

INTERPRETING THE PROJECTIVE HIERARCHY IN EXPANSIONS OF THE REAL LINE

PHILIPP HIERONYMI AND MICHAEL TYCHONIEVICH

ABSTRACT. We give a criterion when an expansion of the ordered set of real numbers defines the image of $(\mathbb{R}, +, \cdot, \mathbb{N})$ under a semialgebraic injection. In particular, we show that for a non-quadratic irrational number α , the expansion of the ordered $\mathbb{Q}(\alpha)$ -vector space of real numbers by \mathbb{N} defines multiplication on \mathbb{R} .

1. INTRODUCTION

The main technical result is the following generalization of [4, Theorem 1.1].

Theorem A. Let \mathcal{R} be an expansion of the ordered set $(\mathbb{R}, <)$. If \mathcal{R} defines an open interval $U \subseteq \mathbb{R}$, a closed and discrete set $D \subseteq \mathbb{R}_{\geq 0}$, and functions $f : D \rightarrow \mathbb{R}$ and $g : \mathbb{R}^3 \times D \rightarrow D$ such that

- (i) $f(D)$ is dense in U ,
- (ii) for every $a, b \in U$ and $d, e \in D$ with $a < b$ and $e \leq d$

$\{c \in \mathbb{R} : g(c, a, b, d) = e\} \cap (a, b)$ has non-empty interior,

then \mathcal{R} defines every subset of D^n and every open subset of U^n for every $n \in \mathbb{N}$.

Hence a structure \mathcal{R} that satisfies the assumptions of Theorem A defines the image of $(\mathbb{R}, +, \cdot, \mathbb{N})$ under a semialgebraic injection. The theory of such a structure is undecidable.

The significance of Theorem A comes from the fact that it is applicable outside the setting of expansions of the ordered *field* of real numbers. In particular, Theorem A allows us to settle some open questions about expansions of the additive group of real numbers. The most significant is the following answer to questions raised by Chris Miller. A real number is called non-quadratic if it is not the solution to a quadratic equation with rational coefficients.

Theorem B. Let $\alpha \in \mathbb{R}$ be a non-quadratic irrational number and let $f : \mathbb{R} \rightarrow \mathbb{R}$ be the function that maps x to αx . Then $(\mathbb{R}, <, +, \mathbb{N}, f)$ defines multiplication on \mathbb{R} .

Note that the sets $\alpha\mathbb{N}$ and $\alpha^2\mathbb{N}$ are definable in $(\mathbb{R}, <, +, \mathbb{N}, f)$. Since α is assumed to be non-quadratic, Theorem B follows immediately from the following stronger result.

Theorem C. Let $\alpha, \beta, \gamma \in \mathbb{R}$ be such that α, β, γ are linearly independent over \mathbb{Q} . Then $(\mathbb{R}, <, +, \alpha\mathbb{N}, \beta\mathbb{N}, \gamma\mathbb{N})$ defines multiplication on \mathbb{R} .

Date: September 12, 2012.

2000 Mathematics Subject Classification. Primary 03C64.

Theorems B and C are in stark contrast to results about $(\mathbb{R}, <, +, \mathbb{N})$. This structure admits a quantifier elimination result and its theory is decidable (due independently to Weispfenning [7] and Miller [5]). However, the structures in Theorem B and C define multiplication on \mathbb{R} and hence every projective set. This is a much stronger property in respect to what kind of sets are definable than the property of just defining multiplication on \mathbb{N} . Consider $(\mathbb{R}, <, +, \mathbb{N})^\#$, the expansion of $(\mathbb{R}, <, +, \mathbb{N})$, by all nonempty subsets of all cartesian products \mathbb{N}^k , where k ranges over all natural numbers. This structure defines multiplication on \mathbb{N} , is undecidable, but by Friedman and Miller [3] every definable set is a union of an open set and a discrete set.

Theorem A can also be applied to expansions by analytic functions. Consider the structure $(\mathbb{R}, <, +, \sin)$. Marker and Steinhorn showed in unpublished work that every definable set in this expansion is a union of an open set and a discrete set¹; for a proof of this result, see Toffalori and Vozoris [6, Theorem 2.7]. Adding a predicate for \mathbb{N} to this structure destroys this tameness completely.

Theorem D. The expansion $(\mathbb{R}, <, +, \sin, \mathbb{N})$ defines multiplication on \mathbb{R} .

