Mathematical Institute
Slovak Academy of Sciences, Bratislava

Preprint 23/1996

Ivan Korec

Definability of addition from multiplication and neighbourhood relation and some related results

July 15, 1996

PREPRINT SERIES

DEFINABILITY OF ADDITION FROM MULTIPLICATION AND NEIGHBOURHOOD RELATION AND SOME RELATED RESULTS

IVAN KOREC, BRATISLAVA

ABSTRACT. We shall show that the operation $+$ on the set $\mathbb{N}$ of nonnegative integers is definable from $\times$ and the neighbourhood relation $\mathrm{Neib} = \{(x,y) \in \mathbb{N}^2 \mid |x-y| = 1\}$. The same result is proved for the divisibility relation $|$ instead of $\times$. If we replace $\mathbb{N}$ by the set $\mathbb{Z}$ of all integers then $+$ is definable from Neib and $\times$ but it is not definable from Neib and divisibility, and even from Neib, divisibility and the constant 1. Similar results for some commutative rings are presented.

1. INTRODUCTION

The basic structure of arithmetic is $\langle \mathbb{N}; +, \times \rangle$ where $\mathbb{N}$ denotes the set of nonnegative integers and $+$, $\times$ denote addition and multiplication on $\mathbb{N}$. (In formulas the symbol $\times$ will be often replaced by a dot or deleted. Fixed exponents will denote repeated multiplication.) The relations and operations on $\mathbb{N}$ which are first order definable in this structure are called *arithmetical*. By definability we shall always understand first order definability. (We use the classical first order predicate calculus with equality, e.g. by [Sh]. However, relational and functional symbols will usually have fixed meaning; it will depend only on the base set of the considered structure.) Almost all operations and relations on $\mathbb{N}$ known from mathematical praxis are arithmetical. (Concrete counterexamples can be found mainly in metamathematics. Of course, when we consider classes of relations or functions they very often contain also non-arithmetical elements.) For example, 0, 1, $<$, $\leq$ in their usual meaning are arithmetical. We shall deal also with $\mathbf{s}$ (the successor) and $|$ (the divisibility relation); they also are arithmetical. As more complicated examples we can present the exponentiation, the set of primes, the prime counting function $\pi(x)$ and Gödel's coding function $\beta(x, y, z)$; even these examples take very low position in so called arithmetical hierarchy.

There were many attempts to replace the operations $+$, $\times$ by simpler ones so that the definability power of the obtained structure is the same as that of $\langle \mathbb{N}; +, \times \rangle$. A pioneer work in this area was made J. Robinson [Ro] who (among other results) replaced $+$ by $\mathbf{s}$ and simultaneously $\times$ by $|$. In other words, she was able to define (by first order formulas) $+$, $\times$ in the structure $\langle \mathbb{N}; \mathbf{s}, | \rangle$. From definability point

---

1991 *Mathematics Subject Classification.* Primary 03F30, Secondary 11A99.
Key words and phrases. Definability, Undecidability, Neighbourhood relation.
This work was supported by Grant 2/1227 of Slovak Academy of Sciences.

of view, $\mathbf{s}$ is strictly weaker than $+$ and the relation $|$ is strictly weaker than $\times$. Nevertheless, $\mathbf{s}$, $|$ taken together are as strong as $+$, $\times$. (This concerns first order definability. By second order formulas, where variables for sets and relations may be used, $+$ is definable from $\mathbf{s}$.)

We shall continue in this direction, and we shall try to replace $\mathbf{s}$ by the relation Neib defined as follows:

$$\mathrm{Neib}(x,y) \iff y=\mathbf{s}(x) \vee x=\mathbf{s}(y). \tag{1.1}$$

Notice that Neib is the least symmetrical relation which contains the graph of $\mathbf{s}$ (i.e., its symmetrical closure). We shall call it neighbourhood relation from the obvious reasons. The following theorem shows that Neib is strictly weaker than $\mathbf{s}$ with respect to the definability. Nevertheless, it possesses an important property of $\mathbf{s}$.

Theorem 1.1. (i) Every natural number is definable in $\langle \mathbb{N}; \mathrm{Neib}\, \rangle$.

(ii) The successor $\mathbf{s}$ is not definable in $\langle \mathbb{N}; \mathrm{Neib}\, \rangle$.

Proof. (i) We can define

$$x=0 \iff \exists! y\ \mathrm{Neib}(x,y), \qquad x=1 \iff \mathrm{Neib}(x,0),$$
$$x=2 \iff \mathrm{Neib}(x,1) \wedge x \neq 0, \qquad \dots$$

(ii) Let us consider a structure $\langle \mathbb{N}^*; \mathbf{s}^* \rangle$ elementarily equivalent but not isomorphic to $\langle \mathbb{N}; \mathbf{s} \rangle$ (i.e., a nonstandard model of the theory of successor). Let the operation $\mathbf{s}^+$ on $\mathbb{N}^*$ coincide with $\mathbf{s}^*$ on the standard part, and coincide with the predecessor function on the non-standard part of $\mathbb{N}^*$. The neighbourhood relations defined from $\mathbf{s}^*$, $\mathbf{s}^+$ coincide. It is impossible to define (by the same formula which defines $\mathbf{s}$ from Neib) two distinct functions from the same relation. $\square$

Since Neib is strictly weaker than $\mathbf{s}$ (in the sense of definability) a question arises in which structures $\mathbf{s}$ can be replaced by Neib (with preserving definability power). It will be answered positively for the structures $\langle \mathbb{N}; \mathbf{s}, \times \rangle$ and $\langle \mathbb{N}; \mathbf{s}, | \rangle$.

