Communications in Algebra

ISSN: 0092-7872 (Print) 1532-4125 (Online) Journal homepage: http://www.tandfonline.com/loi/lagb20

Defining Multiplication in Some Additive Expansions of Polynomial Rings

Françoise Point, Michel Rigo & Laurent Waxweiler

To cite this article: Françoise Point, Michel Rigo & Laurent Waxweiler (2016) Defining Multiplication in Some Additive Expansions of Polynomial Rings, Communications in Algebra, 44:5, 2075-2099, DOI: 10.1080/00927872.2015.1028236

To link to this article: http://dx.doi.org/10.1080/00927872.2015.1028236

Published online: 25 Apr 2016.

Communications in Algebra®, 44: 2075–2099, 2016

ISSN: 0092-7872 print/1532-4125 online
DOI: 10.1080/00927872.2015.1028236

Taylor & Francis
Taylor & Francis Group

DEFINING MULTIPLICATION IN SOME ADDITIVE EXPANSIONS OF POLYNOMIAL RINGS

Françoise Point[1], Michel Rigo[2], and Laurent Waxweiler[2]
[1]*Département de Mathématique, Le Pentagone Université de Mons, Mons, Belgium*
[2]*University of Liège, Department of Mathematics, Liège, Belgium*

Adapting a result of R. Villemaire on expansions of Presburger arithmetic, we show how to define multiplication in some expansions of the additive reduct of certain Euclidean rings. In particular, this applies to polynomial rings over a finite field.

Key Words: Cobham's theorem; Euclidean ring; Multiplication; Multiplicatively independent elements; Numeration system; Undecidable theory.

2010 Mathematics Subject Classification: Primary: 03B25; Secondary: 11U05, 03D05.

1. INTRODUCTION

It is well known that the theory of the ring of integers is undecidable (see, for instance, [27]) and also, as a consequence of a result of Presburger on the natural numbers, that the theory of the group of integers is decidable [24], [11, Theorem 32E]. In a more general setting, R. Robinson showed that under some rather general hypothesis, integral commutative domains R (with multiplicative identity) have an undecidable theory. It is in particular the case for polynomial rings of the form $\mathbb{F}_p[X]$, p being a prime number, and for $\mathbb{Q}[X]$. Again, if one considers their additive reducts as R-modules, one can put some conditions on the ring that guarantee the decidability of the corresponding theory. See, for instance, [32], [10].

As we shall recall below, the question about where lies the boundary between decidability and undecidability for expansions of $\mathbb{Z}$ has been extensively studied. (We follow the terminology used by model-theorists [12], namely by *expansion* of $\mathbb{Z}$, we mean a structure with the same domain but endowed with more primitive operations [12, p. 9], and we will reserve the word *extension* when we increase the domain of the structure.) In the present article, we extend some results known for expansions of $\mathbb{Z}$ to polynomial rings over a finite field and to certain Euclidean domains. First let us examine the decidability point of view.

Let $\mathscr{L}$ be a finite language. A first-order $\mathscr{L}$-structure is *finite automaton presentable* (for short, FA-presentable) if the elements of the domain can be

Received December 23, 2013; Revised December 4, 2014. Communicated by D. Macpherson.
Address correspondence to Michel Rigo, University of Liège, Department of Mathematics, Grande traverse 12 (B37), B-4000 Liège, Belgium; E-mail: M.Rigo@ulg.ac.be

represented by (finite) strings in a regular language $D \subset \Sigma^*$ over some alphabet Σ in such a way that some finite automata also check whether or not the atomic relations hold for a given tuple of elements of the structure [20, Section 2], [13]. FA-presentability is a strong condition on the structure [21]:

- FA-presentable groups are locally abelian-by-finite;
- FA-presentable rings are locally finite;
- FA-presentable rings without zero-divisors are the finite fields.

Many properties of finite automata, e.g., the emptiness problem, are well known to be decidable. Therefore, one way to prove decidability of a countable structure is to be able to prove that the structure is FA-presentable. This scheme has been extensively used for expansions of the Presburger arithmetic $(\mathbb{N}, +)$, and using the interpretability of $(\mathbb{Z}, +)$ in $(\mathbb{N}, +)$, one can easily get the corresponding decidability result for expansions of $\mathbb{Z}$ whenever the additional primitives of the language are interpretable too [12, Section 5.3].

Let P_r be the set of powers of $r \geq 2$. For instance, J. R. Büchi has shown that $(\mathbb{N}, +, P_2)$ is decidable using the fact that all the corresponding definable subsets are recognizable by a finite 2-automaton. This means that representations in base 2 of the elements of a definable subset form a language accepted by a finite automaton over $\{0, 1\}$ which is thus called a *2-automaton*. (In order to avoid confusion with the above use of *expansions*, instead of speaking of binary (or base 2) expansions of integers, we will use the terminology *representations* in base 2, or 2-representations.) More generally, one can introduce r-automaton to accept or reject r-representations of some natural numbers. In Büchi's article, a stronger (but incorrect) result was stated, namely that the weak monadic second-order theory $\mathrm{Th}_\omega(\mathbb{N}, S)$ of $\mathbb{N}$ with the successor function S, is bi-interpretable with $\mathrm{Th}(\mathbb{N}, +, P_2)$. The mistake was later on pointed out by R. McNaughton [17] who suggested to replace the predicate P_2 with the binary predicate $\epsilon_2(x, y)$ interpreted by "*x is a power of 2 and appears in the 2-representation of y*." It is easily seen that this predicate is interdefinable with the unary function $V_2(y)$ that maps $y \neq 0$ to the highest power of 2 dividing it.

The quantifier complexity of the definable subsets of $(\mathbb{N}, +, V_2)$ has no more than three alternations of quantifiers: $\exists\forall\exists$. This result has been obtained by R. Villemaire by showing that any subset of $\mathbb{N}^n$ which is recognizable by a finite 2-automaton is definable in $(\mathbb{N}, +, V_2)$ [34]. He has also shown the undecidability of the structure $(\mathbb{N}, +, V_2, V_3)$ [34]. This last result has been generalized by A. Bès as follows: the structure $(\mathbb{N}, +, V_2, P_3)$ is also undecidable [2]. It is worth noting that both Villemaire's and Bès' results rely on a slight generalization of the following result of C. Elgot and M. Rabin [9, Theorem 2]. Let g be a strictly increasing function from P_2 to P_2 with the property that *g skips at least one value between two consecutive arguments*:

$$\forall n \forall m \ (n < m \ \rightarrow \ 2.g(n) < g(m)).$$

Then $\mathrm{Th}(\mathbb{N}, +, V_2, n \mapsto g(n))$ is undecidable. (One defines addition and multiplication on the exponents of powers of 2.) W. Thomas showed that in the above undecidability result, one only needs to assume that g is a strictly increasing function such that for infinitely many $x \in P_2$, $g(2.x) > 2.g(x)$ [33, Theorem 2]. Then

R. Villemaire proved that if one further assumes that g is such that there exists $d > 1$ such that

$$\forall n \geq 1 \; \exists m \; (n < m < 2^d.n \; \& \; 2.g(m) < g(2.m)),$$

then multiplication is definable in $\mathrm{Th}(\mathbb{N}, +, V_2, n \mapsto g(n))$ (and not only on the exponents of the elements of P_2) [35, Lemma 4.4].

We have stated these undecidability results with the primes 2 and 3. Nevertheless, the undecidability of both $(\mathbb{N}, +, V_p, V_q)$ and $(\mathbb{N}, +, V_p, P_q)$ holds for any pair of natural numbers $p, q \geq 2$ which are multiplicatively independent, i.e., such that the only integers $k, \ell \geq 0$ such that $p^k = q^\ell$ are $k = \ell = 0$.

Our aim is to extend these results to any polynomial ring over a finite field and more generally to some Euclidean commutative integral domains. The motivation to study structure related to a polynomial ring over a finite field finds its origins in the so-called theorem of Cobham [5]. This theorem is well known for natural numbers. Let $p, q \geq 2$ be two multiplicatively independent natural numbers. Let X be a set of integers which is recognized simultaneously by a p-automaton and by a q-automaton. Then X is ultimately periodic. Cobham's theorem has given a major impulse to the study of sets of integers recognizable by means of finite automata [3, 8]. In this context, Villemaire's work has led to interesting developments concerning p-recognizable sets in a logical setting [18, 19, 29]. It is desirable to shed some new light on a possible analogue of Cobham's theorem in the context of sets of polynomials over a finite field which are recognizable by means of finite automata for all polynomial bases P. In this number system, the sets of polynomials over a finite field that are recognized by a P-automaton have revealed more properties than those observed for integers and deserve further investigations [25, 26].

Our main results (Theorem 2.11 and Theorem 2.25) can be roughly sketched as follows (precise definition of the framework is needed). Under some natural assumptions on an Euclidean ring R and on two multiplicatively independent elements $r, s \in R$, we prove the undecidability of the theory of the structure $(R, +, -, 0, \preceq, V_r, V_s)$, expanded by finitely scalar multiplications, where the pre-ordering $\preceq$ is related to the Euclidean function associated with R and where V_r is a function analogous to the one introduced for the integers. Then we obtain a similar result under the additional assumption that every element of R has a decomposition in terms of powers of r. In that last case, the only hypothesis on r and s is that they are multiplicatively independent, and we show how to define the graph of multiplication in our structure.

Let $\mathbb{F}_q$ be a finite field. In the case where $R = \mathbb{F}_q[X]$, with techniques similar to the ones used by C. Elgot and M. Rabin, L. Waxweiler has shown [36] that multiplication can be defined in the structure

$$(\mathbb{F}_q[X], +, V_r, V_s, \preceq, \{\cdot u; u \in \mathbb{F}_q[X]\}),$$

where r and s are multiplicatively independent polynomials, $\preceq$ is a pre-ordering induced by the degree function, and $\cdot u$ is the scalar multiplication by $u \in \mathbb{F}_q[X]$. This is a typical instance of the cases we are considering here.

In [30], A. Sirokofskich showed that the theory of the structure

$$(\mathbb{F}_q[X], +, P_X, \preceq, \{\cdot u; u \in \mathbb{F}_q[X]\})$$

is model-complete. Using that result, she showed in [31] that the existential theory of the structure $(\mathbb{F}_q[X, X^{-1}], +, P_X, \{\cdot u; u \in \mathbb{F}_q[X]\})$ is decidable. Moreover, she proved that one can interpret the theory of $(\mathbb{Z}, +, |, 0, 1)$ in the theory of the expansion

$$(\mathbb{F}_q[X, X^{-1}], +, P_X, D, \{\cdot u; u \in \mathbb{F}_q[X]\}),$$

where the binary predicate $D(u, v)$ expresses that $\frac{u}{v} \in P_X$ (and so the latter theory is undecidable).

Recall that, as shown by A. Bès in case of $R = \mathbb{Z}$, the structure $\mathrm{Th}(\mathbb{Z}, +, 0, \leq, V_r, P_s)$ is undecidable [2], with r, s two multiplicatively independent elements. A remaining question is whether one can extend such a result to other Euclidean rings and in particular to polynomial rings over a (finite) field.

2. EUCLIDEAN RINGS

In this article, all rings R are commutative and integral, i.e., without zero-divisors, with $1 \neq 0$. In addition, we assume that they are Euclidean rings (unless otherwise stated). So, in particular, they are principal ideal domains (PID) and thus unique factorization domains (UFD) [14, Theorem 2.23]. Note also that if R is a PID, then $R[X]$ is a UFD (but of course not necessarily Euclidean). Let us review basic facts about these rings, for details see [14, Sections 2.14 and 2.15]. Set $R^\star := R \setminus \{0\}$.

Recall that an element $a \in R^\star$ is *irreducible* if a is non-invertible and if, whenever $a = b.c$, then b or c is invertible. An element $a \in R$ is *prime* if a is nonzero and non-invertible, and if $a|b.c$, then $a|b$ or $a|c$. In a UFD, any irreducible element is prime.

Since any element $a \in R^\star$ can be written in a unique way, up permutation of factors, as a product of prime elements times an invertible element, we will speak of its *prime decomposition*. The *support* of a is the set of prime elements appearing in its prime decomposition. This set is denoted by $supp(a)$.

Recall that an *Euclidean function* is a map $\delta : R^\star \to \mathbb{N}$ such that

$$\forall x \ \ \forall y \neq 0 \ \ \exists q, z \ ((x = y.q + z) \ \& \ (z = 0 \text{ or } \ \delta(z) < \delta(y))). \qquad (1)_E$$

One can also take the range of δ to be an ordinal [28], but we restrict ourselves to $\mathbb{N}$.