Several remarks about the proof of Theorem A and its connection to earlier work are in order. A stronger form of Theorem A was proved for expansions of the ordered fields in [4], but we will show that this result follows from Theorem A in this setting. The proof of Theorem A is not a minor modification of the proof of Theorem 1.1 in [4]. The latter proof depends crucially on the definability of multiplication and does not transfer to our setting. In order to establish the conclusion of Theorem A, it is enough to show that every subset of all cartesian products D^k , where k ranges over \mathbb{N} , is definable. For every $n \in \mathbb{N}$, boxes with endpoints in $f(D)$ form a countable basis of the induced topology on U^n . Hence we only need to show that the set of endpoints is definable. Similar to the earlier work in [4] our approach relies on the idea of regarding the function f as a definable approximation scheme. The key idea here is to realize that for every $c \in U$, the set of best approximations of c (see Definition 1) is definable and varies heavily in c . Given a subset $X \subseteq D^k$, in order to show that X is definable, we describe a family of definable sets (Y_a) , depending on a parameter a , such that Y_a is the image of a definable subset of the set of best approximations of a under the function g . We then find a $c \in \mathbb{R}$ such that $Y_c = X$. The parameter c will be constructed as a limit of a subset of $f(D)$. As in the earlier work, this construction rests on the topological completeness of \mathbb{R} .

The outline of the paper is as follows. In Section 2 some definitions and a few basic results are established. The proof of Theorem A and the details of how Theorem B to D follow from Theorem A can be found in Section 3. Section 4 contains a couple of remarks about the optimality of Theorem A.

Acknowledgements. The authors would like to thank Chris Miller for help in preparing this paper and the anonymous referee for very helpful remarks.

Notation. We will write \mathbb{N} for $\{1, 2, 3, \dots\}$.

¹For expansions of \mathbb{R} , this property is equivalent to being locally o-minimal.

2. DEFINITIONS

In the following, let \mathcal{R} be an expansion of the ordered set $(\mathbb{R}, <)$ such that \mathcal{R} defines an open interval $U \subseteq \mathbb{R}$, a closed and discrete set $D \subseteq \mathbb{R}_{\geq 0}$ and a function $f : D \rightarrow U$ with $f(D)$ dense in U . In this section, we will introduce several definitions and establish some of their properties.

Definition 1. Let $c \in U$. We say $d \in D$ is a **best approximation of c from the left** if $f(d) < c$ and

$$f(D_{<d}) \cap (f(d), c) = \emptyset.$$

We write $L(c)$ for the set of best approximations of c from the left. Similarly, we say $d \in D$ is a **best approximation of c from the right** if $f(d) > c$ and

$$f(D_{<d}) \cap (c, f(d)) = \emptyset.$$

and write $R(c)$ for the set of best approximations of c from the right.

By density of $f(D)$ in U , $\sup f(L(c)) = c = \inf f(R(c))$ for every $c \in U$.

Definition 2. Let $d \in D$ and let (L, R) be a pair of finite subsets of $D_{\leq d}$. We say (L, R) is a **finite approximation up to d** if

- (1) $f(d_l) < f(d_r)$, for $d_l \in L, d_r \in R$,
- (2) f is strictly increasing on L and strictly decreasing on R ,
- (3) for every $e \in D_{\leq d}$

$$(f(L \cap D_{\leq e}) \cap [f(e), \infty)) \cup (f(R \cap D_{\leq e}) \cap (-\infty, f(e)]) \neq \emptyset$$

If $e \in D$ with $e > d$ and (L', R') is an approximation up to e such that $L \subseteq L'$ and $R \subseteq R'$, we say (L', R') is an **extension** of (L, R) up to e .

Lemma 3. Let (L, R) be a pair of finite subsets of D and let $d \in D$. Then the following are equivalent

- (i) (L, R) is a finite approximation up to d ,
- (ii) if $\max f(L) \leq c \leq \min f(R)$, then

$$L(c) \cap D_{\leq d} = L \text{ and } R(c) \cap D_{\leq d} = R.$$

Proof. The proof of (ii) \Rightarrow (i) is immediate from the definition of a finite approximation. For the other implication, suppose that (L, R) is a finite approximation. Since L and R are finite, $\max f(L) < \min f(R)$ by (1). Let $c \in \mathbb{R}$ be such that $\max f(L) < c < \min f(R)$. Now (2) and (3) guarantee that $L(c) \cap D_{\leq d} = L$ and $R(c) \cap D_{\leq d} = R$. \square