Further we shall consider structures with the base set $\mathbb{Z}$, i. e. the set of all (rational) integers. The meaning of $+$, $\times$, $|$, $\mathbf{s}$, Neib, $<$ is extended to $\mathbb{Z}$ in the obvious way. For example, we define $\mathbf{s}(x) = 1 + x$, and then Neib by (1.1). The symbol $\mathbb{N}$ will be used also as a unary predicate symbol; $\mathbb{N}(x)$ means that x is nonnegative. In the structure $\langle \mathbb{Z}; +, \mathbb{N} \rangle$ (and in every structure where $+$, $\mathbb{N}$ are definable) a bijection F between the whole set $\mathbb{Z}$ and the set $\mathbb{N}$ is definable. Indeed, we can easily define 0, 1 and then F e.g. by the formula

$$y = F(x) \iff \mathbb{N}(x) \wedge y = x + x \vee \neg\mathbb{N}(x) \wedge y + 1 + x + x = 0.$$

We can extend the notion of arithmetical sets to subsets of $\mathbb{Z}$ as follows: A set $X \subseteq \mathbb{Z}$ is said to be arithmetical if the set $F(X) = \{F(y) \mid y \in X\}$ is arithmetical. (Of course, a set $X \subseteq \mathbb{N}$ is arithmetical in the new sense if if and only if it is arithmetical in the original sense.) Similarly we can use F to extend the notions of arithmetical functions and relations. It can be proved that a function or relation on $\mathbb{Z}$ is arithmetical if and only if it is definable in in the structure $\langle \mathbb{Z}; +, \times \rangle$. (The substantial idea in the proof is application of Four squares theorem to define $\mathbb{N}$.) Hence $\langle \mathbb{Z}; +, \times \rangle$ plays for the set $\mathbb{Z}$ a similar role as $\langle \mathbb{N}; +, \times \rangle$ plays for $\mathbb{N}$.

D. Richard [Ri] extended the above mentioned result of J. Robinson to the set $\mathbb{Z}$ of arbitrary integers. He proved that $+$, $\times$ are definable in the structure $\langle \mathbb{Z}; \mathbf{s}, | \rangle$ (all relations and operations are extended to $\mathbb{Z}$ in the usual way). We shall show that $\mathbf{s}$ can be replaced (again with preserving definability power) by Neib in the structure $\langle \mathbb{Z}; \mathbf{s}, \times \rangle$ and it cannot be replaced in $\langle \mathbb{Z}; \mathbf{s}, | \rangle$. We shall also prove a stronger result that $+$ is nor definable in the structure $\langle \mathbb{Z}; \mathrm{Neib}, |, 1 \rangle$.

A difference between the situations with some "additive" structures with the base sets $\mathbb{N}$ and $\mathbb{Z}$ can be seen from the graphs in Figure 1. Here $\mathcal{A} \longrightarrow \mathcal{B}$ denote that every relation (or operation or constant) which is definable in $\mathcal{A}$ is also definable in $\mathcal{B}$; hence $\mathcal{B}$ is in some sense stronger than $\mathcal{A}$. (We compare only structures with the same base set.) A double line substitutes arrows in both directions, i.e. equivalence of structures from definability point of view. Arrows which can be obtained by transitivity are not drawn. We can see that the graph for the base set $\mathbb{Z}$ (on the right) is much more complex than the graph for the base set $\mathbb{N}$. (Moreover, joining another constants to some of the structures on $\mathbb{Z}$ may give further structures, not equivalent with the displayed ones. By the first part of Theorem 1.1 joining constants is unnecessary in the displayed structures on $\mathbb{N}$.)

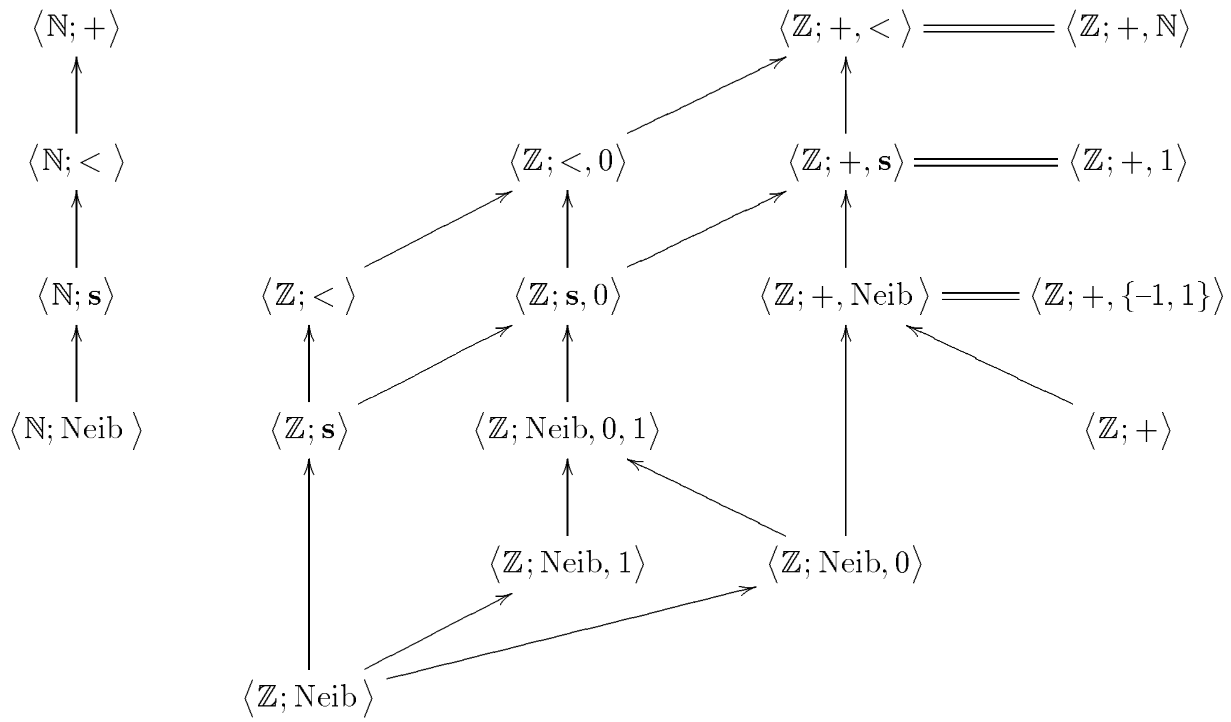

Figure 1. Comparison of definability power of some structures.