An Euclidean ring can be equipped with several Euclidean functions, but without loss of generality we may assume it is equipped with one which satisfies in addition [28, Proposition 4] the following property:

$$\delta(1) = 0 \ \& \ [\forall x \neq 0 \ \ \forall y \neq 0 \ \ \delta(x.y) \geq \delta(x)]. \qquad (2)_E$$

Lemma 2.1. *Let $(R, +, \cdot, 0, 1, \delta)$ be an Euclidean ring equipped with an Euclidean function $\delta : R^\star \to \mathbb{N}$ satisfying $(1)_E$ and $(2)_E$ as above. Let $s \in R^\star$.*

Then s is invertible if and only if $\delta(s) = 0$ and for all $s_1 \in R^\star$, we have $\delta(s_1) = \delta(s.s_1)$.

If s is non-invertible element, then for all $s_1 \in R^\star$, we have $\delta(s_1) < \delta(s.s_1)$. In particular, $\delta(s) < \delta(s^2)$ and $\{\delta(s^n) : n \in \mathbb{N}\}$ is cofinal in $\mathbb{N}$, i.e., for every $m \in \mathbb{N}$, there exists k such that $m \leq \delta(s^k)$.

Proof. First, suppose s is invertible. Let t be such that $s.t = 1$. By $(2)_E$, $\delta(s_1.s) \geq \delta(s_1) = \delta(s_1.s.t) \geq \delta(s_1.s)$. Now take $s_1 = 1$, so $0 = \delta(1) = \delta(s)$. Now suppose that $\delta(s) = 0$. By $(1)_E$, there exist q, z such that $1 = q.s + z$ with $\delta(z) < \delta(s)$ if z is nonzero. So, we conclude that $q.s = 1$.

Second, assume that s is not invertible. Let $s_1 \in R^\star$, and set $u := s.s_1$. By $(1)_E$, there exist $q, z \in R$ such that either ($s_1 = u.q + z$ and $\delta(z) < \delta(u)$) or $s_1 = u.q$. In the second case, $s_1.(1 - s.q) = 0$, and so s is invertible, a contradiction. Hence $s_1 = u.q + z$ and $s_1.(1 - q.s) = z$. By $(2)_E$, we have $\delta(s_1) \leq \delta(z) < \delta(u)$. □

Examples of Euclidean rings.

- The ring $\mathbb{Z}$ of integers and the ring $\mathbb{Z}[i]$ of Gaussian integers with a function δ being the logarithm of the norm function.
- Let q be a prime power, the ring $\mathbb{F}_q[X]$ of polynomials over the finite field $\mathbb{F}_q$ with a function δ being the degree function.
- Let p be a prime natural number, the ring $\mathbb{F}_p[[X]]$ of formal power series over $\mathbb{F}_p$, with a function δ being the X-adic valuation.
- Let R be an Euclidean ring and S a subset of R stable by multiplication (with $0 \notin S$). Then the localization $R.S^{-1}$ is again an Euclidean ring [28, Proposition 7]. (In particular, the ring $\mathbb{F}_q[X, X^{-1}]$ is Euclidean.)
- Let R be a PID with finitely many prime ideals, and let v_i be the valuations corresponding to these maximal ideals. Then R with a function $\delta(x) := \sum_i v_i(x)$ is an Euclidean ring [28, Proposition 5].

Definition 2.1. Let $(R, +, \cdot, 0, 1, \delta)$ be an Euclidean ring equipped with an Euclidean function $\delta : R^\star \to \mathbb{N}$ satisfying $(1)_E$ and $(2)_E$. Let $r \in R^\star$ be a non-invertible element. Let $P_r := \{r^n : n \in \mathbb{N}\}$. We define two functions λ_r, V_r from $R^\star$ to P_r as follows:

- The function $\lambda_r : R^\star \to P_r$ maps u to the highest power r^n of r with the property that $\delta(r^n) \leq \delta(u) < \delta(r^{n+1})$. Thanks to Lemma 2.1, λ_r is well defined.
- The function $V_r : R^\star \to P_r$ sending u to the highest power of r dividing u. It is well defined because R is a UFD.

We extend λ_r and V_r on the whole of R by setting $\lambda_r(0) := 0$ and $V_r(0) := 0$.

Lemma 2.2. *Let $(R, +, \cdot, 0, 1, \delta)$ be an Euclidean ring equipped with an Euclidean function $\delta : R^\star \to \mathbb{N}$ satisfying $(1)_E$ and $(2)_E$. Then, the function $\lambda_r : R^\star \to P_r$ defined above has the following properties*:

(1) $\forall x \neq 0\ \forall y \neq 0\ \ (\lambda_r(x) = y \leftrightarrow \lambda_r(y) = y\ \&\ \delta(y) \leq \delta(x) < \delta(r \cdot y)$ *and* $\lambda_r(1) = 1$;

(2) $\forall x \neq 0$ $((\lambda_r(x) = x \leftrightarrow \lambda_r(x.r) = x.r)$ & $\lambda_r(\lambda_r(x)) = \lambda_r(x))$;
(3) $\forall x \neq 0$ $(\lambda_r(x) = \lambda_r(\epsilon.x))$, *for any invertible element* $\epsilon \in R^\star$.

Proof. (1) Let $n \in \mathbb{N}$. Since r is not invertible, we have by Lemma 2.1, that $\delta(r^n) < \delta(r^{n+1})$ and so $\lambda_r(r^n) = r^n$. Moreover, the set $\{\delta(r^n) : n \in \mathbb{N}\}$ is cofinal in $\mathbb{N}$.

(2) By definition, $\lambda_r(x) = x$ implies that $x = r^m$, for some $m \in \mathbb{N}$. In that case, $\lambda_r(x.r) = \lambda_r(r^{m+1}) = x.r$. Suppose now that $\lambda_r(x.r) = x.r$, then $x.r = r^k$ for some $k \in \mathbb{N}$. Note that $k \geq 1$ since r is not invertible. Since R has no zero-divisors, we get that $x = r^{k-1}$, and so $\lambda_r(x) = x$.

(3) By Lemma 2.1, for an invertible element $\epsilon \in R^\star$, $\delta(x.\epsilon) = \delta(x)$. Hence, we have that $\lambda_r(x) = \lambda_r(x.\epsilon)$.

□

Lemma 2.3. *Let R be a UFD. Let $r \in R^\star$ be a non-invertible element such that no sum of at least two powers of that element is invertible, except* 1. *Let k, $\ell \in \mathbb{N}^\star$. We have $r^k - 1 | r^\ell - 1$ if and only if $k | \ell$.*

Proof. If $\ell = nk$, for some $n \geq 1$, then $r^\ell - 1 = (r^k - 1)(r^{(n-1)k} + r^{(n-2)k} + \cdots + r^k + 1)$.

We only have to prove that, if $r^k - 1 | r^\ell - 1$, then $k | \ell$ (and, in particular, $k \leq \ell$). We proceed by induction on $\ell + k$. We may clearly assume that $k \neq \ell$. As a first case, if $k + \ell = 3$, then the result obviously holds if $k = 1$ and $\ell = 2$. Suppose now that $k = 2$ and $\ell = 1$. Assume that $r^2 - 1 | r - 1$. Since R is a UFD, $r + 1$ is invertible, but by assumption, this implies that $r + 1 = 1$ and thus $r = 0$. We get a contradiction with the fact that $r \in R^\star$. So this situation does not occur. We assume that the result holds for $3 \leq k + \ell < n$.

Assume that we have $r^\ell - 1 = (r^k - 1).q$, with $k + \ell = n$, and thus

$$r^\ell = r^k.q - (q - 1). \tag{1}$$

First assume that $\ell > k$. So r^k divides $q - 1$. There exists u such that $q - 1 = r^k.u$. Then we have $r^\ell = r^k.(q - u)$. Since R is a UFD, we get $r^{\ell-k} = q - u$, i.e., $r^{\ell-k} - 1 = (r^k - 1).u$. By the induction hypothesis, $k | \ell - k$ and so $k | \ell$.

Suppose now that $\ell < k$ (we will show that this situation never occurs). From (1), we deduce that $q - 1 = r^\ell(r^{k-\ell}.q - 1)$. Thus there exists some u such that $q - 1 = r^\ell.u$. So $q = r^\ell.u + 1$ and $r^\ell - 1 = (r^k - 1).(r^\ell.u + 1)$. So, we get $1 = r^{k-\ell} - u + r^k.u$, i.e.,

$$1 - r^{k-\ell} = (r^k - 1).u.$$

If $k - \ell < \ell$, i.e., $k < 2\ell$, then by the induction hypothesis, we get $k | k - \ell$. Thus $k - \ell \geq k$, which is a contradiction.

If $k = 2\ell$, in that case set $r^k = s$. The initial assumption $r^k - 1 | r^\ell - 1$ can be rewritten as $s^2 - 1 | s - 1$, i.e., $s + 1 | 1$, as observed in the case $k = 2$ and $\ell = 1$,

which contradicts our assumption. More generally, with the same reasoning, we may assume that k is not a multiple of ℓ.

Otherwise, $k > 2\ell$. Then since $r^k - 1 | r^\ell - 1$ and $r^k - 1 | r^{k-\ell} - 1$, we have that $r^k - 1 | r^\ell.(1 - r^{k-2\ell})$. Since $r^k - 1$ and r^ℓ have no prime factors in common, $r^k - 1 | 1 - r^{k-2\ell}$.

Either $k - 2\ell < \ell$, so we apply the induction hypothesis and we obtain a contradiction, or $k - 2\ell > \ell$ ($k \neq 3\ell$). Then since $r^k - 1 | r^\ell - 1$ and $r^k - 1 | r^{k-2\ell} - 1$, we have that $r^k - 1 | r^\ell.(1 - r^{k-3\ell})$. Since $r^k - 1$ and r^ℓ have no prime factors in common, $r^k - 1 | 1 - r^{k-3\ell}$.

We iterate the above reasoning and suppose that for any $j \in \mathbb{N}^\star$ such that $j\ell < k$, we have $r^k - 1 | r^\ell.(1 - r^{k-j\ell})$. Further we may assume that j is chosen such that $k < (j+1)\ell$, so $k - j\ell < \ell$, and so we may apply the induction hypothesis and get a contradiction. So, we have that, if $r^k - 1 | r^\ell - 1$, then $\ell \geq k$. □

Corollary 2.4 ([22, Theorem 2]). *Under the same hypothesis on R and r as in Lemma 2.3, let f be the partial multiplication restricted to $R \times P_r$, namely $f(u, r^n) := u.r^n$, where $u \in R$ and $r^n \in P_r$. Then the theory of $(R, +, 0, 1, P_r, f)$ is undecidable.*

Proof. One interprets the structure $(\mathbb{N}, +, |)$, where $|$ is a binary relation symbol for division, in $(R, +, 0, 1, P_r, f)$ as follows: $\mathbb{N}$ is in bijection with P_r, $(n + m = k$ iff $f(r^n, r^m) = r^k)$ and we interpret division, using the above lemma, as $(n|m$ iff $\exists u\, f(u, r^n) + 1 = r^m + u)$. □

Definition 2.2. Let $(R, +, \cdot, 0, 1, \delta)$ be an Euclidean ring equipped with an Euclidean function $\delta : R^\star \to \mathbb{N}$ satisfying $(1)_E$ and $(2)_E$. We introduce a (total) pre-ordering $\preceq$ on R as follows. Let $r,\ s \in R^\star$. We write $r \preceq s$, if $\delta(r) \leq \delta(s)$, and we set $0 \prec r$, for all $r \in R^\star$, where as usual for any $u, v \in R$ $u \prec v$ if $(u \preceq v \,\&\, \neg(v \preceq u))$.

Note that for $r \in R^\star$ a non-invertible element, $\preceq$ induces on P_r a total order (Lemma 2.1).

We may reformulate the fact that, if $\delta(s) = 0$, then s is invertible, and the properties $(1)_E$ and $(2)_E$ above in terms of the relation $\preceq$. Hence, the ring $(R, +, \cdot, \preceq, 0, 1)$ that we are considering satisfies the following assumptions:

(1) $(R, +, \cdot, 0, 1)$ is a commutative integral domain which is a UFD and $\preceq$ is a transitive relation with minimum 0 such that $\forall x \forall y\ (x \preceq y$ or $y \preceq x)$;
(2) $\forall x \neq 0\ ((\forall y \neq 0\ x \preceq y) \to \ (\exists u\ x.u = 1))$;
(3) $\forall x\ \ \forall y \neq 0\ \exists q\ \exists z\, (x = y.q + z \,\&\, (z = 0\ \text{ or }\ z \prec y))$;
(4) $\forall x \neq 0\ \ \forall y \neq 0\ \ x \preceq x.y$.

