The Journal of Symbolic Logic
Volume 84, Number 3, September 2019

INTERPRETING ARITHMETIC IN THE FIRST-ORDER THEORY OF ADDITION AND COPRIMALITY OF POLYNOMIAL RINGS

JAVIER UTRERAS

Abstract. We study the first-order theory of polynomial rings over a GCD domain and of the ring of formal entire functions over a non-Archimedean field in the language $\{1, +, \perp\}$. We show that these structures interpret the first-order theory of the semi-ring of natural numbers. Moreover, this interpretation depends only on the characteristic of the original ring, and thus we obtain uniform undecidability results for these polynomial and entire functions rings of a fixed characteristic. This work enhances results of Raphael Robinson on essential undecidability of some polynomial or formal power series rings in languages that contain no symbols related to the polynomial or power series ring structure itself.

In [19], J. Robinson studied the first-order theories of several arithmetical structures with operations and relations *a priori* weaker than addition and multiplication, and showed that first-order arithmetic, the first-order theory of the natural numbers in the language of rings, was definable in them. For example (and to be used later in this article), she showed the next theorem.

THEOREM ([19], Theorem 1.2). *Addition and multiplication of positive integers are arithmetically definable in terms of the successor operation and the relation of divisibility.*

Many authors have added more arithmetical structures to the list of those in where addition and multiplication is definable, and we refer interested readers to the surveys found in [3, 10].

In a different direction, R. Robinson showed in [20] how to interpret first-order arithmetic inside the ring theories of different rings, and also managed to prove the essential undecidability of some ring theories in some cases where he could not show how to interpret arithmetic. The latter he did, for example, for polynomial rings over an integral domain.

Throughout this article we will use the following language and interpretations. Let $\mathcal{L} = \{1, +, \perp\}$ be a first-order language where 1 is a constant symbol, $+$ a 2–ary function symbol and $\perp$ a 2–ary relation symbol. Over any ring with unity we will interpret 1 as 1, $+$ as addition and $\perp$ as coprimality (*i.e., to have no common divisors other than units*).

Over the natural numbers, let the *neighbour* binary relation, denoted by Neib, be the one satisfied by all pairs (n, m) such that $|n - m| = 1$.

Received October 29, 2018.
2010 *Mathematics Subject Classification.* Primary 03B25, Secondary 12L05.
Key words and phrases. undecidability, polynomial rings, language of rings.

0022-4812/19/8403-0015
DOI:10.1017/jsl.2019.21

Our main theorem refers to two different types of structures. We will recall both definitions for ease of reading. First, a GCD domain is an integral domain where every pair of elements has a greatest common divisor, i.e., a common divisor that divides every other common divisor. Some properties of GCD domains are listed in Proposition 3.1.

The second definition is from non-Archimedean analysis. If $(k, |\,|)$ is a field together with a non-Archimedean absolute value $|\cdot|$, the ring of (formal) entire functions in one variable with coefficients in k is given by

$$\mathcal{A}_k = \left\{ \sum_n a_n t^n \in k[\![t]\!] : \forall \rho \in \mathbb{R}^+, \lim_n |a_n| \rho^n \to 0 \right\}.$$

There is a slight abuse of notation here, as $\mathcal{A}_k$ depends not only on k but also on the absolute value. This should not affect the results presented in this article.

The aim of this article is to show the following result.

Main Theorem. *The structure* $\langle \mathbb{N}; 1, \mathrm{Neib}, | \rangle$ *is interpretable in any of the following structures*:

i. $\langle R[t]; 1, +, \perp \rangle$, *where* R *is a commutative GCD domain with unity*; *and*
ii. $\langle \mathcal{A}_k; 1, +, \perp \rangle$, *where* $(k, |\,|)$ *is a field together with a non-Archimedean absolute value* $|\cdot|$.

Moreover, this interpretation depends solely on the characteristic of the base ring or field.

For an application of this result to decidability problems, observe that

$$\mathrm{Th}\,\langle \mathbb{N}; 1, \mathrm{Neib}, | \rangle = \mathrm{Th}\,\langle \mathbb{N}; 1, n \mapsto (n+1), | \rangle = \mathrm{Th}\,\langle \mathbb{N}; 1, +, \cdot \rangle.$$

The first equality is a result of I. Korec [9]; the second is the theorem of J. Robinson cited above. As the first-order theory of the natural numbers in the language of rings is undecidable, we obtain undecidability results for both types of rings.

Corollary. *There are no algorithms that decide whether*

i. *a given* $\mathcal{L}$*-formula holds true in* $R[t]$, *for a fixed commutative GCD domain with unity* R; *and*
ii. *a given* $\mathcal{L}$*-formula holds true in* $\mathcal{A}_k$, *for a fixed field* k *with a non-Archimedean absolute value.*

Furthermore, the fact that the interpretation of $\langle \mathbb{N}; 1, \mathrm{Neib}, | \rangle$ depends only on the characteristic of the ring allows us to conclude a stronger uniform undecidability result.

Theorem. *There is no algorithm to decide whether a given* $\mathcal{L}$*-formula holds true in every element of a collection of polynomial rings over GCD domains and formal rings of entire functions over non-Archimedean fields, with the sole restriction that all of them must be of the same characteristic.*

As examples of this last result, there is no algorithm to decide whether a given $\mathcal{L}$-formula holds true in every polynomial ring over GCD domains of a given characteristic, nor is there one to decide whether a given $\mathcal{L}$-formula holds true in each of the rings $\mathcal{A}_{\mathbb{C}_p}$ as p varies over the prime numbers.

Remark. The formulas used to interpret $\mathrm{Th}\,\langle \mathbb{N}; 1, \mathrm{Neib}, | \rangle$ are obtained explicitly in this article. Combining them with the results of J. Robinson and I. Korec, the

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

number of quantifier alterations required for interpreting arithmetic in each of the structures considered can be computed, and are as follows:

- the interpretation of arithmetic in $\langle R[t]; 1, +, \perp \rangle$, where characteristic zero R is a commutative GCD domain with unity, requires 7 quantifier alterations;
- the same problem in positive characteristic requires 15 alterations;
- the interpretation of arithmetic in $\langle \mathcal{A}_k; 1, +, \perp \rangle$, where k has characteristic zero, requires 5 alterations; and finally
- the same problem in positive characteristic requires 8 alterations.

Note that none of the structures we study, despite being polynomial rings or subrings of the ring of formal power series (both in a single indeterminate), have a symbol for the indeterminate, nor a symbol related to it (e.g., multiplication by t, or a predicate for being nonconstant). This is more in line with Raphael Robinson's work in the language of rings, but different from the majority of results for rings of polynomials or power series, where some extra such symbols are added to the language. For instance, similar results for a language with coprimality and two successor functions (one for the regular successor, the other for $x \mapsto x + t$) have been obtained by M. Vsemirnov (for polynomial rings over finite fields [21]) and J.-L. Riquelme (for rings of entire p-adic functions [18]). Other results for the integers with successor and either divisibility or coprimality are due to D. Richard [16, 17] (for the full theory) and to L. Lipshitz [11], A. P. Bel'tjukov [2], and L. van den Dries and A. Wilkie [7] (for the existential theory).

Other related results have been obtained using the full language of rings. Undecidability of the theory of a polynomial ring over a domain was shown by R. Robinson, as stated before; for even more general rings of constants, some work is currently being undertaken by E. Naziazeno, M. Barone, and N. Caro [13]. If one also allows a symbol for the indeterminate t in the language, there are much stronger positive–existential undecidability results for polynomial rings over domains by J. Denef [5, 6], for rings of entire functions over fields of characteristic zero by L. Lipschitz and T. Pheidas [12] and for rings of entire functions over fields of positive characteristic by N. Garcia-Fritz and H. Pasten [8]. For more results in this direction we direct the reader to the surveys [14, 15].

The proof of the Main Theorem will be split into the power series and polynomial ring cases, and again into the positive and zero characteristic cases. This article is organised in the following way: in Section 1 we define a weak analogue of divisibility that is $\mathcal{L}$-definable in our structures, and with it a set of irreducible-like elements we will use continuously throughout this article.

In Section 2 we give the proof for the structures over $\mathcal{A}_k$. As these rings have nicer properties than general GCD domains, this proof is much shorter than the remainder of the article, but it follows the same fundamentals and is useful to have in mind before moving onto later sections.

From Section 3 onwards we work on the structure over $R[t]$. In that Section we show that for polynomials of a certain type we have a form of unique factorisation, despite R being a general GCD domain. This amount of control over a language where divisibility is not (necessarily) definable will be crucial for the sections to come.

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

In Sections 4 and 5 we show the Main Theorem for the polynomial rings of zero and positive characteristic, respectively. These proofs follow the ideas introduced in Section 2 earlier, and most of the results of these sections are for shaping our set of irreducible-like elements from Section 1 into a set of elements for which the ideas previously introduced can be applied.

About this last point: the main problem that arises when moving from the case where R is a field (Section 2) to the general case where R is a GCD domain is the fact that R may have elements that fit our irreducible-like definition from Section 1 and interfere with our interpretation of the natural numbers inside $R[t]$. Sections 4 and 5 are about figuratively *weeding out* these elements by finding additional first-order properties to isolate the "good" elements.

