Available online at www.sciencedirect.com

ScienceDirect

ELSEVIER

Journal of Algebra 315 (2007) 76–120

JOURNAL OF
Algebra

www.elsevier.com/locate/jalgebra

On von Neumann regular rings with an automorphism

Ehud Hrushovski [a,1], Françoise Point [b,*,2]

[a] Department of Mathematics, Hebrew University at Jerusalem, 91904 Jerusalem, Israel
[b] Institut de Mathématique, Université de Mons-Hainaut, Le Pentagone, 6, avenue du Champ de Mars,
B-7000 Mons, Belgium

Received 13 October 2005

Available online 18 May 2007

Communicated by Jan Saxl

Abstract

We study the first-order theory of Bezout difference rings. In particular we show that rings of sequences very rarely have decidable theories as difference rings, or even decidable model completions.

Keywords: Difference rings; Existentially closed models; (Un)decidable theories

1. Introduction

A *difference ring* is a ring R with a distinguished endomorphism σ (see [7]). In this paper we will assume σ is an automorphism. Difference *fields* enjoy a rich model theory; their study started in the nineties with the axiomatization (denoted by *ACFA*) of the existentially closed difference fields (see [10]). A different kind of difference ring is the ring of sequences over a finite field. A well-known theorem of Büchi implies that these rings too have a decidable theory. A whole spectrum of difference rings incorporating these two types exists, and is of considerable interest; see [15,28]. We study the decidability of such rings, and show that the two known cases of difference fields, and of sequences over finite fields, are quite exceptional: in a rather general setting, away from small neighborhoods of these two classes, the first-order theory T is

[*] Corresponding author.
E-mail addresses: ehud@math.huji.ac.il (E. Hrushovski), point@logique.jussieu.fr (F. Point).

[1] Supported by Israel Science Foundation Grant number 244/03.

[2] Senior Research Associate at the "Fonds National de la Recherche Scientifique."

0021-8693/$ – see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2007.05.006

undecidable, and has no model companion, namely the class of existentially closed models of T is not first-order axiomatizable (see [16, Theorem 8.3.6]). See Proposition 5.1 for a general statement of this kind; see also Section 3 for rings of sequences over infinite fields.

On the other hand, we show there does exist a universal domain for von Neumann regular commutative difference rings, as well as for lattice-ordered commutative difference rings (Sections 7, 8). Thus the model companion fails to exist only for reasons of definability. We also prove decidability results for these rings in the language of modules (Section 2), and for von Neumann regular commutative difference rings whose spectrum is fixed by the automorphism (Section 6), or for which the automorphism has finite order (Sections 4, 6).

In the rest of the introduction we describe the results in more detail.

First, we will consider the difference rings of sequences over a field; we will examine the decidability of such structures first in a language of modules and then in the difference ring language. Let (K, σ) be a perfect difference field and assume that the fixed subfield $C := Fix(K)$ is algebraically closed. Then, consider $(C^{\omega}_{\mathcal{F}}, \sigma_t)$, the ring of sequences over C quotiented out by the Frechet filter $\mathcal{F}$ endowed with the shift automorphism defined by $\sigma_t(c_i)_{\mathcal{F}} = (c_{i+1})_{\mathcal{F}}$. Make the additional assumption on K that its algebraic closure can be embedded in $(C^{\omega}_{F}, \sigma_t)$ with σ_t extending σ. Then every Picard–Vessiot extension associated with a linear difference system over K embeds in $(C^{\omega}_{F}, \sigma_t)$ [28]. We will translate this universality property of $(C^{\omega}_{F}, \sigma_t)$ in the language of modules as follows. Given a K-algebra R with an endomorphism σ, leaving K invariant, one can always consider R as a right module over the skew polynomial ring $K[t; \sigma]$ with the commutation rule $k.t = t.k^{\sigma}$, $k \in K$; the action of t on R is defined by: $r.t = \sigma(r)$, $r \in R$. The skew polynomial ring $K[t; \sigma]$ is right Ore (and left Ore if σ is an automorphism of K).

In the special case of $R := (C^{\omega}_{F}, \sigma_t)$, we will axiomatize its theory T_m as a module over the skew polynomial ring $K[t; \sigma]$, with the previous assumptions on K (see Proposition 2.6). We will show that the theory T_m admits positive quantifier elimination (see Proposition 2.7) and that any difference K-algebra embeds in a model of T_m (see Corollary 2.11). Moreover, we will prove that a quantifier elimination result holds in a richer two-sorted structure, a sort for the module with the usual module language and another sort for the fixed subfield of K with the field language (see Proposition 2.14). So, in that structure, we can quantify both over the module elements and over the fixed subfield elements. (A similar result has been obtained by Moshe Kamensky [22] for the two-sorted theory of modules over $K[t_1, \ldots, t_m]$, where $t_1, \ldots, t_m$ are commuting indeterminates.)

Then, working now in the full ring language, we will show that a partial dichotomy result holds for the class of commutative von Neumann difference rings (R, σ) of characteristic 0. Recall that a commutative von Neumann regular ring is a commutative ring satisfying the following axiom: $\forall x\ \exists y\ (x^2.y = x\ \&\ y^2.x = y)$.

Exactly one of the following holds.

(I) For some natural number n, σ^n fixes the maximal spectrum $MSpec(R)$ of the ring R and we get decidability results for the class of existentially closed such rings (see Propositions 6.6, 6.10). We use the Boolean product representation of commutative von Neumann regular rings [6,12], the decidability of *ACFA* [11], and transfer results due to S. Burris and H. Werner [5].

(II) The theory of any such difference ring is undecidable (see Proposition 5.1). In particular, we will obtain that the theory of non-principal ultraproducts of Picard–Vessiot difference total rings is undecidable (see Corollary 5.3).

We will generalize this undecidability result to the class of Bezout commutative difference rings R of characteristic 0 as follows. Suppose that the fixed subring $Fix(\sigma)$ of R is an integral domain and that for every natural number n there exists a prime ideal π such that $\pi, \ldots, \sigma^n(\pi)$ are pairwise co-maximal and have a trivial intersection with $Fix(\sigma)$. Then, the theory of (R, σ) is undecidable (see Corollary 5.11). An application of this result is the undecidability of the difference ring $\mathbb{C}\{z^{-1}\}$ (see Examples 5.9).

In the characteristic p case, with p a prime number, for von Neumann regular commutative difference rings, whenever the sizes of the orbits are bounded, we obtain a decidability result similar to the one obtained in the characteristic 0 case (see Propositions 6.6, 6.10); and when the automorphism σ has orbits of arbitrarily large cardinalities, in the case where $Fix(\sigma)$ is an infinite field, we obtain an analogous undecidability result (see Proposition 5.1). However, when $Fix(\sigma)$ is finite, we obtain a new class of decidable structures as follows. Let R be the ring of sequences over a finite field, indexed by the integers, with the shift automorphism. Then, the theory of such a ring is decidable as a consequence of a result of Büchi on the decidability of the weak-monadic second-order theory of the natural numbers with the successor function (see Proposition 3.2 and Corollary 3.3). Moreover, we prove that its theory is model-complete (see Proposition 3.4), using finite automata.

Note that our results lead to the question whether there exists a decidable difference ring (R, σ) such that σ has an infinite orbit on $MSpec(R)$ and $Fix(\sigma)$ is infinite.

Finally, we prove an amalgamation result. Let $\mathcal{C}$ be a class of $\mathcal{L}$-structures, let σ be a new function symbol and denote by $\mathcal{C}_\sigma$ the subclass of the elements of $\mathcal{C}$ considered as $\mathcal{L}_\sigma$-structures, where σ is interpreted by an automorphism. When $\mathcal{C}$ is a model-complete class of von Neumann commutative regular rings (these have been identified in the mid-seventies using Fefermann–Vaught transfer type results) we will show that in some cases, the subclass of existentially closed elements of $\mathcal{C}_\sigma$ has a universal domain, namely a model U embedding every countable model in a unique way, up to $Aut(U)$-conjugacy.

Our precise result reads as follows: the classes of commutative von Neumann regular perfect difference rings (where a perfect ring is either a ring of characteristic zero or a ring of characteristic p closed under pth roots), in the language of rings with the pseudo-inverse and extra symbols for the automorphism, its inverse, and pth-roots in characteristic p, have the amalgamation property (see Propositions 7.6, 7.7). So, as a universal class with amalgamation, this is a Robinson class (see [18, §8]). Further, the subclass of its existentially closed models is not elementary (see Proposition 7.11).

We will prove similar results for a subclass of the class of lattice-ordered commutative difference rings (see Proposition 8.3).

2. The theory of modules

The ring $S = K[t; \sigma]$ is a skew polynomial ring over the difference field (K, σ) with the commutation rule given by $k.t = t.k^\sigma$, $k \in K$. We will write any element $p(t)$ of S as $\sum_{i=0}^{n} t^i.a_i$ and we will consider the category of all right S-modules; let T_S denote its theory.

Since σ is an automorphism of K, the ring S is a left and right Euclidean domain and so left and right principal ideal domain (see [8, Proposition 2.1.1]). This implies that any matrix with coefficients in S can be put in diagonal form (see [19]) and so the (p.p.) primitive positive formulas can easily be described.

Proposition 2.1. *(See [19, p. 176].) Let S_0 be a right and left Euclidean domain and A be an $m \times n$ matrix with coefficients in S_0. Then there exist invertible matrices P, Q such that $P.A.Q$*

is diagonal. Moreover, if $d_1, \dots, d_k$ are the non-zero coefficients occurring on the diagonal, then d_i divides d_{i+1}, $1 \leqslant i \leqslant k$.

Corollary 2.2. *Any positive primitive formula $\phi(v)$ is equivalent in T_S to a p.p. formula of the form*: $\bigwedge_i \exists w_i \; w_i.s_i = v.r_i$, $s_i, r_i \in S$.

To the p.p. formula:

$$v.\big(t^n + t^{n-1}.a_{n-1} + \cdots + a_0\big) = 0,$$

we will associate the difference equation:

$$\sigma V = V.A,$$

where A $\in M_n(K)$ and V is the tuple $(v, \sigma v, \dots, \sigma^{n-1} v)$

$$\big(\sigma v \;\; \sigma^2 v \;\; . \; . \;\; \sigma^n v\big) = \big(v \;\; \sigma v \;\; . \; . \;\; \sigma^{n-1} v\big) \begin{pmatrix} 0 & 0 & 0 & \dots & -a_0 \\ 1 & 0 & 0 & \dots & -a_1 \\ & \ddots & & & \vdots \\ & & \ddots & & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}.$$

Note that whenever $a_0 \neq 0$, $A \in GL_n(K)$. Moreover, we may assume that we are in that case since σ is an automorphism.

Now, let us recall some results on Picard–Vessiot extensions which will be useful to understand the theory of modules of our ring of sequences over an algebraically closed field C with the shift σ_t.

Definition 2.3. Let (K, σ) be a difference field and fix a first-order linear system of the form $\sigma Y = Y.A$, where $A \in GL_n(K)$. Suppose R is a commutative K-algebra. Then R is a Picard–Vessiot ring w.r.t. this equation if the following conditions hold:

(1) One may extend σ to an automorphism (also denoted σ) of the ring R.
(2) R has no non-trivial (two-sided) difference ideals.
(3) There exists a matrix U in $GL_n(R)$ such that $\sigma U = U.A$.
(4) No proper K-subalgebra of R satisfies conditions (1), (2), (3).

In the sequel, we will use the following results of [28]. From now on, we will assume that the difference field (K, σ) is perfect (i.e. either of characteristic zero or of characteristic p and closed under pth roots) and that the *subfield $C := Fix(\sigma)$ of constants*, consisting of the elements fixed by the automorphism, is *algebraically closed*.

(1) To a linear difference equation over K, one can associate a unique Picard–Vessiot ring [28, Section 1.1]. This Picard–Vessiot ring is the direct product of finitely many copies of a domain and the automorphism acts as a cyclic permutation of theses copies [28, Corollary 1.16]. If one considers the direct product of the field of fractions of this domain, one obtains a *total* Picard–Vessiot ring.

(2) *Further*, we will now assume that (K, σ) is a difference subfield of $(C^{\omega}_{\mathcal{F}}, \sigma_t)$, that it contains the algebraically closed subfield of constants C and that the algebraic closure of K is included in $C^{\omega}_{\mathcal{F}}$. We will call such difference field a *PV-field*. Let $\sigma Y = Y.A$ be a first-order linear difference system with $A \in GL_n(K)$. Then the Picard–Vessiot ring associated to this system embeds in $C^{\omega}_{\mathcal{F}}$. Moreover, there is a matrix Z in $GL_n(C^{\omega}_{\mathcal{F}})$ such that every solution is a C-linear combination of the columns of Z (see Proposition 4.1 in [28]).

Examples 2.4. Examples of PV-fields are [28, Chapter 1, p. 4]:

$\mathbb{C}(z)$ the field of rational functions over $\mathbb{C}$;
$\mathbb{C}(\{z^{-1}\})$ the fraction field of the ring of power series in z^{-1} that converge in a neighborhood of infinity, with automorphism $(z^{-1} \to z^{-1}/z^{-1} + 1)$;
the field $\mathbb{C}((z^{-1}))$ of Laurent series in z^{-1} and the algebraic closure of $\mathbb{C}((z^{-1}))$ with automorphism $(z^{-1})^{1/m} \to (z^{-1})^{1/m}.(1 + (z^{-1}))^{-1/m}$.

In each case, the embedding into the ring $(\mathbb{C}^{\omega}_{F}, \sigma_t)$ is the following: $f \to (f(0), f(1), \ldots)$.