We will consider various reducts of the ring structure. First let us consider the additive structure. Let $\mathcal{L}_R := \{+, -, 0, .s;\ s \in R\}$ be the language of right R-modules where, for any element $s \in R$, $.s$ denotes the unary function sending an element $u \in R$ to its scalar multiplication by s, namely $u.s$.

It is well known that the theory T_R of right R-modules is decidable in the following case. Recall that a domain is a *Dedekind domain* if every ideal decomposes uniquely as a product of prime ideals.

Proposition 2.5 ([10, Theorem 5.4]). *Let R be a recursively presented Dedekind ring with decidable word problem. Suppose there is an effective listing of the distinct maximal ideals M_i, and suppose the cardinality (∞ or a finite integer) of R/M_i is computable from i. Then T_R is decidable.*

In particular, if $R = \mathbb{Z}$, or $R = \mathbb{F}_p[X]$, then the above proposition applies.

Now still forgetting about multiplication, but enriching the module structure on R, we will consider the following expansions. Let $r \in R^\star$ be a non-invertible element and $\mathscr{L}_\lambda := \mathscr{L}_R \cup \{\lambda_r, \preceq\}$, where λ_r is a unary function symbol that will be interpreted as in Definition 2.1. In Lemma 2.2, we have seen that the function λ_r satisfies certain properties in any Euclidean ring R that we expressed in the language $\mathscr{L}_R \cup \{\preceq\}$. Below we will collect these together with properties of $(R, \preceq)$ that can be expressed in $\mathscr{L}_\lambda$. In particular, this will entail that the theory T below is consistent.

Definition 2.3. Let T be the following $\mathscr{L}_\lambda$-theory:

(1) $\preceq$ is a total pre-ordering;
(2) T_R, the $\mathscr{L}_R$-theory of right R-modules;
(3) $\forall x \exists y \exists z \;\; x = y.s + z \;\&\; (z \prec s \text{ or } z = 0)$, for every non-invertible $s \in R^*$;
(4) $\forall x \neq 0 \; x \prec x.s$, for every non-invertible $s \in R^*$;
(5) $\lambda_r(1) = 1$ and $\forall x \neq 0 \; ((\lambda_r(x) = x \leftrightarrow \lambda_r(x.r) = x.r) \;\&\; \lambda_r(\lambda_r(x)) = \lambda_r(x))$ and $\lambda_r(0) = 0)$;
(6) $\forall x \neq 0 \, \forall y \neq 0 \;\; (\lambda_r(x) = y \leftrightarrow \lambda_r(y) = y \;\&\; y \preceq x \prec y \cdot r)$;
(7) $\forall x \neq 0 \; (\lambda_r(x) = \lambda_r(x.\epsilon))$, for every invertible element $\epsilon \in R$.

Alternatively, we may replace axiom scheme (2), by the $\mathscr{L}_{\mathbb{Z}}$-theory of abelian groups and the properties of scalar multiplication by $.r$. For ease of notation, we will also use the unary predicate P_r, which is definable using the function λ_r by $P_r(x) \leftrightarrow \lambda_r(x) = x$. Conversely, note that the function λ_r is quantifier-free definable in the structure $(R, +, 0, \preceq, P_r, .r)$.

In the last section, with some further (natural) restrictions on R, we will prove decidability results for $Th(R, +, 0, \lambda_r, \preceq_r)$, where $\preceq_r$ is a pre-ordering associated with the r-representation of the elements of R. In case $R = \mathbb{F}_p[X]$, this pre-ordering coincides with the one induced by the degree of a polynomial, and in case $R = \mathbb{Z}$, it coincides with the usual order $\leq$ on the absolute values of an element. In the latter case, one can axiomatize the theory of R (in that language), and one obtains more precise results on its complexity. It would be interesting to see under which hypothesis one gets an analogous result for $R = \mathbb{F}_p[X]$.

Let us quickly review the case where $R = \mathbb{Z}$. Taking, for instance $r = 2$, one shows that the theory of $(\mathbb{Z}, +, -, 0, 1, \leq, \lambda_2)$ is axiomatized by the axioms of discretely ordered abelian groups with smallest strictly positive element 1, axioms (5) $\rightarrow$ (7), plus congruence axioms (axiom scheme (3) is replaced by axiom scheme: $\forall x \forall y \; \bigvee_{i=0}^{n-1} x = n.y + i$, $n \geq 2$, and one has to specify which congruences are satisfied by powers of 2). It admits quantifier-elimination in the language $\{+, -, 0, 1, \leq, \lambda_2, \cdot/n; n \in \mathbb{N}^\star\}$, where $x/n = y$ if and only if $\bigvee_{i=0}^{n-1} x = n.y + i$. It is complete, has a recursive axiomatization, and so it is decidable [6, 7, 23]. The proof of the decidability of the theory of $(\mathbb{Z}, +, -, 0, 1, \leq, V_2)$, as recalled in the introduction, is done by completely different methods, using finite automata theory.

We can write down some properties that this function V_r (interpreted as in Definition 2.1) satisfies in any model of T:

$$V_r(1) = 1 \;\&\; V_r(0) = 0,$$
$$\forall x \neq 0\ (V_r(x) = x \to V_r(x.r) = x.r),$$
$$\forall x V_r(x) = V_r(\epsilon x), \text{ for any invertible element } \epsilon,$$
$$\forall x \neq 0\ (\lambda_r(x) = x \leftrightarrow V_r(x) = x),$$
$$\forall x \neq 0\ (V_r(x) \preceq x \prec \lambda_r(x).r),$$
$$\forall x\ \forall y\ ((V_r(x) = V_r(y)) \to V_r(x) \preceq V_r(y + x)).$$

The proof of the following proposition is analogous to [2, Lemma 2.7].

Proposition 2.6. *Let R be a commutative integral domain which is a UFD. Then, the structures $(R, +, 0, V_r, \cdot r)$ and $(R, +, 0, V_{r^n}, \cdot r)$ are interdefinable.*

Proof. Thanks to Lemma 2.3, note that the set of powers of r^n is the set of powers r^k of r such that $r^n - 1 | r^k - 1$. Otherwise stated, if y is a power of r^n, then there exists z such that $(y - 1) = z.(r^n - 1)$. Consequently, we get

$$V_{r^n}(u) = y \leftrightarrow V_r(y) = y \;\&\; \exists z\ (y - 1) = z.(r^n - 1) \;\&\; \bigvee_{i=0}^{n-1} y.r^i = V_r(u).$$

Conversely, we also have $V_r(u) = y \;\leftrightarrow\; [(\bigwedge_{i=1}^{n-1} V_{r^n}(u.r^i) = V_{r^n}(u) \;\&\; y = V_{r^n}(u))$ or

$$\bigvee_{i=1}^{n-1} \left(V_{r^n}(u.r^i) = V_{r^n}(u).r^n \;\&\; y = V_{r^n}(u).r^{n-i} \;\&\; \bigwedge_{j=0}^{i-1} V_{r^n}(u.r^j) = V_{r^n}(u) \right) \Bigg].$$

□

Definition 2.4. Let $u \in R^\star$. We will call an *r-representation* of u the as

$$u = \sum_{n=0}^{k} r^n.u_n$$

with $u_n \prec r$, for $0 \leq n \leq k$ and $u_k \neq 0$. For each $u \in R^\star$ with $u \prec r$, we define a binary predicate $X_{r,u}(x, y)$ as follows: it holds if and only if $x \in P_r$ and y has an r-representation where x occurs with coefficient u. Note that, at this stage, we do not require that all elements have at least such an r-representation (see Definition 2.10 later on).

Remark 2.7. Suppose u has two r-representations, namely $\sum_{n=0}^{k} r^n.u_n$ and $\sum_{n=0}^{k} r^n.v_n$. Then $u_0 - v_0 \equiv 0$ (modulo r). So if we impose uniqueness of the r-representations, we need to assume that the elements $u_n \prec r$, $u_n \in R^\star$, are not congruent to 0 modulo r (or that there is a finite set of representatives of $R/(r.R)$ in R with respect to which any element of $R^\star$ has an r-representation).

In the next lemma, we show that we can retrieve from an r-representation of u, the value of $V_r(u)$.

Lemma 2.8. *Suppose that u has an r-representation of the form $\sum_{n=m}^{k} r^n.u_n$ with $m \leq k$ and $u_m \neq 0$. If $V_r(u) = r^\ell$, then $m = \ell$.*

Proof. It is clear that r^m divides $V_r(u)$, so $\ell \geq m$. We proceed by contradiction and assume that $\ell > m$. Since $V_r(u) = r^\ell$, we have $\sum_{n=m}^{k} r^n.u_n = r^\ell.s$ with r not dividing s. So we get

$$\sum_{n=m+1}^{k} r^{n-m}.u_n + u_m = r^{\ell-m}.s$$

with $\delta(u_m) < \delta(r)$ because by definition of an r-representation $u_m \prec r$. From the equality above, since $\ell > m$, we derive that r divides u_m, i.e., there exists x such that $r.x = u_m$. This implies, by $(2)_E$, that $\delta(r) \leq \delta(u_m)$, a contradiction. □

Definition 2.5. We say that hypothesis $(\mathbf{C+})_r$ is satisfied whenever the following weak compatibility condition between $\preceq$ and $+$ holds, for a given r-representation. Given any finite sum $u \neq 0$ of distinct powers of r,

$$u = \sum_{i=0}^{n} r^{m_i} \qquad \text{with } m_0 < \cdots < m_n;$$

then we have $r^{m_n} \preceq u \prec r^{m_n+1}$ or equivalently $\lambda_r(u) = r^{m_n}$. In other words, given an element $u \in R^\star$ which has an r-representation as a finite sum of powers of r, these powers lie between $V_r(u)$ and $\lambda_r(u)$ (for the pre-ordering $\preceq$).

We say that hypothesis $(\mathbf{C}\times)$ is satisfied whenever the following weak compatibility condition between $\preceq$ and $\times$ holds: for all non-invertible elements $u_1, u_2, u_3 \in R^\star$ such that $u_1 \prec u_2$, then $u_1.u_3 \prec u_2.u_3$.

Consider the ring $\mathbb{Z}[i]$ of Gaussian integers, and let $r = -2 + i$. Then hypothesis $(\mathbf{C+})_r$ does not hold; namely, write $u = -1 + i$ as $(-2 + i).1 + 1$. We have $\neg((-2 + i) \preceq u)$. For $(\mathbf{C+})_r$ to hold, we can choose for instance r of the form $n \pm i$, for n large enough.

Hypothesis $(\mathbf{C+})_r$ is satisfied for $R = \mathbb{Z}$, $R = \mathbb{F}_p[X]$, and also for any $R \subset \mathbb{R}$ when the pre-ordering is induced by the absolute value (and $r > 0$). Hypothesis $(\mathbf{C}\times)$ is satisfied whenever the pre-ordering is induced by a valuation or a norm.

Remark 2.9. Under the hypothesis $(\mathbf{C+})_r$, we will show that certain sets are definable in $(R, +, 0, \preceq, V_r)$. We begin by defining the unary predicate $X_1(u)$ which will be interpreted as the subset of elements of R which have an r-representation with coefficients 1. First we distinguish the case where $P_r(u)$ holds. Then we express that given any power x of r between $V_r(u)$ and $\lambda_r(u)$, we can decompose u as a sum of either two elements $u_0,\ u_1$, or three elements $u_0,\ u_1,\ x$ depending on the fact that this power x does occur in an r-representation of u or not, and the powers occurring in an r-representation of u_0 (respectively, u_1) are strictly smaller (respectively larger)

than x. Moreover given another power $y \neq x$ of r between $V_r(u)$ and $\lambda_r(u)$, we can decompose either u_0 or u_1 in a similar way. Therefore, we can express u as a sum of powers of r between $V_r(u)$ and $\lambda_r(u)$; by Lemma 2.8, $V_r(u)$ is the smallest such power, and by hypothesis $(\mathbf{C+})_r$, $\lambda_r(u)$ is the largest such one.