In the last section we shall also consider similar and related questions for some other rings, in particular for the rings of residue classes modulo n.

2. DEFINABILITY OF + IN THE STRUCTURES $\langle \mathbb{N}; \mathrm{Neib}, \times \rangle$ AND $\langle \mathbb{N}; \mathrm{Neib}, | \rangle$.

Lemma 2.1. *$x \in \mathbb{N}$ is a sum of three odd squares if and only if $x \equiv 3 \pmod 8$.*

Proof. Let $x \in \mathbb{N}$ and $x \equiv 3 \pmod 8$. By [Na] x is a sum of three squares. Since every square is congruent with 0 or 1 modulo 4 all three squares must be odd. For the converse we can use that every odd square is congruent with 1 modulo 8. □

Theorem 2.2. *Addition + is definable in $\langle \mathbb{N}; \mathrm{Neib}, \times \rangle$.*

Proof. We shall use the idea from [Ro] that for positive integers x, y, z

$$z = x + y \iff (1 + xz)(1 + yz) = 1 + z^2(1 + xy); \tag{2.1}$$

the cases with 0 can be easily expressed separately. However, we immediately obtain only the relation

$$\mathrm{PM}(x, y, z) \iff z = x + y \lor z = |x - y|. \tag{2.2}$$

We can define PM by the formula

$$\begin{aligned}\mathrm{PM}(x, y, z) \iff & z \neq 0 \land \exists u, v, w\big(\mathrm{Neib}(4xz, u) \land \mathrm{Neib}(4yz, v) \land \\ & \qquad\qquad \land \mathrm{Neib}(4xy, w) \land \mathrm{Neib}(uv, 4z^2 w)\big) \lor \\ & \lor z = 0 \land x = y.\end{aligned} \tag{2.3}$$

Indeed, if we understand PM by the previous formula then the latest formula is true. We shall show the implication $\Longleftarrow$ for $z \neq 0$. If $\mathrm{Neib}(a, b)$ then $b = a \pm 1$ (for $a = 0$ the minus sign cannot occur, but we shall not pay attention to that now). Hence the main part concerning $z \neq 0$ of the formula above states

$$u = 4xz \pm 1, \qquad v = 4yz \pm 1, \qquad w = 4xy \pm 1, \qquad uv = 4z^2 w \pm 1,$$

hence $(4xz \pm 1)(4yz \pm 1) = 4z^2(4xy \pm 1) \pm 1$, and therefore

$$16xyz^2 \pm 4xz \pm 4yz \pm 1 = 16xyz^2 \pm 4z^2 \pm 1$$

for some choice of signs. The congruence modulo 4 show that the last signs on both sides must coincide. If we remove the equal members on both sides and divide by $4z$ we obtain $\pm x \pm y = \pm z$ which is equivalent with $|x \pm y| = z$, i.e. $\mathrm{PM}(x, y, z)$. The case $z = 0$ and the implication $\Longrightarrow$ are easy.

Now we shall define the congruence classes modulo 4 (as unary predicates). We shall use the notation $x \equiv_4 i$ for them $(0 \leq i < 4)$. It is easy to define two of them:

$$x \equiv_4 0 \iff \exists y(4y = x), \qquad x \equiv_4 2 \iff \exists y, z\big(\mathrm{Neib}(2y, z) \land x = 2z\big).$$

For the other two congruence classes classes we define at first odd squares and two congruence classes modulo 8 (denoted similarly as above):

$$\begin{aligned}\mathrm{OddSq}(x) &\iff \exists y, z\big(\mathrm{Neib}(2y, z) \land x = z^2\big), \\ x \equiv_8 4 &\iff \exists y, z\big(\mathrm{Neib}(2y, z) \land x = 4z\big), \\ x \equiv_8 3 &\iff \exists u, v, w, y, z\big(\mathrm{OddSq}(u) \land \mathrm{OddSq}(v) \land \mathrm{OddSq}(w) \land \\ & \qquad \mathrm{PM}(u, v, y) \land y \equiv_4 2 \land \mathrm{PM}(y, w, x) \land \mathrm{PM}(x, 1, z) \land z \equiv_8 4\big).\end{aligned}$$

In the latest formula Lemma 2.1 was used. By PM we expressed $y = |u \pm v|$, but for the minus sign we would have $4|y$, which is excluded. Therefore $y = u + v$, and $y \equiv 2 \pmod 8$. Further, using z we expressed $x \equiv 3$ or $5 \pmod 8$, which exclude the minus sign in $x = |y \pm w|$; therefore together we expressed $x = y + w = u + v + w$.