Lemma 4. Let $(d_n)_{n \in \mathbb{N}}$ be a strictly increasing sequence of elements in D and for every $n \in \mathbb{N}$, let (L_n, R_n) be a finite approximation up to d_n such that both L_n and R_n are non-empty, and (L_n, R_n) is an extension of (L_m, R_m) for every $m, n \in \mathbb{N}$ with $m < n$. Then there is a unique $c \in U$ such that

- (i) $(L(c) \cap D_{\leq d_n}, R(c) \cap D_{\leq d_n}) = (L_n, R_n)$ for all $n \in \mathbb{N}$, and
- (ii) $\{c\} = \bigcap_{n \in \mathbb{N}} [\max f(L_n), \min f(R_n)]$.

In such a situation, we say c is **approximated** by $((L_n, R_n))_{n \in \mathbb{N}}$.

Proof. Let $(d_n)_{n \in \mathbb{N}}$ and $((L_n, R_n))_{n \in \mathbb{N}}$ satisfy the assumptions. Since $L_m \subseteq L_n$ and $R_m \subseteq R_n$ for every $m, n \in \mathbb{N}$ with $m < n$, the sequence $(\max f(L_n))_{n \in \mathbb{N}}$ is increasing, the sequence $(\min f(R_n))_{n \in \mathbb{N}}$ is decreasing and $\max f(L_n) < \min f(R_n)$ for every $n \in \mathbb{N}$. Hence the set $\bigcap_{n \in \mathbb{N}} [\max f(L_n), \min f(R_n)]$ is a non-empty subset

of U . Let c be an element in this intersection. By Lemma 3, $L_n = L(c) \cap D_{\leq d_n}$ and $R_n = R(c) \cap D_{\leq d_n}$ for every n . Hence

$$\bigcup_{n \in \mathbb{N}} L_n = L(c) \text{ and } \bigcup_{n \in \mathbb{N}} R_n = R(c).$$

Since $\sup f(L(c)) = \inf f(R(c))$, we get $\bigcap_{n \in \mathbb{N}} [\max f(L_n), \min f(R_n)] = \{c\}$. \square

Lemma 5. Let $d_1, d_2 \in D$ with $d_1 \leq d_2$ and let (L, R) be a finite approximation up to d_1 . Then there is a unique extension (L', R') of (L, R) up to d_2 such that $L = L'$.

Proof. Let $c \in \mathbb{R}$ be such that $\max f(L) < c < \min f(R)$ and there is no $e \in D$ with $e \leq d_2$ and $\max f(L) \leq f(e) < c$. It is easy to see that $L(c) \cap D_{\leq d_1} = L$, $R(c) \cap D_{\leq d_1} = R$ and $L(c) \cap (d_1, d_2] = \emptyset$. Hence $(L, R(c) \cap D_{\leq d_2})$ extends (L, R) . The uniqueness follows from Lemma 3. \square

We call (L', R') the **right extension** of (L, R) up to d_2 .

Definition 6. Let $d_1, d_2 \in D$ with $d_1 < d_2$. We say f **splits** between d_1 and d_2 , if for every $e_1, e_2 \in D$ with $e_1, e_2 \leq d_1$ and $f(e_1) < f(e_2)$, there is $e_3 \in D$ with $d_1 < e_3 \leq d_2$ such that $f(e_1) < f(e_3) < f(e_2)$.

By density of $f(D)$, for every $d_1 \in D$ there is $d_2 \in D$ such that $d_1 < d_2$ and f splits between d_1 and d_2 . If f splits between d_1 and d_2 and $d > d_2$, then f splits between d_1 and d .

3. PROOFS

Proof of Theorem A. Let \mathcal{R} be an expansion of the ordered set $(\mathbb{R}, <)$. Assume that \mathcal{R} defines an open interval $U \subseteq \mathbb{R}$, a closed and discrete set $D \subseteq \mathbb{R}_{\geq 0}$ and functions $f : D \rightarrow \mathbb{R}$ and $g : \mathbb{R}^3 \times D \rightarrow D$ such that

- (i) $f(D)$ is dense in U ,
- (ii) for every $a, b \in \mathbb{R}$ and $d, e \in D$ with $a < b$ and $e \leq d$

$$\{c \in \mathbb{R} : g(c, a, b, d) = e\} \cap (a, b) \text{ has non-empty interior,}$$

Let $W \subseteq U^m$ be open. We have to show that W is definable. Since the lexicographic order topology on \mathbb{R}^m has a countable basis and $f(D)$ is dense in U , we can find a sequence $((s_n, r_n))_{n \in \mathbb{N}}$ of elements in D^{2m} such that

$$\bigcup_{n \in \mathbb{N}} (f(s_{n,1}), f(r_{n,1})) \times \dots \times (f(s_{n,m}), f(r_{n,m})) = W.$$

It is only left to show that the range of these sequences is definable. We will show that for every $m \in \mathbb{N}$ every subset of D^m is definable.