Definition 2.5. Let $\mathcal{L}_S$ be the language of S-modules, i.e. $\{+, -, 0, .r; r \in S\}$, where $.r$ denotes right multiplication by elements of S.

Let T_m be the following theory:

(1) T_S the theory of all right S-modules,
(2) $\forall g\ \exists f\ (f.t = g)\ \&\ \forall g\ (g.t = 0 \to g = 0)$, "$\sigma$ is an automorphism,"
(3) $\forall g\ \exists f\ (f.p(t) = g)$, with $p(t)$ ranging over the irreducible polynomials of S and $p(0) \neq 0$, "divisibility,"
(4) $\exists v \neq 0\ (v.p(t) = 0)$, with $p(t)$ ranging over the irreducible polynomials of S and $p(0) \neq 0$, "torsion."

Note that (3) and (4) are schemes of axioms, one for each irreducible element $p(t)$ of $S - \{t\}$. Axiom scheme (3) even though it is stated only for irreducible polynomials holds in models of T_m for any polynomial. Using axiom (2), we get axiom scheme (4) for polynomials of the form $t^m.p(t)$ with $p(0) \neq 0$.

Proposition 2.6. *T_m is consistent.*

Proof. Let us show that $C^{\omega}_{\mathcal{F}}$ is a model of T_m. First, it is an S-module with the action of t defined as follows: $m.t = \sigma_t(m)$, $m \in C^{\omega}_{\mathcal{F}}$.

By Proposition 4.1 in [28], the set of solutions of $v.(t^n + t^{n-1}.a_{n-1} + \cdots + a_0) = 0$, with $a_0 \neq 0$ in $C^{\omega}_{\mathcal{F}}$ is a C-vector space of dimension n and so there exists $v \neq 0$ such that $v.(t^n + t^{n-1}.a_{n-1} + \cdots + a_0) = 0$.

It remains to show that $\forall g\ \exists f\ p(t).f = g$ holds in $C^{\omega}_{\mathcal{F}}$, where $p(t) \in S$. Let $g' = (g_i)_{i \in \omega}$ belong to C^{ω} be such that $g = g'_{\mathcal{F}}$. Let $p(t) = t^n + t^{n-1}.a_{n-1} + \cdots + a_0$. We will first define $f' = (f_i)_{i \in \omega}$ in C^{ω} as follows. Choose arbitrarily $f_0, \ldots, f_{n-1}$ and then set $f_n = g_0 - (\sum_{i=0}^{n-1} a_i.f_i)$, and recursively $f_{n+k} = g_k - (\sum_{i=0}^{n-1} a_i.f_{k+i})$. Set $f = f'_{\mathcal{F}}$. □

In the next proposition, we will show that T_m admits positive q.e., namely any p.p. formula is equivalent to a conjunction of atomic formulas.

Proposition 2.7. *In T_m, any p.p. formula $\phi(v_1, \dots, v_n)$ (respectively $\phi(v)$) is equivalent to a conjunction of atomic formulas (respectively to an atomic formula).*

Proof. Write $\phi(v_1, \dots, v_n)$ in the form $\exists \bar{w}\ \bar{w}.A = \bar{v}.B$, where A and B are matrices with coefficients in S. By Proposition 2.1, there exist invertible matrices P and Q such that $P.A.Q$ is a diagonal matrix. So, the formula $\phi(v_1, \dots, v_n)$ is equivalent in any model of T_S to $\exists \bar{w}'\ \bar{w}'.P.A.Q = \bar{v}.B.Q$. Since any model of T_m is divisible, $\phi(v_1, \dots, v_n)$ is equivalent (in T_m) to a conjunction of formulas of the form $\bigwedge_{j=1}^{k} \sum_{i=1}^{n} v_i.t_{i,j} = 0$, where $t_{i,j} \in S$.

If $n = 1$, since S is a right Euclidean ring, $\phi(v_1)$ is equivalent to $v_1.gcd(t_{1,1}, \dots, t_{1,k}) = 0$. □

Corollary 2.8. *Any submodule of any model of T_m is a pure submodule.*

Lemma 2.9. *Let M be a model of T_m. Then for any pair of non-zero polynomials $p_1(t)$, $p_2(t)$ with* $\deg(p_1(t)) > \deg(p_2(t))$ *and* $p_1(0) \neq 0$, *there exists $v \in M$ such that $v.p_1(t) = 0 \wedge v.p_2(t) \neq 0$.*

Proof. We will prove the lemma by induction on the pair of degrees of $p_1(t)$ and $p_2(t)$. The case of a pair of degrees of the form $(d, 0)$, with $d \geqslant 1$, is taken care of by axiom scheme (4) since $p_1(0) \neq 0$.

By axiom scheme (4), there is an element $u \in M - \{0\}$ such that $u.p_1(t) = 0$. Either $u.p_2(t) \neq 0$ and we found the desired element u, or $u.p_2(t) = 0$. In that last case, let $p(t) \in S - \{0\}$ be of minimal degree with $u.p(t) = 0$. So, $p(t)$ is of degree greater than or equal to 1 and, applying the fact that S is right Euclidean, $p(t)$ divides both $p_1(t)$ and $p_2(t)$. Let $q_1(t), q_2(t) \in S - \{0\}$ with $p_1(t) = p(t).q_1(t)$ and $p_2(t) = p(t).q_2(t)$, $1 \leqslant \deg(q_1(t)) < \deg(p_1(t))$ and $\deg(q_2(t)) < \deg(p_2(t))$. Note that $\deg(q_2(t)) < \deg(q_1(t))$ and $q_1(0) \neq 0$. We may apply the induction hypothesis to the pair $(q_1(t), q_2(t))$, so there exists an element $w \in M$ with $w.q_1(t) = 0$ and $w.q_2(t) \neq 0$. By axiom scheme (3) we can find an element $v \in M$ with $v.p(t) = w$ and so we have that $v.p_1(t) = 0$, whereas $v.p_2(t) \neq 0$. □

Proposition 2.10. *T_m is complete and admits quantifier elimination in $\mathcal{L}_S$.*

Proof. We apply the Baur–Monk p.p. elimination theorem for theories of modules (see for instance [26]) and Proposition 2.7.

In order to prove completeness, it suffices to describe the index of p.p. definable subgroups (included in the domain of a model of T_m) in one another. Let M be a model of T_m. Given any two p.p. formulas $\phi(v)$, $\psi(v)$ with $T_S \vdash \psi \rightarrow \phi$, using the proof of Proposition 2.7, we reduce ourselves to consider the case where $\phi(M) = ann(p_1(t))$ and $\psi(M) = ann(p_2(t))$ with $p_1(t), p_2(t) \in S$. Note that since $Fix(\sigma) \cap K$ is infinite, all the indices are either trivial or infinite.

Since σ is an automorphism of K, we may write $p_1(t) = t^{m_1}.q_1'(t) = q_1(t).t^{m_1}$ and $p_2(t) = t^{m_2}.q_2'(t) = q_2(t).t^{m_2}$, for some $q_1(t), q_1'(t), q_2(t), q_2'(t) \in S$, $m_1, m_2 \in \mathbb{N}$, with $q_1(0), q_2(0)$ both non-zero. Applying axiom (2), we have that $ann(p_1(t)) = ann(q_1(t))$ and $ann(p_2(t)) = ann(q_2(t))$. So, $ann(q_2(t)) \subseteq ann(q_1(t))$, which implies by Lemma 2.9, that $\deg(q_1(t)) \geqslant \deg(q_2(t))$.

If $\deg(q_1(t)) > \deg(q_2(t))$, we apply Lemma 2.9 in order to find an element $v \in ann(p_1(t)) - ann(p_2(t))$.

If $\deg(q_1(t)) = \deg(q_2(t))$, we apply the Euclidean algorithm and we get $q_1(t) = q_2(t).k + q(t)$, $k \in K - \{0\}$, $q(t) \in S$ with $\deg(q(t)) < \deg(q_2(t))$. If $q(t) = 0$, we get that $ann(q_1(t)) = ann(q_2(t))$ and so, $ann(p_1(t)) = ann(p_2(t))$.

If $q(t) \neq 0$, we apply Lemma 2.9 to the pair $(q_1(t), q(t))$ and we find an element v belonging to $ann(q_1(t)) - ann(q(t))$ and so it also belongs to $ann(q_1(t)) - ann(q_2(t))$. So, we found an element in $ann(p_1(t)) - ann(p_2(t))$.

Quantifier elimination in T_m then follows from the above completeness result. □

Corollary 2.11. *Let R be a difference ring which is a K-algebra over a PV-field K. Then, as a $K[t;\sigma]$-module, R embeds into some model of T_m.*

Proof. Let us first show that one can embed R into a model of axiom scheme (3). Consider the ring of sequences R^{ω} endowed with the endomorphism $\tilde{\sigma}$ defined as follows: $\tilde{\sigma}((r_i)_{i\in\omega}) := (\sigma(r_{i+1})_{i\in\omega})$, with $r_i \in R$. Let $\mathcal{F}$ be the Frechet filter on ω. Then R embeds into the difference ring $R^{\omega}_{\mathcal{F}}$ of sequences modulo the Frechet filter, sending $r \to (r)_{\mathcal{F}}$ and $(R^{\omega}_{\mathcal{F}}, \tilde{\sigma})$ satisfies axiom scheme (3). The proof of this last assertion is similar to the proof of Proposition 2.6. Namely, let $p(t) = t^n + t^{n-1}.a_{n-1} + \cdots + a_0$ and let $g' = (g_i)_{i\in\omega}$ belong to R^{ω} be such that $g = g'_{\mathcal{F}}$. We first define $f' = (f_i)_{i\in\omega}$ in R^{ω} as follows. Choose arbitrarily $f_0, \ldots, f_{n-1}$ and then set $f_n = g_0^{\sigma^{-n}} - (\sum_{i=0}^{n-1} a_i . f_i)^{\sigma^{-n}}$, and recursively $f_{n+k} = g_k^{\sigma^{-n}} - (\sum_{i=0}^{n-1} a_i . f_{k+i})^{\sigma^{-n}}$. Finally, set $f = f'_{\mathcal{F}}$.

Then it suffices to observe that the direct product: $R^{\omega}_{\mathcal{F}} \oplus C^{\omega}_{\mathcal{F}}$ satisfies (1)–(4). □

In the following corollary, we will use the notion of *splitting algorithm* (see [27, Definition 9]).

Corollary 2.12. *Let K_1 be a recursively presented subfield of K with a splitting algorithm, let S_1 be the corresponding skew polynomial ring and denote by $T_{m,1}$ the corresponding theory of S_1-modules. Then, $T_{m,1}$ is decidable.*

Alternatively, we shall consider a two-sorted theory of modules, with quantification over the module elements and over the elements of the fixed subfield C of K. For each non-zero natural number n, we will add new relation symbols which hold on the n-tuples of C-linearly dependent elements of the module; these predicates will be denoted by D_n, $n \in \omega$; we also add predicates $T_{n,\theta(\bar{x},\bar{y})}$, $n \in \omega$ and θ a formula in the field language, that will hold on pairs of $n+1$ tuples of elements $\{(v_0, \bar{v}), (w_0, \bar{w})\}$ where $\bar{v}$ and $\bar{w}$ are C-linearly independent and (v_0, w_0) lie in the "same" way in the subspaces generated respectively by $\bar{v}$ and by $\bar{w}$. More precisely, the tuple of coefficients of the linear combination expressing v_0 in terms the elements $\bar{v}$ and those expressing w_0 in terms the elements $\bar{w}$ satisfy the formula θ.

Definition 2.13. We will now formally define the language $\mathcal{L}$. It consists of two unary relations symbols: M and C, the sort M will be endowed with the language of S-modules $\mathcal{L}_S$; the sort C with the field language $\mathcal{L}_f$; we have a new function symbol $\cdot$ from $M \times C$ to M; and new relation symbols on M, for each $n \in \omega$ and each open $\mathcal{L}_f$-formula θ, $D_n(.,\ldots,.)$ and $T_{n,\theta}(\bar{v};\bar{w})$.

Let $T_{M,C}$ be the following theory:

(1) the $\mathcal{L}_S$-theory T_m on the sort M,
(2) the $\mathcal{L}_f$-theory of algebraically closed fields on the sort C,
(3) M is a C-vector space with scalar multiplication $\cdot$,
(4) $\forall v \in M\ \forall c \in C\ (v \cdot c).t = (v.t) \cdot c$,
(5) $\forall v \in M\ \forall c \in C\ (v \cdot c).k = (v.k) \cdot c$, for all $k \in K$,
(6) $\forall v_1 \in M \cdots \forall v_n \in M\ \forall c_1 \in C \cdots \forall c_n \in C$
$(\bigvee_{i=1}^{n} c_i \neq 0\ \&\ \sum_{i=1}^{n} v_i . c_i = 0 \leftrightarrow D_n(v_1, \ldots, v_n))$, $n \geqslant 1$, $n \in \omega$,

(7) $\forall v_0 \in M \cdots \forall v_n \in M\ \forall w_0 \in M \cdots \forall w_n \in M\ [\neg D_n(v_1, \ldots, v_n)$ and $\neg D_n(w_1, \ldots, w_n)] \rightarrow [T_{n,\theta}(v_0, v_1, v_2, \ldots, v_n;\ w_0, w_1, w_2, \ldots, w_n)$ iff $(\exists k_1 \neq 0 \cdots \exists k_n \neq 0 \in C\ \exists l_1 \neq 0 \cdots \exists l_n \neq 0 \in C\ \theta(k_1, \ldots, k_n, l_1, \ldots, l_n)$ and $v_0 + v_1.k_1 + \cdots + v_n.k_n = 0$ and $w_0 + w_1.l_1 + \cdots + w_n.l_n = 0)]$, for each open $\mathcal{L}_f$-formula θ and natural number n.