Now we can define

$$\begin{aligned} x \equiv_4 1 &\iff \exists y\big(y \equiv_8 3 \wedge \mathrm{PM}(y, 2, x)\big), \\ x \equiv_4 3 &\iff \exists y\big(y \equiv_4 1 \wedge \mathrm{PM}(y, 2, x)\big). \end{aligned}$$

Finally, we can define

$$\begin{aligned} z = x + y \iff & \exists u, v\big(\mathrm{Neib}(4x, u) \wedge u \equiv_4 3 \wedge \mathrm{Neib}(4y, v) \wedge v \equiv_4 1 \wedge \mathrm{PM}(u, v, 4z)\big) \vee \\ & \vee x = 0 \wedge z = y. \end{aligned}$$

Indeed, in the substantial part of the presented formula we have $u = 4x - 1$, $v = 4y + 1$, and $|u \pm v| = 4z$. Since $4 \not| u - v$ plus sign holds in the latest equality, and hence $4z = u + v = 4x + 4y$, i.e. $z = x + y$. $\square$

Lemma 2.3. *Multiplication* $\times$ *is definable in* $\langle \mathbb{N}; \mathrm{Neib}, | \rangle$.

Proof. We shall follow the idea from [Ro]; however, since we deal with Neib instead of $\mathbf{s}$ some new considerations are necessary. Let $\perp$ denote the coprimeness relation and let $\circ$ denote the least common multiple. Both $\perp$, $\circ$ are definable from $|$, and hence we can freely use them. Notice that for relatively prime integers $\circ$ coincides with the product $\times$.

The operation $\times$ can be defined by the formula:

$$\begin{aligned} z = x \times y \iff & x = 0 \wedge z = 0 \vee y = 0 \wedge z = 0 \vee x = 1 \wedge z = y \vee y = 1 \wedge z = x \vee \\ & \vee x \neq 0 \wedge x \neq 1 \wedge y \neq 0 \wedge y \neq 1 \wedge \\ & \wedge \forall x_1, y_1, w\Big(x_1 \perp x \wedge y_1 \perp y \wedge w \perp x_1 \wedge w \perp y_1 \wedge x_1 \perp y_1 \wedge \\ & \wedge \exists u\big(w|u \wedge \mathrm{Neib}(x_1 \circ x, u)\big) \wedge \exists u\big(w|u \wedge \mathrm{Neib}(y_1 \circ y, u)\big) \implies \\ & \qquad \implies \exists u\big(w|u \wedge \mathrm{Neib}(u, z \circ x_1 \circ y_1)\big)\Big). \end{aligned}$$

To prove that, assume $z = x \times y$ at first; we have to prove the right-hand side of the defining formula. The cases $x \le 1$, $y \le 1$ are easy; let $x > 1$, $y > 1$. Take arbitrary x_1, y_1, w which satisfy the coprimeness conditions. Then

$$\exists u\big(w|u \wedge \mathrm{Neib}(x_1 \circ x, u)\big)$$

means $x_1 x \equiv \pm 1 \pmod w$, and similarly we obtain $y_1 y \equiv \pm 1 \pmod w$. (The formulas with $\pm$ ought to be understood here as disjunctions.) Then we have $x_1 y_1 x y \equiv \pm 1 \pmod w$ and hence $x_1 y_1 z \equiv \pm 1 \pmod w$. The latest formula means $w|(x_1 y_1 z \pm 1)$, which can be rewritten as the consequent in the defining formula.

Now assume that the right-hand side of the defining formula holds; we have to prove $z = xy$. We shall again assume $x > 1$, $y > 1$. Let us choose $w > xy + z$

coprime with both x, y. There are x_1, y_1 relatively prime to x, y, z and to each other such that

$$x_1 x \equiv 1 \pmod{w}, \qquad y_1 y \equiv 1 \pmod{w}. \tag{2.4}$$

Hence by the consequent of the right-hand side of the defining formula we have $zx_1y_1 \equiv \pm 1 \pmod{w}$. Multiplying by xy and using the congruences (2.4) we obtain $z \equiv \pm xy \pmod{w}$. Since $w > z + xy$ the latest congruence does not hold for the sign $-$, hence we have $z \equiv xy \pmod{w}$, and then $z = xy$. $\square$

Theorem 2.4. *The operations* $+$, $\times$ *are definable in the structure* $\langle \mathbb{N}; \mathrm{Neib}, | \rangle$.

Proof. It suffice to combine Lemma 2.3 and Theorem 2.2. $\square$

By the classical result of K. Gödel the first order theory of $\langle \mathbb{N}; +, \times \rangle$ is undecidable. Therefore Theorem 2.2 and Theorem 2.4 immediately imply:

Corollary 2.5. *The first order theories of* $\langle \mathbb{N}; \mathrm{Neib}, \times \rangle$ *and* $\langle \mathbb{N}; \mathrm{Neib}, | \rangle$ *are undecidable.*

3. The case of arbitrary integers

At first we prove that $\mathbb{N}$ can be replaced by $\mathbb{Z}$ in Theorem 2.2.

Theorem 3.1. *The operation* $+$ *is definable in the structure* $\langle \mathbb{Z}; \mathrm{Neib}, \times \rangle$.

Proof. We can define $\mathbb{N}$ (as a unary predicate) by the formula

$$\mathbb{N}(x) \iff \exists y (x = y^2) \vee \exists y, z \big(yz \neq 0 \wedge \mathrm{Neib}(xy^2, z^2)\big).$$

Let $\mathbb{N}(x)$ (i.e. $x \geq 0$) at first. If x is a square then the first member of the right-hand side is valid. If x is not a square then the equation $z^2 - xy^2 = 1$ (i.e., Pell's equation with the unknowns z, y) has a solution in positive integers. For this solution obviously $\mathrm{Neib}(xy^2, z^2)$, i.e. the second member of the right-hand side holds. So we have proved the implication $\Longrightarrow$.