The author wants to thank T. Pheidas and H. Pasten for their insight and useful comments on this work, and is especially grateful to C. Martinez and X. Vidaux for commenting on and criticising earlier versions of the manuscript. This gratitude also extends to the anonymous referee for their comments and suggestions.

§1. A definable weak analogue of divisibility. Fix a commutative ring R with unity. Let A be a subring of $R[\![t]\!]$ containing $R[t]$ and such that every unit of A is a unit of R. For this section, let

$$\mathcal{M} = \langle A; 1, +, \perp \rangle .$$

In this section we will define a binary relation on A, weaker than regular divisibility but definable in $\mathcal{M}$. With it, we will be able to count the number of irreducible factors of certain elements of $R[t]$, and in particular be able to define the set T_x of powers (p-th powers in the positive characteristic case) of some suitable $x \in R[t]$.

Our desired relation, denoted by $x \lhd y$, is defined as

$$\forall z \big(z \perp y \to z \perp x \big).$$

Note that in a UFD $x \lhd y$ is equivalent to stating that the radical of x divides the radical of y. We also define $x \approx y$ as

$$x \lhd y \wedge y \lhd x,$$

which attempts to capture the property of having the same irreducible factors. Obviously, the problem in a general GCD domain is the fact that not every nonunit need be divisible by an irreducible factor, but we will show later that we will obtain a UFD-like behaviour by restricting our sets using first-order properties.

First, some basic results about these two new relations.

LEMMA 1.1. *Fix $x, y, z \in A$.*

(a) *$\lhd$ is a partial order relation; $\approx$ is an equivalence relation.*
(b) *If x divides y then $x \lhd y$.*
(c) *If $x \lhd y$ and $x \lhd z$, then $x \lhd y + z$.*
(d) *If u is a unit, then $u \approx 1$ and $u \lhd x \lhd 0$*
(e) *If x is irreducible and $y \lhd x$, then either $y \approx x$ or $y \approx 1$.*

PROOF. The first four statements are trivial.

(e) If y is not a unit, then $y \not\perp y$. Hence $y \not\perp x$, and there exists a nonunit d dividing both x and y. As x is irreducible, d must be associate to x, thus x divides y and $x \lhd y$. ⊣

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

LEMMA 1.2. *The set $A^\times$ of units of A (hence of R as well) is definable in $\mathcal{M}$.*

PROOF. We have

$$A^\times = \{x \in A : \mathcal{M} \models x \perp x\}. \qquad \dashv$$

The set $D_1 \subseteq A$ is defined as the set of minimal elements of $(A \setminus A^\times, \lhd)$. By Lemma 1.1, it is definable in $\mathcal{M}$ as

$$D_1 = \left\{x \in A : \mathcal{M} \models \forall y \notin A^\times \left(y \lhd x \to y \approx x\right)\right\} \setminus A^\times.$$

If A were a factorial ring, then D_1 would consist of powers of irreducibles and their associates.

LEMMA 1.3. *Every irreducible element of A is in D_1.*

PROOF. This follows from Lemma 1.1(e). $\dashv$

We recursively define the sets D_n by

$$D_n = \Bigg\{x \in A : \exists x_1, \ldots, x_n \in D_1 \left(\bigwedge_i x_i \lhd x \wedge \bigwedge_{i \neq j} x_i \perp x_j \wedge \forall y \in D_1 \left(y \lhd x \to \bigvee_i y \approx x_i\right)\right) \wedge \forall z \left(z \lhd x \to \left(z \approx x \vee z \in A^\times \vee z \in \bigcup_{i=1}^{n-1} D_i\right)\right)\Bigg\}.$$

The set D_n collects all elements of A which are not coprime to exactly n distinct equivalence classes in $D_1/\approx$. In case A is a factorial ring, it is the set of elements with exactly n irreducible factors (up to multiplication by a unit).

§2. The case of $\mathcal{A}_k$. Let $(k, |\cdot|)$ be a field with a non-Archimedean absolute value. We have the obvious ring inclusions $k \subseteq k[t] \subseteq \mathcal{A}_k \subseteq k[\![t]\!]$. We recall the following consequence of the Weierstrass Preparation Theorem for $T_1(k)$ (see for example [4], Chapter 5).

PROPOSITION 2.1. $\mathcal{A}_k^\times = k^\times$.

For the rest of this section, let

$$\mathcal{M} = \langle \mathcal{A}_k; 1, +, \perp \rangle.$$

We obtain the definable sets $D_n \subseteq \mathcal{A}_k$ as described in the previous section.

LEMMA 2.2. *0 is the only maximal element of $(\mathcal{A}_k, \lhd)$.*

PROOF. A maximal element x of $(\mathcal{A}_k, \lhd)$ must be divisible by every linear polynomial of $k[t]$. Working in a completion of k, x will be an entire function which is zero on a dense set, hence $x = 0$. $\dashv$

COROLLARY 2.3. *The relations $x = 0$ and $x = y$, and the function $x \mapsto -x$ are definable in $\mathcal{M}$.*

LEMMA 2.4. *Let $x \in \mathcal{A}_k$ be a polynomial of positive degree with no repeated roots over its splitting field. The set of multiples of x is definable in $\mathcal{M}$.*

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

PROOF. As x has no repeated factors, an entire function y is a multiple of x if and only if every element of D_1 that divides x divides y as well, and for irreducible elements dividing and not being coprime to are equivalent. ⊣

2.1. Characteristic zero. Assume that the characteristic of k, and hence of $\mathcal{A}_k$, is zero. A polynomial $x \in A$ of positive degree is linear if and only if

- x is in D_1, and
- for all units y, the sum $x + y$ is also in D_1.

Fixing a linear polynomial x of positive degree, the set B_x of all elements of the form cx^n with c a unit and n positive can be defined as the set of all elements of D_1 not coprime to x.

LEMMA 2.5. *Given a linear polynomial x, the set of powers of x is defined by the formula*

$$y \in B_x \wedge \neg(y - 1 \perp x - 1).$$

PROOF. If y is a power of x, $x - 1$ divides $y - 1$. For the converse, write $y = cx^n$, and assume that $x - 1$ divides $cx^n - 1$. As $x - 1$ also divides $cx^n - c$, it must then divide the difference $c - 1$, and thus $c = 1$. ⊣

We now show how to interpret $\langle \mathbb{N}; 1, \mathrm{Neib}, | \rangle$ in the set of powers of a linear polynomial x.

LEMMA 2.6. *For positive n and m, the difference $x^n - x^m$ is in D_2 if and only if $|n - m| = 1$.*

PROOF. If $|n - m| = 1$, the difference $x^n - x^m$ only has the irreducible factors x and $x - 1$. If $|n - m| = k > 1$, the difference $x^n - x^m$ has these two factors, but is also divisible by $x^{k-1} + x^{k-2} + \cdots + 1$, which is not divisible by either and thus adds at least one extra distinct irreducible factor to $x^n - x^m$. ⊣

LEMMA 2.7. *For positive n and m, $x^m - 1$ is a multiple of $x^n - 1$ if and only if $n|m$.*

This is a known result. Note that the first part of the equivalence is definable because of Lemma 2.4.

2.2. Positive characteristic. Let p be the characteristic of k. We say that a polynomial in $k[t]$ is *basic* if it is of the form $ct^{p^n} + d$ for c a unit, $d \in k$ and $n \in \mathbb{N}$.

LEMMA 2.8. *Every basic polynomial is in D_1, and every element $x \in \mathcal{A}_k$ such that for any unit y their sum $x + y$ is still in D_1 is basic.*

PROOF. A basic polynomial $ct^{p^n} + d$ factors as the p^n-th power of an irreducible element over an algebraic closure of k; hence, it factors as a power of an irreducible over k and belongs to D_1.

For the second statement, if $x \in \mathcal{A}_k$ is as described and c_0 is its constant term, then $x - c_0 \in D_1$ and hence $x = ct^m + c_0$ for some $c \in k$ and $m \in \mathbb{N}$. As $c_0 + c$ is either 0 or a unit, $x - (c_0 + c) \in D_1$, thus $ct^m - c$ is a power of an irreducible factor and m is a power of p. ⊣

Thus the set of basic polynomials is definable in $\mathcal{M}$.

Given a basic polynomial x, let B_x be the set of all basic polynomials not coprime to x, and let T_x be the set given by

$$\{y : \mathcal{M} \models y \in B_x \wedge y - 1 \in B_{x-1}\}.$$

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

As not being coprime is a transitive relation within the set of basic polynomials, note that if $a \in T_b$ then $T_a = T_b$.

LEMMA 2.9. *Given a basic polynomial x, the set T_x has a unique polynomial y of minimal degree. This polynomial is not a p-th power. Moreover,*

$$T_x = \left\{ y^{p^n} : n \in \mathbb{N} \right\}.$$

PROOF. Assume that there are two distinct polynomials $y, z \in T_x$ of minimal degree. As y, z and x are in D_1 and none of them is coprime to x, they all must have the same irreducible as their only irreducible factor; as y and z are of the same degree, there exists a unit u such that $y = uz$. Similarly, as $y - 1$, $z - 1$ and $x - 1$ are basic and not pairwise coprime, there exists a unit v such that $y - 1 = v(z - 1)$. Putting these relations together, we obtain $u = v = 1$ and $y = z$.

