terms is ± 1); moreover, $\eta(1, \boldsymbol{b}, \mu + 1)$ holds when $\eta(1, \boldsymbol{b}, \mu)$ holds, because μ and $\mu + 1$ have the same denominator; thus, (*) triggers the conclusion $\eta(1, \boldsymbol{b}, \boldsymbol{\zeta})$.

Likewise, by plugging into (*) any prime $\boldsymbol{p} \equiv 1 \mod 4$ as b, and any odd prime $\boldsymbol{q}$ such that the Legendre symbol $\left(\frac{\boldsymbol{q}}{\boldsymbol{p}}\right)$ equals -1 as a, one gets that the denominator of $\boldsymbol{\zeta}$ is not divisible by $\boldsymbol{p}$ or by $\boldsymbol{q}$. Things are so because $\eta(\boldsymbol{q}, \boldsymbol{p}, \mu)$ holds precisely for those $\mu \in \mathbb{Q}$ whose denominator is prime to $\boldsymbol{p}$ and to $\boldsymbol{q}$. ⊣

3.2.2 Specification of the notion "being a natural number" in the arithmetic of rational integers

The property "being a natural number" is captured by the following formula (due to Raphael Mitchel Robinson, cf. [13, p. 109]):

$$a \in \mathbb{N} \iff a \in \mathbb{Z} \;\&\; \exists x \, \exists y \Big(\begin{array}{l} x \in \mathbb{Z} \;\&\; y \in \mathbb{Z} \;\&\; y \neq 0 \;\&\; \\ (x^2 - a)(x^2 - a\,y^2 - 1) = 0 \end{array} \Big).$$

When $a < 0$, in fact, neither the equation $x^2 = a$ admits any solution in $\mathbb{Z}$, nor does the equation $x^2 - a\,y^2 = 1$ under the constraint $y \neq 0$. On the other hand, if $a \geqslant 0$ and a is not a perfect square then, as is well known, the Pell equation $x^2 - a\,y^2 = 1$ admits infinitely many solutions with $y > 0$ in $\mathbb{Z}$. The following specification of slightly greater appeal has later been proposed by

[2] In [13, pp. 107–108], the propositions colored in red in this proof are derived from a general theorem due to Hasse (1923).

Zhi-Wei Sun (cf. [20, p. 210]):

$$a \in \mathbb{N} \iff a \in \mathbb{Z} \ \& \ \exists x \, \exists y \Big(\quad x \in \mathbb{Z} \ \& \ y \in \mathbb{Z} \ \& \ y \neq 0 \ \& \ x^2 = (4\,a+2)\,y^2 + 1 \quad \Big) .$$

In either of these specifications of $\mathbb{N}$, the inequality $y \neq 0$ can be replaced by an equality, at the price of using more existential variables; in fact, since

$$y \in \mathbb{Z} \implies \Big(\ y \neq 0 \iff \exists u \, \exists v \Big(\ u \in \mathbb{Z} \ \& \ v \in \mathbb{Z} \ \& \ y = (2\,u-1)\,(3\,v-1) \ \Big) \Big)$$

holds (cf. [26, p. 209] by Shih-Ping Tung),[3] we have

$$a \in \mathbb{N} \iff a \in \mathbb{Z} \ \& \ \exists x \, \exists u \, \exists v \Big(\quad x \in \mathbb{Z} \ \& \ u \in \mathbb{Z} \ \& \ v \in \mathbb{Z} \ \& \ x^2 = (4\,a+2)\,(2\,u-1)^2\,(3\,v-1)^2 + 1 \quad \Big) .$$

The nuisance of the negative literal $y \neq 0$ can be avoided altogether by resorting to Lagrange's four-square theorem, which gives us:

$$a \in \mathbb{N} \iff \exists w \, \exists x \, \exists y \, \exists z \quad w^2 + x^2 + y^2 + z^2 = a \, ,$$

where variables are supposed to range over $\mathbb{Z}$. As remarked in [8, p. 253], this specification can be ameliorated:

$$a \in \mathbb{N} \iff \exists x \, \exists y \, \exists z \quad x + x^2 + y^2 + z^2 = a \, .$$

The following specification of comparable appeal had been proposed by R. M. Robinson in [17]:

$$a \in \mathbb{N} \iff \exists x \, \exists y \, \exists z \quad x^2 + y^2 + z^2 = 4\,a + 1 \, .$$