Now we shall prove $\Longleftarrow$. The situation with the first member is obvious. Let the second member of the right-hand side hold. Then $x = \frac{z^2 \pm 1}{y^2} \geq 0$ (because $z^2 \geq 1$), and hence $\mathbb{N}(x)$.

Now we can define the graph of the addition on $\mathbb{N}$, i.e. the relation

$$\mathrm{Add}_{\mathbb{N}} = \big\{ (x, y, z) \in \mathbb{N}^3 \ \big| \ z = x + y \big\} \tag{3.1}$$

by the method used in Theorem 2.2. The constants 0, 1 cannot be defined like in Theorem 1.1, but they can be defined from the multiplication in the usual way. Then we can use Neib to define any integer as a constant, e.g.:

$$x = -1 \iff \mathrm{Neib}(x, 0) \wedge x \neq 1, \qquad x = 2 \iff \mathrm{Neib}(x, 1) \wedge x \neq 0.$$

The main necessary modification is that we must explicitly relativize the variables to the set $\mathbb{N}$. For example, we shall define PM in its original sense, i.e.

$$\mathrm{PM} = \big\{ (x, y, z) \in \mathbb{N}^3 \ \big| \ z = x + y \vee z = |x - y| \big\};$$

we shall not use (2.2). To do that, (2.3) must be modified as follows

$$\begin{aligned}\mathrm{PM}(x,y,z) \iff & \mathbb{N}(x) \wedge \mathbb{N}(y) \wedge \mathbb{N}(z) \wedge z \neq 0 \wedge \\ & \wedge \exists u,v,w\big(\mathbb{N}(u) \wedge \mathbb{N}(v) \wedge \mathbb{N}(w) \wedge \\ & \qquad \wedge \mathrm{Neib}(4xz,u) \wedge \mathrm{Neib}(4yz,v) \wedge \\ & \qquad \wedge \mathrm{Neib}(4xy,w) \wedge \mathrm{Neib}(uv,4z^2w)\big) \vee \\ & \vee z = 0 \wedge \mathbb{N}(x) \wedge x = y.\end{aligned}$$

The definitions of $\equiv_4 i$ and $\equiv_8 i$ ought to be treated similarly (we do not extend them to $\mathbb{Z}$ in this proof). After that we can define

$$\begin{aligned}\mathrm{Add}_{\mathbb{N}}(x,y,z) \iff & \exists u,v\big(\mathrm{Neib}(4x,u) \wedge u \equiv_4 3 \wedge \mathrm{Neib}(4y,v) \wedge \\ & \qquad \wedge v \equiv_4 1 \wedge \mathrm{PM}(u,v,4z)\big) \vee \\ & \vee x = 0 \wedge \mathbb{N}(y) \wedge z = y;\end{aligned}$$

relativization of variables in the first member of the right-hand side is already hidden in its atomic subformulas.

We can also define unary $-$ by the formula $-x = x \times (-1)$ (where -1 is treated as constant). Using unary $-$ and $\mathrm{Add}_{\mathbb{N}}$ we can easily define the addition on $\mathbb{Z}$. We must only express usual high-school rules for determining the absolute value and the sign of the result. $\square$

Later we show that $\mathbb{N}$ cannot be replaced by $\mathbb{Z}$ in Theorem 2.4. Now we shall investigate definability in the structure $\langle \mathbb{Z}; \mathrm{Neib}, | \rangle$. To formulate the results, we introduce the following notation

$$\begin{aligned}\mathrm{AbsA} &= \big\{(x,y,z) \in \mathbb{Z}^3 \;\big|\; |x| + |y| = |z|\big\},\\ \mathrm{AbsM} &= \big\{(x,y,z) \in \mathbb{Z}^3 \;\big|\; |xy| = |z|\big\},\\ \mathrm{AbsNb} &= \big\{(x,y) \in \mathbb{Z}^2 \;\big|\; \mathrm{Neib}(|x|,|y|)\big\}.\end{aligned}$$

The introduced relations correspond in an obvious sense to (the graphs of) the addition and the multiplication on $\mathbb{N}$ and to the neighbourhood relation on $\mathbb{N}$. (The relation associated to $|$ by the same way would be $|$ again; therefore we did not introduce it.)

Theorem 3.2. *The unary operation $-$ and the relations* AbsA, AbsM, AbsNb *are definable in the structure* $\langle \mathbb{Z}; \mathrm{Neib}, | \rangle$.

Proof. The constant 0, the relation of associateness $\sim$ and the unary operation $-$ can be defined from $|$ by the formulas

$$x = 0 \iff \forall y\,(y|x), \qquad x \sim y \iff x|y \wedge y|x,$$
$$y = -x \iff y \sim x \wedge (x \neq 0 \implies y \neq x).$$

After that, AbsNb can be defined by the formula

$$\mathrm{AbsNb}(x,y) \iff \mathrm{Neib}(x,y) \vee \mathrm{Neib}(x,-y).$$

The relation $\sim$ is a congruence relation of the structure $\langle \mathbb{Z}; \mathrm{AbsNb}, | \rangle$, and the corresponding factor structure is isomorphic to $\langle \mathbb{N}; \mathrm{Neib}, | \rangle$. Therefore we can follow the proof of Lemma 2.3, and define AbsM. After that we can follow the proof of Theorem 2.2, and define AbsA. We shall not give all technical details but only some comments to them. We cannot define constants and functions; we have to define suitable predicates instead of them. For example, we cannot define the constant 4 but we can define a unary predicate symbol for $\{4, -4\}$. An important auxiliary predicate is

$$\mathrm{AbsPM} = \ \big\{(x, y, z) \in \mathbb{Z}^3 \ \big| \ |z| = |x| + |y| \vee |z| = \big||x| - |y|\big|\big\}.$$