Let $A \subseteq D^m$ and let $((a_{i,1}, \dots, a_{i,m}))_{i \in \mathbb{N} \cup \{0\}}$ be an enumeration of A . We will now show that A is definable.

Let $c = (c_1, c_2, c_3) \in \mathbb{R}^3$. Let δ_c be the successor function on the well-ordered set $(L(c_1), <)$ and let δ_c^i denote the i -th iterate of δ_c . For notational convenience, let δ_c^0 be the identity function on $L(c_1)$. For $i = 1, \dots, m$, define functions $l_{c,i} : L(c_1) \rightarrow \mathbb{R}$ by

$$l_{c,i}(e) = \max f(L(c_3) \cap D_{\leq \delta_c^{i-1}(e)})$$

and $r_{c,i} : L(c_1) \rightarrow \mathbb{R}$ by

$$r_{c,i}(e) = \min f(R(c_3) \cap D_{\leq \delta_c^{i-1}(e)}).$$

Let X_c be the set

$$\{e \in L(c_1) : L(c_2) \cap [e, \delta_c(e)] \neq \emptyset\}.$$

Finally consider

$$Y_c := \{(d_1, \dots, d_m) \in D^m : e \in X_c, d_i = g(c_3, l_{c,i}(e), r_{c,i}(e), \delta_c^{i-1}(e))\}.$$

Note that Y_c is definable. The idea behind the above definition of Y_c is to construct a tuple $c = (c_1, c_2, c_3) \in \mathbb{R}^3$ such that every $e \in L(c_1)$ picks $d_1 \in L(c_3)$ and $d_2 \in R(c_3)$ such that $g(c_3, d_1, d_2, e)$ has the desired value in D . The task of $L(c_2)$ is to code where a new tuple begins.

Proposition 7. There is $c \in \mathbb{R}^3$ such that $Y_c = A$.

Proof. We will construct a sequence $(d_n)_{n \in \mathbb{N} \cup \{0\}}$ of elements in D and three strictly increasing sequences of finite approximations $((L_{i,n}, R_{i,n}))_{n \in \mathbb{N} \cup \{0\}}$ for $i = 1, 2, 3$, where $(L_{i,n}, R_{i,n})$ is a finite approximation up to d_n and $(L_{i,n}, R_{i,n})$ is an extension of $(L_{i,k}, R_{i,k})$ for every $k, n \in \mathbb{N} \cup \{0\}$ with $k < n$. We will construct these four objects such that they have the following additional properties: for all $n \in \mathbb{N} \cup \{0\}$

- (I) $_n$ $L_{1,n} = \{d_k : k \in \mathbb{N}_{\leq n}\}$,
- (II) $_n$ $d_n \geq a_{i,j}$, for $i \leq n, j \leq m$,

and if $n \geq 1$ and $n = ms + t$ for some $s, t \in \mathbb{N} \cup \{0\}$ with $1 \leq t \leq m$,

- (III) $_n$ $L_{2,n} \cap [d_{n-1}, d_n] \neq \emptyset$ iff $t = 1$,
- (IV) $_n$ for all $x \in (\max f(L_{3,n}), \min f(R_{3,n}))$,

$$g(x, \max f(L_{3,n-1}), \min f(R_{3,n-1}), d_{n-1}) = a_{s,t}.$$

For $n = 0$, let $d \in D$ be such that $d \geq a_{0,t}$ for every $t \leq m$. Let d_0 be the smallest element in D larger than d such that $f(d_0) < f(e)$ for all $e \in D$ with $e \leq d$. Take $a \in U$ such that $a > f(d_0)$, but $a < f(e)$ for all $e \in D$ with $e < d_0$. Set $L_{1,0} = L(a) \cap D_{\leq d_0}$ and $R_{1,0} = R(a) \cap D_{\leq d_0}$. By construction of d_0 , $L_{1,0} = \{d_0\}$. Let $(L_{2,0}, R_{2,0})$ be the right extension of (\emptyset, \emptyset) up to d_0 and let $(L_{3,0}, R_{3,0})$ be an arbitrary extension of (\emptyset, \emptyset) up to d_0 such that both $L_{3,0}$ and $R_{3,0}$ are non-empty.