So, let $X_1(u) \leftrightarrow \phi(u)$, where $\phi(u) := P_r(u)$ or

$$\begin{aligned}
&\forall x\ ((P_r(x)\ \&\ V_r(u) \preceq x \preceq \lambda_r(u)) \rightarrow \exists u_0 \exists u_1\ u = u_0 + u_1 \text{ or } u = u_0 + x + u_1\ \&\\
&\lambda_r(u_0) \prec x\ \&\ x \prec V_r(u_1))\ \&\ \lambda_r(u_1) = \lambda_r(u)\ \&\ V_r(u_0) = V_r(u)\ \&\\
&\forall y\ ((P_r(y)\ \&\ V_r(u) \preceq y \preceq \lambda_r(u_0)) \rightarrow \exists u_0' \exists u_1'\ u_0 = u_0' + u_1' \text{ or } u_0 = u_0' + y + u_1'\ \&\\
&\lambda_r(u_0') \prec y\ \&\ y \prec V_r(u_1'))\ \&\ \lambda_r(u_1') = \lambda_r(u_0)\ \&\ V_r(u_0') = V_r(u_0)\ \&\\
&\forall z\ ((P_r(z)\ \&\ V_r(u_1) \preceq z \preceq \lambda_r(u_1)) \rightarrow \exists u_0' \exists u_1'\ u_1 = u_0' + u_1' \text{ or } u_1 = u_0' + z + u_1'\ \&\\
&\lambda_r(u_0') \prec z\ \&\ z \prec V_r(u_1'))\ \&\ \lambda_r(u_1') = \lambda_r(u_1)\ \&\ V_r(u_0') = V_r(u_1).
\end{aligned}$$

The predicate $X_{r,1}(x, y)$ (see Definition 2.4) on $P_r \times X_1$ is definable in $(R, +, -, 0, \preceq, V_r)$ by the following formula:

$$\begin{aligned}
P_r(x)\ \&\ V_r(y) \preceq x \preceq \lambda_r(y)\ \&\ \exists y_0 \exists y_1\ \ [&y = y_1 + x + y_0\\
&\&\ (y_1 \neq 0 \rightarrow (\lambda_r(y) = \lambda_r(y_1)\ \&\ x \prec V_r(y_1)))\\
&\&\ \lambda_r(y_0 + x) = x\ \&\ (y_0 \neq 0 \rightarrow \lambda_r(y_0) \prec x)\ \&\ V_r(y_0 + x) = V_r(y)].
\end{aligned}$$

Note that if hypothesis $(\mathbf{C+})_r$ does not hold, one can still define in some cases these predicates. It suffices to be able to define for an element u written as a sum of powers of r, the highest power of r occurring in that sum.

Notation 2.1. Let $\mathcal{M}$ be an $\mathcal{L}$-structure. We will denote by $Th_\omega(\mathcal{M})$ the weak monadic second-order theory of $\mathcal{M}$; it is the extension of the first-order theory of $\mathcal{M}$ allowing quantification over finite subsets of M, the domain of $\mathcal{M}$ (rather than just over elements of M) [12, Section 2.8].

Lemma 2.10. *Let $r \in R^\star$ be non-invertible. Then in* $\mathrm{Th}(R, +, \preceq, V_r, .r)$, *one can interpret* $\mathrm{Th}_\omega(\mathbb{N}, S)$ *and* $\mathrm{Th}_\omega(P_r, .r)$, *under assumption* $(\mathbf{C+})_r$.

Proof. Let $n := \{n_1, \ldots, n_k\}$ be a finite subset of $\mathbb{N}$. It is in bijection with the finite subset $\{r^{n_1}, \ldots, r^{n_k}\}$ of P_r, and it is interpreted by the element $[n]$ of R equal to $\sum_{i \in n} r^i$. The set X_1 of elements u of R which have an r-representation with coefficients 1 is defined by the formula $\phi(u)$ (see Remark 2.9).

The successor function is interpreted by scalar multiplication $.r$ on P_r.

The relation $m \in n$ is interpreted by the binary predicate $X_{r,1}(r^m, [n])$ (see Definition 2.4 and Remark 2.9). □

Definition 2.6. Let $r_1, r_2 \in R^\star$. We say that r_1 and r_2 are *multiplicatively independent*, if there do not exist nonzero natural numbers m, $n \in \mathbb{N}^\star$ such that $r_1^n = r_2^m$.

Definition 2.7. Let $(E, \leq)$ be infinite totally discretely ordered set. Let $a \in E$, and then $S(a)$ is the smallest element of E strictly bigger than a, namely $S(a) = b$ iff $\forall c\ ((a < c) \leftrightarrow b \leq c)$.

As we recalled in the introduction, there are several variants of the notion of *skipping* functions. We will use the following terminology.

Definition 2.8. Let $(E, \leq)$ be infinite totally discretely ordered set. We will say that a function $h : E \to E$, is a *skipping* function if for infinitely many $a \in E$, $h(S(a)) > S(h(a))$. We will say that h is a *regular skipping* function if for all $a \in E$, $h(S(a)) > S(h(a))$.

Before considering the general case of multiplicatively independent elements, we will place ourselves in the special case where none of the two supports is included in the other one (where the support of an element is the set of its prime divisors, see Section 2). One proceeds as in the case of $\mathbb{N}$, first by proving the existence of a strictly increasing *skipping* function on P_r and then by interpreting the ring of natural numbers on that definable subset of P_r.

In the general case of multiplicatively independent elements, we will show that there exists a definable finite partition of P_r and, on each element of this partition, the existence of a skipping function. Under a further assumption on the r-representations of elements of R, namely the assumption $(\mathbf{Rep})_r$ introduced in Definition 2.10, we will use such function in order to define multiplication in our structure (which *a priori* is stronger than interpreting $(\mathbb{N}, +, .)$ on P_r).

Definition 2.9. Let $r, s \in R$ be two non-invertible elements, and we will use the following notation. Let r_s be the product of all prime factors occurring in the intersection of the supports of r and s. We make the convention that, in case where the intersection of the supports of r and s is empty, then $r_s := 1$.

Theorem 2.11. *Assume that R satisfies hypotheses $(\mathbf{C}+)_r$ and $(\mathbf{C}\times)$. Let $r, s \in R^\star$ be two non-invertible elements such that neither the support of r is included in the support of s nor the support of s is included in the support of r. Then the theory of*

$$(R, +, -, 0, \preceq, V_r, V_s, \cdot r, \cdot s, \cdot r_s)$$

is undecidable.

In order to show the existence of a skipping function, we will consider two cases. Since R is a UFD, we may write $r = r_0.r_1$ and $s = s_0.s_1$, with r_0, r_1, s_1 pairwise co-prime and $supp(r_0) = supp(s_0)$. Note that if the intersection of these supports is empty, then we set $r_0 = s_0 = 1$. We will distinguish whether or not r_0 and s_0 are multiplicatively dependent. As a special case, we first treat the case where $r_0 = s_0$ (which contains the main arguments used when r_0 and s_0 are multiplicatively dependent).

Lemma 2.12. *Assume that R satisfies hypothesis $(\mathbf{C}\times)$. Assume that $r = r_0.r_1$ and $s = r_0.s_1$, with r_0, r_1, s_1 pairwise co-prime and that $s \preceq r$. Then, in $(R, +, -, 0, \preceq, V_r, V_s, \cdot r)$,*

one can define a strictly increasing function $h : P_r \to P_r$ (with respect to $\preceq$) which is a skipping function.

Proof. We will construct a definable strictly increasing function $h : P_r \to P_r$, such that $r^{c+1}.h(r^n) \preceq h(r^{n+c})$, for some strictly positive constant $c \in \mathbb{N}$ (which implies that h is a skipping function).

We first define a least common multiple of r^n and s^m, up to an invertible element, as follows. We will use the notation $\mathrm{lcm}(r^n, s^m) \sim u$ where u is any element satisfying the formula $\phi(u, r^n, s^m) :=$

$$V_r(u) = r^n \;\&\; V_s(u) = s^m \;\&\; \forall x\,((V_r(x) = r^n \;\&\; V_s(x) = s^m) \to u \preceq x).$$

Note that, if $m \geq n$, then $\mathrm{lcm}(r^n, s^m)$ is, up to an invertible element, equal to $r_0^m.r_1^n.s_1^m$.

The function h is obtained as the composition of the following three strictly increasing functions.

Let $h_1 : P_r \to P_s, r^n \mapsto s^m$, where s^m is the least element of P_s with $r^n \prec s^m$. Let us denote $m := v_s(n)$. We have $v_s(n) \geq n+1$. Indeed, since $s \preceq r$, by hypothesis $(\mathbf{C}\times)$ on R, $s^2 \preceq r.s \preceq r^2$ and iterating, we get $s^n \preceq r^n$. Moreover, h_1 is strictly increasing: since $s^{m-1} \preceq r^n \prec s^m$, we have $s^{m-1}.r \preceq r^{n+1} \preceq s^m.r$. Since $s \preceq r$, we have $s^m \preceq s^{m-1}.r \preceq r^{n+1}$ and so $h_1(r^n) \prec h_1(r^{n+1})$.

Let $h_2 : P_r \to R, r^n \mapsto \mathrm{lcm}(r^n, h_1(r^n))$. (It is an abuse of notation since $\mathrm{lcm}(r^n, h_1(r^n))$ is only defined up to an invertible element, but as we will see below, it will not matter.)

Finally, let $h : P_r \to P_r, r^n \mapsto r^k$, where $r^k := r.\lambda_r(h_2(r^n))$, namely r^k is the least element of P_r strictly larger (for $\prec$) than $h_2(r^n)$. So h is definable in $(R, +, -, 0, \preceq, V_r, V_s, \cdot r)$ and strictly increasing.

By Lemma 2.1, since s_1 is non-invertible, there exists a constant c such that $r \preceq s_1^c$. Let us show that $r^{c+1}.h(r^n) \preceq h(r^{n+c})$.

Write

$$\mathrm{lcm}(r^n, h_1(r^n)) \sim r_0^{v_s(n)}.r_1^n.s_1^{v_s(n)} \quad \text{and} \quad \mathrm{lcm}(r^{n+1}, h_1(r^{n+1})) \sim r_0^{v_s(n+1)}.r_1^{n+1}.s_1^{v_s(n+1)}$$

with $n < v_s(n) < v_s(n+1)$. So $r.\mathrm{lcm}(r^n, h_1(r^n)).s_1^{v_s(n+1)-v_s(n)} \preceq \mathrm{lcm}(r^{n+1}, h_1(r^{n+1}))$.

Therefore, if $r^{k-1} \preceq \mathrm{lcm}(r^n, h_1(r^n)) \prec r^k$, then $r^k \preceq r.\mathrm{lcm}(r^n, h_1(r^n)) \prec r^{k+1}$ and $r^k \preceq r.\mathrm{lcm}(r^n, h_1(r^n)).s_1^{v_s(n+1)-v_s(n)} \preceq \mathrm{lcm}(r^{n+1}, h_1(r^{n+1}))$. Since $v_s(n+1) - v_s(n) \geq 1$, and by choice of c, we get that $r^{c+1}.\mathrm{lcm}(r^n, h_1(r^n)) \preceq \mathrm{lcm}(r^{n+c}, h_1(r^{n+c}))$. By definition of h, we get that $r^{c+1}.h(r^n) \preceq h(r^{n+c})$. □

Corollary 2.13. *Under the same hypothesis on R as in Lemma 2.12, assume that $r = r_0.r_1$ and $s = s_0.s_1$, r_0, s_0 being multiplicatively dependent, namely $r_0^n = s_0^m$, for some $n, m \in \mathbb{N} \setminus \{0\}$ and r_0, r_1, s_1 are pairwise co-prime. Assume that $s^m \preceq r^n$. Then in $(R, +, -, 0, \preceq, V_r, V_s, \cdot r, \cdot s)$, one can define a strictly increasing function $h : P_{r^n} \to P_{r^n}$ (with respect to $\preceq$) which is a skipping function.*

Proof. The proof is analogous to the one of the preceding lemma, replacing r (respectively, s) by a power r^n (respectively, by s^m). □

Proposition 2.14. *Assume that R satisfies hypothesis $(\mathbf{C}\times)$. Assume that neither the support of r, nor the support of s is included in the support of other one. Then, in*

$(R, +, -, 0, \preceq, V_r, V_s, \cdot r, \cdot s, \cdot r_s)$, one can define a strictly increasing function h: $P_r \to P_r$ (with respect to $\preceq$) which is a skipping function.

Proof. Since R is a UFD, we may write $r = r_0.r_1$ and $s = s_0.s_1$, with r_0, r_1, s_1 pairwise co-prime and $supp(r_0) = supp(s_0)$. The case where r_0 and s_0 multiplicatively dependent was treated in Lemma 2.12 and Corollary 2.13. The remaining case is when r_0 and s_0 are multiplicatively independent. Since R is a UFD, r_0 and s_0 can be decomposed as a product of their prime factors $p_0, \cdots, p_\ell$ as follows (up to an invertible element).