Suppose that y is a p-th power, say $y = w^p$. Then w is a basic polynomial with the same irreducible factor as y, and $w - 1$ has the same irreducible factor as $y - 1$. Hence $w \in T_y = T_x$, contradicting the minimality of the degree of y.

As every polynomial in T_y has the same unique distinct irreducible factor, and the degree of y divides the degree of every other polynomial in T_y (they are powers of p), then every element of T_y is of the form cy^n for some unit c and natural number n. We conclude like in Lemma 2.5. ⊣

PROPOSITION 2.10. *For $n, m \in \mathbb{N}$, the difference $y^{p^n} - y^{p^m}$ is in D_p if and only if $|n - m| = 1$.*

PROOF. If $|n - m| = 1$, the difference $y^{p^n} - y^{p^m}$ only has the basic factors y, $y - 1, \ldots, y - (p - 1)$. If $|n - m| = k > 1$, the difference $y^{p^n} - y^{p^m}$ has these p factors, but is also divisible by $y^{p^{k-1}} + y^{p^{k-2}} + \cdots + 1$, which is coprime to all of them and thus adds at least one extra distinct irreducible factor to $y^{p^n} - y^{p^m}$. ⊣

COROLLARY 2.11. *The element of minimal degree y is definable from x.*

PROOF. Note that y is the only element in T_x such that there exists *exactly one* $z \in T_x$ satisfying $z - y \in D_p$, namely $z = y^p$. ⊣

COROLLARY 2.12. *The set of all linear polynomials is definable in $\mathcal{M}$.*

PROOF. A basic polynomial z is linear if it is the element of minimal degree of T_z and, for each unit u, $z + u$ is the element of minimal degree of T_{z+u}. ⊣

Given a linear polynomial x, we show how to interpret $\langle \mathbb{N}; 1, \mathrm{Neib}, | \rangle$ in the set T_x. We have already interpreted Neib, we show now how to interpret divisibility.

LEMMA 2.13. *Let $a, b \in \mathbb{N}$ be nonzero. Then $x^{p^a} - x + 1 | x^{p^b} - x + 1$ if and only if a divides b and $\frac{b}{a} \equiv 1 \bmod p$.*

PROOF. Suppose that $x^{p^a} - x + 1 | x^{p^b} - x + 1$. Thus $b \geq a$. We claim that for any i such that $b \geq ai$ we have $x^{p^a} - x + 1 | x^{p^{b-ai}} - x + (1 - i)$.

Indeed, for $i = 0$ we have this already, and if it holds for some i then if $b \geq a(i+1)$ we have that $x^{p^a} - x + 1$ divides $x^{p^{b-ai}} - x^{p^{b-a(i+1)}} + 1$ and thus $x^{p^a} - x + 1$ divides

$$\left(x^{p^{b-ai}} - x + (1 - i) \right) - \left(x^{p^{b-ai}} - x^{p^{b-a(i+1)}} + 1 \right) = x^{p^{b-a(i+1)}} - x + (1 - (i + 1)).$$

Let l be the largest i such that $b \geq ai$. Then as $b - al < a$ and $x^{p^a} - x + 1 | x^{p^{b-al}} - x + (1 - l)$ the polynomial $x^{p^{b-al}} - x + (1 - l)$ must be zero, hence $b = al$ and $p | 1 - l$.

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

For the converse, we claim that for any i we have $x^{p^a} - x + 1 | x^{p^{ai}} - x + i$. Again we proceed by induction. The case $i = 1$ is clear, and if it holds for some i then as $x^{p^a} - x + 1$ divides $x^{p^{a+ai}} - x^{p^{ai}} + 1$ it also divides

$$\left(x^{p^{ai}} - x + i\right) + \left(x^{p^{a+ai}} - x^{p^{ai}} + 1\right) = x^{p^{a(i+1)}} - x + (i+1). \qquad \dashv$$

COROLLARY 2.14. *Let $a, b \in \mathbb{N}$ be nonzero. Then $x^{p^a} - x + 1 | x^{p^b} - x - 1$ if and only if a divides b and $\frac{b}{a} \equiv -1 \bmod p$.*

PROOF. Almost the same as above. In this case we need to show by induction that for any i such that $b \geq ai$ we have $x^{p^a} - x + 1 | x^{p^{b-ai}} - x + (1+i)$. $\dashv$

The next Proposition shows how to interpret divisibility within the set T_x for x linear. Recall that, because of Lemma 2.4, any statement of the form $x^{p^n} - x + 1 | x^{p^m} - x^{p^k} + 1$ is definable in $\mathcal{M}$.

PROPOSITION 2.15. *Let x be a linear polynomial and $n, m \in \mathbb{N}$ be nonzero. Then n divides m if and only if either $x^{p^n} = x^{p^m}$ or*

$$\mathcal{M} \models \exists x_0, \ldots, x_p \in T_x \left(x_0 = x^{p^n} \wedge x_p = x^{p^m} \right.$$
$$\left. \wedge \bigwedge_{i=0}^{p-1} \left(\left(x^{p^n} - x + 1 | x_{i+1} - x_i + 1 \right) \vee x_{i+1} = x_i \right) \right).$$

PROOF. If the formula is satisfied by $x_i = x^{p^{n_i}}$, then by the previous Lemma and its Corollary n divides all of the n_i. Conversely, if $m = kn$ with $k = qp + r$ and $1 \leq r < p + 1$, we can take

- $x_i = x^{(qp+i)n}$ for $1 \leq i \leq r$, and
- $x_{i+1} = x_i$ otherwise.

And then $x_p = x^{p^m}$ and the formula is satisfied. $\dashv$

§3. Polynomials over a GCD domain. We recall some properties of GCD domains (cf., for example, [1]).

PROPOSITION 3.1. *Let R be a GCD domain. Then*

(i) *every irreducible element of R is prime*:
(ii) *$R[t]$ is also a GCD domain*;
(iii) *every element of R that factors as a product of irreducibles does so uniquely (up to associates and order of factors); and*
(iv) *if a non-constant polynomial in $R[t]$ is irreducible, then it is also irreducible in $R_{(0)}[t]$, where $R_{(0)}$ is the field of fractions of R.*

Fix a commutative GCD domain R with unity. For the rest of this article, let

$$\mathcal{M}_R = \langle R[t]; 1, +, \perp \rangle .$$

In this section we will obtain some UFD-like properties for polynomials of positive degree in $R[t]$. This will allow us to define their sets of powers in a similar fashion to the previous section, and later interpret the natural numbers.

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

LEMMA 3.2. *Every linear polynomial in $R[t]$ with coprime coefficients is irreducible.*

PROOF. Let x be one such polynomial. As the coefficients are coprime, no constant nonunit divides x. As R is a domain, x cannot be written as the product of two polynomials of positive degree. ⊣

LEMMA 3.3. *Let $x \in R[t]$ be a polynomial of positive degree. If $x \in D_1$, then $x = c\gamma^n$, where c is a unit, n a positive integer and γ an irreducible polynomial of positive degree in t.*

PROOF. As R is a GCD domain, the gcd of all the coefficients of x exists. Call it g. Then g and $\frac{x}{g}$ are coprime and both divide x, hence g must be a unit because x belongs to D_1.

We list all nonunit divisors of x, and let γ be one such divisor of minimal degree. By the previous reasoning, γ is a polynomial of positive degree in t, and as any divisor of γ would be a divisor of x as well, γ is irreducible.

Write $x = \gamma y$. If y is not a unit, then it must be coprime to anything that x is coprime to—and thus y and γ cannot be coprime. Hence γ divides y. Iterating this process, as x has finite degree and γ has positive degree, this must halt after a finite number of steps, and $x = c\gamma^n$ for some c and n as stated. ⊣

COROLLARY 3.4. *Every polynomial of positive degree is divisible by an irreducible polynomial of positive degree.*

PROOF. Suppose not. Let x be a polynomial of positive degree not divisible by any irreducible polynomials of positive degree of the least possible degree, which must be at least two because of Lemma 3.2. We may replace x by $\frac{x}{g}$, where g is the gcd of the coefficients of x, as we are not interested in constant divisors.

As x is not irreducible, it can be written as the product of two nonunits. But as every constant divisor of x is a unit, x is divisible by a polynomial of smaller degree which, by the minimality of the degree of x, must be divisible by an irreducible polynomial of positive degree. ⊣

Let $\mathcal{P} = R[t] \setminus R$ be the set of elements of $R[t]$ which are polynomials in of positive degree. Note that the product of a nonzero element of $R[t]$ and an element of $\mathcal{P}$ lies in $\mathcal{P}$, and that the irreducible element t belongs to $\mathcal{P}$. Then, by the same reasoning as Euclid's proof of the infinity of primes, $\mathcal{P}$ contains infinitely many monic irreducible elements. As every element in $\mathcal{P}$ has finite degree as a polynomial in t, no element of $\mathcal{P}$ is divisible by every irreducible element. Thus no nonzero element of $R[t]$ is divisible by every element of D_1, and hence 0 is the only maximal element of $(R[t], \lhd)$. We have shown the following.