(8) $\exists v_1 \cdots v_d \in M\ (\neg D_d(v_1, \ldots, v_d) \wedge \bigwedge_{i=1}^{d} p(t).v_i = 0)$, $p(t)$ ranging over the irreducible polynomials of S of degree d, $d \in \omega$, "torsion."

Note that in axiom scheme (7), the elements $k_i \in C$ and $l_i \in C$, whenever they exist, are uniquely determined.

Also, in any model of the theory $T_{M,C}$ and any tuple of non-zero elements $v_0, \ldots, v_n \in M$, we have that $D_2(v_0, v_1)$ iff $T_{1,x=x}(v_0, v_1; v_0, v_1)$, and if $n \geqslant 2$,

$T_{n,x=x}(v_0, v_1, \ldots, v_n)$ is equivalent to $D_{n+1}(v_0, v_1, \ldots, v_n)$ and $\neg D_n(v_1, \ldots, v_n)$. Then, by induction on n, we see that we can express $D_{n+1}(v_0, v_1, \ldots, v_n)$ by a quantifier-free formula in the module language augmented by the predicates $T_{n,x=x}$.

Also, we would have gotten similar results, using a simpler language, namely by only adding to the two-sorted language the predicates $T_{n,\theta}$; we would have deleted axiom scheme (6) and in axiom schemes (7) and (9), we would have replaced the occurrences of $D_n(v_1, \ldots, v_n)$ by $\exists c_1 \in C \cdots \exists c_k \in C\ [(\bigvee_{i=1}^{k} c_i \neq 0)\ \&\ \sum_{i=1}^{k} v_i.c_i = 0]$.

Proposition 2.14. *The theory $T_{M,C}$ admits q.e. in $\mathcal{L}$ and is complete.*

Proof. Now we have to consider formulas where the quantified variables are both from the module and from the subfield C included in $Fix(\sigma)$.

The terms $s(v_0, \bar{v}; k_0, \bar{k})$ can be put in the form $\sum_i v_i.(\sum_j t^j.a_j.f_j(k_0, \bar{k}))$, where $v_0, \bar{v}$ are variables ranging over M, $k_0, \bar{k}$ are variables ranging over C, $a_j \in K$ and $f_j(k_0, \bar{k})$ are L_f-terms.

We can rewrite the term $s(v_0, \bar{v}; k_0, \bar{k})$ as

$$\sum_{i=0}^{n} v_i.r_{i0}(t, \bar{k}) + \sum_{i=0}^{n} v_i.r_{i1}(t, \bar{k}).k_0 + \cdots + \sum_{i=0}^{n} v_i.r_{id}(t, \bar{k}).k_0{}^{d}.$$

First, let us assume that there are no predicates $T_{n,\theta}$ appearing in the formula.

Consider the formula: $\exists k_0\ [\bigwedge_i t_i(\bar{v}, k_0, \bar{k}) = 0\ \&\ \bigwedge_j s_j(\bar{v}, k_0, \bar{k}) \neq 0\ \&\ \theta(k_0, \bar{k})]$, where θ is an open $\mathcal{L}_f$-formula. Assume that in all the terms occurring in the above formula, the powers of k_0 that occur are among $\{k_0, \ldots, k_0^d\}$.

We can rewrite it as

$$\exists \bar{l} \Bigg[\bigwedge_{j \in J_1} \sum_{i=0}^{n} v_i.r_{ij0}(t, \bar{k}) + \sum_{i=0}^{n} v_i.r_{ij1}(t, \bar{k}).l_1 + \cdots + \sum_{i=0}^{n} v_i.r_{ijd}(t, \bar{k}).l_d = 0$$

$$\wedge \bigwedge_{j \in J_2} s_j(\bar{v}, \bar{l}, \bar{k}) \neq 0$$

$$\text{and} \quad \exists k_0 \left(\theta(k_0, \bar{l}, \bar{k})\ \&\ \bigwedge_{i=1}^{d} l_i = k_0^i \right) \Bigg].$$

Then we have to make a disjunction of cases according to which subsets of the elements $w_{j\ell} := \sum_{i=0}^{n} v_i.r_{ij\ell}(t,\bar{k})$, $1 \leqslant \ell \leqslant d$, $j \in J_1 \cup J_2$, are linearly independent over C. Thanks to the fact that in the case of linearly independent elements the coefficients are uniquely determined, the above conjunction is equivalent to a disjunction of conjunctions, the conjunctions consisting either of two equations or of one equation and one inequation. Let us examine the conjunctions more closely.

In the case of two equations, we use the predicate $T_{n,\bar{x}=\bar{y}}$ and in the case of one equation and an inequation the negation of this predicate (again we use the fact that the coefficients, if they exist, are unique). Indeed, assume that both sets $\{w_{1j},\dots,w_{dj}\}$, $\{w_{1j'},\dots,w_{dj'}\}$ are linearly independent over C, then:

$[\exists f_1 \cdots \exists f_d \bigwedge_{z=1}^{3} w_{0z} + \sum_{m=1}^{d} w_{mz}\cdot f_m = 0]$ is equivalent to $[\exists f_1 \cdots \exists f_d \bigwedge_{z=1}^{2} w_{0z} + \sum_{m=1}^{d} w_{mz}\cdot f_m = 0]$ and $[\exists f_1 \cdots \exists f_d \bigwedge_{z=1,z=3} w_{0z} + \sum_{m=1}^{d} w_{mz}\cdot f_m = 0]$.

In turn, $[\exists f_1 \cdots \exists f_d \bigwedge_{z=1}^{2} w_{0z} + \sum_{m=1}^{d} w_{mz}\cdot f_m = 0]$ is equivalent to the atomic formula $T_{d,\bar{x}=\bar{y}}(w_{01}, w_{11}, \dots, w_{d1}; w_{02}, w_{12}, \dots, w_{d2})$.

Now, consider the case where an inequation occurs:

$$\exists f_1 \cdots \exists f_d \left[\bigwedge_{z=1}^{2} w_{0z} + \sum_{m=1}^{d} w_{mz}\cdot f_m = 0 \quad \text{and} \quad w_{03} + \sum_{m=1}^{d} w_{m3}\cdot f_m \neq 0\right].$$

It is equivalent to

$$T_{d,\bar{x}=\bar{y}}(w_{01}, w_{11}, \dots, w_{d1}; w_{02}, w_{12}, \dots, w_{d2}) \quad \&$$
$$\neg T_{d,\bar{x}=\bar{y}}(w_{01}, w_{11}, \dots, w_{d1}; w_{03}, w_{13}, \dots, w_{d3}).$$

Suppose now that there are some predicates T_{m,θ_m} or their negations occurring in the above formula. Then we replace each predicate $T_{m,\theta_m}(\bar{s},\bar{s}')$, where $\bar{s},\bar{s}'$ are tuples of terms in the elements $\bar{v}$ with coefficients in S which depend on parameters $\bar{k}, k_0 \subset C$, by:

$$\big(\exists r_1 \neq 0 \cdots \exists r_m \neq 0 \in C\ \exists s_1 \neq 0 \cdots \exists s_m \neq 0 \in C \theta_m(\bar{r},\bar{s})$$

and

$$t_0 + t_1.r_1 + \cdots + t_m.r_m = 0 \quad \& \quad t'_0 + t'_1.s_1 + \cdots + t'_m.s_m = 0\big).$$

Then, we rewrite the terms along coefficients of the form: monomials in $k_0, \bar{l}, \bar{r}, \bar{s}$, that we enumerate in some order: $m_0, \dots, m_d$. So, we get

$$\exists k_0,\ \exists \bar{l} \exists \bar{r} \exists \bar{s} \bigwedge_j \sum_{i=0}^{n'} v_i.r_{ij0}(t,\bar{k}).m_0 + \sum_{i=0}^{n'} v_i.r_{ij1}(t,\bar{k}).m_1 + \cdots + \sum_{i=0}^{n'} v_i.r_{ijd}(t,\bar{k}).m_d = 0 \quad \&$$
$$\theta(k_0,\bar{l},\bar{k}) \quad \& \quad \theta_m(\bar{r},\bar{s}).$$

We replace this last formula by

$$\exists \bar{h} \bigwedge_j \sum_{i=0}^{n'} v_i.r_{ij0}(t,\bar{k}).h_0 + \sum_{i=0}^{n'} v_i.r_{ij1}(t,\bar{k}).h_1 + \cdots + \sum_{i=0}^{n'} v_i.r_{ijd}(t,\bar{k}).h_d = 0 \quad \&$$

$$\exists k_0,\ \exists \bar{l} \exists \bar{r} \exists \bar{s}\ \theta'(\bar{l},\bar{k},\bar{r},\bar{s},k_0) \quad \& \quad \bigwedge_{i=0}^{d} m_i(k_0,\bar{l},\bar{r},\bar{s}) = h_i.$$

Using now quantifier elimination in algebraically closed fields, we get that the formula

$$\exists k_0,\ \exists \bar{l} \exists \bar{r} \exists \bar{s}\ \theta'(\bar{l},\bar{k},\bar{r},\bar{s},k_0) \quad \& \quad \bigwedge_{i=0}^{d} m_i(k_0,\bar{l},\bar{r},\bar{s}) = h_i$$

is equivalent to a quantifier-free formula $\theta''(\bar{h})$.

Now, we proceed as above grouping pairwise the equations and using the predicates $T_{n',\theta''}$.

Now consider a formula where we quantify over a module variable.

$$\exists v_0 \bigwedge_i t_i(v_0,\bar{v},\bar{k}) = 0 \quad \& \quad \bigwedge_j s_j(v_0,\bar{v},\bar{k}) \neq 0 \quad \& \quad T_{n,\theta_n}(\bar{v},v_0) \quad \& \quad \neg T_{m,\theta_m}(\bar{v},v_0).$$

If a predicate T_{n,θ_n} appears, we replace the corresponding atomic formula by

$$\exists k_1 \cdots \exists k_n \in C - \{0\}\ \exists l_1 \cdots \exists l_n \in C - \{0\}\ \theta(\bar{k},\bar{l}) \quad \& \quad v_0.r_0(\bar{k},\bar{l}) = -\sum_{i=1}^{n} v_i.r_i(\bar{k},\bar{l}),$$

where for each values of the parameters r_0, r_i belong to S. So, we get a system of equations and inequations.

The system of equations in the matrix form is of the form $\exists (v_0,\bar{v})\ (v_0,\bar{v}).B = 0$, where B is a matrix with coefficients in S, with parameters varying over C. Using Proposition 2.1, we get that there exist invertible matrices P and Q such that $P.B.Q$ is a diagonal matrix.

Set $(w_0,\bar{w}) := (v_0,\bar{v}).P^{-1}$. Let $w_0.s_0 = 0$ be the first equation. Then, we consider the inequations one by one. Let $w_0.t_0 + \cdots \neq 0$ be the first one. Using the Euclidean algorithm, we may assume that either s_0 divides t_0, which can be expressed in the coefficients in K of those two elements of S, or the degree of t_0 is strictly smaller than the degree of s_0. If a solution w_0 satisfies $w_0.t_0 + \cdots = 0$, then we add to it an element of $ann(s_0) - ann(t_0)$.

If a predicate $\neg T_{m,\theta_m}$ appears, then suppose that such w_0 does not satisfy the predicate i.e. $T_{m,\theta}(w_0,\ldots)$ holds, then whenever we add to w_0 a non-zero element of $ann(s_0)$ say w_0', we have $T_{m,\theta}(w_0 + w_0',\ldots)$ (note that we have infinitely many choices for w_0').

More generally, if we consider the system

$$\exists w_0 \left(w_0.s_0 = 0\ \&\ w_0.t_0 \neq u_0 \&\ \cdots\ \&\ w_0.t_\ell \neq u_\ell\ \&\ \bigwedge_m \neg T_{m,\theta_m} \right),$$

we proceed as in the first case in order to reduce to a disjunction of cases where either we get a formula on the elements of C with parameters in K or where $\deg(t_i) < \deg(s_0)$ for all $i \geqslant 0$. Then, we have to look at the cosets of the subspaces $ann(t_i)$ inside $ann(s_0)$ and in order to satisfy the system, we have possibly to add to a solution of the first equation an element w_0' of $ann(s_0)$

which does not belong to a finite subset of certain cosets of the subspaces $ann(t_i)$, $0 \leqslant i \leqslant \ell$. Since those last subspaces are of dimension strictly less than the dimension of $ann(s_0)$ (by axiom scheme (8)) and the index of any of such subspaces in $ann(s_0)$ is infinite, this is always feasible. □

3. Rings of sequences over a field F

In this section, we will consider rings with an *endomorphism*, namely rings of sequences over a field F with the shift σ_t. We will show that the theory of the underlying Boolean algebra of idempotents with the shift σ_t, is decidable but that whenever the field F is infinite, the theories of those difference rings are undecidable. Our decidability results below will be a consequence of the decidability result due to Büchi of the second-order theory of $\mathcal{N} := (\mathbb{N}, S, \leqslant)$, where S is the successor function $x \rightarrow x + 1$ and $\leqslant$ is the usual order on the natural numbers. The proof of that last result used finite automata theory that we will again appeal to, later in that section.