Let $r_0 = {p_0}^{\alpha_0}.\cdots.{p_\ell}^{\alpha_\ell}$ and $s_0 = {p_0}^{\beta_0}.\cdots.{p_\ell}^{\beta_\ell}$. W.lo.g. let $\frac{\alpha_0}{\beta_0} = min_i\{\frac{\alpha_i}{\beta_i}\}$ and $\frac{\alpha_\ell}{\beta_\ell} = max_i\{\frac{\alpha_i}{\beta_i}\}$. By replacing r and s by a power, we may assume that $\alpha_0 = \beta_0$ and $\theta := \frac{\alpha_\ell}{\beta_\ell} > 1$. We will define a strictly increasing function f from P_r to P_r sending r^n to $r^{\lceil n.\theta \rceil}$. Choosing c such that $r^{c+1}.f(r^n) \leq f(r^{n+c})$, we get a skipping function. In order to get $(c+1) + \lceil n.\theta \rceil \leq \lceil (n+c).\theta \rceil$, we choose c such that $c + 2 + n.\theta \leq n.\theta + c.\theta$, i.e., $2 \leq c.(\theta - 1)$.

In order to define f, we will use the scalar multiplication by r_s (introduced in Definition 2.9), and we first define $g : P_r \to P_s : r^n \mapsto s^{\lceil n.\theta \rceil}$ by the following formula: $g(x) = y$ iff $x \in P_r$ & $y \in P_s$ and $(\star)$ $\forall u$ $((V_r(u.r_s) \succeq x \ \& \ V_s(u) \succeq y) \to V_r(u) \succeq x)$ and y is the smallest power of s satisfying $(\star)$.

Assume that u satisfies $(V_r(u.r_s) \succeq x \ \& \ V_s(u) \succeq y)$; then $u.r_s = x.x_1$ and $u = y.y_1$. By assumption, y is of the form ${p_0}^{\beta_0.m}.\cdots.{p_\ell}^{\beta_\ell.m}.s_1^m$ and $x = {p_0}^{\alpha_0.n}.\cdots.{p_\ell}^{\alpha_\ell.n}.r_1^n$. Since R is a UFD, we get that $u = {p_0}^{\alpha_0.n-1}.\cdots.{p_\ell}^{\alpha_\ell.n-1}.r_1^n.x_1 = {p_0}^{\beta_0.m}.\cdots.{p_\ell}^{\beta_\ell.m}.s_1^m.y_1$. If u satisfies the implication in $(\star)$, then $\bigwedge_{i=0}^{\ell} \beta_i.m \geq \alpha_i.n$. The exponent m corresponding to a smallest such u is equal to $\lceil \frac{\alpha_\ell}{\beta_\ell} \rceil.n$.

Now we define a function $h : P_s \to P_r : s^m \mapsto r^m$. It is defined in a similar way as above, by $h(x) = y$ iff $x \in P_s$& $y \in P_r$ and $(\star\star)$ $\forall u$ $((V_s(u.r_s) \succeq x \ \& \ V_r(u) \succeq y) \to V_s(u) \succeq x)$ and y is the smallest power of r satisfying $(\star\star)$.

Assume that u satisfies as $(V_s(u.r_s) \succeq x \ \& \ V_r(u) \succeq y)$; then $u.r_s = x.x_1$ and $u = y.y_1$. By assumption, y is of the form ${p_0}^{\alpha_0.n}.\cdots.{p_\ell}^{\alpha_\ell.n}.r_1^n$ and $x = {p_0}^{\beta_0.m}.\cdots.{p_\ell}^{\beta_\ell.m}.s_1^m$. Since R is a UFD, we get that $u = {p_0}^{\beta_0.m-1}.\cdots.{p_\ell}^{\beta_\ell.m-1}.s_1^m.x_1 = {p_0}^{\alpha_0.n}.\cdots.{p_\ell}^{\alpha_\ell.n}.r_1^n.y_1$. If u satisfies the implication in $(\star\star)$, then $\bigwedge_{i=0}^{\ell} \alpha_i.n \geq \beta_i.m$. The exponent n corresponding to a smallest such u is equal to $\lceil \frac{\alpha_1}{\beta_1} \rceil.m$, namely $n = m$.

The function f is the composition of g and h. □

Remark 2.15. Note that, in [34, Lemma 3.4], the author does not define the multiplication of two elements but rather their least common multiple. However, as shown by the third author in Chapter 8 of his thesis [36], this is enough to define a skipping function using the ideas of [34]. We followed here the same treatment.

Question 2.1. Recall that R. Villemaire has shown the undecidability of $(\mathbb{N}, +, V_p, V_q)$ with p, q being multiplicatively independent integers. Then, the result has been generalized by A. Bès to the undecidability of $(\mathbb{N}, +, V_p, P_q)$. It is therefore natural to consider the following question. Can we define such a skipping function in $(R, +, -, 0, \preceq, P_r, V_s)$, where P_r is a unary predicate for powers of r and r, s two multiplicatively independent elements, as in the integer case?

Proof of Theorem 2.11. Without loss of generality, from now on we will assume that $s \preceq r$. We show that one can interpret $(\mathbb{N}, +, \cdot)$ in $(R, +, 0, \preceq, V_r, V_s, \cdot r, \cdot s, \cdot r_s)$

in the following way. We take the set P_r of powers of r, and we define addition and multiplication on the exponents of these powers, following the proof of C. Elgot and M. Rabin [9] and its generalization due to W. Thomas [33]. First note that we can code in that structure finite subsets of P_r (see Lemma 2.10).

C. Elgot and M. Rabin show [9, Theorem 2] that, if one has a strictly monotone regular skipping function $h : \mathbb{N} \to \mathbb{N}$, then one can define in $Th_\omega(\mathbb{N}, <, h)$ a function

$$g : \mathbb{N} \to \mathbb{N} \text{ such that } g^{-1}(a) \text{ is infinite for all } a. \qquad (\star)$$

Using such function, they show how to define uniformly any finite binary relation on $\mathbb{N}$ [9, Theorem 1]. Then one uses the recursive definitions of $+$ and $\cdot$ to interpret the full arithmetic in $Th_\omega(\mathbb{N}, S, h)$ ([9, Section 1]).

W. Thomas generalized their result to the case where one has a strictly monotone skipping function $h : \mathbb{N} \to \mathbb{N}$. He first defined a function g in $(\mathbb{N}, S, h)$ with the property that $M := \{a \in \mathbb{N} : g^{-1}(a) \text{ is infinite}\}$ is infinite and definable. Then, he relativized the previous proof to M defining addition and multiplication on M, which enabled him to interpret full arithmetic in $Th_\omega(\mathbb{N}, S, h)$. For the convenience of the reader, we will give the main steps of the above argument, and since we will apply it to a subset of P_r, for clarity of exposition, we will replace $\mathbb{N}$ by E, a countable discretely ordered set with a minimum.

Claim 2.16. Let $(E, \leq)$ be a countable infinite discretely totally ordered set with a minimum and h a strictly increasing regular skipping function. Then there is a function g satisfying $(\star)$ definable in $Th_\omega(E, \leq, h)$.

Proof of Claim: Denote by S the successor function on E. Let $g(x) = n$ if $x = h^m(S(h(n)))$ for some n, $m \in \mathbb{N}$, and $g(x) = 0$, otherwise. Such a function g is well defined. Suppose $h^m(S(h(n))) = h^{m+k}(S(h(n')))$, with $k \neq 0$; then $S(h(n))$ would belong to the image of h, a contradiction, and $h^m(S(h(n))) \neq h^m(S(h(n')))$, with $n \neq n'$ since h is strictly increasing.

By construction, $g^{-1}(n)$ is infinite: It is equal to $\{h^m(S(h(n))) : m \in \mathbb{N}\}$.

Finally, g is definable in $Th_\omega(E, S, h)$. Let

$$G(x, y) := \forall \alpha \; (x \in \alpha \; \& \forall z \; (h(z) \in \alpha \to z \in \alpha) \to S(h(y))) \in \alpha.$$

Then $g(x) = y$ iff $G(x, y) \vee (\forall u \neg G(x, u) \; \& \; y = 0)$ holds. □

Claim 2.17. There exists a formula $F(., ., .)$ in $Th_\omega(E, \leq, g)$ such that, for any finite subset $R \subset E \times E$, there exists a finite subset α of E such that $F(\alpha, x, y)$ holds iff $(x, y) \in R$.

Proof of Claim: Let $R := \{(x_1, y_1), \ldots, (x_k, y_k)\}$. Since g is surjective, there exists n_1 such that $g(n_1) = x_1$. Since $g^{-1}(y_1)$ is infinite, there exists $n_2 > n_1$ such that $g(n_2) = y_1$. Then we find $n_3 > n_2$ such that $g(n_3) = x_2$, etc. So let $\alpha := \{n_1, n_2, \cdots, n_{2k-1}, n_{2k}\}$ with $n_1 < n_2 < \cdots < n_{2k}$ and $g(n_{2i-1}) = x_i$, $g(n_{2i}) = y_i$.

We define two auxiliary formulas: $Od(\alpha, x)$ and $Next(\alpha, x, y)$, where assuming that we enumerated α respecting the order on E, $Od(\alpha, x)$ means that x belongs to

α and has an odd index and $Next(\alpha, x, y)$ means that x, y belong to α and y is the next element in the enumeration after x.

$Next(\alpha, x, y) := x \in \alpha \ \& \ y \in \alpha \ \& x < y \ \& \ \forall z \ (x < z < y \to \neg(z \in \alpha))$.

$Od(\alpha, x) := x \in \alpha \ \& \ \forall \beta \ ((\beta \subset \alpha \ \& \ \forall y) \ y \in \alpha \ \& \forall z \neg Next \ (\alpha, z, y) \to y \in \beta) \ \& \ \forall y \ \forall z \forall u \ (y \in \beta \ \& \ Next(\alpha, y, u) \ \& \ Next(\alpha, u, z) \to z \in \beta) \to x \in \beta)$.

Let $F(\alpha, x, y) := \exists u \exists v \ (u \in \alpha \ \& \ v \in \alpha \ \& \ Od(\alpha, u) \ \& \ Next(\alpha, u, v) \ \& \ g(u) = x \ \& \ g(v) = y)$. □

Claim 2.18. Assuming such formula F exists, let us show we can interpret $(\mathbb{N}, +, \cdot)$ in $Th_\omega(E, \leq, h)$. Recall that S denotes the successor function on E.

Proof of Claim: First we construct an auxiliary formula depending on α and z expressing that, on the interval $(0, z)$, the finite relation coded by α is 1 to 1.

$Func(\alpha, z) := \forall x \ (x \leq z \to \exists! y \, F(\alpha, x, y)$. We enumerate E respecting the order, $E = (e_n)_{n \in \mathbb{N}}$. We define an operation $\oplus$ (respectively, $\otimes$) on E such that $e_{n_1} \oplus e_{n_2} = e_{n_1 + n_2}$ (respectively, $e_{n_1} \otimes e_{n_2} = e_{n_1 \cdot n_2}$). Denote by 0_E the smallest element of E (it is definable with $\leq$).

This operation $\oplus$ on E with $(e_{n_1} = x, e_{n_2} = y, e_{n_1 + n_2} = z)$ is then defined by

$$\exists \alpha \ Func(\alpha, y) \ \& \ (0_E, e_{n_1}) \in \alpha \ \& \ \forall (u, v)(u < y \ \& \ (u, v) \in \alpha \to (S(u), S(v)) \in \alpha) \ \& \ (y, z) \in \alpha.$$

The operation $\otimes$ on E $(e_{n_1} = x, e_{n_2} = y, e_{n_1 . n_2} = z)$ is defined by

$$(0_E, x) \in \alpha, \ (y, z) \in \alpha \ \& \ \forall (u, v)(u < y \ \& \ (u, v) \in \alpha \to (u \oplus x, v \oplus x) \in \alpha),$$

where $u \oplus x$ has been defined by the preceding formula. □

Finally, we will show how to adapt the above proof if we only have a strictly increasing skipping function h. First, one constructs a function g with infinitely many infinite inverse images definable in $Th_\omega(E, S, h)$, then one shows that the set of elements with that property is definable, and finally one relativizes the above results to that definable set.

Claim 2.19. There is a definable function g in $Th_\omega(E, S, h)$ with infinitely many infinite inverse images.

Proof of Claim: Define $g(x) := y$ if $x = h^m(S(h(y)))$ for some m and if there is no z such that $h(z) = S(h(y))$, and otherwise set $g(x) = 0$.

Let $G(x, y) := \forall \alpha (x \in \alpha \& \forall z ((h(z) \in \alpha \to z \in \alpha) \& (\neg(\exists z h(z) = S(h(y))))) \to S(h(y)) \in \alpha)$.