COROLLARY 3.5. *The relation $x = 0$ is definable in $\mathcal{M}_R$.*

COROLLARY 3.6. *The function $x \mapsto -x$ and the relation $x = y$ are definable in $\mathcal{M}_R$.*

To each $x \in R[t]$ we associate a set $\mathrm{Irr}(x) \subseteq D_1/\approx$ consisting of all equivalence classes $[y] \in D_1/\approx$ such that $y \lhd x$. This is well–defined. Any Boolean relation between the Irr sets is definable in $\mathcal{M}_R$ (for instance, given x, y, z we can write formulas that hold when $\mathrm{Irr}(x) \subseteq \mathrm{Irr}(y)$ or $\mathrm{Irr}(x) = \mathrm{Irr}(y) \cup \mathrm{Irr}(z)$).

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

§4. Interpretation in $\mathcal{M}_R$, characteristic zero case. Throughout this section, let R be a commutative GCD domain with unity of characteristic zero. We define the following subsets of $R[t]$:

$$T = \left\{ x \in D_1 : \mathcal{M}_R \models \forall u \in R^\times \left((x + u \in D_1) \wedge \left(((x-1) \lhd (u-1)) \to u = 1 \right) \right) \right\}.$$

$$\text{For } x \in T, \quad T_x = \left\{ y \in D_1 : \mathcal{M}_R \models \left(x \approx y \wedge (x-1) \lhd (y-1) \right) \right\}.$$

LEMMA 4.1. *Let $x \in T$ be a polynomial of positive degree in t. Then x is irreducible.*

PROOF. By Lemma 3.3, $x = c\gamma^n$ for some unit c, irreducible γ and positive integer n. By definition of T, $c\gamma^n - c \in D_1$; by Lemma 3.3 again we have $c\gamma^n - c = d\alpha^m$ for some unit d, irreducible α and positive integer m. As $\gamma - 1$ divides $c\gamma^n - c$, we can write $\gamma - 1 = e\alpha^l$ for some unit e and positive integer l.

Then $\gamma^n - 1 = \frac{d}{c}\alpha^m$, and $(\gamma - 1)^n = e^n \alpha^{ln}$. As γ and α have positive degree in t, by comparing degrees and coefficients we have $n = 1$. ⊣

PROPOSITION 4.2. *Let $x \in T$, $c \in R^\times$, $n \in \mathbb{N}_{>0}$ be such that $cx^n \in T_x$. Then $c = 1$.*

PROOF. We have

$$x - 1 \lhd cx^n - 1 \quad \text{(definition of } T_x\text{)}.$$

$$x - 1 \lhd cx^n - c \quad \text{(divisibility)}.$$

$$x - 1 \lhd c - 1 \quad \text{(Lemma 1.1 (iii))}.$$

By definition of T, this implies $c = 1$. ⊣

LEMMA 4.3. *Let $x \in T$ be a polynomial of positive degree in t. Then $T_x = \{x^n : n \in \mathbb{N}_{>0}\}$.*

PROOF. By Lemma 4.1, x is irreducible. As every element of T_x has a common factor with x, Lemma 3.3 implies that $T_x \subseteq \{cx^n : c \in R^\times \wedge n \in \mathbb{N}_{>0}\}$. By Proposition 4.2, $T_x \subseteq \{x^n : n \in \mathbb{N}_{>0}\}$.

Assume that $x^m \in T_x$ and $x^{m+1} \notin T_x$ for some $m \geq 1$. Then there exists $y \in R[t]$ coprime with x^m but not coprime with x^{m+1}. Let z be a nonunit that divides both y and x^{m+1}, and write $x^{m+1} = zw$. By Lemma 4.1 and item i of Proposition 3.1, x is prime, and thus divides either z or w. If x were to divide z, it would divide y as well, contradicting the fact that y and x^m are coprime.

Write $w = xr$. Then $x^{m+1} = zw = zxr$, hence $x^m = zr$. This contradicts the fact that x^m and y are coprime. ⊣

We define the set

$$Z = \left\{ x \in T : \mathcal{M}_R \models \left(\exists! w \in T_x \, (x - w \in D_2) \wedge \forall a \in T_x \left(a \neq x \to \exists!^{(2)} b \in T_x (a - b \in D_2) \right) \right) \right\}.$$

where we write $\exists!^{(n)} x(P(x))$ as shorthand for *there exist exactly n elements x satisfying property P*. We will use this notation again during this article.

If $y, z \in T_x$ are such that $\mathcal{M}_R \models y - z \in D_2$ we will refer to them as *neighbours*. The set Z consists of those $x \in T$ such that x has only one neighbour in T_x, but every other element of T_x has two neighbours.

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

Recalling the proof for the case of fields given in Section 2, in there we defined the set of linear polynomials in t and, for each one of them, the set of all its powers. This cannot be done for general R (just consider the case where R is itself a polynomial ring on another variable), but our aim now is to refine Z into a definable set of irreducibles "nice" enough so that we can define their respective set of powers. We begin by showing that it contains the most basic irreducible polynomial.

PROPOSITION 4.4. *Z is nonempty.*

PROOF. We will show that $t \in Z$. Clearly t belongs to T. Hence $T_t = \{t^n : n \in \mathbb{N}_{>0}\}$. The conclusion follows from the next lemma. ⊣

LEMMA 4.5. *Let $a, b \in \mathbb{N}_{>0}$. The difference $t^a - t^b$ has exactly 2 distinct irreducible factors if and only if $|a - b| = 1$.*

PROOF. Same proof as Lemma 2.6. ⊣

For $x, y \in Z$ we say that x and y are *comparable*, denoted by xCy, if

$$\forall x_i \in T_x \exists y_i \in T_y \, (x - y \lhd x_i - y_i) \wedge \forall y_i \in T_y \exists x_i \in T_x \, (x - y \lhd x_i - y_i) \, .$$

Note that comparability is by definition a symmetric relation. We say that x *observes* y, denoted by xOy, if

$$\forall x_i \in T_x \exists y_j \Big((y \lhd y_j) \wedge (x - y \approx x_i - y_j) \Big).$$

For $x \in Z$, we will say that x is

- *standard* if $\{x^n : n \in \mathbb{N}_{>0}\} = T_x$; and
- *nonstandard* if $\{x^n : n \in \mathbb{N}_{>0}\} \neq T_x$.

We say that $z \in T_x$ is *strange* if it is not of the form x^n.

LEMMA 4.6. *Let $n > 1$ be such that x^n is in T_x. Then $x^{n-1} \in T_x$.*

PROOF. As $x^n \in T_x$, we have

$$\mathrm{Irr}(x) \subseteq \mathrm{Irr}(x^{n-1}) \subseteq \mathrm{Irr}(x^n) = \mathrm{Irr}(x).$$ ⊣

COROLLARY 4.7. *Let $x \in Z$. T_x has strange elements if and only if x is nonstandard.*

PROOF. As the neighbourhood relation is irreflexive and symmetric, and as there is one element of T_x with exactly one neighbour and every other element of T_x has exactly two neighbours, then T_x must be infinite. ⊣

LEMMA 4.8. *Let $x, y \in R$ and $n \in \mathbb{N}_{>0}$ be such that $t - x \lhd t^n - y$. Then $y = x^n$.*

PROOF. As $t - x \lhd t^n - x^n$, we have that $t - x \lhd x^n - y$. But $x^n - y$ is constant as a polynomial in t, and thus it must be the zero polynomial. ⊣

PROPOSITION 4.9. *An element $x \in Z$ is comparable to t if and only if it is standard.*

PROOF. Let $x \in Z$ be nonstandard. By Lemma **??**, $x \in R$. Let $y \in T_x$ be a strange element; as $y \in D_1$ and $y \approx x$ we have that $y \in R$. If x and t were comparable, there would exist an element $t^n \in T_t$ such that $t - x \lhd t^n - y$. By the previous Lemma, $y = x^n$, contradicting the fact that y is strange.

If $x \in Z$ is standard then, as $x - t \lhd x^n - t^n$, x and t are comparable. ⊣

LEMMA 4.10. *Fix $x \in R$. Then $t - x \approx (t - x)^n$.*

PROOF. This follows from item iii of Proposition 3.1. ⊣

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

PROPOSITION 4.11. *Let $x \in Z$ be nonstandard. Then t observes x, but x does not observe t.*

PROOF. Let $z \in T_x$ be a strange element. If x observes t, then there exists γ with $t \lhd \gamma$ such that $t - x \approx \gamma - z$. As both sides of the equivalence are polynomials in t and $t - x$ is irreducible, there exist a unit u and a positive integer n satisfying $\gamma - z = u(t-x)^n$. Comparing coefficients of t^0, $z = ux^n$. By Proposition 4.2, $u = 1$, contradicting the fact that z was strange. Hence x does not observe t.

For the other direction: fix $t^n \in T_t$. By taking $\gamma = t^n - (t-x)^n$, we have $x \lhd \gamma$ and, by the previous Lemma, $t - x \approx t^n - \gamma$. Thus t observes x. ⊣

We can now refine Z into a subset consisting only of standard elements: as shown in Section 2, we look for irreducible elements for which we can define their sets of powers.