Definition 3.1. Let $\mathcal{B}_0$ be the set of idempotents of the difference ring $(\mathbb{C}^{\omega}_{\mathcal{F}}, +, ., 0, 1, \sigma_t)$, where $\mathcal{F}$ is the Frechet filter on ω. For $a, b \in \mathcal{B}_0$, define $a \oplus b = a + b - a.b$ and $a^{`} = 1 - a$. Then, $(\mathcal{B}_0, \oplus, ., ^{`}, 0, 1, \sigma_t)$ is an atomless Boolean algebra with an automorphism σ_t.

Let $\mathcal{L}_\sigma$ be $\mathcal{L}_{\text{rings}} \cup \{\sigma\}$.

Proposition 3.2. *The $\mathcal{L}_\sigma$-structures $(\mathbb{F}_2^{\omega}, +, ., 0, 1, \sigma_t)$, $(\mathbb{F}_2^{\mathbb{Z}}, +, ., 0, 1, \sigma_t)$ are decidable, as well as the Boolean algebra with an automorphism $(\mathcal{B}_0, \oplus, ., 0, 1, \sigma_t)$.*

Proof. One interprets these structures in the monadic second-order theory of $\mathcal{N}$ and uses the result of Büchi (see [3]). First, a sequence of 0 and 1 can be thought as the characteristic function of a subset s of $\mathbb{N}$, the shift function applied to this sequence is just the characteristic function of the subset s' defined as $n \in s'$ iff $S(n) \in s$. One can easily define the disjoint union and intersection of two subsets of $\mathbb{N}$. So, this entails the decidability of the two rings.

Finally, an element of $\mathcal{B}_0$ can be viewed as an equivalence class of an infinite sequence of natural numbers modulo the Frechet filter by defining

$$s_1 \sim s_2 \quad \text{iff } \exists n \in \mathbb{N}\ \forall m \in \mathbb{N}\ \big(m \geqslant n \rightarrow (m \in s_1 \text{ iff } m \in s_2)\big). \qquad \square$$

Note that the theory of all Boolean algebras with a non-locally finite group of automorphisms is undecidable. One interprets the theory of Boolean pairs (see [4]).

Corollary 3.3. *Let F be a finite field, then the difference ring R of sequences $(F^{\mathbb{Z}}, \sigma_t)$ is decidable.*

Proof. Let $\mathcal{B}$ be the Boolean algebra of idempotents of R. It is a difference subring of R, which is isomorphic to $(\mathbb{F}_2^{\mathbb{Z}}, +, ., 0, 1, \sigma_t)$. Let $F = \{f_1, \ldots, f_n\}$, for some natural number n. Any element $r \in F^{\mathbb{Z}}$ can be written as $\sum_{i=1}^{n} f_i.e_i$, where $f_i \in F$ and $e_i \in \mathcal{B}$ with $\{e_1, \ldots, e_m\}$ a partition of 1 of size at most n. Moreover, since $Fix(R) = F$, we get that $\sigma(r) = \sum f_i.\sigma(e_i)$.

To any $\mathcal{L}_\sigma$-formula $\psi(x_1, \ldots, x_m)$, we shall associate an $\mathcal{L}_\sigma$-formula $\phi(z_1, \ldots, z_{n.m})$ such that for any $\bar{r} \in R$ there exists $\bar{e} \in \mathcal{B}$ such that $\psi(\bar{r})$ holds in R iff $\bigwedge_{i=1}^{m} r_i = \sum_{j=1}^{n} f_j.e_{ji}$ and $\phi(\bar{e})$ holds in $\mathcal{B}$.

First, given an atomic formula of the form $t(x_1,\dots,x_m)=0$, where $t(\bar{x})$ is an $\mathcal{L}_\sigma$-term, we associate a quantifier-free $\mathcal{L}_\sigma$-formula as follows. Express each x_i as $\sum_{j=1}^n f_j.z_{ij}$, where $z_{ij}, 1 \leqslant i \leqslant n$, are pairwise disjoint idempotents and $\sum_{i=1}^n z_{ij} = 1$. Then $t(x_1,\dots,x_n) = \sum_{h=1}^k t_h(\bar{f}).s_h(\bar{z})$, where t_h is an $\mathcal{L}$-term, s_h is an $\mathcal{L}_\sigma$-term and $s_h(\bar{z}).s_{h'}(\bar{z})=0$, for $1 \leqslant h \neq h' \leqslant k$. We have that $t(\bar{x})=0$ iff $\bigwedge_{h=1}^k (t_h(\bar{f})=0 \vee s_h(\bar{z})=0)$. Let H be the subset of indices h, $1 \leqslant h \leqslant k$ such that $F \models t_h(\bar{f}) \neq 0$. We get:

$$t(\bar{x})=0 \quad \text{iff} \quad \bigwedge_{h\in H} s_h(\bar{z})=0 \ \& \ \bigwedge_i x_i = \sum_{j=1}^n f_j.z_{ij}.$$

(⋆) So a quantifier-free formula $\theta(\bar{x})$ is equivalent to the conjunction $\bigwedge_i x_i = \sum_{j=1}^n f_j.z_{ij}$ & $\phi(\bar{u})$, for some quantifier-free $\mathcal{L}_\sigma$-formula ϕ.

Then, we replace the quantifier $\forall r \in R$ by $\forall z_1,\dots,\forall z_n \in \mathcal{B}$ (similarly for the quantifier $\exists$). So, given a formula $\psi(\bar{a})$ of the form $Q_1x_1\cdots Q_\ell x_\ell \theta(x_1,\dots,x_\ell,\bar{a})$, where θ is a quantifier-free formula, we replace it, using (⋆), by

$$Q_1z_{11}\cdots Q_1z_{1n}\cdots Q_\ell z_{\ell 1}\cdots Q_\ell z_{\ell n}\bigwedge_{i=1}^{\ell}\left(x_i=\sum_{j=1}^n f_j.z_{ij}\wedge\phi(z_{11},\dots,z_{\ell n},\bar{e}_{\bar{a}})\right),$$

where each $a_h = \sum_{i=1}^n f_{hi}.e_{a_{hi}}$, $1 \leqslant h \leqslant m$ and $e_{\bar{a}} := (e_{a_{h1}},\dots,e_{a_{hn}})$.

So, we get that $\psi(\bar{a})$ is equivalent to an $\mathcal{L}_\sigma$-formula $\psi_1(\bar{e}_{\bar{a}})$.

Finally, if ψ is a sentence, then so is ψ_1 and we apply the decidability of $(\mathbb{F}_2^{\mathbb{Z}},+,.,0,1,\sigma_t)$. □

Before proving undecidability results on difference rings of sequences, we will show that the theory of the difference Boolean algebra $\mathcal{B}_0$, that was proven to be decidable at the beginning of this section, is model-complete. We will be using the fact that any definable subset of $(\mathbb{F}_2^{\omega},+,.,0,1,\sigma_t)$ is recognizable by a finite automaton. The finite automata we will be describing are called Muller–McNaughton automata (see for instance [17]); their input are infinite sequences indexed by ω. The (deterministic finite) automaton $A := (Q, q_0, \mathcal{FS}, T)$ has finitely many states: $Q := \{q_0,\dots,q_\ell\}$, with an initial state q_0, a set $\mathcal{FS} := \{F_1,\dots,F_f\} \subset \mathcal{P}(Q)$ of subsets of final states, $F_i \in \mathcal{P}(Q)$, $1 \leqslant i \leqslant f$, and a transition function $T: Q \times \{0,1\}^m \to Q$. An m-tuple of infinite sequences is *accepted by* A if the subset of states this tuple visits infinitely many times belongs to $\mathcal{FS}$, beginning at the initial state q_0, with the rule to go from a state to the next one, given by the transition function T. Such sequences will be called *A-recognizable*. For any $q_i \in Q$, put $A_{q_i} := (Q, q_i, \mathcal{FS}, T)$. This finite automaton only differs from A by its initial state which is now q_i. (So, in this notation $A = A_{q_0}$.)

More generally, letting F be a finite field, we will consider the ring

$$R^* := \left(F^{\omega},+,-,.,0,1,\sigma_t,\sim\right),$$

where σ_t denotes the shift endomorphism, and $\sim$ is the following equivalence relation $(f_n)_{n\in\omega} \sim (g_n)_{n\in\omega}$ iff $\exists n_0\ \forall n > n_0\ (f_n = g_n)$. The decidability of this difference ring can also be proven using a result of B. Hodgson who showed that it suffices to check whether the graphs of the functions and relations of the structure are recognizable (when coded in a specific way) to deduce that the structure is ω-automatic (namely, any 0-definable subset is recognizable by a finite automaton).

If $r \in R^*$ and s a finite sequence of elements of F of length n, we denote by $s^\frown r$ the concatenation of the two sequence s and r. It can be defined algebraically as follows: let τ be the map sending the sequence $(r_0, r_1, \ldots)$ to the sequence $(0, r_0, r_1, \ldots)$, then it is equal to $\tau^n(r) + s$. Note that $\sigma_t \circ \tau$ is the identity.

We say that a subset E of $(R^*)^m$ is *Fraïssé invariant* if for any natural number n and any m-tuple $\bar{s}$ of finite sequences of length n, we have for any $\bar{a} \in (R^*)^m$ that

$$\bar{a} \in E \quad \text{iff } \bar{s} + \tau^n(\bar{a}) \in E.$$

Proposition 3.4. *Let F be any finite field. Let $R := (F^\omega{}_{\mathcal{F}}, +, -, ., 0, 1, \sigma_t)$, where σ_t denotes the shift automorphism. Then, the theory $Th(R)$ of the difference ring R is model-complete.*

Proof. We code elements of F by integers between 0 and $q - 1$, where q is a prime power. Let us denote this subset of integers by $[q]$. We will show that any 0-definable subset $D \subseteq R^m$ is existentially definable.

Let $D^* := i^*(D)$ be the pullback i^* of D to $(R^*)^m$. Then D^* is both σ_t-invariant and Fraïssé invariant. The first property follows from the fact that D is 0-definable and σ_t induces an automorphism of R. Let us check the second property. Let $\bar{s}$ be a tuple of finite sequences of length n. If $\bar{a} \in D^*$, then by definition of the pullback, $\bar{s} + \tau^n(\bar{a}) \in D^*$. Conversely, if $\bar{s} + \tau^n(\bar{a}) \in D^*$, then $\bar{a} = \sigma_t^n(\bar{s} + \tau^n(\bar{a})) \in D^*$ since D^* is σ_t-invariant.

Claim. *Let $E \subset (R^*)^m$ be Fraïssé invariant, and σ_t-invariant. Assume that E is A-recognizable, where A is a finite automaton, as described above. Then, for any $q_i \in Q$, E is also A_{q_i}-recognizable.*

Proof of Claim. We show that A_{q_i} accepts $\bar{r}$ iff $\bar{r} \in E$.

Let $\bar{r}_0$ be an m-tuple of finite sequences (of length n) which labels the path which in the automaton A goes from q_0 to q_i.

If $\bar{r} \in E$ then since E is Fraïssé invariant $\bar{r}_0{}^\frown \bar{r}$ also belongs to E. Since E is A-recognizable, A accepts $\bar{r}_0{}^\frown \bar{r}$. So, A_{q_i} accepts $\bar{r}$. Conversely, suppose that A_{q_i} accepts $\bar{r}$. Then $\bar{r}_0{}^\frown \bar{r}$ is also accepted by A and so it belongs to E. But $\bar{r} = \sigma_t^n(\bar{r}_0{}^\frown \bar{r})$ and since E is σ_t-invariant, then $\bar{r} \in E$.

Now, we want to express by a difference ring formula that $\bar{u} \in D$, making use of the fact that D^* is definable in R^* and so recognizable by a finite automaton say $A := (Q, q_0, \mathcal{FS}, T)$.

In order to do so, we encode the finite set of states by ℓ-tuples, namely $q_1 = (1^\omega, 0^\omega, \ldots, 0^\omega), \ldots, q_\ell = (0^\omega, \ldots, 0^\omega, 1^\omega)$.

First, let us (informally) express that a given m-tuple of sequences $\bar{v} \in R^*$ is accepted by the automaton A: $F^\omega \models \exists y_1 \cdots \exists y_\ell$ such that $(y_1(0), \ldots, y_\ell(0))$ is the initial state, for all but finitely many k $(\bigvee_{j=1}^{f} (y_1(k), \ldots, y_\ell(k)) \in F_j$ and for all t, for all $\tilde{q} \in Q$, if $(y_1(t), \ldots, y_\ell(t)) = q$, then $(y_1(t+1), \ldots, y_\ell(t+1)) \in T(\tilde{q}, \bar{v}(t))$.

Finally, we claim that $\bar{u} := (u_1, \ldots, u_m) \in D$ can be expressed in R by the following existential formula $\phi(\bar{u})$: $\exists y_1 \cdots \exists y_\ell$

$$\bigvee_{i=1}^{f} \bigvee_{\substack{\bar a\in\{0^\omega,1^\omega\}^m\\ \text{where } q'_j\in T(q_j,\bar a)}} \bigwedge_{q_j\in F_i} (\bar y - q_j)^* = \big(\bar y^\sigma - q'_j\big)^* \leqslant \prod_{z=1}^{m} \big(1-(u_z-a_z)^*\big) \quad \text{and}$$

$$\bigvee_{i=1}^{f} \prod_{j\in F_i} (\bar y - q_j)^* = 0.$$

Indeed, let $\bar u \in D$, and let $\bar v \in i^*(\bar u)$. Since D^* is A-recognizable and $\bar v$ is accepted by A, $\phi(\bar u)$ holds. Conversely, if $\phi(\bar u)$ holds, then any $\bar v \in R^*$ in the equivalence class defined by $\bar u$, is accepted by A_{q_i} for some i and so by the claim above, $\bar v \in D^*$ and so $\bar u \in D$. □

Proposition 3.5. *Let F be any field of characteristic zero. Then, the existential $\mathcal{L}_\sigma$-theory of $(F^\omega_{\mathcal{F}}, +, ., -, \sigma_t, 0, 1)$ is undecidable.*

Proof. We will show that one can define $\mathbb{Z}$ by an existential formula and we will use the undecidability result of Y. Matijasevich for solvability of diophantine equations over $\mathbb{Z}$.