Suppose that $n \geq 1$ and that d_k and $((L_{i,k}, R_{i,k}))$ are already constructed for $k < n$ and $i = 1, 2, 3$ satisfying (I) $_k$, (II) $_k$ and, if $k \geq 1$, (III) $_k$ and (IV) $_k$. Let $s, t \in \mathbb{N} \cup \{0\}$ be such that $n = ms + t$ with $1 \leq t \leq m$. Take $d \in D$ such that

- (A) $d > d_{n-1}$ and f splits between d_{n-1} and d and
- (B) $d > \max\{a_{i,j} : i \leq n, j = 1, \dots, m\}$.

By (II) $_{n-1}$, $d_{n-1} > a_{s,t}$. By (ii), there are

$$b_1, b_2 \in (\max f(L_{3,n-1}), \min f(R_{3,n-1}))$$

such that $g(x, \max f(L_{3,n-1}), \min f(R_{3,n-1}), d_{n-1}) = a_{s,t}$ for all $x \in (b_1, b_2)$. Take $b_3 \in (b_1, b_2)$ and $d' \in D$ larger than d such that

$$b_1 < \max f(L(b_3) \cap D_{\leq d'}) < \min f(R(b_3) \cap D_{\leq d'}) < b_2.$$

We will choose $(L_{3,n}, R_{3,n})$ as an extension of $(L(b_3) \cap D_{\leq d'}, R(b_3) \cap D_{\leq d'})$. Any such extension will satisfy (IV) $_n$. But first we have to choose d_n and $(L_{i,n}, R_{i,n})$

for $i = 1, 2$.

Let $(L_{1,n-1}, R)$ be the right extension of $(L_{1,n-1}, R_{1,n-1})$ up to d' . Let d_n be the smallest element in D larger than d' such that

$$\max f(L_{1,n-1}) < f(d_n) < \min f(R).$$

Then $(L_{1,n-1} \cup \{d_n\}, R)$ extends $(L_{1,n-1}, R)$ and is a finite approximation up to d_n . Set $(L_{1,n}, R_{1,n}) := (L_{1,n-1} \cup \{d_n\}, R)$. Hence this extension satisfies $(I)_n$ and d_n satisfies $(II)_n$.

If $t \neq 1$, let $(L_{2,n}, R_{2,n})$ be the right extension of $(L_{2,n-1}, R_{2,n-1})$ up to d_n . Now suppose that $t = 1$. Since f splits between d_{n-1} and d_n , there is a minimal $e \in D$ with $d_{n-1} < e < d_n$ such that

$$\max f(L_{2,n-1}) < f(e) < \min f(R_{2,n-1}).$$

Then $(L_{2,n-1} \cup \{e\}, R_{2,n-1})$ extends $(L_{2,n-1}, R_{2,n-1})$ and is a finite approximation up to e . Let $(L_{2,n}, R_{2,n})$ be an arbitrary extension of $(L_{2,n-1} \cup \{e\}, R_{2,n-1})$ up to d_n . It follows directly that $(L_{2,n}, R_{2,n})$ satisfies $(III)_n$.

Finally set $(L_{3,n}, R_{3,n}) := (L(b_3) \cap D_{\leq d_n}, R(b_3) \cap D_{\leq d_n})$. Since $d_n \geq d'$, $(L_{3,n}, R_{3,n})$ is an extension of $(L(b_3) \cap D_{\leq d'}, R(b_3) \cap D_{\leq d'})$. As mentioned above, such an extension satisfies $(IV)_n$.