COROLLARY 4.12. *The set* $Z_1 = \left\{x \in Z : \mathcal{M}_R \models \forall y \in Z\left(xCy \vee xOy\right)\right\}$ *contains t and does not contain any nonstandard elements.*

LEMMA 4.13. *Let $x \in Z_1$ and $n, m \in \mathbb{N}_{>0}$. $x^n - x^m \in D_2$ if and only if $|n-m| = 1$.*

PROOF. By the above corollary, $T_x = \{x^n : n \in \mathbb{N}_{>0}\}$ for any $x \in Z_1$. If $n \neq m$, then

$$\mathrm{Irr}(x^{n+1} - x^n) \subseteq \mathrm{Irr}(x^m - x^n)$$

and if also $n > 1$ then

$$\mathrm{Irr}(x^{n-1} - x^n) \subseteq \mathrm{Irr}(x^m - x^n).$$

Clearly $x^m - x^n$ does not belong to D_1. By definition of Z, x^n must have exactly two neighbours (one if $n = 1$). The inclusions above show that these neighbours must be x^{n+1} and x^{n-1} (only the former when $n = 1$). ⊣

We will write $y \sim_x z$ to indicate that $y, z \in T_x$ and they are neighbours. We define the set

$$\begin{aligned} Z_2 = \Big\{ x \in Z_1 : \forall y, z \in T_x \Big(& \big(y - 1 \approx z - 1 \to y = z\big) \wedge \\ & \big(y \sim_x z \to \mathrm{Irr}(y - z) = \mathrm{Irr}(x-1) \cup \mathrm{Irr}(x)\big) \wedge \\ & y \neq z \to \exists! w \in T_x \Big(\big(\mathrm{Irr}(y - z) = \mathrm{Irr}(w-1) \cup \mathrm{Irr}(x)\big) \wedge \\ & \forall z' \sim_x z \exists! w' \sim_x w \left(y \neq z' \to \mathrm{Irr}(y - z') = \mathrm{Irr}(w'-1) \cup \mathrm{Irr}(x)\right) \wedge \\ & \forall w' \sim_x w \exists! z' \sim_x z \left(\mathrm{Irr}(y - z') = \mathrm{Irr}(w'-1) \cup \mathrm{Irr}(x)\right) \Big) \Big) \Big\}. \end{aligned}$$

As the next results will illustrate, the refining of Z_1 into Z_2 is necessary to interpret divisibility of the exponents of the powers in T_x. The formula above aims to restrict all divisibility relations between elements of the form $x^n - 1$ to the unavoidable ones, namely, that $x^n - 1$ divides $x^m - 1$ if and only if n divides m.

PROPOSITION 4.14. $t \in Z_2$.

This will follow from the next two lemmas:

LEMMA 4.15. *Let $n, m \in \mathbb{N}_{>0}$ be such that $t^n - 1 \approx t^m - 1$. Then $n = m$.*

PROOF. This follows from item iv of Proposition 3.1. ⊣

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

LEMMA 4.16. *Let $n, m \in \mathbb{N}_{>0}$ with $n > m$. Then* $\mathrm{Irr}(t^n - t^m) = \mathrm{Irr}(t^{n-m} - 1) \cup \mathrm{Irr}(t)$.

PROOF. Let y be an irreducible divisor of $t^n - t^m$. We can assume y to be monic. Moving into $R_{(0)}[t]$, y factors into a power of t, say y_1, and a factor of $t^{n-m} - 1$, say y_2. But both y_1 and y_2 have coefficients in R, and thus one of them must be equal to 1. Hence $y \in \mathrm{Irr}(t^{n-m} - 1) \cup \mathrm{Irr}(t)$. ⊣

PROPOSITION 4.17. *Let $x \in Z_2$ and $n, m \in \mathbb{N}_{>0}$ with $n > m$. Then* $\mathrm{Irr}(x^n - x^m) = \mathrm{Irr}(x^{n-m} - 1) \cup \mathrm{Irr}(x)$.

PROOF. By induction on $n - m$. If $n = m + 1$, then as $x^n \sim_x x^m$ we have $\mathrm{Irr}(x^n - x^m) = \mathrm{Irr}(x - 1) \cup \mathrm{Irr}(x)$. Assume that, for all $i < k$, $\mathrm{Irr}(x^{m+i} - x^m) = \mathrm{Irr}(x^i - 1) \cup \mathrm{Irr}(x)$. Then either $\mathrm{Irr}(x^{m+k} - x^m) = \mathrm{Irr}(x^k - 1) \cup \mathrm{Irr}(x)$ or $\mathrm{Irr}(x^{m+k} - x^m) = \mathrm{Irr}(x^{k-2} - 1) \cup \mathrm{Irr}(x)$. If $k = 2$ then x^1 only has one neighbour and the second case is discarded; if $k > 2$ then, by the inductive hypothesis $\mathrm{Irr}(x^{m+k-2} - x^m) = \mathrm{Irr}(x^{k-2} - 1) \cup \mathrm{Irr}(x)$, and by the uniqueness quantifier in the last line of the definition of Z_2 the second case is discarded as well. ⊣

For $x \in Z_2$, define the set $N_x = \{x^n : n \in \mathbb{N}\} = T_x \cup \{1\}$.

PROPOSITION 4.18. *For $x \in Z_2$, the relation* $\mathrm{Nb}_x(x^a, x^b)$ *on the set* $(N_x)^2$ *given by* $|a - b| = 1$ *is definable in* $\mathcal{M}_R$.

PROOF. By Lemma 4.13, the formula

$$(x^a = 1 \wedge x^b = x) \vee (x^a = x \wedge x^b = 1) \vee x^a - x^b \in D_2$$

defines this relation. ⊣

PROPOSITION 4.19. *For $x \in Z_2$, the relation* $\mathrm{Div}_x(x^a, x^b)$ *on the set* $(N_x)^2$ *given by $a|b$ is definable in* $\mathcal{M}_R$.

PROOF. We claim that the formula

$$x^b = 1 \vee \left(x^a \neq 1 \wedge x^a - 1 \lhd x^b - 1\right)$$

defines this relation. Indeed, the cases $a = 0$ and $b = 0$ are covered; for the other cases, if a divides b then $x^a - 1$ divides $x^b - 1$, and hence $x^a - 1 \lhd x^b - 1$. For the converse, assume that $a, b \in \mathbb{N}$ are such that $x^a - 1 \lhd x^b - 1$.

Let $c = \gcd(a, b)$. There exist positive integers h, k such that $bh = ak + c$. Then $x^a - 1 \lhd x^b - 1 \lhd x^{bh} - 1$. As $x^a - 1 \lhd x^{ak} - 1$, we have $x^a - 1 \lhd x^{ak}(x^c - 1)$; as $x^{ak} - 1$ and x are coprime and $\mathrm{Irr}(x^{ak}(x^c - 1)) = \mathrm{Irr}(x^c - 1) \cup \mathrm{Irr}(x)$, we have that $x^a - 1 \lhd x^c - 1$. But as c divides a, we also have that $x^c - 1 \lhd x^a - 1$. By the definition of the set Z_2, this implies that $x^a = x^c$. As x is not a unit, $a = c$ and thus a divides b. ⊣

THEOREM 4.20. *Fix $x \in Z_2$. The structure* $\langle N_x; x, \mathrm{Nb}_x, \mathrm{Div}_x \rangle$ *is definable in* $\mathcal{M}_R$ *and isomorphic to* $\langle \mathbb{N}; 1, \mathrm{Neib}, | \rangle$.

§5. Interpretation in $\mathcal{M}_R$, positive characteristic case. Throughout this section, let R be a GCD domain of characteristic p. Note that $(\mathbb{F}_p)^\times \subseteq R^\times$.

We define the following sets in $R[t]$:

$$T = \big\{x \in D_1 : \mathcal{M}_R \models \forall u \in R^\times \left((x + u \in D_1)\right.$$
$$\left.\wedge\left(\left(\left((x - 1) \lhd (u - 1)\right) \vee \left(x \lhd (u - 1)\right)\right) \to u = 1\right)\right)\big\}.$$

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

$$\text{For } x \in T, \quad T_x = \left\{ y \in T : \mathcal{M}_R \models \left(x \approx y \wedge x - 1 \approx y - 1 \right) \right\}.$$

$$N = \Big\{ x \in T : \mathcal{M}_R \models \exists \alpha \in T_x \Big(\exists! w \in T_x \, (\alpha - w \in D_p) \wedge \forall a \in T_x \left(a \neq \alpha \to \exists!^{(2)} b \in T_x (a - b \in D_p) \right) \Big) \Big\}.$$

$$Z = \left\{ x \in N : \mathcal{M}_R \models \exists! a \in T_x \Big(x - a \in D_p \Big) \right\}.$$

Same notation as before: if $y, z \in T_x$ are such that $\mathcal{M}_R \models y - z \in D_p$ we will refer to them as *neighbours*.