Then $g(x) = y$ iff $G(x, y) \ \vee \ (\forall u \ \neg G(x, u) \ \& \ y = 0)$. □

Claim 2.20. The set $I(g) := \{a \in E : g^{-1}(a)$ is infinite$\}$ is definable in $(E, \leq, h)$.

Proof of Claim: $x \in I(g)$ iff $\forall y \ \exists z \ (z > y \ \& \ g(z) = x)$ □

Now the proof of the theorem is complete. We first define a skipping function h on P_r in the structure $(R, +, 0, \preceq, V_r, V_s, \cdot r, \cdot s, \cdot r_s)$. Then we define a function g on a definable subset $I(g)$ of P_r in $Th_\omega(P_r, \preceq, \cdot r, h)$. We apply the Claims 2.15, 2.16 to the definable set $(I(g), \preceq, g \restriction_{I(g)})$, and so we interpret the full arithmetic in $Th_\omega(I(g), \preceq, g \restriction_{I(g)})$. Therefore, using Lemma 2.10, also in $Th(R, +, 0, V_r, \preceq, \cdot r, h)$ and ultimately in $Th(R, +, 0, V_r, V_s, \preceq, \cdot r, \cdot s, \cdot r_s)$. Note that hypothesis $(\mathbf{C+})_r$ was used in Lemma 2.10 and hypothesis $(\mathbf{C}\times)$ in Lemma 2.12. □

Now we will put further assumptions on R, namely that any element of R has an r-representation. It will allow us to define first a skipping function on a definable finite partition of P_r and then multiplication in the structure $(R, +, -, 0, \preceq, V_r, V_s, .u; u \in R^\star)$, whenever r and s are two non-invertible elements of $R^\star$ that are multiplicatively independent. We will use the notion of interpretability as defined in [12, Chapter 5, Section 3] (see also the example below the following definition).

Definition 2.10. We consider the compatibility of any r-representation and the δ-function (or, equivalently the pre-ordering $\preceq$). We say that assumption $(\mathbf{Rep})_r$ on R is satisfied whenever the following conditions hold:

- There exists a subset $A \subset \{a \in R^\star : a \prec r\}$ such that any two distinct elements $u_i, u_j \in A$ are incongruent modulo r or, equivalently, are distinct representatives of $R/((r.R) \setminus \{0\})$;
- There exists $R_0 \subset R$ such that $(R, +, \cdot, 0, 1)$ is interpretable with R_0 with the induced operations, where each element of $u \in R_0^\star$ has an *r-representation* of the form $u = \sum_{n=0}^{k} r^n.u_n$ with $u_k \neq 0$ and $u_n \in A$ for $0 \leq n \leq k$, and $r^k \preceq u \prec r^{k+1}$ and conversely any element u of that form belongs to R_0.

If, in addition, such a subset A can be chosen finite, we will denote the resulting assumption by $(\mathbf{Rep})_{r,fin}$.

For instance, if $R = \mathbb{Z}$ and δ is the logarithm of the absolute value, $R_0 = \mathbb{N}$. About the interpretation, a positive integer n can be represented as the pair $(n, 0) \in \mathbb{N} \times \mathbb{N}$ and a negative integer m is represented as $(0, m) \in \mathbb{N} \times \mathbb{N}$. Then to define addition, we have $(a, 0) + (0, b) = (a - b, 0)$ whenever $a \geq b$, and $(a, 0) + (0, b) = (0, b - a)$, otherwise. Formally, $\mathbb{Z}$ is in one-to-one correspondence with a definable subset of $\mathbb{N} \times \mathbb{N}$, and operations in $\mathbb{Z}$ are definable in this new set.

One could also impose further (definable) conditions on the r-representations to get uniqueness. For instance, one could allow two sets of digits, say A and A', but impose that all the coefficients belong either to A or to A'.

Under assumption $(\mathbf{Rep})_{r,fin}$, we associate with an element of $R_0^\star$ a finite word over the alphabet A.

Remark 2.21. We can make the following observations:

(1) If R satisfies $(\mathbf{Rep})_{r,fin}$, then it also satisfies $(\mathbf{Rep})_{r^n,fin}$, with $n \geq 2$;
(2) Let R be a commutative integral domain. Let $\alpha \in R$ and $A \subset \mathbb{Z}$. Then $\{\alpha, A\}$ is called *a number system* for R if any $u \in R$ has a unique representation of the form $\sum_{i=0}^{k} c_i.\alpha^i$, $c_i \in A$ and $c_k \neq 0$ if $u \neq 0$. It is a *canonical number system* if $A \subset \mathbb{N}$.

The only integral domains having a number system are either polynomial rings over $\mathbb{F}_p$, or of the form $\mathbb{Z}[\alpha]$, where α is algebraic over $\mathbb{Q}$ [15, Theorem 1].

(3) There are also results in the non-integral case, for instance in the case of a ring of the form $\mathbb{Z}[X]/(P(X))$, where $P(X)$ is not necessarily irreducible [1, 16]. In [1], conditions on the coefficients of the polynomial $P(X)$ under which P is a base of the canonical system are given.

Remark 2.22. Note that adding $-$ to the structure $(R, +, 0, \preceq, V_r, V_s)$ and considering therefore $(R, +, -, 0, \preceq, V_r, V_s)$ has an importance in terms of the complexity of the corresponding formulas. For instance, suppose that we consider the formula $u = V_r(x - y)$. If $-$ is not in the language of our structure, then the former atomic formula is equivalent to an existential formula such as $\exists z(x = y + z \& u = V_r(z))$.

Lemma 2.23. *Under assumption* $(\mathbf{Rep})_r$*, the following relations are first-order definable in* $(R, +, -, 0, V_r, \preceq)$*, let* $u \in R_0$:

$X_r(u_0, u)$ *expressing that* $u_0 \in P_r$ *occurs in the r-representation of* u *(with some coefficient)*;

$X_{r,1}(u_0, u)$ *expressing that* $u_0 \in P_r$ *occurs in the r-representation of* u *with coefficient* 1;

$X_1(u)$ *expressing that any element of* P_r *which occurs in the r-representation of* u *occurs with coefficient* 1.

Proof. Since we are assuming that $u \in R_0$, the relations $X_{r,1}$ and X_1 can be expressed using the formulas stated in Remark 2.9. It remains to consider $X_r(u_0, u)$. Then $u_0 \in P_r$, and it occurs in the corresponding r-representation of u iff the following formula holds:

$$V_r(u_0) = u_0 \,\&\, \exists u_0' \exists u_1\, \exists u_2\ (V_r(u_0') = \lambda_r(u_0') = u_0) \,\&\, (((u_0 = V_r(u) \,\&\, u = u_0' + u_2) \vee\ (u_0 = \lambda_r(u) \,\&\, u = u_0' + u_1) \vee\ (u = u_1 + u_0' + u_2)) \,\&\, (\lambda_r(u_2) = \lambda_r(u) \,\&\, u_0 \prec V_r(u_2) \,\&\, \lambda_r(u_1) \prec u_0 \,\&\, V_r(u_1) = V_r(u))).$$

Lemma 2.24. *Under assumption* $(\mathbf{Rep})_r$*, for any* $a \in A$*, the relation* $X_{r,a}$ *is definable in* $(R, +, -, 0, .a, V_r, \preceq)$.

Proof. We have $X_{r,a}(x, y)$ iff $P_r(x)$ and $V_r(y) \preceq x \preceq \lambda_r(y)$ and $\exists y_1 \exists y_2\ (y = y_1 + x.a + y_2 \,\&\, (y_1 \neq 0 \to (\lambda_r(y) = \lambda_r(y_1) \,\&\, x \prec V_r(y_1))) \,\&\, \lambda_r(x.a + y_2) = x \,\&\, (y_2 \neq 0 \to \lambda_r(y_2) \prec x) \,\&\, V_r(x.a + y_2) = V_r(y))$ □

Theorem 2.25. *Assume that* R *satisfies* $(\mathbf{Rep})_{r,fin}$, $(\mathbf{C}+)_r$ *and* $(\mathbf{C}\times)$. *Let* $r, s \in R^\star$ *be two non-invertible elements which are multiplicatively independent. Then the graph of multiplication is definable in* $(R, +, -, 0, \preceq, V_r, V_s, \cdot r, \cdot s, \cdot r_s, \{.a; a \in A\})$*, and the theory of that structure is undecidable.*

In the case where r and s are multiplicatively dependent, note that by Proposition 2.6, V_s is definable in $(R, +, -, 0, V_r, \cdot r)$. We will see in Section 3 that under natural assumptions, the theory of $(R, +, -, 0, \preceq, V_r, \cdot r)$ is decidable.

Lemma 2.26. *Assume that R satisfies hypothesis* (**C**×). *In* $(R, +, -, 0, \preceq, V_r, V_s, \cdot r, \cdot s, \cdot r_s)$ *there is a definable finite partition* $(E_i)_{i\leq d}$ *of* P_{r^n}, *for some natural numbers* $n \geq 1$ *and* $d \geq 1$ (*only depending on* r *and* s), *and a function* $h : P_r \to P_r$ *such that, on each* E_i, *its restriction is a regular skipping function.*

Proof. Since R is a UFD, we may write $r = \mu.p_1^{\alpha_1}.\cdots.p_e^{\alpha_e}$ and $s = \nu.p_1^{\beta_1}.\cdots.p_f^{\beta_f}$, with μ, ν invertible elements, $p_1, \ldots, p_e, \ldots, p_f$ prime elements of R, $\alpha_1, \ldots, \alpha_e, \beta_1, \ldots, \beta_f \in \mathbb{N}$. Depending on the supports of r and s, and the respective multiplicities of the irreducible elements in each of these supports, we will define a partition of P_{r^n}, for some $n \geq 1$. The cardinality of that partition will also be determined in terms of r and s.

In all cases, we will show that we can define a strictly increasing definable function h on P_{r^n}, which satisfies $r^{n.d}.h(r^{n.m}) \prec h(r^{n.m+n.d})$, $d, m \geq 1$. Then one can define a finite partition $(E_i)_{i\leq d}$ of P_{r^n} such that on each E_i, h is a regular skipping function. Let $E_i := \{x \in P_r : \bigwedge_{j=0}^{i-1} r^j.h^{(j)}(x) \in Im(h) \ \& \ r^i.h(x) \notin Im(h)\}$, where $h^{(j)}$ denotes the composition of h, j times with itself.

(i) The case where neither the support of r, nor the support of s is included in the other one, has been dealt with in Proposition 2.14.

(ii) Assume that the support of s is strictly included in the support of r, namely $f < e$ and for $1 \leq i \leq f$, $\frac{\alpha_i}{\beta_i} = \frac{\alpha}{\beta}$ with $\alpha, \ \beta \in \mathbb{N}^\star$. So $r^\beta = s^\alpha.s_1$ with $s, \ s_1$ coprime. Without loss of generality, we replace r with r^β and s by s^α, and so we have $r = s.s_1$.

By Lemma 2.1, $s \prec r$ and so $s^n \prec r^n$, and if m is the smallest natural number such that $r^n \prec s^m$, $m \geq n+1$. As in Lemma 2.12, we define $h_1(r^n) := s^m$.

Let d be the smallest natural number such that $s \prec s_1^d$; d will be equal to the cardinality of that partition.

By our choice of m, $s^{m-1} \prec r^n$, so $s^{m-1}.r^d \prec r^{n+d}$, i.e., $s^{m-1}.s^d.s_1^d \prec r^n.r^d$. We have $s^m.s^d = s^{m-1}.s.s^d \prec s^{m-1}.s^d.s_1^d \preceq r^n.r^d$, and so $h_1(r^n).s^d \prec h_1(r^n.r^d)$.

We have $V_s(r^n) = V_s(s^n.s_1^n) = s^n$. Define $g : P_s \to P_r$ as the function which sends s^n to r^n; $g(x) = y$ is definable by the formula $V_s(y) = x$. It is strictly increasing since $s \prec s.s_1 = r$ and so $s^n \prec r^n$.

We define $h = g \circ h_1 : P_r \to P_r : r^n \to g(h_1(r^n))$, and it has the property that $h(r^n).r^d = g(h_1(r^n)).g(r^d) \prec g(h_1(r^n.r^d)) = h(r^n.r^d)$. So there exists $z \in P_r - im(h)$ with $h(r^n) \prec z \prec h(r^n.r^d)$, and h is definable as the composition of two definable functions.