Let us define $\mathbb{Z}$ as follows: $x \in \mathbb{Z}$ iff ($\sigma_t(x) = x$ and $\exists y$ $(\sigma_t(y) - y)^2 = 1$ and $x - y$ and y are zero-divisors)).

Let $y = (y(n))_{\mathcal{F}}$. Since y is a zero-divisor, for infinitely many n we have that $y(n) = 0$, now since $(\sigma_t(y) - y)^2 = 1$, this implies that for cofinitely many n we have that $y(n) = \sigma_t(y)(n) \pm 1$ and finally we know that $y(n) = x(n)$ for infinitely many n. □

Proposition 3.6. *Let F be a non-algebraic field of characteristic p* (*i.e. F has an element which does not belong to the algebraic closure of the prime field*)*. Then, we can interpret the ring* $(\mathbb{Z}, +, ., 0, 1)$ *in the difference ring* $(F^\omega_{\mathcal{F}}, +, ., -, \sigma_t, 0, 1)$ *and so the $\mathcal{L}_\sigma$-theory of this last ring is undecidable.*

Proof. We will define in $F^\omega_{\mathcal{F}}$ the set of integral powers of any non-algebraic element a of $F - \tilde{\mathbb{F}}_p$. Note that the set of such elements a is $\exists\forall$-definable by the following formula $I(a)$: $a \in Fix(\sigma_t)$ & $\exists z$ ($\sigma_t(z) = a.z$ and $\forall z' \in Fix(\sigma_t)(z - z')$ is not a zero divisor).

We define the (infinite) set of integral powers $P(a)$ of a as follows: $x \in P(a)$ iff ($\sigma_t(x) = x$ and $\exists y$ $(\sigma_t(y) - a.y).(\sigma_t(y) - a^{-1}.y) = 0$ and $x - y$ and $y - 1$ are zero-divisors).

Given two non-algebraic elements a, b, we will put an equivalence relation on the set of 2-tuples (a, x), where $I(a)$ and $''x \in P(a)''$ hold, identifying (a, a^n) with (b, b^n), $n \in \omega$.

We proceed as follows. Let a, b be such that $I(a)$ & $I(b)$. First assume that $P(a) \cap P(b) = \{1\}$. Define the function $h_{a,b}(x) = y$ from $P(a)$ to $P(b)$ by the following formula: $x \in P(a)$, $y \in P(b)$ and $x.y^{-1} \in P(a.b^{-1})$. (Note that if $I(a)$ and $I(b)$ hold and $P(a) \cap P(b) = \{1\}$, then $I(a.b^{-1})$ holds too.) In the general case, we define the function $f_{a,b}(x) = y$ from $P(a)$ to $P(b)$ as follows: $\exists c$ ($I(c)$ & $P(c) \cap (P(a) \cup P(b)) = \{1\}$ & $h_{c,b} \circ h_{a,c}(x) = y$).

The equivalence relation $\sim$ is then defined on the set

$$\mathcal{Z} := \big\{(a, x) \in F^\omega_{\mathcal{F}} \times F^\omega_{\mathcal{F}}\colon\ I(a) \,\&\, x \in P(a)\big\} \quad \text{by:} \quad (a, x) \sim (b, y) \quad \text{iff} \quad f_{a,b}(x) = y.$$

Let $(a, x), (b, y) \in \mathcal{Z}$, then we define

$$(a, x) \oplus (b, y) := \big(a, x.f_{a,b}(y)\big) \quad \text{and} \quad (a, x) \otimes (b, y) := \big(a, f_{a,x} \circ f_{a,b}(y)\big).$$

It is easy to check that the relation $\sim$ is a congruence relation for the operations $\oplus$ and $\otimes$. The identity for $\oplus$ is $(a,1)_\sim$ and for $\otimes$, $(a,a)_\sim$.

Therefore $(\mathcal{Z}/{\sim}, \oplus, \otimes, (a,1)_\sim, (a,a)_\sim)$ is isomorphic to $(\mathbb{Z}, +, ., 0, 1)$ and so this latter structure is first-order interpretable in $(F^{\omega}_{\mathcal{F}}, +, ., -, \sigma_t, 0, 1)$ from which the undecidability result follows [16, Theorem 5.5.7]. □

Remark 3.7. Note that in the case where F is an infinite algebraic field of characteristic p, we can interpret in $(F^{\omega}_{\mathcal{F}}, +, ., -, \sigma_t, 0, 1)$ an infinite class[3] of finite rings of the form $\mathbb{Z}/m\mathbb{Z}$ and so we also obtain the undecidability of this difference ring. (This will also be a consequence of a more general undecidability result for a class of von Neumann regular commutative difference rings (see Proposition 5.1).)

Let a be an algebraic element over $\mathbb{F}_p$ i.e. an element satisfying the formula $A(a) := a \in Fix(\sigma_t)$ & $\exists z \neq 0\ (\sigma_t(z) = a.z$ and $\exists z' \in Fix(\sigma_t) - \{0\}\ (z - z')$ is a zero divisor).

We want to identify two algebraic elements a and b such that $a^n = 1$ and $b^n = 1$, where n is minimal such. This is the case whenever the following formula holds $E(a,b)$: $a \in Fix(\sigma_t)$ & $b \in Fix(\sigma_t)$ & $\exists z_0 \neq 0\ \exists z_1 \neq 0\ \exists z_2 \neq 0\ [\sigma_t(z_1) = a.z_1$ & $\sigma_t(z_2) = b.z_2$ & $z_0 - z_1$ is a zero-divisor and $z_0 - z_2$ is a zero-divisor].

We define the set $P(a)$ as in the proof above. Then, on the (finite) set $P(a)$ of powers of a, one defines for $x, y \in P(a)$, $x \oplus y = z$ by $x.y = z$ and $x \otimes y = z$ by $z = f_{a,x}(y)$, where the function f is defined as in the above proof.

Then the ring $(\mathbb{Z}/m\mathbb{Z}, +, ., 0, 1)$ is isomorphic to $(P(a), \oplus, \otimes, 1, a)$ where $A(a)$ holds and a is an algebraic element such that $a^m = 1$ with m minimal such.

4. Decidability of the difference ring $(C^n, +, \cdot, \sigma_n)$

In view of the undecidability results of the previous section, we will examine the theories of difference rings of the form $(C^n, +, \cdot, \sigma_n)$ where C is an algebraically closed field of characteristic p with the convention *in that section* that p is either equal to 0 or to a prime number, and where σ_n is an automorphism acting as the cyclic permutation of order n on the factors, $n \in \omega$.

Recall that this kind of difference rings occurred as total Picard–Vessiot rings attached to a difference equation. Namely, given a difference equation with coefficients in a perfect difference field K with an algebraically closed field of constants, then the Picard–Vessiot ring R attached to this equation is a K-algebra of the form $\bigoplus_{1 \leqslant i \leqslant m-1}(D_i, \sigma_m)$, where D_i is a domain and $\sigma(D_i) = D_{i+1(\text{modulo } m)}$. The total Picard–Vessiot ring is obtained by taking the fraction field of these domains and extending the automorphism σ_m accordingly. Finally, one can embed the fraction field of each D_i in its algebraic closure and extend the automorphism accordingly.

We will show that the theories of such difference von Neumann commutative rings can be axiomatized by the following sets $T_{n,p}$ of axioms.

(1) the theory of commutative rings R of characteristic p (with the convention above) satisfying: $\forall x\ \exists y\ (x^2.y = x$ & $y^2.x = y)$, with an automorphism σ_n,
(2) the Boolean algebra $\mathcal{B}_n$ of idempotents of R is atomic and there are exactly n atoms: $\{e_0, \ldots, e_{n-1}\}$; σ_n acts as the cyclic permutation of order n on these atoms, namely $\sigma_n(e_i) = e_{i-1}$, $1 \leqslant i \leqslant n$, and $e_n = e_0$,

[3] I.e. there exists a definable family $R(a)$ of interpretable rings, and a definable set D such that for any $a \in D$, for some m, $R(a) \cong \mathbb{Z}/m\mathbb{Z}$, and infinitely many such m occur.

(3) the set of fixed elements of σ_n is an algebraically closed field and

$$R = Fix(\sigma_n).e_0 + \cdots + Fix(\sigma_n).e_{n-1}.$$

Note that this set of axioms implies that $\sigma_n^n = 1$.

Proposition 4.1. *The theory $T_{n,p}$ is $\aleph_1$-categorical, model-complete, complete and decidable.*

Proof. We apply the Lindström criterion in order to show that $T_{n,p}$ is model-complete (see [16, Theorem 8.3.4]). First, all models of $T_{n,p}$ are infinite. The union of a chain of models of $T_{n,p}$ is still a model of $T_{n,p}$. Finally, if we take two models (R_1, σ_1), (R_2, σ_2) of $T_{n,p}$ of cardinality $\aleph_1$, then $F_1 := Fix_{R_1}(\sigma_1)$ and $F_2 := Fix_{R_2}(\sigma_2)$ being two algebraically closed fields of cardinality $\aleph_1$ and of the same characteristic are isomorphic by Steinitz Theorem; denote by f_0 the isomorphism from F_1 to F_2. Let $e_0, \dots, e_{n-1}$ and $u_0, \dots, u_{n-1}$ be the atoms of respectively R_1 and R_2, then we define $f : R_1 \to R_2$ sending $r = r_0.e_0 + \cdots + r_{n-1}.e_{n-1}$, where $r_i \in F_1$, to $f_0(r_0).u_0 + \cdots + f_0(r_{n-1}).u_{n-1}$. Let us check that it preserves the automorphisms: $f(\sigma_1(r)) = \sigma_2(f(r))$. We have that $\sigma_1(r) = r_0.e_{n-1} + r_1.e_0 + \cdots + r_{n-1}.e_{n-2}$, so $f(\sigma_1(r)) = f_0(r_0).u_{n-1} + f_0(r_1).u_0 + \cdots + f_0(r_{n-1}).u_{n-2}$.

The decidability of $T_{n,p}$ follows from the fact that it is complete and recursively axiomatizable. □

In particular, in $T_{n,p}$ any formula is equivalent to an existential formula. In fact, we can show more, namely that any existential formula in $T_{n,p}$ is equivalent to a quantifier free formula with extra parameters in $(\mathcal{B}_n, \sigma)$ (see Corollary 4.4).

This will give another proof that for each n, the difference ring of finite sequences $(\mathbb{C}^n, +, ., \sigma_n)$, where σ_n is the cyclic permutation of order n, is decidable.

However, note that using the same formula as in the proof of Proposition 3.5, we can show that an ultraproduct of the $(\mathbb{C}^n, +, ., \sigma_n)$ with respect to an ultrafilter containing for each m the multiples of m, is undecidable.

Remark 4.2. Note that $(\mathbb{C}^n, \sigma_n)$ embeds in $(\mathbb{C}^{n.m}, \sigma_{n.m})$. Indeed, we send $(r_0, \dots, r_{n-1})$ to $(r_0, \dots, r_{n-1}, r_0, \dots, r_{n-1}, \dots, r_0, \dots, r_{n-1})$.

Now, we will consider the case where σ acts non-trivially on each factor.

In the following, we will often use the fact that in a von Neumann regular commutative ring R, there is an homeomorphism between the Stone space $X(R)$ of the Boolean algebra $\mathcal{B}(R)$ of the idempotents of R and the maximal spectrum $MSpec(R)$ of R. (We will often identify those two spaces.)

Z. Chatzidakis and E. Hrushovski in [11] have given an axiomatization *ACFA* for the class of existentially closed models of the theory of difference fields, in the language $\mathcal{L}_\sigma$. It expresses the following properties of a field K.

(1) σ is an automorphism of K.
(2) K is an algebraically closed field.
(3) For every irreducible variety U and every variety $V \subset U \times \sigma(U)$ projecting generically onto U and $\sigma(U)$ and every algebraic set W properly contained in V, there is $a \in U(K)$ such that $(a, \sigma(a)) \in V - W$.

Observe that the third scheme of axioms is elementary; L. van den Dries and K. Schmidt showed how to express in a first-order way that a variety is (absolutely) irreducible [14].

In [11], the authors show that *ACFA* is the model companion of the theory of difference fields. Note that the fixed field by σ in a model of *ACFA* is a pseudo-finite field.

We consider the theory $T_{n,\sigma}$:

(1) R is a von Neumann regular commutative ring with an automorphism σ.
(2) The Boolean algebra $\mathcal{B}(R)$ of idempotents of R is atomic, it has exactly n atoms: $\{e_0, \ldots, e_{n-1}\}$ and σ acts as the cyclic permutation of order n on these atoms (so the restriction of σ^n on $\mathcal{B}(R)$ is the identity and each $R.e_i$ is a field).
(3) $(R.e_i, \sigma^n, +, ., 0, e_i)$, $0 \leqslant i < n$, is a model of *ACFA*.