For $i = 1, 2, 3$, let $c_i \in U$ be the unique element that is approximated by $((L_{i,n}, R_{i,n}))_{n \in \mathbb{N} \cup \{0\}}$ and let $c = (c_1, c_2, c_3)$. It is left to show that $Y_c = A$. Since $((L_{i,n}, R_{i,n}))_{n \in \mathbb{N} \cup \{0\}}$ approximates c_i , we have by Lemma 3 that

$$L_{i,n} = L(c_i) \cap D_{\leq d_n} \text{ and } R_{i,n} = R(c_i) \cap D_{\leq d_n}.$$

By $(I)_n$,

$$L(c_1) = \{d_n : n \in \mathbb{N} \cup \{0\}\} \text{ and } \delta_c^i(d_n) = d_{n+i}.$$

Let $n \in \mathbb{N}$ and $s, t \in \mathbb{N}$ such that $n = ms + t$ with $1 \leq t \leq m$. By $(III)_n$,

$$L(c_2) \cap [d_{n-1}, d_n] \neq \emptyset \text{ iff } t = 1.$$

Hence

$$X_c = \{d_{ms} : s \in \mathbb{N} \cup \{0\}\}.$$

Since for every $k \in \mathbb{N}$

$$\max f(L(c_3) \cap D_{\leq d_k}) = \max f(L_{3,k}) \text{ and } \min f(R(c_3) \cap D_{\leq d_k}) = \min f(R_{3,k}),$$

we have for $i = 1, \dots, m$

$$l_{c,i}(d_{ms}) = \max f(L_{3,ms+i-1}) \text{ and } r_{c,i}(d_{ms}) = \min f(R_{3,ms+i-1}).$$

By $(IV)_{ms+i}$,

$$g(c_3, l_{c,i}(d_{ms}), r_{c,i}(d_{ms}), \delta_c^{i-1}(d_{ms})) = a_{s,i}.$$

Thus $Y_c = A$. □

A first application of Theorem A. Let \mathcal{R} be an expansion of the ordered field of real numbers $(\mathbb{R}, <, +, \cdot)$. We will show that in this setting assumption (ii) in Theorem A follows from assumption (i).

Theorem E. If \mathcal{R} defines a function $f : D \rightarrow U$ such that D is closed and discrete, $U \subseteq \mathbb{R}$ is an open interval and $f(D)$ is dense in U , then \mathcal{R} defines every open subset of \mathbb{R}^n for every $n \in \mathbb{N}$.

Proof. For every subinterval of \mathbb{R} , \mathcal{R} defines a bijection between this interval and \mathbb{R} . Hence we can assume that $U = (0, 1)$. After replacing D by

$$\{d \in D : \forall e \in D \ e < d \rightarrow f(e) \neq f(d)\},$$

we can assume that f is injective. We now construct a function $g : \mathbb{R}^3 \times D \rightarrow D$, definable in \mathcal{R} , that satisfies condition (ii) of Theorem A. First let $h : \mathbb{R}^2 \times D \rightarrow \mathbb{R}$ be given by

$$h(a, b, e) := \begin{cases} a + \frac{f(e)}{b-a} & \text{if } a < b, \\ a & \text{otherwise.} \end{cases}$$

Note that for fixed $a, b \in \mathbb{R}$ with $a < b$, the function $e \mapsto h(a, b, e)$ is injective and its image is a subset of the interval (a, b) . Then define $g : \mathbb{R}^3 \times D \rightarrow D$ such that $g(c, a, b, d)$ is the $e \in D_{\leq d}$ such that $|c - h(a, b, e)|$ is minimal. Since $D_{\leq d}$ is finite, g satisfies condition (ii) in Theorem A. \square

As a corollary, every expansion of the real field that satisfies the assumption of Theorem E defines \mathbb{N} . This was already shown in [4, Theorem 1.1]. Easy modifications of the above proof show that one needs only assume the definability of a homeomorphism between a bounded interval and an unbounded interval rather than the definability of multiplication.

Proof of Theorem C. We deduce Theorem C from Theorem A. For ease of notation, we assume that $\gamma = 1$. So let $\alpha, \beta \in \mathbb{R}$ such that $1, \alpha, \beta$ are linearly independent over \mathbb{Q} . We will now show that $(\mathbb{R}, <, +, \mathbb{N}, \alpha\mathbb{N}, \beta\mathbb{N})$ defines multiplication on \mathbb{R} .