LEMMA 5.1. *Given $x, y \in T$, $x \in T_y$ if and only if $T_x = T_y$.*

PROOF. $\approx$ is an equivalence relation. ⊣

LEMMA 5.2. *If $x \in N$, then $T_x \subseteq N$.*

PROOF. At no point in the formula defining N is the specific element x of T_x used, only the set T_x itself – any other $y \in T_x$ would do as well. ⊣

We can think of N as the union of some of the sets T_x satisfying the following property : we want T_x to have a single element with exactly one neighbour and every other element with exactly two neighbours, as we aim to use this construction to interpret the natural numbers. The set Z collects, from each $T_x \subseteq N$, the unique element with exactly one neighbour. The definable function $\iota : N \to Z$ that maps x to the only element in $T_x \cap Z$ is thus well–defined.

PROPOSITION 5.3. *Let $x \in T$, $c \in R^\times$, $n \in \mathbb{N}$ be such that $cx^n \in T_x$. Then $c = 1$ and $n = p^m$ for some $m \in \mathbb{N}$.*

PROOF. We have

$$x - 1 \lhd cx^n - 1 \quad \text{(definition of } T_x\text{)}.$$

$$x - 1 \lhd cx^n - c \quad \text{(Lemma 1.1(b))}.$$

$$x - 1 \lhd c - 1 \quad \text{(Lemma 1.1(c))}.$$

By definition of T, this implies $c = 1$.

Assume that $x-1 \approx x^n-1$. As $x-1 \in D_1$, then $x^{n-1}+x^{n-2}+\cdots+1$ is either a unit or is $\approx$–equivalent to $x-1$. If it is a unit, say u, then $u-1 = x(x^{n-2}+x^{n-3}+\cdots+1)$. By definition of T, this implies that $u = 1$ and $n = 1$.

In the other case, we have

$$x - 1 \approx 1 + \sum_{i=1}^{n-1} x^i.$$

$$x - 1 \lhd 2 + \sum_{i=1}^{n-2} x^i \quad \text{(adding } x - 1 \lhd 1 - x^{n-1}\text{)}.$$

$$x - 1 \lhd 3 + \sum_{i=1}^{n-3} x^i \quad \text{(adding } x - 1 \lhd 1 - x^{n-2}\text{)}.$$

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

Inductively, $x - 1 \lhd n$. This implies that n is a multiple of p, say $n = pk$. Then

$$x - 1 \approx x^n - 1 \approx (x^k - 1)^p \approx x^k - 1.$$

Iterating this procedure, the conclusion follows. ⊣

As in the case of characteristic zero, we aim to refine the set Z to get a set of sufficiently "nice" elements, so that their respective T_x are the sets of p^n-th powers in order to apply the ideas from Section 2.

PROPOSITION 5.4. *Z is nonempty.*

PROOF. We will show that $t \in Z$. This will follow from the next lemmas.

LEMMA 5.5. *Let $R_{(0)}$ be the field of fractions of R and let $w \in R_{(0)}^{\times}$. Suppose that for some $m, n \in \mathbb{N}$ the polynomial $\left(t^{p^n} + w\right)^m$ has all of its coefficients in R and is irreducible in $R[t]$. Then m is a power of p.*

PROOF. Write $m = hp^k$, with h and p coprime. Then

$$\left(t^{p^n} + w\right)^m = \left(t^{p^{n+k}} + w^{p^k}\right)^h = \sum_{i=0}^{h} \binom{h}{i} w^{ip^k} t^{(h-i)p^{n+k}}.$$

As h is a unit in R and hw^{p^k} is the coefficient of $t^{(h-1)p^{n+k}}$, then $w^{p^k} \in R$; as this polynomial is irreducible, $h = 1$. ⊣

LEMMA 5.6. *For any $n \in \mathbb{N}$ and $u \in R$, $t^{p^n} + u \in T$.*

PROOF. As $t^{p^n} + u$ is monic, any irreducible divisor of it must be (an associate of) a polynomial of positive degree in t. If $u = 0$ and y is an irreducible divisor of t^{p^n} then it must be a monomial, and thus $y \approx t$ and $\operatorname{Irr}\left(t^{p^n}\right) = \{[t]\}$.

If $u \neq 0$, there exist $m, r \in \mathbb{N}$ and $w \in R_{(0)}$ such that $t^{p^m} + w$ is irreducible in $R_{(0)}[t]$ and $t^{p^n} + u = \left(t^{p^m} + w\right)^{p^r}$. Let $y_1, y_2 \in R[t]$ be monic irreducible divisors of $t^{p^n} + u$ in $R[t]$. As $R_{(0)}[t]$ is a unique factorisation domain, and by the previous Lemma, there exist $s_1, s_2 \in \mathbb{N}$ such that $y_i = \left(t^{p^m} + w\right)^{s_i}$. Hence $s_1 = s_2$ and $t^{p^n} + u \in T$. ⊣

COROLLARY 5.7. $T_t = \left\{t^{p^n} : n \in \mathbb{N}\right\}$.

LEMMA 5.8. *Let $a, b \in \mathbb{N}$. $t^{p^a} - t^{p^b} \in D_p$ if and only if $|a - b| = 1$.*

PROOF. The case $a = b$ is clear. Without loss of generality we may assume that $a > b$, and thus

$$t^{p^a} - t^{p^b} = t^{p^b}\left(t^{p^{a-b}-1} - 1\right)^{p^b}.$$

This has (at least) the p distinct irreducible factors $(t - i)$, for $i \in \mathbb{F}_p$.

If $a - b > 1$, by moving to $R_{(0)}[t]$ we can see that these irreducible factors are not enough, as $t^{p^{a-b}-1} - 1$ has no repeated roots.

If $a - b = 1$, $(t^p - t)^{p^b}$ can be written as a product of linear irreducible factors in $R[t]$. If some y irreducible divides it, then as that same factorisation over linear irreducible factors works in $R_{(0)}[t]$ we have that y must be one of these factors. Thus $(t^p - t)^{p^b} \in D_p$. ⊣

This concludes the proof of Proposition 5.4. ⊣

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

LEMMA 5.9. *Let $x \in Z$ be a polynomial of positive degree in t. Then $T_x = \{x^{p^n} : n \in \mathbb{N}\}$.*

PROOF. The proof follows the proof of Lemma 5.9, using Proposition 5.3 to show that $T_x \subseteq \{x^{p^n} : n \in \mathbb{N}\}$. ⊣

We will need the following definitions:
For $x \in Z$, we will say that x is

- *standard* if $\{x^{p^n} : n \in \mathbb{N}\} = T_x$; and
- *nonstandard* if $\{x^{p^n} : n \in \mathbb{N}\} \neq T_x$.

We say the $z \in T_x$ is *strange* if it is not of the form x^{p^n}. As before, T_x has strange elements if and only if x is nonstandard.

For $x, y \in Z$, we say that x and y are *comparable*, denoted by $x \, C \, y$, if

$$\forall x_i \in T_x \exists! y_i \in T_y \, (x - y \approx x_i - y_i) \wedge \forall y_i \in T_y \exists! x_i \in T_x \, (x - y \approx x_i - y_i) \, .$$

This relation is symmetric. Finally, we define the set

$$Z_0 = \{x \in Z : \mathcal{M}_R \models \exists y \in Z \, (\neg y \, C \, x \wedge \forall z \in T_y \exists \gamma \, (x \lhd \gamma \wedge \gamma - z \approx x - y))\} \, .$$

PROPOSITION 5.10. *An element $x \in Z$ is comparable to t if and only if it is standard.*

PROOF. Let $x \in Z$ be nonstandard. By Lemma 5.9, $x \in R$. Let $y \in T_x$ be strange, and assume that t and x are comparable. Hence there exists n such that $t - x \approx t^{p^n} - y$. As $t - x \approx t^{p^n} - x^{p^n}$, then $t - x \lhd x^{p^n} - y$. But the right hand side is in R, hence it must be zero, which contradicts the fact that y is strange.

If $x \in Z$ is standard and constant as a polynomial in t, by the same reasoning as the previous paragraph we conclude that $x \, C \, t$. The only case remaining is when x is a polynomial of positive degree in t. If $t - x$ is a constant, it is clear that $t - x \approx t^{p^n} - x^{p^m}$ if and only if $m = n$.

Assume that $t - x$ is not a constant, $m \neq n$ and $t - x \approx t^{p^n} - x^{p^m}$. As $t - x \lhd t^{p^m} - x^{p^m}$, this implies that $t - x \lhd t^{p^n} - t^{p^m}$. Without loss of generality suppose that $n > m$. We have $t^{p^n} - t^{p^m} \approx \left(t^{p^{n-m}} - t\right)^{p^m}$.