Proposition 4.3. *The theory $T_{n,\sigma}$ is model-complete and decidable.*

Proof. Let R be a model of $T_{n,\sigma}$, let $\mathcal{B}(R)$ be its Boolean algebra of idempotents; it has n atoms. Let $X(R)$ be the Stone space of $\mathcal{B}(R)$. Then, as a set $X(R)$ is in bijection with the set $\{\pi, \sigma(\pi), \ldots, \sigma^{n-1}(\pi)\}$, where $\pi \in MSpec(R)$. Then the ring R is isomorphic (as a ring) to a finite direct product of simple rings $R \cong (R/\pi \times R/\sigma^{-1}(\pi) \times R/\sigma^{-2}(\pi) \times \cdots \times R/\sigma^{-n+1}(\pi))$, $(\sigma^n(\pi) = \pi)$, where each of the $R/\sigma^{-i}(\pi)$, $1 \leqslant i \leqslant n-1$ is isomorphic to $R.e_i$. Using the above isomorphism, we will identify any element r of R with an n-tuple of the form: $(r_0, r_1, \ldots, r_{n-1})$ with each $r_i \in R/\sigma^{-i}(\pi)$.

The automorphism σ acts on each factor of the direct product by sending $R/\sigma^{-i}(\pi)$ to $R/\sigma^{-i+1}(\pi)$ and $\tau := \sigma^n$ is an automorphism of each factor.

If we calculate the images of $r = (r_0, \ldots, r_{n-1})$ by the iterates of σ we get: letting $k = n.k_1 + k_2$ with $0 \leqslant k_2 < n$, and with the convention that we calculate the indices modulo n,

$$r^\sigma = \left(r_1^\sigma, \ldots, r_{n-1}^\sigma, r_0^\sigma\right),$$

$$\ldots$$

$$r^{\sigma^k} = \left({r_{k_2}}^{\tau^{k_1}\sigma^{k_2}}, \ldots, {r_{k_2+n-1}}^{\tau^{k_1}\sigma^{k_2}}\right).$$

We want to show that any existential formula $\phi(\bar{x})$ is equivalent to a universal formula. Let $\phi(\bar{x})$ be of the form $\exists\, \bar{u}\phi(\bar{u}, \bar{x})$, where $\phi(\bar{u}, \bar{x})$ is a quantifier-free formula of the form:

$$\bigwedge_{i \in I} p_i\left(\bar{u}, \sigma(\bar{u}), \ldots, \sigma^k(\bar{u}), \bar{x}\right) = 0 \wedge \bigwedge_{j \in J} q_j\left(\bar{u}, \sigma(\bar{u}), \ldots, \sigma^k(\bar{u}), \bar{x}\right) \neq 0.$$

Let $\mathcal{P}_{J,n}$ be the set of partitions of J into n subsets or less.

We have the following equivalence: $\exists \bar{r} \in R R \models \phi(\bar{r}, \bar{x})$ iff

$$\bigvee_{\{J_0, \ldots, J_{n-1}\} \in \mathcal{P}_{J,n}} \bigwedge_{h=0}^{n-1} R/\sigma^{-h}(\pi) \models \exists \bar{r}_h\ \exists \bar{r}_{h+1}^\sigma \cdots \exists \bar{r}_{h+n-1}^{\sigma^{n-1}}$$

$$\left(\bigwedge_{i \in I} p_i\left(\bar{r}_h, \bar{r}_{h+1}^\sigma, \ldots, \bar{r}_{h+k_2}^{\tau^{k_1}\sigma^{k_2}}, \bar{x}.e_h\right) = 0 \wedge \bigwedge_{j \in J_h} q_j\left(\bar{r}_h, \bar{r}_{h+1}^\sigma, \ldots, \bar{r}_{h+k_2}^{\tau^{k_1}\sigma^{k_2}}, \bar{x}.e_h\right) \neq 0\right).$$

Note that for any $\mathcal{L}$-formula χ, we have $R/\sigma^{-h}(\pi) \models \chi(\bar{u})$ with $\bar{u} \subseteq R/\sigma^{-h}(\pi)$, iff $R/\pi \models \chi^{\sigma^h}(\bar{u}^{\sigma^h})$, where χ^{σ^h} is defined by replacing in the formula χ the quantifier $\forall r$ by $\forall r^{\sigma^h}$ and $\exists r$ by $\exists r^{\sigma^h}$.

This allows us to express every first-order property in R/π using only the automorphism τ. Therefore, we may now use that *ACFA* is a model-complete theory and so in R/π that any existential formula is equivalent to a universal formula.

So, there exists a universal formula $\theta(\bar{x})$ such that $\exists \bar{r} \in R\ R \models \phi(\bar{r}, \bar{x})$ is equivalent to $R/\pi \models \theta(\bar{x}.e_0, \ldots, \bar{x}.e_h{}^{\sigma^h}, \ldots)$, where θ is a universal formula. Now, it remains to express everything back in R, using the fact that $R/\pi \cong R.e_0$. We transform the formula $\theta(\bar{y})$ as follows: replace the universal quantifier $\forall x$ by $\forall x\ (x = x.e_0)$, replace the atomic formula $t(\bar{x}) = 0$ by $t(\bar{x}).e_0 = 0$. We denote the transformed formula by $\theta_{e_0}(\bar{y}, e_0)$. So,

$$R/\pi \models \theta\big(\bar{x}.e_0, \ldots, \bar{x}.e_h{}^{\sigma^h}, \ldots\big) \quad \text{iff} \quad R \models \theta_{e_0}\big(\bar{x}.e_0, \ldots, \bar{x}.e_h{}^{\sigma^h}, \ldots, e_0\big).$$

So, by induction on the complexity of the formula, this allows us to show that any formula is equivalent to an existential formula. In particular, any sentence is equivalent to an existential sentence. Moreover, by the above, any existential sentence in R is equivalent, by a recursive procedure, to an existential sentence in R/π. Since R/π is a model of *ACFA* and *ACFA* is decidable (see [11, (1.6)]), it entails that $T_{n,\sigma}$ is decidable. □

Going back to the setting of Proposition 4.1, we will assume that $\sigma^n = 1$. So, instead of working with *ACFA*, we work with ACF and so we may use the quantifier elimination result for that last theory. Therefore, in the proof above the formula θ can be chosen quantifier-free and so, the formula θ_{e_0} is also quantifier-free.

Corollary 4.4. *The theory $T_{n,p}$ admits quantifier elimination in the language where we add n constants to be interpreted in models of $T_{n,p}$ by the atoms of the Boolean algebra of idempotents.*

Let $T^f_{n,\sigma}$ be the following theory:

(1) R is a von Neumann commutative regular ring with an automorphism σ.
(2) The Boolean algebra $\mathcal{B}(R)$ of R is atomic and there are exactly n atoms: $\{e_0, \ldots, e_{n-1}\}$ and σ acts as the cyclic permutation of order n on these atoms (so the restriction of σ^n on the Boolean algebra of idempotents is the identity and each $R.e_i$ is a field).

Proposition 4.5. *$T_{n,\sigma}$ is the model-companion of $T^f_{n,\sigma}$.*

Proof. We use the result of Chatzidakis and Hrushovski showing that *ACFA* is the model companion of the theory of difference fields (see Theorem 1.1 in [11]). Let $R \models T^f_{n,\sigma}$ and let $\{e_0, \ldots, e_{n-1}\}$ be the atoms of R. Then each $(R.e_i, \sigma^n)$ is a difference field, the automorphism σ of R sends each field $R.e_i$ to $R.e_{i+1}$, $0 \leqslant i \leqslant n-2$, and $R.e_{n-1}$ to $R.e_0$; denote that σ_i its restriction to $R.e_i$, $0 \leqslant i \leqslant n-1$. We consider the n-sorted structure

$$\mathcal{S} := (R.e_0, \ldots, R.e_{n-1}, \sigma_i; 0 \leqslant i \leqslant n-1).$$

Let F be a (pure) field isomorphic to $R.e_0$. Then $\mathcal{S}$ is isomorphic to an n-sorted structure of the form $(F, \ldots, F, \mathbf{1}, \ldots, \mathbf{1}, \tau)$, where the identity $\mathbf{1}$ goes from the ith copy of F to the $(i+1)$th, $0 \leqslant i \leqslant n-2$, and τ goes from the $(n-1)$th copy of F to the 0th one.

By the above result, (F, τ) extends to a model $(K, \tilde{\tau})$ of *ACFA* and so $\mathcal{S}$ embeds into $(K, \ldots, K, \mathbf{1}, \ldots, \mathbf{1}, \tilde{\tau})$. Finally we consider the von Neumann regular difference ring which is the direct product of these copies of K with the automorphism induced by the tuple $(\mathbf{1}, \ldots, \mathbf{1}, \tilde{\tau})$. This gives us a model of $T_{n,\sigma}$ into which (R, σ) embeds. □

5. Undecidability results for commutative difference Bezout rings

In this section, we will generalize the undecidability result we proved for difference rings of sequences over a field either of characteristic zero (Proposition 3.5) or of characteristic p which contains a non-algebraic element over the prime field (Proposition 3.6).

This will not only entail the undecidability of the non-principal ultraproducts over ω of the $(\mathbb{C}^n, +, ., \sigma_n)$ but also of their *limit theory* i.e. the set of sentences true in all but finitely many of them, and similarly of the $(\tilde{\mathbb{F}}_p^n, +, ., \sigma_n)$, $n \in \omega$.

Let us recall some well-known undecidable finitely axiomatizable subtheories of Peano arithmetic.

Let Q be the following $\{s(.), +, ., 0\}$-theory, where s is a unary function symbol:

$$\begin{aligned}
&\forall x, \forall y\ \big[\big(s(x) = s(y)\big) \to (x = y)\big],\\
&\forall y\ \big[0 \neq s(y)\big],\\
&\forall x\ [x + 0 = x],\\
&\forall x, \forall y\ \big[x + s(y) = s(x + y)\big],\\
&\forall x\ [x.0 = 0],\\
&\forall x, \forall y\ \big[x.s(y) = (x.y) + x\big],\\
&\forall x\ \big[(0 \neq x) \to \big(\exists y\ x = s(y)\big)\big].
\end{aligned}$$

Then, Q has been shown to be essentially undecidable (i.e. any consistent theory T' containing it, is undecidable (see II.5, Theorem 9, p. 60 in [29])). One shows that every recursive function is definable in the following subtheory *Rec* (this subtheory is denoted by R in [29]); note that this entails that *Rec* is essentially undecidable. We will write $u \leqslant v$ for $\exists w\ u + w = v$.

Let *Rec* be the following theory: with the convention that $s^0(0) = 0$, it consists in an infinite list of axioms indexed by $n, m \in \mathbb{N}$:

$$\begin{aligned}
&s^n(0) + s^m(0) = s^{n+m}(0),\\
&s^n(0).s^m(0) = s^{n.m}(0),\\
&s^n(0) \neq s^m(0), \quad \text{for } n \neq m,\\
&\forall x\ \left(\big(x \leqslant s^n(0)\big) \to \left(\bigvee_{i=0}^{n} x = s^i(0)\right)\right),\\
&\forall x\ \big(x \leqslant s^n(0)\big) \vee \big(s^n(0) \leqslant x\big).
\end{aligned}$$

Every *truncated semi-ring* of the integers between 0 and n, $n \in \mathbb{N}$, satisfies the following theory Q_c. [By "truncated semi-ring," we mean the following. The domain is the integers in the interval $[0; n]$ and the operations $\oplus$ and $\otimes$ on that domain are defined as follows. Let $0 \leqslant a, b \leqslant n$, then we check in $(\mathbb{N}, +, .)$ whether $a + b \leqslant n$ and $a.b \leqslant n$, we set $a \oplus b = a + b$ (respectively $a \otimes b = a.b$); if $a + b \geqslant n$ (respectively $a.b \geqslant n$), we set $a \oplus b = n$ (respectively $a \otimes b = n$).]

Let Q_c be the following $\{s(.), +, ., 0, c\}$-theory, where s is a unary function symbol, $+$, . are binary function symbols and $0, c$ are constants. Again, we will write $u \leqslant v$ for $\exists z\ (x + z = y)$.

$$
\begin{aligned}
&(0) \quad 0 \neq c,\\
&(1) \quad \forall x \neq c\ \forall y \neq c\ \bigl(s(x) = s(y) \rightarrow x = y\bigr),\\
&(2) \quad \forall y \neq c\ \bigl(y \neq s(y)\bigr) \quad \& \quad s(c) = c,\\
&(3) \quad \forall x\ (x + 0 = x),\\
&(4) \quad \forall x\ \forall y\ \bigl(x + s(y) = s(x + y)\bigr),\\
&(5) \quad \forall x\ (x.0 = 0),\\
&(6) \quad \forall x\ \forall y\ \bigl(x.s(y) = (x.y) + x\bigr),\\
&(7) \quad \forall x\ \bigl(0 \neq x \rightarrow \exists y\ x = s(y)\bigr),\\
&(8) \quad \forall x\ (0 \leqslant x \leqslant c) \quad \& \quad \forall x\ \forall y\ (x \leqslant y \vee y \leqslant x).
\end{aligned}
$$

Let M be an infinite model of Q_c and let T_{fin} be its theory. Let us show that T_{fin} does contain *Rec*, which will entail the undecidability of T_{fin}. First, note that M contains the subset $\{s^n(0)\colon n \in \mathbb{N}\}$. Suppose not, then $c = s^n(0)$ for some n, which we choose minimal such. By axiom 8, any element $a \in M$ satisfies: $0 \leqslant a \leqslant s^n(0)$. So, there exists $b \in M$ such that $a + b = s^n(0)$. Either, $b = 0$ and so $a = s^n(0)$ or by axiom 7, there exists $b' \in M$ such that $b = s(b')$. By axiom 4, $s(a + b') = s^n(0)$ and so by axiom 1, $a + b' = s^{n-1}(0)$. Iterating the above reasoning at most $n - 1$ times we get that a is of the form $s^m(0)$ with $0 \leqslant m \leqslant n$. Therefore, M is finite, a contradiction.