[3] It is easy to see that 0 cannot be represented in the form $(2\,u-1)\,(3\,v-1)$ whereas 2, -1, and all odd positive integers—and, hence, all prime numbers—can. Moreover, $(2\,u-1)\,(3\,v-1)\,(2\,u'-1)\,(3\,v'-1) = \big(2\,(u+u'-2\,u\,u')-1\big)\,\big(3\,(v+v'-3\,v\,v')-1\big)$. In consequence of this and of the four-square theorem, $a \neq 0$ can be stated over $\mathbb{Q}$ as:

$$(\exists d, u, u_1, u_2, u_3, u_4, v, v_1, v_2, v_3, v_4) \Big(\ d \cdot a = (2 \cdot u - 1) \cdot (3 \cdot v - 1) \ \& \ \big(u = 0 \vee u \cdot u = 1 + u_1 \cdot u_1 + u_2 \cdot u_2 + u_3 \cdot u_3 + u_4 \cdot u_4 \big) \ \& \ (v = 0 \vee v \cdot v = 1 + v_1 \cdot v_1 + v_2 \cdot v_2 + v_3 \cdot v_3 + v_4 \cdot v_4) \Big) .$$

In either case, the clue to the three-variable existential definition of $\mathbb{N}$ in $\mathbb{Z}$ is Legendre's three-square theorem.

A curious two-variable arithmetic definition of $\mathbb{N}$ in $\mathbb{Z}$ also appears in [17]:

$$a \in \mathbb{N} \iff \exists\, x\, \exists\, y \Big(\quad a = y^2 \quad \vee \quad \big(y^3 = y + a\, y\, x^2 \quad \& \quad y^3 \neq y \big) \quad \Big).$$

Here, too, a disturbing negative literal appears.

3.2.3 Arithmetical definition of addition in terms of multiplication and either successor or 'less than'

It emerges from [13] that, in the arithmetic of $\mathbb{Z}$, the biimplication

$$a + b = c \iff \mathtt{S}\,(\mathtt{S}\,(c) \cdot \mathtt{S}\,(c) \cdot \mathtt{S}\,(b \cdot \mathtt{S}\,(a))) \;=\; \mathtt{S}\,(\mathtt{S}\,(a) \cdot \mathtt{S}\,(c)) \cdot \mathtt{S}\,(b \cdot \mathtt{S}\,(c))\,;$$

holds and, consequently, so do

$$\begin{aligned} a + b = c \iff \exists\, p\, \exists\, q\, \exists\, r\, \exists\, s\, \exists\, t \Big(\quad & \mathtt{S}\,(q \cdot q \cdot r) = s \cdot t \quad \& \quad \mathtt{S}\,(a) = p \quad \& \\ & \mathtt{S}\,(c) = q \quad \& \quad \mathtt{S}\,(b \cdot p) = r \quad \& \\ & \mathtt{S}\,(p \cdot q) = s \quad \& \quad \mathtt{S}\,(b \cdot q) = t \quad \Big), \end{aligned}$$

and

$$\begin{aligned} a + b = c \iff \exists\, p\, \exists\, q\, \exists\, r\, \exists\, s\, \exists\, t\ \forall\, u \Big(\quad & q \cdot q \cdot r < s \cdot t \quad \& \\ & \neg(\, q \cdot q \cdot r < u \quad \& \quad u < s \cdot t\,) \quad \& \\ & a < p \quad \& \\ & \neg(\, a < u \quad \& \quad u < p\,) \quad \& \\ & c < q \quad \& \\ & \neg(\, c < u \quad \& \quad u < q\,) \quad \& \\ & b \cdot p < r \quad \& \\ & \neg(\, b \cdot p < u \quad \& \quad u < r\,) \quad \& \\ & p \cdot q < s \quad \& \\ & \neg(\, p \cdot q < u \quad \& \quad u < s\,) \quad \& \\ & b \cdot q < t \quad \& \\ & \neg(\, b \cdot q < u \quad \& \quad u < t\,) \\ \Big). \end{aligned}$$

Recent sitography

- http://www-math.mit.edu/~poonen/papers/ae.pdf
- http://www.math.umd.edu/~laskow/713/Spring17/carolslides.pdf
  http://websupport1.citytech.cuny.edu/faculty/vgitman/nywimn/nywimn2/files/carolslides.pdf
- http://www-math.mit.edu/~poonen/papers/nonsquares.pdf
- https://www.cs.auckland.ac.nz/~nies/Students/YanKRobinsonEssay.pdf
- https://annals.math.princeton.edu/wp-content/uploads/Koenigsmann.pdf

3.3 . . . TO BE CONTINUED. . .