In its definition we can use the idea of the formula (2.3). However, we shall need more bounded variables: besides u, v, w we shall need auxiliary variables corresponding to the composed terms which occur in (2.3) and to (some) their subterms. The reason is that we have to use the predicate AbsM instead of the operation $\times$. $\square$

Theorem 3.1 and Theorem 3.2 tell us that the structure $\langle \mathbb{N}; +, \times \rangle$ is *interpretable* in every of the structures $\langle \mathbb{Z}; \mathrm{Neib}, \times \rangle$ and $\langle \mathbb{Z}; \mathrm{Neib}, | \rangle$. (From Theorem 3.3 we need here only statements about AbsA and AbsM. Informally, we can translate any formula concerning $\langle \mathbb{N}; +, \times \rangle$ into a formula concerning the mentioned structures.) Therefore we have:

Corollary 3.3. *The first order theories of* $\langle \mathbb{Z}; \mathrm{Neib}, \times \rangle$ *and* $\langle \mathbb{Z}; \mathrm{Neib}, | \rangle$ *are undecidable.*

Now we shall show some undefinability results, in particular we shall prove that $\mathbb{N}$ cannot be replaced by $\mathbb{Z}$ in Theorem 2.4.

Theorem 3.4. *The operation* $\mathbf{s}$ *is not definable in the structure* $\langle \mathbb{Z}; \mathrm{Neib}, | \rangle$.

Proof. We shall use an automorphism argument. Let us consider the bijection $x \mapsto -x$. It preserves Neib and $|$, hence it is an automorphism of the considered structure. However, it does not preserve $\mathbf{s}$, hence $\mathbf{s}$ cannot be definable. $\square$

Remark. We followed the argument used by D. Richard in [Ri] to prove that $\mathbf{s}$ is not definable in $\langle \mathbb{Z}; +, | \rangle$.

Now we shall prove a strenghtheness of Theorem 3.4 where the constant 1 will be joined to the considered structure. A nice property of the new structure is that all integers are definable in it as constants. However, the property also causes that the automorphism argument cannot be applied to the new structure. Nevertheless, it can be applied to a nonstandard model.

Lemma 3.5. *The unary relation* $\mathbb{N}$ *is not definable in the structure* $\langle \mathbb{Z}; \mathrm{Neib}, |, 1 \rangle$.

Proof. Let us consider an elementary extension $\langle \mathbb{Z}^*; \mathrm{Neib}^*, |^*, 1, \mathbb{N}^* \rangle$ of the structure $\langle \mathbb{Z}; \mathrm{Neib}, |, 1, \mathbb{N} \rangle$. (I.e., the later structure is a proper substructure of the former, and they are elementarily equivalent. It can be constructed e.g. as an ultrapower.) Let us define the bijection $f : \mathbb{Z}^* \to \mathbb{Z}^*$ as follows

$$f(x) = \begin{cases} x & \text{if } x \in \mathbb{Z} \\ -x & \text{if } x \in \mathbb{Z}^* \setminus \mathbb{Z} \end{cases}$$

Informally, f changes the signs of all infinite (or: nonstandard) elements and preserves the signs of all finite (or: standard) elements. Then f is an automorphism of $\langle \mathbb{Z}^*; \mathrm{Neib}^*, |^*, 1\rangle$ but it does not preserve $\mathbb{N}^*$. Therefore $\mathbb{N}^*$ is not definable in $\langle \mathbb{Z}^*; \mathrm{Neib}^*, |^*, 1\rangle$, and then also $\mathbb{N}$ is not definable in $\langle \mathbb{Z}; \mathrm{Neib}, |, 1\rangle$ $\square$

Theorem 3.6. *The operation $+$ is not definable in the structure $\langle \mathbb{Z}; \mathrm{Neib}, |, 1\rangle$.*

Proof. If $+$ is definable then also $\mathbf{s}$ would be definable (by the formula $\mathbf{s}(x) = x+1$). Then by [Ri] both $+$, $\times$, and therefore also $\mathbb{N}$, would be definable. However, by Lemma 3.5 $\mathbb{N}$ is not definable. $\square$

The reason for nondefinability in the above theorems was that it is impossible to distinguish nonnegative integers. We can see that also from Theorem 3.7, where $\mathbb{N}$ is joined explicitly to the structure.

Theorem 3.7. *The operations $+$, $\times$ are definable in the structures $\langle \mathbb{Z}; \mathrm{Neib}, |, \mathbb{N}\rangle$.*

Proof. We can apply Theorem 3.2 to define 0, AbsA, AbsM. Then we can define

$$\begin{aligned} z = x \times y \iff & \mathrm{AbsM}(x,y,z) \wedge \\ & \wedge \big(z \neq 0 \implies \big(\mathbb{N}(z) \iff (\mathbb{N}(x) \iff \mathbb{N}(y))\big)\big). \end{aligned}$$

Now we can apply Theorem 3.1 or (more suitable) we can define $+$ by a similar (but longer) formula. As we mentioned in the proof of Theorem 3.1 we only need to express some high-school rules. We shall omit further details. $\square$

Remark. The relation $\mathbb{N}$ need not be given so explicitly. For example, $+$, $\times$ are definable also in the structures $\langle \mathbb{Z}; \mathrm{Add}_{\mathbb{N}}, |\rangle$, $\langle \mathbb{Z}; \mathrm{Neib}_{\mathbb{N}}, |\rangle$, $\langle \mathbb{Z}; \mathrm{AbsNb}, |_{\mathbb{N}}\rangle$, where $\mathrm{Add}_{\mathbb{N}}$ is given by (3.1), and $\mathrm{Neib}_{\mathbb{N}}$, $|_{\mathbb{N}}$ are restrictions of Neib, $|$ to the set $\mathbb{N}$. The operations $+$, $\times$ are also definable in the structure $\langle \mathbb{Z}; \mathrm{Neib}_{\mathbb{N}}, |\rangle$; however, the author conjectures that they are not definable in the structure $\langle \mathbb{Z}; \mathrm{Neib}, |_{\mathbb{N}}\rangle$.