Then we check that the subset $\{s^n(0)\colon n \in \mathbb{N}\}$ of M satisfies *Rec* and so the theory of M will include *Rec*. The first three schemes of axioms of *Rec* are easily checked using the inductive definitions of $+$ and . in models of Q_c. The fourth scheme of axioms is proven in the same way as the fact that c was not equal to an element of the form $s^n(0)$ and the last axiom of *Rec* is a particular case of the last axiom of Q_c.

Let (R, σ) be a commutative difference ring. Let $MSpec(R)$ be the maximal spectrum of R, i.e. the set of maximal (ring) ideals of R, endowed with the following topology: a basic open set is of the form $\{\pi \in MSpec(R)\colon r \notin \pi\}$, where $r \in R$. Recall that this space is compact, and since we work with the maximal spectrum instead of the prime spectrum, it is Hausdorff.

Either there exists n such that σ^n fixes $MSpec(R)$ or for all m there exists a maximal ideal π such that $\sigma^m(\pi) \neq \pi$. In the latter case, if we take $m = n!$, we get that for all n, there exists a maximal ideal π such that $\pi, \sigma(\pi), \ldots, \sigma^n(\pi)$ are pairwise distinct.

In the first case, if we further assume that R is a commutative semi-simple ring, then the intersection of its maximal ideals is the zero ideal, and so R embeds into the subdirect product of difference fields. In the next section, we will show under the additional hypothesis that σ fixes $MSpec(R)$, that the theory of $(R, +, ., \sigma)$ has a model-companion (see Proposition 6.8). If in addition R von Neumann regular and if $\sigma^n = \mathbf{1}$ for some n, then the theory of $(R, +, ., \sigma)$ has a model-companion (see Proposition 6.10), improving on the results of the previous section.

In the second case, we have the following undecidability results working under the additional hypothesis that the subring fixed by σ is an infinite field. First, we will consider the case when R is a commutative von Neumann regular ring. In Section 6, we will review more systematically a few properties about these rings, but for convenience of the reader we state here some basic facts used below. Given any element $b \in R$, there exists an element $c \in R$ with $b = b.(b.c)$ and $c = c.(b.c)$. From this, it follows that $b.c$ is an idempotent and that such element c is uniquely determined; c is called the pseudo-inverse of b. In a von Neumann commutative regular ring, it is convenient to add a unary function symbol $*$ sending b to c. Let $\mathcal{B}(R)$ be the Boolean algebra of idempotents of R. We have that $MSpec(R)$ coincides with $Spec(R)$ the prime spectrum of R and is homeomorphic to the Stone space of $\mathcal{B}(R)$. Such a ring R can be represented as a Boolean product of fields (see Section 6). For gaining some intuition in the proof below, it might be useful to identify an element with its image in such a representation, however we will not formally use such identification.

The property that no power of σ fixes $Spec(R)$ is equivalent to the property that no power of σ fixes $\mathcal{B}(R)$. Moreover, if the intersection of the fixed subring $Fix(\sigma)$ of σ with $\mathcal{B}(R)$ is equal to $\{0, 1\}$, then $Fix(\sigma)$ is a field (see Lemma 6.2).

Proposition 5.1. *Let R be a commutative von Neumann regular difference ring for which $Fix(\sigma)$ is an infinite field. Assume that no power of σ fixes $\mathcal{B}(R)$. Then we can interpret either Q or T_{fin} in the theory of R. So, the theory of R is undecidable.*

Proof. Set $F := Fix(\sigma)$.

Since no power of σ fixes $Spec(R)$, for every non-zero natural number n, there exists a maximal ideal π such that $\pi, \sigma(\pi), \ldots, \sigma^n(\pi)$ are pairwise distinct. This entails that there is an idempotent e such that $e + \pi = 1 + \pi$ and $e, \sigma(e), \ldots, \sigma^{n-1}(e)$ are pairwise disjoint. The element $u = e + \sigma(e) + \cdots + \sigma^{n-1}(e)$ is again an idempotent and

$$e = u - u.\sigma(u), \quad \sigma^n(e) = \sigma(u) - \sigma(u).u. \tag{1}$$

Denote by B_n the subset of $\mathcal{B}(R)$ consisting of all idempotents u such that $u = e + \sigma(e) + \cdots + \sigma^{n-1}(e)$, where $e, \sigma(e), \ldots, \sigma^{n-1}(e)$ are pairwise disjoint elements of $\mathcal{B}(R)$.

Let $u \in B_n$, set $e = u - u.\sigma(u)$ and let $I_e = Ann(e) := \{r \in R\colon r.e = 0\}$. Then I_e is a definable ideal included in π (indeed $(1 - e) \in \pi$ and if $r.e = 0$, then $r.(1 - e) = r$, so $r \in \pi$). Since, $1 - e \in I_e$ and for all $0 \leqslant i < j \leqslant n$, $\sigma^i(e).\sigma^j(e) = 0$, $1 - \sigma^j(e) \in \sigma^j(I_e)$, we have that $\sigma^i(e).(1 - \sigma^j(e)) = \sigma^i(e)$ and so, for all $0 \leqslant i < j \leqslant n$,

$$\sigma^i(I_e) + \sigma^j(I_e) = R. \tag{2}$$

Note that for $1 \leqslant i \leqslant n$, we have

$$\sigma^i(I_e) = Ann\big(\sigma^i(e)\big). \tag{3}$$

Case 1. The characteristic of R is equal to zero.

First, we define the subset $[0; n] := \{0, 1, \ldots, n\}$ of F by a formula (with parameters) which does not depend on n.

Let $u \in R$, set

$$F(u) := \big\{ f \in F \colon \exists r \; r \in Ann\big(u - u.\sigma(u)\big) \text{ and } \big(\sigma(r) - r\big).\big(\sigma(r) - r + 1\big) \in Ann\big(\sigma(u)\big) \text{ and } \\ r - f \in Ann\big(\sigma(u) - \sigma(u).u\big) \big\}.$$

Claim 1. *For $u \in B_n$, $F(u) = [0; n]$.*

First note that $\sigma(I_e) \cap \cdots \cap \sigma^n(I_e) = Ann(\sigma(u))$ *(*use *(3)* and the fact that $\sigma(u) = \sigma(e) + \cdots + \sigma^n(e)$*).*

Proof. ($\supseteq$) By hypothesis on $e = u - u.\sigma(u)$ (see (2)), we may apply the Chinese Remainder Theorem, and so there exists $r \in R$ such that

$$\begin{aligned} &r - k \in \sigma^k(I_e), \quad \text{for } k = 0, \ldots, m \quad \text{and} \\ &r - m \in \sigma^k(I_e), \quad \text{for } k = m, \ldots, n. \end{aligned} \tag{4}$$

For $k = n$, $r - m \in \sigma^n(I_e) = Ann(\sigma(u) - \sigma(u).u)$ (see (1)).

By (4), we have:

$$\sigma(r) - k \in \sigma^{k+1} I_e \quad \text{for } k = 0, \ldots, m \quad \text{and} \quad \sigma(r) - m \in \sigma^{k+1} I_e \quad \text{for } k = m, \ldots, n.$$

So, $(\sigma(r) - r).(\sigma(r) - r + 1) \in \sigma(I_e) \cap \cdots \cap \sigma^n(I_e) \subseteq Ann(\sigma(u))$.

Therefore, for any $0 \leqslant m \leqslant n$, $m \in F(u)$.

($\subseteq$) First, let us show that if $r \in I_e$ and $(\sigma(r) - r).(\sigma(r) - r + 1) \in \sigma(I_e) \cap \cdots \cap \sigma^n(I_e)$, then $r.(r-1).\cdots.(r-n) \in \sigma^n(I_e)$.

By induction on k, we prove that $r.\cdots.(r-k) \in \sigma^k(I_e)$.

Let us show that it holds for $k = 1$. First, since $r \in I_e$, $\sigma(r) \in \sigma(I_e)$. Then, since $Ann(\sigma(e)) = \sigma(I_e) \subseteq Ann(\sigma(u))$, we have that $(\sigma(r) - r).(\sigma(r) - r + 1) \in \sigma(I_e)$. So for any prime ideal q containing $\sigma(I_e)$, either $\sigma(r) - r \in q$ or $\sigma(r) - (r - 1) \in q$. Thus, for any such ideal q, either $r \in q$ or $r - 1 \in q$. Therefore, $r.(r-1) \in \sigma(I_e)$.

Assume that it holds for k and let us show it for $k + 1$. Let q be a prime ideal containing $\sigma^{k+1}(I_e)$. By hypothesis, $(\sigma(r) - r).(\sigma(r) - r + 1) \in \sigma^{k+1}(I_e)$, since q is prime, either $(\sigma(r) - r) \in q$ or $(\sigma(r) - r + 1) \in q$. By inductive hypothesis, $r.\cdots.(r-k) \in \sigma^k(I_e)$, and so $\sigma(r).\cdots.(\sigma(r) - k) \in \sigma^{k+1}(I_e)$. So, either $\sigma(r) \in q, \ldots$, or $\sigma(r) - k \in q$. Replacing $\sigma(r)$ by either r or $r - 1$, we get that for any such ideal q, $r.(r-1).\cdots.(r-k).(r-(k+1)) \in q$. Therefore, $r.(r-1).\cdots.(r-k).(r-(k+1)) \in \sigma^{k+1}(I_e)$.

Now, let $f \in F(u)$. Since $\sigma^n(e) = \sigma(u) - \sigma(u).u$ (see (1)), we have that $r - f \in \sigma^n(I_e)$. Also, by the above, $r.(r-1)\cdots(r-n) \in \sigma^n(I_e)$, so we have that $f(f-1)\cdots(f-n) \in \sigma^n(I_e)$; but F is a field, so $\bigvee_{i=0}^n (f - i) = 0$. So, we obtain that $F(u) = [0; n]$. □

Now, we want to define the set of such subsets.

Consider the following subset *Ind* of $\mathcal{B}(R)$:

$$Ind := \big\{ u \in R \colon u^2 = u \;\&\; u.\sigma(u) \neq \sigma(u) \;\&\; u.\sigma(u) \neq u \;\& \\ 0 \in F(u) \;\&\; \big[\big(\exists! y \in F(u)\big)\,(\forall x \neq y)\,\big(x \in F(u) \Rightarrow x + 1 \in F(u)\big) \;\&\; \big(y + 1 \notin F(u)\big)\big]\big\}.$$

For $u \in Ind$, we will denote the element y appearing in the formula defining Ind, by c_u.

By Claim 1, for every $n \in \mathbb{N}$ and $u \in B_n$, $F(u)$ is equal to the subset $[0; n]$. So, the set Ind contains B_n.

Let $\psi(f, u)$ be the following formula: $u \in Ind$ & $f \in F(u)$ & $F(u) \models Q_c$ (with the constant c appearing in the language of Q_c interpreted as c_u).

Let

$$M_1 = \{ f \in F \colon \exists u\ \psi(f, u) \}.$$

Then $\bigcup_n [0; n] \subseteq M_1$.

Let

$$M_0 := \{ f \in F \colon \exists u\ [\psi(f, u)\ \&\ \forall f' \in F(u)\ \exists u'\ \psi(f'.f, u')\ \&\ \psi(f' + f, u')\ \&$$
$$\forall f''\ (\exists u''\ \psi(f'', u'') \to F(u'') \subseteq F(u) \text{ or } F(u) \subseteq F(u''))] \}.$$

Claim 2. *M_0 is an infinite model of either Q_c or Q.*

Proof. First, we have that M_0 contains $\bigcup_n [0; n]$. Indeed, by the above, for $u \in B_n$ we have $F(u) = [0; n]$ and this subset is a model of Q_c with the constant c interpreted by n. Let $f, f' \in [0; n]$, then $f.f'$ and $f + f'$ belong to $[0; \max\{n^2, 2n\}]$. Moreover there exists u' such that this interval is equal to $F(u')$. Therefore, M_0 includes $[0; n]$.

Let $f, f' \in M_0$. So there exists u, u' such that $\psi(f, u)$ & $\psi(f', u')$. So, we get that either $F(u) \subseteq F(u')$ or $F(u') \subseteq F(u)$. W.l.o.g. suppose we are in the first case. By assumption, there exists u'' such that $\psi(f'.f, u'')$ & $\psi(f' + f, u'')$.

Then, either M_0 has an element c such that for an idempotent u such that $\psi(c, u)$ holds, we have that $\forall f \in M_0$ $(\forall u''\ \psi(f, u'') \to F(u'') \subseteq F(u))$, otherwise we get a model of Q. □

Case 2. Suppose now that the ring R is of characteristic p.

Take a non-principal ultrapower of R. Then there is an element $\mu \in F - \tilde{\mathbb{F}}_p$ where $\tilde{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$. The (finite) set of distinct integral powers of μ, namely $[1; \mu^n] = \{1, \mu, \ldots, \mu^i, \ldots, \mu^n\}$ will play the role of the subset $[0; n]$ and the successor function will be interpreted by multiplication by μ. Addition will be interpreted as multiplication and to interpret multiplication, we will first interpret division. This allows us to interpret the least common multiple lcm of two elements, then the square of an element can be defined as $lcm(x, x + 1) - x$ and $x.y = 1/2.((x + y)^2 - x^2 - y^2)$.

Let us indicate the modifications needed from the characteristic zero case.