Since for every $n \in \mathbb{N}$ the subgroups $n\alpha\mathbb{N}$ and $n\beta\mathbb{N}$ are definable, we can assume that $1 < \alpha < \beta$. For every $a \in \mathbb{R}$, let $\lfloor a \rfloor_\beta$ be the largest element in $\beta\mathbb{N}$ smaller than a if such an element exists, and 0 otherwise. Consider $f : \mathbb{N} \rightarrow (0, \beta)$ and $f_\alpha : \alpha\mathbb{N} \rightarrow (0, \beta)$, where

$$f(n) := n - \lfloor n \rfloor_\beta \text{ and } f_\alpha(n\alpha) := n\alpha - \lfloor n\alpha \rfloor_\beta.$$

Both f and f_α are definable and the images of f and f_α are dense in $(0, \beta)$ by Kronecker's Approximation Theorem (see [1, Theorem 7.8]). Define a function $h_1 : \mathbb{R}_{>0} \times \mathbb{N} \times \mathbb{N} \rightarrow \alpha\mathbb{N}$ such that $h_1(u, d, e)$ is the minimum of the set of all $x \in \alpha\mathbb{N}$ such that

$$f_\alpha(x) \in (f(e), f(e) + u) \text{ and } f(\mathbb{N} \cap (0, d]) \cap (f(e), f_\alpha(x)] = \emptyset,$$

in other words, given (u, d, e) , h_1 returns the smallest $x \in \alpha\mathbb{N}$ such that $f_\alpha(x)$ is larger than $f(e)$, but the difference is smaller than u and there is no $y \in \mathbb{N}$ such that $y \leq d$ and $f(y)$ is between $f(e)$ and $f_\alpha(x)$. We will see that given u and d , each $e \in \mathbb{N}_{\leq d}$ is uniquely determined by the distance between $f_\alpha(x)$ and $f(e)$. Define a function $h_2 : \mathbb{R}_{>0} \times \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z}$ by

$$h_2(u, d, e) := f_\alpha(h_1(u, d, e)) - f(e).$$

For fixed $d \in \mathbb{N}$ and $u \in \mathbb{R}$, it follows directly from the linear independence of $1, \alpha, \beta$ over \mathbb{Q} that the function that maps e to $h_2(u, d, e)$ is injective on $\mathbb{N} \cap [0, d]$. Then let $g : \mathbb{R}^3 \times \mathbb{N} \rightarrow \mathbb{N}$ be defined such that if $b > a$, $g(c, a, b, d)$ is the $e \in \mathbb{N} \cap [0, d]$ such that

$$|(c - a) - h_2((b - a), d, e)|$$

is minimal, and $g(c, a, b, d) = 1$, if $b \leq a$. The function g satisfies condition (ii) of Theorem A.

Hence by Theorem A, every subset of \mathbb{N}^n is definable for every $n \in \mathbb{N}$. Let $[\cdot] : \mathbb{R} \rightarrow \mathbb{Z}$ be the usual floor function. Since $1 < \alpha$, the floor function is injective on $\alpha\mathbb{N}$. Thus every subset of $\mathbb{N}^n \times (\alpha\mathbb{N})^m$ is definable for every $n, m \in \mathbb{N}$. In particular, both multiplication on \mathbb{Z} and scalar multiplication by α on \mathbb{Z} is definable.

We will now show that multiplication by α^2 is definable on \mathbb{Z} as well. Since every subset of $\mathbb{Z}^3 \times (\alpha\mathbb{Z})^2$ is definable, the map $\mathbb{Z} \times \mathbb{Z} \times \alpha\mathbb{Z} \rightarrow \mathbb{Z} \times \alpha\mathbb{Z}$ given by

$$(n_1, n_2, \alpha m) \rightarrow (n_1 n_2, \alpha n_1 m)$$

is definable. Thus the function $\mathbb{Z} \times (\mathbb{Z} + \alpha\mathbb{Z}) \rightarrow \mathbb{Z} + \alpha\mathbb{Z}$ that maps $(n_1, n_2 + \alpha m)$ to $n_1 n_2 + \alpha n_1 m$ is definable. Since this function is continuous and $\mathbb{Z} + \alpha\mathbb{Z}$ is a dense subset of \mathbb{R} , the function $\mathbb{Z} \times \mathbb{R} \rightarrow \mathbb{R}$ that maps (n, a) to na is definable. Fixing α^2 in the second coordinate, we get that multiplication by α^2 is definable on \mathbb{Z} .