As $(t^{p^{n-m}} - t)$ splits over $\mathbb{F}_{p^{n-m}}$, there exist $T \in \left(\mathbb{F}_{p^{n-m}} \cap R\right)[t]$ and $u \in R^\times$ such that $x - t = uT$. Note that every nonzero coefficient in uT is a unit. As $x \in T$, $uT + t$ and every element of the form $uT + t + c$ for some unit c must be in D_1. Thus T must be of degree 0 or 1 as a polynomial in t, hence irreducible, and $t^{p^n} - x^{p^m}$ must be a p^n-th power of it. Thus $n = m$. ⊣

LEMMA 5.11. *Z_0 contains all nonstandard $x \in Z$.*

PROOF. Let $x \in Z$ be nonstandard. By the previous Proposition, it is not comparable to $y = t$. For any $n \in \mathbb{N}$, we may take $\gamma = x^{p^n}$ and, as $x \in R$, then $t^{p^n} - x^{p^n} \approx t - x$. ⊣

LEMMA 5.12. *$t \notin Z_0$.*

PROOF. Any $y \in Z$ not comparable to t must be nonstandard, and thus there exists a strange element $z \in T_y$. We claim that for any γ such that $t \lhd \gamma$ we have that $\gamma - z \not\approx t - y$. Indeed, assume that they are equivalent. As y is not comparable to t, it belongs to R, and thus $t - y$ is irreducible and $\gamma - z = u(t - y)^d$ where u is a unit and d is the degree of γ as a polynomial in t. As γ is divisible by t, we have

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

$z = uy^d$. by Proposition 5.3, $u = 1$ and d is a power of p, contradicting the fact that z is strange. ⊣

PROPOSITION 5.13. *The set $Z_1 = Z \setminus Z_0$ contains t. Every element of Z_1 is standard.*

LEMMA 5.14. *Let $x \in Z_1$ and $n, m \in \mathbb{N}$. $x^{p^n} - x^{p^m} \in D_p$ if and only if $|n - m| = 1$.*

PROOF. We know that x has exactly one neighbour, and as $a|b$ implies $\mathrm{Irr}(a) \subseteq \mathrm{Irr}(b)$ we have

$$\mathrm{Irr}\,(x^p - x) \subseteq \mathrm{Irr}\left(x^{p^2} - x\right) \subseteq \cdots \subseteq \mathrm{Irr}\left(x^{p^i} - x\right) \subseteq \cdots$$

As $|\mathrm{Irr}\,(x^p - x)| \geq p$, we have $x^p - x \in D_p$ and $\left|\mathrm{Irr}\left(x^{p^i} - x\right)\right| > p$ for every $i > 1$. Suppose that $x^{p^n} - x^{p^m} \in D_p$. As $\mathrm{Irr}\left(x^{p^{(a-b)}} - x\right) \subseteq \mathrm{Irr}\left(x^{p^n} - x^{p^m}\right)$, we conclude that $|n - m| = 1$. For the converse, if $n \neq 0$ by definition of Z there must be two elements $y \in T_x$ such that $x^{p^n} - y \in D_p$. And, as x is standard, every $y \in T_x$ must be of the form x^{p^r}. ⊣

Let $Z_2 = \{x \in Z_1 : \mathcal{M}_R \models \forall y \in Z_1\,(x\ C\ y)\}$. By Proposition 5.10, Z_2 contains t.

We also define the set

$$Z_3 = \Big\{x \in Z_2 : \mathcal{M}_R \models \forall y \in Z_2 \forall x_i \in T_x \forall y_i \in T_y \Big((x_i - y_i \approx x - y) \to \Big(\big(\forall x_j \in T_x\,(x_j - x_i \in D_p \to \exists y_j \in T_y\,(y_j - y_i \in D_p \wedge x_j - y_j \approx x - y)) \wedge \forall y_j \in T_y\,(y_j - y_i \in D_p \to \exists x_j \in T_x\,(x_j - x_i \in D_p \wedge x_j - y_j \approx x - y))\big)\Big)\Big)\Big\}.$$

This definition requires every element x of Z_3 to satisfy the following: given any $y \in Z_2$, we know that $x\ C\ y$ (by definition of Z_2) and hence there exists a bijection f between T_x and T_y such that, for any $x_i \in T_x$, $f(x_i)$ is the unique element of T_y satisfying $x_i - f(x_i) \approx x - y$. For x to be in Z_3 means that if x_i and x_j are neighbours, $f(x_i)$ and $f(x_j)$ must be neighbours as well; as $f(x) = y$, this inductively implies the next result.

COROLLARY 5.15. *Let $x, y \in Z_3$ and $m, n \in \mathbb{N}$. $x - y \approx x^{p^n} - y^{p^m}$ if and only if $n = m$.*

COROLLARY 5.16. *Z_3 is nonempty.*

PROOF. By the proof of Proposition 5.10, $t \in Z_3$. ⊣

Recall that the definable map $\iota : N \to Z$ sends an element $y \in N$ to the unique $x \in Z$ such that $y \in T_x$. Let N_3 be the preimage of Z_3 under ι.

We will say that two elements $x, y \in N_3$ are *equipotent*, denoted by $x \sim y$, if $x - y \approx \iota(x) - \iota(y)$. This relation is definable in $\mathcal{M}_R$.

COROLLARY 5.17.
- $N_3 = \bigcup_{x \in Z_3} T_x$.
- *If $x, y \in Z_3$ and $m, n \in \mathbb{N}$, then $x^{p^n} \sim y^{p^m}$ if and only if $n = m$.*
- *$\sim$ is an equivalence relation on N_3.*
- *Each equivalence class of $\sim$ contains exactly one element of each T_x as x varies in Z_3.*

Each equivalence class is definable in $\mathcal{M}_R$. We will denote them as $\{E^n : n \in \mathbb{N}\}$, where $E^n = \left[t^{p^n}\right]$. Given $x \in Z_3$ and an equivalence class E, $x_{\restriction_E}$ will denote the unique element in $T_x \cap E$.

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

We will write $\overline{N}$ for the quotient $N_3/\sim$ and for the first-order structure induced on it by $\mathcal{M}_R$. It is interpretable in $\mathcal{M}_R$. If $\phi(x_1,\dots,x_n)$ is a $\mathcal{L}-formula$ and $E_1,\dots E_n$ are classes in $\overline{N}$, we will write

$$\overline{N} \models \phi(E_1,\dots,E_n)$$

when $\mathcal{M}_R \models \forall x \in Z_3 \phi\left(x_{\restriction_{E_1}},\dots,x_{\restriction_{E_n}}\right)$.

LEMMA 5.18. *E^0 is definable in the interpreted structure $\overline{N}$.*

PROOF. E^0 is the unique element in the set

$$\left\{x \in \overline{N} : \overline{N} \models x = \iota(x)\right\}. \qquad \dashv$$

PROPOSITION 5.19. *The relation $\mathrm{Nb}(E^a,E^b)$ given by $|a-b|=1$ is definable in the interpreted structure $\overline{N}$.*

PROOF. By Lemma 5.14, this relation is given by the set

$$\left\{(x,y) \in \overline{N} : \overline{N} \models x-y \in D_p\right\}. \qquad \dashv$$

We want to define the relation $\mathrm{Div}(E^a,E^b)$ given by $a|b$ in the interpreted structure $\overline{N}$. In order to do this, we first obtain some divisibility properties of the polynomials of the form $t^{p^n}-t^{p^m}+1$.

LEMMA 5.20. *Let $a,b \in \mathbb{N}$ be nonzero. Then $t^{p^a}-t+1 | t^{p^b}-t+1$ if and only if a divides b and $\frac{b}{a} \equiv 1 \bmod p$.*

COROLLARY 5.21. *Let $a,b \in \mathbb{N}$ be nonzero. Then $t^{p^a}-t+1 | t^{p^b}-t-1$ if and only if a divides b and $\frac{b}{a} \equiv -1 \bmod p$.*

PROOF. Same proofs as Lemma 2.13 and Corollary 2.14, respectively. $\dashv$

We define the relation $K(E,F,G)$ by the set

$$\left\{(E,F,G) \in \overline{N} : \overline{N} \models \left(F=G \vee E-E^0+1 \lhd G-F+1\right)\right\}.$$

This is clearly definable in the interpreted structure $\overline{N}$ and has the following three properties:

LEMMA 5.22. *Let a,b,c be positive integers. $\overline{N} \models K(E^a,E^b,E^c)$ if and only if either $b=c$ or $t^{p^a}-t+1$ divides $t^{p^c}-t^{p^b}+1$.*

PROOF. If $\overline{N} \models K(E^a,E^b,E^c)$ then, for any $x \in Z_3$, either $x^{p^b}=x^{p^c}$ or $x^{p^a}-x+1 \lhd x^{p^c}-x^{p^b}+1$. In particular this holds for $x=t$. We conclude by noting that $t^{p^a}-t+1$ has no repeated roots and thus $t^{p^a}-t+1 \lhd t^{p^c}-t^{p^b}+1$ is equivalent to $t^{p^a}-t+1 | t^{p^c}-t^{p^b}+1$.