(iii) Assume that the support of s is included in the support of r, namely $f \leq e$, and assume without loss of generality that $1 = \frac{\alpha_1}{\beta_1} = min\{\frac{\alpha_i}{\beta_i} : 1 \leq i \leq f\}$, and $\frac{\alpha_f}{\beta_f} = max\{\frac{\alpha_i}{\beta_i} : 1 \leq i \leq f\} > 1$ since r^{β_1} and r (respectively, s^{α_1} and s) are multiplicatively dependent. In this case, we will replace P_r with $P_{r^{\beta_1}}$.

First define $h_1 : P_r \to P_s : r^n \to s^m$, where $m = \lceil n.\frac{\alpha_f}{\beta_f} \rceil$. This function is strictly increasing and definable by the formula: $h_1(x) = y$ iff $\forall u \ (y \preceq V_s(u) \to x \preceq V_r(u))$.

Let $u = \epsilon.p_1^{\gamma_1}.\cdots.p_e^{\gamma_e}$, where ϵ is invertible and $\gamma_i \in \mathbb{N}$. (We may restrict ourselves to this case since the irreducible elements of R occurring in the support of

u different from $p_1, \ldots, p_e$ do not play a role when we apply the functions V_r and V_s.)

By Lemma 2.1, $y = s^{\ell_1} \prec V_s(u)$ if $\ell_1 < min\{\lfloor \frac{\gamma_i}{\alpha_i} \rfloor; 1 \leq i \leq e\}$ and $x = r^{\ell_2} \prec V_r(u)$ if $\ell_2 < min\{\lfloor \frac{\gamma_i}{\beta_i} \rfloor; 1 \leq i \leq e\}$.

Let $g : P_s \to P_r : s^\ell \to r^\ell$. The function g is definable and strictly increasing. Let $\phi(y) := \forall u\ (y \preceq V_r(u) \to x \preceq V_s(u))$. We define $g(x) = y$ by

$$V_r(y) = y\ \&\ \phi(y)\ \&\ \forall z\ (\phi(z) \to y \preceq z).$$

We define $h := g \circ h_1$, which sends r^ℓ to r^k, where $k := \lceil \ell.\frac{\alpha_f}{\beta_f} \rceil$. The function h is strictly increasing as the composition of two strictly increasing functions, and it has the property that for all $x \in P_r$ there is $z \in P_r$ with $h(x) \prec z \prec h(x.r^{\beta_f})$. This follows from the fact that $r^{\beta_\ell}.h(r^\ell) \prec h(r^{\ell+\beta_f}) = h(r^\ell).r^{\alpha_f}$ since $\beta_f < \alpha_f$. Indeed, $\lceil (\ell + \beta_f).\frac{\alpha_f}{\beta_f} \rceil = \lceil \ell.\frac{\alpha_f}{\beta_f} \rceil + \alpha_f$. □

Proposition 2.27. *Assume that R satisfies hypothesis $(\mathbf{C}\times)$ and that we have a definable partition $(E_i)_{i \leq d}$ of P_r and a regular skipping function h on E_i. In $(R, +, -, 0, \preceq, V_r, \cdot r, h)$, we may define functions $H_i(x, y) : P_r \times E_i \to P_r$ with the following properties. For all $x \in P_r$, $H_i(x, .)$ is injective on E_i, and for all $y \in E_i$, we have $x \preceq H_i(x, y)$.*

Proof. Recall that S denotes the successor function on P_r (given by scalar multiplication by $\cdot r$). Let $H_i(x, y) = h^{(t)}(S \circ h(y))$, where t is minimal such that $h^{(t)}(S \circ h(y)) \succeq x$. Since h is strictly increasing, such a t exists.

Let us show that $H_i(x, .)$ is injective. Suppose that $H_i(x, y) = H_i(x, y')$. So $h^{(t)}(S \circ h(y)) = h^{(t')}(S \circ h(y'))$. Without loss of generality, $t \geq t'$, since h is injective we get that $h^{(t-t')}(S \circ h(y)) = S \circ h(y')$. Since $S \circ h(y') \notin im(h)$, we have that $t = t'$ and using again the injectivity of h, that $y = y'$.

Let $\psi(u, x, y) := u \neq 0\ \&\ X_{r,1}(S \circ h(y), u)\ \&\ \forall t\ (t \prec x\ \&\ X_{r,1}(t, u) \to X_{r,1}(h(t), u))$.

We define H_i in the following way: $H_i(x, y) = z$ iff

$$\exists u \forall v\ [\psi(u, x, y) \& (\psi(v, x, y) \to u \preceq v) \& P_r(z)\ \&\ X_{r,1}(z, u)$$
$$\&\ \forall w((P_r(w)\ \&\ X_{r,1}(w, u)) \to w \preceq z)].$$

□

Remark 2.28. In the previous proposition, one can replace $(R, +, -, 0, \preceq, V_r, \cdot r, h)$ with $(R, +, -, 0, \preceq, V_r, V_s, \cdot r, \cdot r_s)$. Strictly speaking, in a first order structure, functions are defined over the whole domain, but h is only defined over P_r (or P_{r^n}). Of course, as an alternative, one can also consider that $h(x)$ is zero whenever x does not belong to the domain of h.

Definition 2.11. We define $MaxH_i(x, y) : P_r \times E_i \to P_r$ as $max\{H_i(x, y') : y' \preceq y\}$.

Proof of Theorem 2.25. Recall that we work in the language $\mathcal{L} := \{+, -, 0, V_r, V_s, \prec, \cdot r, \cdot s, \cdot r_s, \{.a; a \in A\}\}$. Assume that the partition of P_r constructed above has c elements, namely $P_r = \sqcup_{i=1}^{c} E_i$.

First, using the functions H_i, given $u,\ w \in R$, we express that the coefficients of the r-representations of u, respectively of w, restricted to E_i are the same between two powers $u_1 \prec u_2$ of r that we denote as follows: $v = w\ \restriction_{[u_1 u_2[\cap E_i}$.

Let L_i be the following 4-ary relation $L_i \subset R \times R \times P_r \times P_r$:

$$L_i(v, w, u_1, u_2) := P_r(u_1) \,\&\, P_r(u_2) \,\&u_1 \prec u_2 \,\&\, MaxH_i(u_1, \lambda_r(v)) \prec u_2\&$$
$$\forall u\ (P_r(u) \,\&\, u \in E_i \rightarrow (\bigwedge_{a\in A} X_{r,a}(u, v) \leftrightarrow X_{r,a}(H_i(u_1, u), w))).$$

Then, define $L(v, w_1, \ldots, w_c, u_1, u_2)$ as $\bigwedge_{i=1}^{c} L_i(v, w_i, u_1, u_2)$.

Letting $x, y, z \in R$, we want to express by an $\mathcal{L}$-formula $\times(x, y, z)$ that $x.y = z$. Without loss of generality, we assume that $y \neq 0$ and that the r-representation of $y := \sum_{k=0}^{\ell-1} a_k.r^k$, with $\ell \geq 1$, $a_k \in A$, $a_{\ell-1} \neq 0$. Then $x.y = \sum_{k=0}^{\ell-1} x.a_k.r^k$, and note that the scalar multiplication $.a_k \in A$ is in our language $\mathcal{L}$.

The idea is the same as in [34]; however, as in [36], we slightly modify the coding by adding an element which will be used as a counter.

We will make use of an auxiliary element $y_\ell \in R$ such that

$$\chi(y, y_\ell) := (\lambda_r(y_\ell) = \lambda_r(y) \,\&\, \forall u\ (X_r(u, y_\ell) \rightarrow X_{r,1}(u, y_\ell)))$$

holds; the r-representation of y_ℓ solely consists of 1's, and it has the same length as the r-representation of y. It will serve as a counter: we will construct $x.y$ in ℓ steps.

We will code the following sequence: Start with the subsequence $(0, y, y_\ell)$. Then the second subsequence is $(x.a_{\ell-1}, y - a_{\ell-1}.\lambda_r(y), y_\ell - \lambda_r(y_\ell))$. To construct the next element, we make a disjunction of cases whether $a_{\ell-2}$ is zero or not.

If $\lambda_r(y_\ell - \lambda_r(y_\ell)) = \lambda_r(y - a_{\ell-1}.\lambda_r(y))$, then the next element is

$$(x.a_{\ell-1}.r + x.a_{\ell-2}, y - a_{\ell-1}.\lambda_r(y) - a_{\ell-2}\lambda_r(y - \lambda_r(y)), y_\ell - \lambda_r(y_\ell) - \lambda_r(y_\ell - \lambda_r(y_\ell))),$$

and if $\lambda_r(y - a_{\ell-1}.\lambda_r(y)) \prec \lambda_r(y_\ell - \lambda_r(y_\ell))$, the next element is

$$(x.a_{\ell-1}.r, y - a_{\ell-1}.\lambda_r(y), y_\ell - \lambda_r(y_\ell) - \lambda_r(y_\ell - \lambda_r(y_\ell))).$$

We proceed like that until we reach an element of the form $(x.a_{\ell-1}.r^{\ell-1} + \cdots + x.a_0, 0, 0)$, namely $(x.y, 0, 0)$.

In order to code up that sequence, we will separate each subsequence from the next by a semicolon and use colons for distinguishing between elements of a subsequence. We make use of *simple* markers and *double* markers; the simple markers will replace the commas, and the double markers, the semicolons. To that end, we use $(w, w') \in R^2$ whose r-representations only contain 0's and 1's, namely such that $X_1(w)$ & $X_1(w')$ holds (see Lemma 2.23). The sequence w' will only be used for distinguishing between simple and double markers.

A simple marker is a sequence $((0, 1), (0, 0))$ and a double marker $((0, 1), (0, 1))$ occurring in (w, w'). More formally, we will define a marker (simple or double) as a power t of r which in addition satisfies $SM(t, w, w') := t \in P_r$ and t occurs in w but not in w' and the value t' such that $t'.r = t$ occurs neither in w nor in w'. So, formally, $X_{r,1}(t, w)$ & $\neg X_{r,1}(t, w')$ & $(\forall t'\ (t'.r = t \rightarrow (\neg X_{r,1}(t', w)$ & $\neg X_{r,1}(t', w'))))$.

$DM(t, w, w') := t \in P_r$ and t occurs both in w and in w', but t', where $t'.r = t$, does not occur neither in w, nor in w'. So, formally, $X_{r,1}(t, w)$ & $X_{r,1}(t, w')$ & $(\forall t'\ (t'.r = t \rightarrow (\neg X_{r,1}(t.r, w)\ \neg X_{r,1}(t.r, w'))))$.

Then we have to indicate where to read the result; the marker t is the last simple marker if it is equal to $\lambda_r(w)$. A marker t' is the successor of

another t, if it is the least power t' of r which occurs in w with $t \prec t'$, namely $X_{r,1}(t, w)$ & $X_{r,1}(t', w)$ & $\forall t''$ $(X_{r,1}(t'', w)$ & $t \prec t'' \rightarrow t' \preceq t'')$, and we will denote that power t' by $S_w(t)$. We can iterate that operation defining for any natural number $n \geq 1$, $S_w^{(n)}(t) := S_w \circ S_w^{(n-1)}(t)$.

A marker t in w is the last double marker, denoted by $LDM(w, w')$ if $t = \lambda_r(w) = \lambda_r(w')$. The power of t occurring in w preceding it is a simple marker and is characterized by $t = PLM(w, w')$ if $SM(t, w, w')$ & $S_w(t) = LDM(w, w')$, and finally the last double marker preceding $LDM(w, w')$ is characterized by $t = P^{(2)}LM(w, w')$ if $DM(t, w, w')$ & $S_w^{(2)}(t) = LDM(w, w')$.

Set $y_{\ell,0} := y_\ell$, and suppose that at step $0 \leq j - 1 \leq \ell$, we have the sequence $(v, v', y_{\ell,j-1})$; then at step j, we get either as follows

(1) $(v.r + x.a_{\ell-(j-1)}, v' - \lambda_r(v').a_{\ell-(j-1)}, y_{\ell,j-1} - \lambda_r(y_{\ell,j-1}))$, if $(\lambda_r(y_{\ell,j-1}) = \lambda_r(v')$& $X_{r,a_{\ell-(j-1)}}(\lambda_r(v'), v'))$;
(2) or $(v.r, v', y_{\ell,j-1} - \lambda_r(y_{\ell,j-1}))$ if $\lambda_r(v') \prec \lambda_r(y_{\ell,j-1})$.

Then we replace commas with simple markers and semicolons with double markers and add that these markers are successors. Furthermore, supposing that two successive markers are $t_1 \prec t_2$, we then use the relation L to express that between $t_1 \prec t_2$ we have the element v (for instance).