4. The general case of commutative rings with identity

In every ring $\mathcal{R} = \langle R; +, \times, 1\rangle$ with identity we can define the "successor" operation $\mathbf{s}(x) = 1 + x$ and then also Neib by (1.1). (Of course, the term "neighbourhood relation" is not so transparent as when used for $\mathbb{N}$ or $\mathbb{Z}$.) Analogously as in the previous sections we shall try to replace $+$ be Neib. Before investigating Neib we shall give some results about $\mathbf{s}$.

Theorem 4.1. *Let $\mathcal{R} = \langle R; +, \times, 1\rangle$ be a nontrivial commutative ring with identity. Then the formula*

$$z \neq 0 \implies \big(z = x + y \iff (1+xz)(1+yz) = 1 + z^2(1+xy)\big) \tag{4.1}$$

is true in $\mathcal{R}$ if and only if $\mathcal{R}$ is an integrity domain.

Proof. ("Nontrivial" means to contains at least two elements.) Notice that (4.1) contains (2.1) as the consequent. If we consider the trivial case $z = 0$ separately we could deal with (2.1) instead of (4.1) in what follows.

Validity of (4.1) for integrity domains was mentioned in [Ro] (and it can be easily verified). If $\mathcal{R}$ is not an integrity domain then there are nonzero $u, v \in R$

such that $uv = 0$. Then a counterexample for (1.1) is $(x, y, z) = (v, u, u)$. Indeed, the right-hand side of (2.1) is equivalent with $z(x + y - z) = 0$, i. e. with $uv = 0$ in our case. However, $u \neq v + u$. $\square$

Hence the classical Tarski-Robinson formula (2.1) cannot be used to define $+$ from $\mathbf{s}$ in arbitrary commutative rings with identity. Nevertheless, we can prove:

Theorem 4.2. *Let $\mathcal{R} = \langle R; +, \times, 1\rangle$ be a commutative unitary ring and let $\mathbf{s}$ be the unary operation on R defined by $\mathbf{s}(x) = 1 + x$ for all $x \in R$. Then the operation $+$ is definable in the structure $\langle R; \mathbf{s}, \times\rangle$.*

Proof. The idea is to write the right-hand part of (2.1) twice (in a conjunction), for the ordered triple (x, y, z) and for the ordered triple $(1 + x, y, 1 + z)$. Then it is equivalent with the conjunction of the equations

$$z(x + y - z) = 0, \qquad (1 + z)(x + y - z) = 0. \tag{4.2}$$

Instead of dividing the first equation by z we shall subtract it from the second one, and we obtain $x + y - z = 0$. The defining formula can be

$$\begin{aligned} z = x + y \iff & \mathbf{s}(x \times z) \times \mathbf{s}(y \times z) = \mathbf{s}\big((z \times z) \times \mathbf{s}(x \times y)\big) \wedge \\ & \wedge\, \mathbf{s}(\mathbf{s}(x) \times \mathbf{s}(z)) \times \mathbf{s}(y \times \mathbf{s}(z)) = \mathbf{s}\big((\mathbf{s}(z) \times \mathbf{s}(z)) \times \mathbf{s}(\mathbf{s}(x) \times y)\big). \end{aligned}$$

If we replace $\mathbf{s}$ by its definition and use a less formal notation we can write it as

$$\begin{aligned} z = x + y \iff & (1 + xz) \cdot (1 + yz) = 1 + z^2 \cdot (1 + xy) \wedge \\ & \wedge \big(1 + (1 + x) \cdot (1 + z)\big) \cdot \big(1 + y \cdot (1 + z)\big) = \\ & \qquad = 1 + (1 + z)^2 \cdot \big(1 + (1 + x) \cdot y\big). \quad \square \end{aligned}$$

Now we shall consider the relation Neib in various rings. To formulate the results easily we define:

Definition 4.3. *Let $\mathcal{R} = \langle R; +, \times, 1\rangle$ be a ring with identity. We shall say that addition can be replaced by the neighbourhood relation in $\mathcal{R}$ if the the operation $+$ is definable in the structure $\langle R; \mathrm{Neib}, \times\rangle$, where* Neib *is the binary relation on R defined by*

$$\mathrm{Neib}(x, y) \iff y = 1 + x \vee x = 1 + y \qquad \textit{for all } x, y \in R.$$

Theorem 4.4. *Addition can be replaced by the neighbourhood relation in the following rings:*

1. *every commutative ring with identity of characteristic 2;*
2. *every field (and also every division ring);*
3. *the ring of residue classes modulo n, for every $n > 1$.*

Proof. Let $\mathcal{R} = \langle R; +, \times, 1\rangle$ be a ring with identity. We shall separately consider the cases listed in the theorem.

(1) If $\mathcal{R}$ is commutative and its characteristic is 2 (i.e. if $1+1=0$) then for every $x \in R$ the elements $x+1$, $x-1$ coincide, hence the operation $\mathbf{s}$ can be defined, and we can apply Theorem 4.2.