For the converse, the case $b=c$ is trivial, so assume $t^{p^a}-t+1$ divides $t^{p^c}-t^{p^b}+1$. There exists $g(t) \in R[t]$ such that $t^{p^c}-t^{p^b}+1=(t^{p^a}-t+1)g(t)$. This still holds after replacing t with any $x \in Z_3$, thus

$$\mathcal{M}_R \models \forall x \in Z_3\left(x^{p^a}-x+1 \lhd x^{p^c}-x^{p^b}+1\right)$$

and $\overline{N} \models K(E^a,E^b,E^c)$. $\dashv$

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

COROLLARY 5.23. *Let a, b be positive integers. Then $\overline{N} \models K\left(E^a, E^b, E^{b+a}\right)$. Moreover, if $b > a$ then $\overline{N} \models K\left(E^a, E^b, E^{b-a}\right)$.*

PROOF. By the previous Lemma, the first claim follows from the fact that $t^a - t + 1$ divides $t^{p^{b+a}} - t^{p^b} + 1$, and the second from

$$(t^a - t + 1) \left| \left(t^{p^b} - t^{p^{b-a}} + 1\right) = -\left(t^{p^{b-a}} - t^{p^b} - 1\right). \right. \qquad \dashv$$

COROLLARY 5.24. *Let a, b, c be positive integers such that a divides b. If $\overline{N} \models K(E^a, E^b, E^c)$ then a divides c.*

PROOF. We proceed by cases. If $c \geq b$, we write $l = c - b$ and we have $t^{p^c} - t^{p^b} + 1 = \left(t^{p^l} - t + 1\right)^{p^b}$. It is enough to show that if $t^{p^a} - t + 1$ divides $t^{p^l} - t + 1$ then a divides l. This follows from Lemma 5.20.

If $c < b$, we write $l = b - c$ and we now have $t^{p^c} - t^{p^b} + 1 = \left(-\left(t^{p^l} - t + 1\right)\right)^{p^c}$. In a similar fashion as the previous paragraph, we use Corollary 5.21 to conclude that a divides l. $\dashv$

All these properties of the relation K serve to interpret divisibility in the quotient structure $\overline{N}$:

PROPOSITION 5.25. *The relation $\mathrm{Div}(E^a, E^b)$ given by $a|b$ is definable in the interpreted structure $\overline{N}$.*

PROOF. Let $f = \lfloor \frac{p}{2} \rfloor$. We claim that a divides b if and only if

$$\overline{N} \models E^b = E^0 \vee \left(E^a \neq E^0 \wedge \right.$$
$$\left. \exists E_1, \ldots, E_{f+1} \left(K\left(E^a, E^0, E_1\right) \wedge \bigwedge_{i=1}^{f} K\left(E^a, E_i, E_{i+1}\right) \wedge E^b = E_{f+1} \right) \right).$$

The cases where a or b are zero are covered.

Assume $a, b \neq 0$ satisfy the formula given, and let $n_1, \ldots, n_{f+1}$ be such that

$$\overline{N} \models K\left(E^a, E^0, E^{n_1}\right) \wedge \bigwedge_{i=1}^{f} K\left(E^a, E^{n_i}, E^{n_{i+1}}\right) \wedge E^b = E^{n_{f+1}}.$$

As $\overline{N} \models \left(K\left(E^a, E^0, E^{n_1}\right)\right.$, by Lemma 5.20 we have that a divides n_1; as $\overline{N} \models \bigwedge_{i=1}^{f+1} K\left(E^a, E^{n_i}, E^{n_{i+1}}\right)$ we can recursively use Corollary 5.24 to see that a divides all of the n_i; and as $b = n_{f+1}$ we conclude that a divides b.

Conversely, if a divides b then we can write $b = ka$ and $k = qp + r$ for some nonnegative integers k, q and $r \in \{-f + 1, \ldots, f + 1\}$ an integer.[1] We proceed by cases. If $r \geq 1$, we choose

- $E_1 = E^{(qp+1)a}$;
- for $i \leq r$, $E_i = E^{(qp+i)a}$; and
- for $i > r$, $E_{i+1} = E_i$.

[1] There are no problems in the case $p = 2$ because we do not need the uniqueness of r.

https://doi.org/10.1017/jsl.2019.21 Published online by Cambridge University Press

By construction $E_{f+1} = E^b$. By Lemma 5.20 we have $\overline{N} \models K\left(E^a, E^0, E_1\right)$ and by Corollary 5.23 for each i we have $\overline{N} \models K\left(E^a, E_i, E_{i+1}\right)$.

If $r \leq 1$, we choose

- $E_1 = E^{(qp+1)a}$;
- for $i \leq 2 - r$, $E_i = E^{(qp+2-i)a}$; and
- for $i > 2 - r$, $E_{i+1} = E_i$.

The conclusion follows in the same way as before. ⊣

And we obtain the desired interpretability.

THEOREM 5.26. *The quotient structure* $\langle \overline{N}; E^0, \mathrm{Nb}, \mathrm{Div} \rangle$ *is interpretable in* $\mathcal{M}_R$ *and isomorphic to* $\langle \mathbb{N}; 1, \mathrm{Neib}, | \rangle$.

Acknowledgment. This work was funded by the CONICYT grant FONDECYT/Postdoctorado 3160301.

REFERENCES

[1] D. D. ANDERSON, *GCD domains, Gauss' lemma and contents of polynomials*, ***Non-Noetherian Commutative Ring Theory*** (S. T. Chapman and S. Glaz, editors), Mathematics and its Application, vol 520. Springer, Boston, MA, 2000, pp. 1–31.

[2] A. P. BEL'TJUKOV, *Decidability of the universal theory of natural numbers with addition and divisibility.* (*Russian. English summary*) *Studies in constructive mathematics and mathematical logic, VII*. ***Zap. Naucn. Sem. Leningrad. Otdel. Mat. Inst. Steklov.*** **(*LOMI*)**, vol. 60 (1976), pp. 15–28, 221.

[3] A. BÈS, *A survey of arithmetical definability, in*: *A tribute to Maurice Boffa*. ***Société Mathématique de Belgique*** (2002), pp. 1–54.

[4] S. BOSCH, U. GÜNTZER, and R. REMMERT, ***Non-Archimedean Analysis***, Springer-Verlag, Berlin, 1984.

[5] J. DENEF, *The Diophantine problem for polynomial rings and fields of rational functions*. ***Transactions of the American Mathematical Society***, vol. 242 (1978), pp. 391–399.

[6] ———, *The Diophantine problem for polynomials rings of positive characteristic*. ***Studies in Logic and the Foundations of Mathematics***, vol. 97 (1979), pp. 131–145.

[7] L. VAN DEN DRIES and A. WILKIE, *The laws of integer divisibility, and solution sets of lineal divisibility conditions*, this JOURNAL, vol. 68 (2003), no. 2, pp. 503–526.

[8] N. GARCIA-FRITZ and H. PASTEN, *Uniform positive existential interpretation of the integers in rings of entire functions of positive characteristic*. ***Journal of Number Theory***, vol. 156 (2015), pp. 368–393.

[9] I. KOREC, *Definability of addition from multiplication and neighborhood relation and some related results*, preprint 23/1996 of Math. Institute SAV Bratislava.

[10] ———, *A list of arithmetical structures complete with respect to the first–order definability*. ***Theoretical Computer Science***, vol. 257 (2001), no. 1, pp. 115–151.

[11] L. LIPSHITZ, *The Diophantine problem for addition and divisibility*. ***Transactions of the American Mathematical Society***, vol. 235 (1978), pp. 271–283.

[12] L. LIPSCHITZ and T. PHEIDAS, *An analogue of Hilbert's tenth problem for p-adic entire functions*, this JOURNAL, vol. 60 (1995), no. 4, 1301–1309.

[13] E. NAZIAZENO, M. BARONE, and N. CARO, *First-order definability of rational integers in a class of polynomial rings*, 2017, arXiv:1703.08266.

[14] T. PHEIDAS and K. ZAHIDI, *Undecidability of existential theories of rings and fields*: *A survey, in Hilbert's tenth problem*: *Relations with arithmetic and algebraic geometry* (*Ghent, 1999*). ***Contemporary Mathematics***, vol. 270 (2000), pp. 49–106.

[15] ———, *Analogues of Hilbert's tenth problem*, ***Model Theory with Applications to Algebra and Analysis, vol. 2*** (Z. Chatzidakis, D. Macpherson, A. Pillay, and A. Wilkie, editors), London Mathematical Society Lecture Note Series, vol. 350. Cambridge University Press, Cambridge, 2008, 207–236.

[16] D. RICHARD, *Answer to a problem raised by J. Robinson*: *The arithmetic of positive or negative integers is definable from successor and divisibility*, this JOURNAL, vol. 50 (1985), no. 4, pp. 927–935.

[17] ———, *Definability in terms of the successor function and the coprimeness predicate in the set of arbitrary integers*, this JOURNAL, vol. 54 (1989), no. 4, pp. 1253–1287.

[18] J.-L. RIQUELME, ***Ultrametric value distribution in several variables and some consequences in logic***, Ph.D. thesis, Universidad de Concepcion, Concepcion, Chile, 2015.

[19] J. ROBINSON, *Definability and decision problems in arithmetic*, this JOURNAL, vol. 14 (1949), no. 2, pp. 98–114.

[20] R. ROBINSON, *Undecidable rings*. ***Transactions of the American Mathematical Society***, vol. 70 (1951), pp. 137–159.

[21] M. VSEMIRNOV, *The Woods-Erdös conjecture for polynomial rings*. ***Annals of Pure and Applied Logic***, vol. 113 (2002), pp. 331–344.

DEPARTAMENTO DE MATEMATICA
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
UNIVERSIDAD DE CONCEPCION
CONCEPCION, CHILE
E-mail: javierutreras@udec.cl