Using the relation L to express that between two successive markers, say $t_1 \prec t_2$, $\bigwedge_{i=1}^{c} w_i | [t_1 t_2[$ is equal (for instance) to v, we can write down the following formula:

In case (1): $a_{\ell-j} \neq 0$, i.e., $\lambda_r(y_{\ell,j}) = \lambda_r(v'))$, we get the formula $\pi_{ind,1}(x, v, v', y_{\ell,j}, u, \mathbf{w})$:

$$(L(v.r + x.a_{\ell-(j-1)}, \mathbf{w}, u, S_w(u)) \,\&\, L(v' - \lambda_r(v').a_{\ell-j}, \mathbf{w}, S_w(u), S_w^{(2)}(u)) \,\&$$
$$L(y_{\ell,j} - \lambda_r(y_{\ell,j}), \mathbf{w}, S_w^{(2)}(u), S_w^{(3)}(u))) \,\&\, DM(u, w, w') \,\&\, SM(S_w(u), w, w')$$
$$\&\, SM(S_w^{(2)}(u), w, w');$$

In case (2): $a_{\ell-j} = 0$, i.e., $\lambda_r(v') \prec \lambda_r(y_{\ell,j})$, we therefore obtain the formula $\pi_{ind,0}(x, v, v', y_{\ell,j}, u, \mathbf{w})$:

$$L(v.r, \mathbf{w}, u, S_w(u)) \& L(v', \mathbf{w}, S_w(u), S_w^{(2)}(u)) \& L(y_{\ell,j} - \lambda_r(y_{\ell,j}), \mathbf{w}, S_w^{(2)}(u), S_w^{(3)}(u)) \,\&$$
$$DM(u, w, w') \,\&\, SM(S_w(u), w, w') \,\&\, SM(S_w^{(2)}(u), w, w').$$

We begin with the sequence $(0, y, y_\ell)$ that will be coded by the formula $\pi_{init}(y, y_\ell, w, w', \mathbf{w})$

$$DM(1, w, w') \,\&\, L(0, \mathbf{w}, 1, S_w(1)) \,\&\, L(y, \mathbf{w}, S_w(1), S_w^{(2)}(1)) \,\& L(y_\ell, \mathbf{w}, S_w^{(2)}(1), S_w^{(3)}(1))$$
$$\&\, SM(S_w(1), w, w') \,\&\, SM(S_w^{(2)}(1), w, w'),$$

and then depending on whether the coefficient of r^k in the r-representation of y is zero or not, we describe successive steps in the multiplication of x by $a_{\ell-1}.r^{\ell-1-k} + \cdots + a_{\ell-1-k}$, $0 \leq k \leq \ell - 1$, and finally we express by the formula $\pi_{final}(z, \mathbf{w}, w, w')$ that the last one is of the form $(z, 0)$, namely

$$L(z, \mathbf{w}, P^{(2)}LM(w, w'), PLM(w, w')) \,\&\, L(0, \mathbf{w}, PLM(w, w'), LDM(w, w')).$$

Now putting all these together, we are ready to write down the formula $\pi_{mult}(x, y, z)$. For readability, we will denote the tuple $(w_1, \ldots, w_c)$ by $\mathbf{w}$:

$$\exists w_1 \exists w_2 \cdots \exists w_c \exists w \exists w' \exists y_\ell \ (X_1(w) \ \& \ X_1(w') \ \& \ \chi(y, y_\ell) \ \& \ \pi_{init}(y, y_\ell, w, w', \mathbf{w})$$

$$\& \ \forall u \forall v \forall v' \forall y'_\ell \left(\bigwedge_{a \in A} ((DM(u, w, w') \ \& \ L(v, \mathbf{w}, u, S_w(u)) \ \& \ L(v', \mathbf{w}, S_w(u), S_w^{(2)}(u)) \ \&\right.$$

$$L(y'_\ell, \mathbf{w}, S_w^{(2)}(u), S_w^{(3)}(u)) \ \& \ X_{r,a}(\lambda_r(v'), v') \ \& \ SM(S_w(u), w, w') \ \& \ SM(S_w^{(2)}(u), w, w') \ \&$$

$$\& \ [\lambda_r(y'_\ell) = \lambda_r(v')) \rightarrow \ \pi_{ind,1}(x, v, v', y'_\ell, S_w^{(3)}(u))]$$

$$\& \ [\lambda_r(v') \prec \lambda_r(y'_\ell) \rightarrow \pi_{ind,0}(x, v, v', y'_\ell, S_w^{(3)}(u))]$$

$$\& \ \pi_{final}(z, \mathbf{w}, w, w'). \qquad \square$$

3. DECIDABILITY RESULTS

As recalled in the introduction, FA-presentable structures or *automatic* structures have been introduced by B. Hodgson [13, Definition 2.2.2] and further developed by a number of authors. See for instance [20].

In this section, we would like to determine conditions under which an integral commutative domain R (not necessarily Euclidean) is FA-presentable. We work then under hypothesis $(\mathbf{Rep})_{r,fin}$, for some (non-invertible) element $r \in R^\star$ (see Definition 2.10). Let $A := \{c_i : i \in I\}$, I finite, be a set of representatives in R of $R/\langle r \rangle$. Then under assumption $(\mathbf{Rep})_{r,fin}$, one can represent in a unique way an element of R as a finite word over the alphabet A.

So there is a bijection between R (respectively, R_0) and the set of finite words over some finite alphabet A. Since we assume in this section r-representability of the elements of R from the start, we will not necessarily suppose that R is Euclidean, but note that one can associate with it a partial pre-ordering $\preceq_r$ given by the length of the r-representation. Namely, define $u_1 \preceq_r u_2$ if $u_1 = \sum_{j=0}^{n} c_j r_j$ and $u_2 = \sum_{j=0}^{m} c'_j r^j$ and $c_n \neq 0$, $c_m \neq 0$, $n \leq m$. We define the functions λ_r and V_r as previously (and so they can be read off as, respectively, the first and last nonzero position in an r-representation). Note that scalar multiplication by r of an element corresponds to a shift of its r-representation. So for the structure $(R, +, -, 0, \lambda_r, V_r, \cdot r)$ to be FA-presentable, it remains to check that the graph of $+$ is recognizable by a finite automaton. So, first, given any two elements c_{i1}, $c_{i2} \in A$, we have to know the r-representation of $c_{i1} + c_{i2}$ and then using that information to know that the carry process stops. If this is the case, we will say that the graph of addition is r-recognizable. These ideas lead to the following proposition.

Proposition 3.1. *Let R be an integral commutative domain, and let $r \in R^\star$ be a non-invertible element. Suppose that R satisfies hypothesis $(\mathbf{Rep})_{r,fin}$. Then if the graph of $+$ is r-recognizable, then the structure $(R, +, -, 0, \lambda_r, V_r, \preceq_r, \cdot r)$ is FA-presentable.* $\square$

ACKNOWLEDGMENTS

We would like to thank the referee for her/his careful reading of the paper.

FUNDING

F. Point is Research Director at the "Fonds de la Recherche Scientifique FRS-FNRS".

REFERENCES

[1] Akiyama, S., Pethő A. (2002). On canonical number systems. *Theoret. Comput. Sci.* 270(1–2): 921–933.
[2] Bès, A. (1997). Undecidable extensions of Büchi arithmetic and Cobham-Semënov theorem. *Journal of Symb. Logic* 62(4):1280–1296.
[3] Bruyère, V., Hansel, G., Michaux, C., Villemaire, R. (1994). Logic and *p*-recognizable sets of integers. *Bull. Belg. Math. Soc.* 1:191–238.
[4] Büchi, J.R. (1960). Weak second-order arithmetic and finite automata. *Z. Math. Logik Grundlag. Math.* 6:66–92.
[5] Cobham, A. (1969). On the base-dependence of sets of numbers recognizable by finite automata. *Math. Systems Theory* 3:186–192.
[6] van den Dries, L. (1985). The field of reals with a predicate for powers of two. *Manuscripta Mathematica* 54:187–195.
[7] van den Dries, L. (1985). On expansions of $\mathbb{Q}$ and $\mathbb{Z}$ (Manuscript).
[8] Durand, F., Rigo, M., On Cobham's theorem. To appear in *Handbook of Automata: from Mathematics to Applications*, European Math. Society Publishing house.
[9] Elgot, C. C., Rabin, M. O. (1966). Decidability and undecidability of extensions of second (first) order theory of generalized) successor. *Journal of Symbolic Logic* 31(2):169–181.
[10] Eklof, P., Fischer, E. (1972). The elementary theory of abelian groups. *Ann. Math. Logic* 4:115–171.
[11] Enderton, H. B. (1972). *A Mathematical Introduction to Logic*. New York, London: Academic Press.
[12] Hodges, W. (1993). Model Theory, *Encyclopedia of Mathematics and its applications* 42, Cambridge: Cambridge University Press.
[13] Hodgson, B. R. (1976). *Théories décidables par automate fini*, Ph.D. Thesis, Université de Montréal.
[14] Jacobson, N. (1985). *Basic Algebra 1*, W.H. Freeman and Compagny, San Francisco (second edition).
[15] Kovács, B., Pethő, A. (1991). Number systems in integral domains, especially in orders of algebraic number fields. *Acta Sci.Math.* 55:287–299.
[16] Madritsch, M. M. (2012). The sum-of-digits function of canonical number systems: Distribution in residue classes. *Journal of Number Theory* 132:2756–2772.
[17] McNaughton, R. (1963). Review. *Journal Symbolic Logic* 29(1):100–102.
[18] Michaux, C., Villemaire, R. (1996). Presburger arithmetic and recognizability of sets of natural numbers by automata: new proofs of Cobham's and Semenov's theorems. *Ann. Pure Appl. Logic* 77:251–277.
[19] Muchnik, An. A. (2003). The definable criterion for definability in Presburger arithmetic and its applications. *Theoret. Comput. Sci.* 290:1433–1444.
[20] Nies, A. (2007). Describing groups. *Bull. Symbolic Logic* 13(3):305–339.
[21] Nies, A., Thomas, R.M. (2008). FA-presentable groups and rings *J. Algebra* 320(2):569–585.
[22] Penzin, Ju. G. (1973). Decidability of the theory of integers with addition, order and multiplication by an arbitrary number. *Mat. Zametki* 13:667–675.
[23] Point, F. (2000). On decidable extensions of Presburger arithmetic: from A. Bertrand numeration systems to Pisot numbers. *Journal of Symbolic Logic* 65(3):1347–1374.

[24] Presburger, M. (1929). Über die Vollstä ndigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt *in Comptes Rendus du I congrès de Mathématiciens des Pays Slaves. Warszawa: 92-101*, translated from the german and with commentaries by Dale Jacquette, On the completeness of a certain system of arithmetic of whole numbers in which addition occurs as the only operation, *Hist. Philos. Logic* **12** (1991), no. 2, 225–233.
[25] Rigo, M. (2008). Syntactical and automatic properties of sets of polynomials over finite fields. *Finite Fields Appl.* 14:258–276.
[26] Rigo, M., Waxweiler, L. (2011). Logical characterization of recognizable sets of polynomials over a finite field. *Int. J. Found. Comput. Sci.* 22:1549–1563.
[27] Robinson, R. M. (1951). Undecidable rings. *Trans. Amer. Math. Soc.* 70:137–159.
[28] Samuel, P. (1971). About euclidean rings. *Journal of Algebra* 19:282–301.
[29] Semënov, A. L. (1977). The Presburger nature of predicates that are regular in two number systems *Sibirsk. Mat. Ž.* 18:403–418.
[30] Sirokofskich, A. (2010). On an exponential predicate in polynomials over finite fields *Proc. Amer. Math. Soc.* 138:2569–2583.
[31] Sirokofskich, A. (2012). Decidability questions for a ring of Laurent polynomials *Ann. Pure Appl. Logic* 163(5):615–619.
[32] Szmielew, W. (1955). Elementary properties of Abelian groups. *Fund. Math.* 41: 203–271.
[33] Thomas, W. (1975). A note on undecidable extensions of monadic second order successor arithmetic. *Arch. Math. Logik* 17:43–44.
[34] Villemaire, R. (1992). The theory of $\langle N, +, V_k, V_l \rangle$ is undecidable. *Theoret. Comput. Sci.* 106(2):337–349.
[35] Villemaire, R. (1992). Joining k- and l-recognizable sets of natural numbers, STACS 92 (Cachan, 1992), 83–94, *Lecture Notes in Comput. Sci* 577, Berlin: Springer.
[36] Waxweiler, L. (2009). *Caractère reconnaissable d'ensembles de polynômes à coefficients dans un corps fini*, Ph. D. thesis, University of Liège, Available from http://orbi.ulg.ac.be/handle/2268/11381 (last accessed 1st December 2014).