(2) Let $\mathcal{R}$ be a field (or a division ring; we shall not need commutativity of $\times$). For pairwise distinct $x, y, z \in R$ we have

$$z = x + y \iff \exists u, v\big(xu = y \wedge \mathrm{Neib}(u,v) \wedge z = xv\big) \wedge \\ \wedge\, \exists u, v\big(yu = x \wedge \mathrm{Neib}(u,v) \wedge z = yv\big).$$

Indeed, let the right-hand side hold. Its first member gives

$$z = yv = y \cdot (u \pm 1) = yu \pm y = x \pm y,$$

i.e. $z \in \big\{x+y, x-y\big\}$. Analogously the second member gives $z \in \big\{y+x, y-x\big\}$. (The necessary values of u, v in the first and in the second member may be different.) If the characteristic of $\mathcal{R}$ is 2 then $x+y = x-y$, and hence obviously $z = x+y$. From now on let the characteristic of $\mathcal{R}$ be distinct from 2. We have $x - y \neq y + x$ because otherwise $y + y = 0$, $y = 0$, and then $x = 0$ (by the second member), $x = y$. We also have $x - y \neq y - x$ because otherwise $x = y$. Therefore $z \neq x - y$, and hence $z = x + y$. The other implication is obvious.

The above formula does not cover the cases $x = 0$, $y = 0$, $x = y$. However, it is not difficult to complete these cases. For $x = y$ (and $1 + 1 \neq 0$) we state $z = 2x$, where 2 is defined as in the proof of Theorem 1.1.

(3) If $\mathcal{R}$ is the ring of residue classes modulo $n > 1$ then we can define 0, 1 at first. After that we can define 2, 3, ... , $n-1$ similarly as 2 was defined in the proof of Theorem 1.1. So every element can be defined (as a constant). Since $\mathcal{R}$ is finite every operation on R (hence +, in particular) can be defined. (The presented solution is not uniform: the defining formula depends on n.) □

REFERENCES

[Mo] L. J. Mordell, *Diophantine equations*, Academic Press, London and New York, 1969.

[Na] W. Narkiewicz, *Classical problems in number theory*, PWN, Warsaw, 1986.

[Ro] J. Robinson, *Definability and decision problems in arithmetic*, Journal of Symbolic Logic **14** (1949), no. 2, 98-114.

[Ri] D. Richard, *Answer to a problem raised by J. Robinson: the arithmetic of positive or negative integers is definable from successor and divisibility*, Journal of Symbolic Logic **50** (1985), 927-935.

[Sh] J. R. Shoenfield, *Mathematical logic*, Addison-Wesley, 1967.

MATHEMATICAL INSTITUTE, SLOVAK ACADEMY OF SCIENCES,
ŠTEFÁNIKOVA 49, 81473 BRATISLAVA, SLOVAKIA

E-mail address: korec@savba.sk

This preprint series was founded in 1996. Its purpose is to present manuscripts of submitted or unpublished papers and reports of fellows of the Mathematical Institute of the Slovak Academy of Sciences in Bratislava and its Košice branch. The authors are fully responsible for the content of the preprints. Postal addresses:

Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
SK–814 73 Bratislava
SLOVAKIA

Tel./Fax (+421 7) 5249 7316

Mathematical Institute
Slovak Academy of Sciences
Grešákova 6
SK–040 01 Košice
SLOVAKIA

Tel./Fax (+421 95) 6228291

PostScript files of preprints are available at WWW address:
`http://www.mat.savba.sk/preprints`

Latest preprints of the series:

23/1996 *Ivan Korec*: Definability of addition from multiplication and neighbourhood relation and some related results

22/1996 *Ivan Korec*: Open problems more or less related to generalized Pascal triangles

21/1996 *Sylvia Pulmannová*: On connections among some orthomodular structures

20/1996 *Pekka Lahti, Sylvia Pulmannová*: Coexistent observables and effects in quantum mechanics

19/1996 *Ivan Korec*: Definability of arithmetical operations from Pascal's triangle modulo n and arithmetical functions

18/1996 *Ivan Korec*: Undecidability and uniform definability in classes of structures related to Pascal's triangles modulo n

17/1996 *Beloslav Riečan*: Probability theory on some ordered structures

16/1996 *Beloslav Riečan*: Weak observables in MV algebras

15/1996 *Anatolij Dvurečenskij, Hee Sik Kim*: On connections between BCK-algebras and difference posets

14/1996 *Anatolij Dvurečenskij, Karl Svozil*: Product of partition logics, orthoalgebras and automata

13/1996 *Robin L. Hudson, Sylvia Pulmannová*: Chaotic expansion of elements of the universal enveloping algebra of a Lie algebra associated with a quantum stochastic calculus

12/1996 *Sylvia Pulmannová*: Congruences in partial abelian semigroups

11/1996 *Karol Nemoga, Štefan Schwarz*: An explicit description of the set of all normal bases generators of a finite field

10/1996 *Ján Jakubík*: Subdirect product decompositions of MV-algebras

9/1996 *Ivan Korec*: Reversibility in generalized Pascal triangles and binary reversibility in one-dimensional cellular automata

8/1996 *Jozef Bobok, Milan Kuchta*: X-minimal patterns and generalization of Sharkovskiĭ's theorem

7/1996 *Jarmila Hedlíková, Sylvia Pulmannová*: Generalized difference posets and orthoalgebras

6/1996 *Ján Borsík, Roman Frič*: Pointwise convergence fails to be strict

5/1996 *Miroslav Ploščica*: Affine completions of distributive lattices

4/1996 *Ján Haluška*: Equal temperament and Pythagorean tuning: a geometrical interpretation in the plane

3/1996 *Winfried Just, Peter Vojtáš*: On matrix rapid filters

(continued on inside back cover)

2/1996 *Anatolij Dvurečenskij*: Fuzzy set representations of some quantum structures

1/1996 *Miloslav Duchoň, Beloslav Riečan*: On the product of semigroup valued measures