In order to define multiplication on \mathbb{R} , it is enough to define multiplication on a dense subset of \mathbb{R} . We will show that multiplication is definable on the dense subset $\mathbb{Z} + \alpha\mathbb{Z}$. Since $(a + b)^2 = a^2 + 2ab + b^2$, we just need to prove definability of the squaring function. Let $a \in \mathbb{Z} + \alpha\mathbb{Z}$. Since there are unique $n, m \in \mathbb{Z}$ such that $a = n + \alpha m$ and multiplication by α is definable on \mathbb{Z} , we can define the map $a \mapsto (n, m)$. Since $a^2 = n^2 + 2\alpha nm + \alpha^2 m^2$ and multiplication by α and α^2 is definable on \mathbb{Z} , the squaring function is definable on $\mathbb{Z} + \alpha\mathbb{Z}$.

Proof of Theorem D. We have to show that $(\mathbb{R}, <, +, \sin, \mathbb{N})$ defines multiplication on \mathbb{R} . As before, define a function $h_1 : \mathbb{R}_{>0} \times \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ such that $h_1(u, d, e)$ is the minimum of the set of all $x \in \mathbb{N}$ such that

$$\sin(x) \in (\sin(e), \sin(e) + u) \text{ and } \sin(\mathbb{N}_{\leq d}) \cap (\sin(e), \sin(x)] = \emptyset.$$

and define $h_2 : \mathbb{R}_{>0} \times \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{R}$ by

$$h_2(u, d, e) := \sin(h_1(u, d, e)) - \sin(e).$$

For fixed $d \in \mathbb{N}$ and $u \in \mathbb{R}$, it follows directly from the Lindemann-Weierstrass-Theorem (for a statement, see [2, Theorem 1.4]) that the function that maps e to $h_2(u, d, e)$ is injective on $\mathbb{N}_{\leq d}$. Then define $g : \mathbb{R}^3 \times \mathbb{N} \rightarrow \mathbb{N}$ to be such that for $b > a$, $g(c, a, b, d)$ is the $e \in \mathbb{N}_{\leq d}$ such that $|(c - a) - h_2((b - a), d, e)|$ is minimal, and $g(c, a, b, d) = 1$ for $b \leq a$. Now g satisfies condition (ii) of Theorem A. The definability of multiplication on \mathbb{R} follows as in the proof of Theorem C, using $2\pi\mathbb{N}$ instead of $\alpha\mathbb{N}$.

4. A COUPLE OF REMARKS ABOUT OPTIMALITY

1. To our knowledge, there is no documented example of a structure that satisfies condition (i) of Theorem A, but neither condition (ii) nor the conclusion of the

theorem. Hence it is not known whether condition (ii) follows from condition (i). While Theorem E shows that this implication holds in the setting of expansions of the ordered field of real numbers, we believe that it fails even for expansions of the additive group.

2. At the moment, we do not fully understand the complexity of the definable sets in $(\mathbb{R}, <, +, \alpha\mathbb{N}, \beta\mathbb{N})$. In particular, we do not know whether the assumption or the conclusion of Theorem A holds for this structure, but we suppose that neither does. We have partial results that this structure defines complicated sets such as Cantor sets and infinitely branching trees. However since these are only partial results and the argument is of different nature than the ones presented in this paper, we decided not to include them here.

REFERENCES

- [1] T. M. APOSTOL, *Modular Functions and Dirichlet Series in Number Theory*, 2nd ed. New York: Springer-Verlag, (1997)
- [2] A. BAKER, *Transcendental Number Theory*, Cambridge University Press (1975)
- [3] H. FRIEDMAN, C. MILLER, Expansions of o-minimal structures by sparse sets, *Fund. Math.*, (1) 167 (2001) 55-64
- [4] P. HIERONYMI, Defining the set of integers in expansions of the real field by a closed discrete set, *Proc. Amer. Math. Soc.* 138 (2010) 2163-2168.
- [5] C. MILLER, Expansions of Dense Linear Orders with the Intermediate Value Property, *J. Symbolic Logic* (4) 66 (2001) 1783-1790
- [6] C. TOFFALORI, K. VOZORIS, Notes on local o-minimality, *Math. Logic Quarterly* (6) 55 (2009) 617-632
- [7] V. WEISPFENNING, Mixed real-integer linear quantifier elimination, Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC), ACM, New York, (1999) 129-136

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, DEPARTMENT OF MATHEMATICS, 1409 W. GREEN STREET, URBANA, IL 61801, USA

E-mail address: P@hieronymi.de

DEPARTMENT OF MATHEMATICS, THE OHIO STATE UNIVERSITY, 231 WEST 18TH AVENUE, COLUMBUS, OHIO 43210, USA

E-mail address: tycho@math.ohio-state.edu