Set

$$F(u, \mu) := \{ f \in F \colon \exists r\ r \in Ann(u - u.\sigma(u)) \text{ and } (\sigma(r) - r).(\sigma(r) - r.\mu) \in Ann(\sigma(u)) \text{ and}$$
$$r - f \in Ann(\sigma(u) - \sigma(u).u) \}.$$

Claim 3. *For $u \in B_n$ and $\mu \in F - \tilde{\mathbb{F}}_p$, we have $F(u, \mu) = [1; \mu^n]$.*

The proof of this claim goes as before, replacing m by μ^m with $0 \leqslant m \leqslant n$ and "+1" by "$\cdot\ \mu$." Let us indicate how to interpret division, assuming that $u \in B_n$. Let $x, y \in F(u, \mu)$, then $x \mid y$ iff $\exists z\ (y - z)^*.u \neq u\ \&\ (z - u - u.\sigma(u)).(u - u.\sigma(u)) = 0\ \&\ (\sigma(z) - z.x).u = 0$.

Then, we consider the set of such subsets.

Let the set *Ind* be equal to

$$\bigl\{u \in R\colon\ u^2 = u\ \&\ u.\sigma(u) \neq \sigma(u)\ \&\ u.\sigma(u) \neq u\ \&\\ 1 \in F(u, \mu)\ \&\ \bigl[\bigl(\exists! y \in F(u, \mu)\bigr)\ (\forall x \neq y)\ \bigl(x \in F(u, \mu)\ \Rightarrow\ x.\mu \in F(u, \mu)\bigr)\ \&\\ \bigl(y.\mu \notin F(u, \mu)\bigr)\bigr]\bigr\}.$$

For $u \in \mathit{Ind}$, we will denote the corresponding element y by c_u.

By Claim 3, for every $n \in \mathbb{N}$ and $\mu \in F - \tilde{\mathbb{F}}_p$, and $u \in B_n$, we have $F(u, \mu) = [1; \mu^n]$. So, this set *Ind* includes B_n.

Note that if μ is an element of finite order, say n, then there does not exist any element y such that $y.\mu \notin [1; \mu^n]$.

Let $\psi(f, u, \mu)$ be the following formula: $u \in \mathit{Ind}\ \&\ f \in F(u, \mu)\ \&\ F(u, \mu) \models Q_c$ (with c interpreted as c_u).

Let

$$M_1 = \bigl\{f \in F\colon\ \exists u\ \psi(f, u, \mu)\bigr\}.$$

Then $\mu^{\mathbb{N}} \subseteq M_1$.

Let

$$M_0 := \bigl\{f \in F\colon\ \exists u \exists \mu \in F\ \bigl[\psi(f, u, \mu)\ \&\ \forall f' \in F(u, \mu)\ \exists u'\ \psi(f.f', u', \mu)\ \&\\ \forall f''\bigl(\exists u''\ \psi(f'', u'', \mu) \rightarrow F(u'', \mu) \subseteq F(u, \mu) \text{ or } F(u, \mu) \subseteq F(u'', \mu)\bigr)\bigr]\bigr\}.$$

Claim 4. *M_0 is an infinite model of either Q_c or Q.*

In the following corollary, we revisit the case of a difference ring that already appeared in Section 3 (see Remark 3.7).

Corollary 5.2. *The theories of the difference rings of sequences of the form $(F^{\omega}_{\mathcal{F}}, +, ., -, \sigma_t, 0, 1)$ where F is either an infinite subfield of the algebraic closure of $\mathbb{F}_p$ or an infinite pseudo-finite field, and σ_t is the shift endomorphism, are undecidable.*

Proof. These difference rings are commutative von Neumann regular rings: let $(f_n)_{\mathcal{F}} \in F^{\omega}_{\mathcal{F}}$, then $((f_n)_{\mathcal{F}})^* = (f_n^*)_{\mathcal{F}}$ with $f_n^* = f_n^{-1}$ if $f_n \neq 0$ and $f_n^* = 0$ otherwise. The fixed subrings are $\{(f)_{\mathcal{F}}\colon\ f \in F\}$ and so are infinite since F is infinite. □

Recall that the theory of $((\tilde{\mathbb{F}}_p)^{\omega}_{\mathcal{F}}, +, ., -, 0, 1)$, where $\tilde{\mathbb{F}}_p$ denotes the algebraic closure of $\mathbb{F}_p$, is decidable (see [5]).

Corollary 5.3. *The theories of all non-principal ultraproducts on ω of the following structures with $n \in \omega$, p a prime number and (p_n) an infinite increasing sequence of prime numbers:*

$(C^n,+,.,\sigma_n)$, where C is an algebraically closed field of characteristic 0 (*or of characteristic p_n*), *or $(\mathbb{F}_{p^n}^{\mathbb{Z}},+,.,\sigma_t)$ or $(\mathbb{F}_{p_n}^{\mathbb{Z}},+,.,\sigma_t)$ or equivalently the set of sentences true for all but finitely many of these is undecidable.*

Proof. Any such ultraproduct satisfies the hypothesis of Proposition 5.1. □

Note that no ultraproduct of these structures can satisfy a finitely axiomatizable undecidable theory (such as Q), since otherwise either some $(C^n,+,\cdot,\sigma_n)$ or $(\mathbb{F}_{p^n}^{\mathbb{Z}},+,.,\sigma_t)$ or $(\mathbb{F}_{p_n}^{\mathbb{Z}},+,.,\sigma_t)$ already would, for almost all n (see Section 4).

Recall that a theory T is hereditarily undecidable if every subset of its deductive closure is an undecidable theory (equivalently any completion is undecidable). (See [16, p. 234].)

Corollary 5.4. *Let T_∞ be the theory of von Neumann regular commutative difference rings for which $Fix(\sigma)$ is infinite, together with the infinite scheme of axioms: $e_n^2=e_n$ and $\sum_{i=0}^{n-1}\sigma^i(e_n)=1$ & $\bigwedge_{i\neq j}\sigma^i(e_n).\sigma^j(e_n)=0$ & $\sigma^n(e_n)=e_n$, $n\in\omega$. Then T_∞ is hereditarily undecidable.*

Proof. In any model of T_∞, we interpret an infinite model of Q_c and any such model satisfies *Rec*. (See proof of Theorem 5.5.7 in [16].) □

Definition 5.5. We will say that a commutative ring is b-Bezout if every finitely generated ideal is generated by b elements, with $b\in\mathbb{N}-\{0\}$.

Note that being b-Bezout is equivalent to the condition that the sum of two ideals generated by b elements is again generated by b elements. We can express this property by a first-order sentence; so the class of b-Bezout rings is an elementary class. (In fact, it suffices to express that any ideal generated by $b+1$ elements can be generated by b elements, as follows: $\forall r_1\cdots\forall r_{b+1}\exists s_1\cdots\exists s_b\ \forall a_1\cdots\forall a_{b+1}\ \exists c_1\cdots\exists c_{b+1}\ \sum_{i=1}^{b+1}r_i.a_i=\sum_{j=1}^{b}\ s_j.c_j$.) This generalizes Bezout rings, namely those where every finitely generated ideal is principal.

Examples 5.6. Examples of Bezout rings (or 1-Bezout rings) are: von Neumann regular rings (any finitely generated ideal is generated by an idempotent), valuation domains, the ring of entire functions, the ring of algebraic integers (see [21, p. 72]).

Lemma 5.7. *A ring R is b-Bezout for some b iff the class of finitely generated ideals is uniformly definable* (*with parameters*) *in the class $Mod(R)$ of models of the theory of R.*

Proof. Suppose that R is b-Bezout. Let S be elementary equivalent to R and let I be a finitely generated ideal of S. Then, there exist $s_1,\ldots,s_b$ in S such that $I=\langle s_1,\ldots,s_b\rangle$, so ($x\in I$ iff $\exists a_1,\ldots,\exists a_b\ x=\sum_{i=1}^b s_i.a_i$).

In the other direction, suppose that $\phi(x,x_1,\ldots,x_n)$ is a formula defining a finitely generated ideal in any element S of $Mod(R)$, namely for any parameters $\bar r\subset S$, the set $\{x\in S\colon\ S\models\phi(x,\bar r)\}$ is a finitely generated ideal of S.

Now assume that we can find $R_i\in Mod(R)$ and parameters $\bar r_i\subset R_i$ such that the finitely generated ideal $J_i:=\{x\in R_i\colon\ R_i\models\phi(x,\bar r_i)\}$ is generated by not less than n_i elements with (n_i) a strictly increasing sequence of natural numbers. Let $S:=\prod_U R_i$ be a non-principal ultraproduct of R_i, $i \in \omega$ and U a non-principal ultrafilter on ω. The ideal $J := \prod_U J_i$ of S has the property that $x \in J$ iff the formula $\phi(x, [\bar{r}_i]_U)$ holds, but nonetheless it is not finitely generated, a contradiction. □

Proposition 5.8. *Let R be a commutative difference b-Bezout ring of characteristic* 0. *Suppose that the fixed subring of σ is an infinite field. Then either some power of σ fixes the maximal spectrum of R, or the theory of R is undecidable.*

Proof. W.l.o.g., assume that no power of σ fixes the maximal spectrum of R.

First, we will show that we can define the set $[0; n] = \{0, 1, \ldots, n\}$ by a formula (with parameters of length less than or equal to $3b$) which does not depend on n.

The second part of the proof is similar to the proof of Proposition 5.1.

Let $F := Fix(\sigma)$.

Claim. *There exists $(\bar{s}_0, \bar{s}_1, \bar{s}_2) \in R^{3b}$ such that*

$$F(\bar{s}_0, \bar{s}_1, \bar{s}_2) := \bigl\{f \in F\colon \exists r \ \bigl(r \in \langle \bar{s}_0\rangle \text{ and } \bigl(\sigma(r) - r\bigr).\bigl(\sigma(r) - r + 1\bigr) \in \langle \bar{s}_1\rangle \text{ and } r - f \in \langle \bar{s}_2\rangle\bigr)\bigr\}$$

is equal to $[0; n]$.

The proof of this claim is subdivided into two subclaims.

By assumption on σ, for each n, there exists a maximal ideal π such that π and all $\sigma(\pi), \ldots, \sigma^n(\pi)$ are distinct. We will choose the parameters $(\bar{s}_0, \bar{s}_1, \bar{s}_2)$ such that $\langle \bar{s}_0\rangle$ is included in π, $\langle \bar{s}_1\rangle$ in $\bigcap_{i=1}^n \sigma^i(\pi)$ and $\langle \bar{s}_2\rangle$ in $\sigma^n(\pi)$.

Sub-claim 1. There exist $\bar{s}_0, \bar{s}_1, \bar{s}_2 \in R^b$ such that $\langle \bar{s}_0\rangle \subseteq \pi$, $\langle \bar{s}_1\rangle = \tilde{J}_1 \cap \tilde{J}_2 \cap \cdots \cap \tilde{J}_n$, where $\tilde{J}_i$, $1 \leqslant i \leqslant n$, is a finitely generated ideal included in $\sigma^i(\pi)$, $\bar{s}_2$ generate $\tilde{J}_n$ and $[0; n] \subseteq F(\bar{s}_0, \bar{s}_1, \bar{s}_2)$.

Proof. We have that for any $0 \leqslant i < j \leqslant n$, $\sigma^i(\pi) + \sigma^j(\pi) = R$, so given $0 \leqslant i \leqslant n$ for every j with $j \neq i$, $0 \leqslant j \leqslant n$, we have that $1 = u_{ij} + u_{ji}$ with $u_{ij} \in \sigma^i(\pi)$ and $u_{ji} \in \sigma^j(\pi)$. Set $I_i := \langle u_{ij};\ i \neq j,\ 0 \leqslant j \leqslant n\rangle$, it is included in $\sigma^i(\pi)$; and these ideals I_i, I_j are pairwise co-maximal for each pair $0 \leqslant i < j \leqslant n$, namely $R = I_i + I_j$.

Therefore by the Chinese Remainder Theorem, given n and $0 \leqslant m \leqslant n$, there exists $r \in R$ such that $r - \ell \in I_\ell$, for $\ell = 0, \ldots, m$ and $r - m \in I_\ell$, for $\ell = m, \ldots, n$. So, $\sigma(r) - \ell \in \sigma(I_\ell)$ for $\ell = 0, \ldots, m$ and $\sigma(r) - m \in \sigma(I_\ell)$ for $\ell = m, \ldots, n$. Set $J_\ell := \langle \sigma(I_{\ell-1}), I_\ell\rangle \subseteq \sigma^\ell(\pi)$, $1 \leqslant \ell \leqslant n$. So, $(\sigma(r) - r).(\sigma(r) - r + 1) \in J_1 \cap \cdots \cap J_n$.

Note that the ideals J_i and J_j, for $1 \leqslant i \neq j \leqslant n$, are pairwise co-maximal (since they contain pairwise co-maximal ideals). Since J_1 and J_2 are pairwise co-maximal, we have that $J_1 \cap J_2 = J_1.J_2$. Now, we will define finitely generated ideals $J_l \subseteq \tilde{J}_l \subseteq \sigma^l(\pi)$ in such a way that $\bigcap_l \tilde{J}_l = \tilde{J}_1. \cdots .\tilde{J}_n$. We choose in R^b a tuple of generators $\bar{s}_0$ (respectively $\bar{s}_2$) for $\tilde{J}_1$ (respectively $\tilde{J}_n$) and $\bar{s}_1$ a tuple of generators for $\tilde{J}_1. \cdots .\tilde{J}_n$.

Note that once we have proved that, we have shown using the above that $[0; n] \subseteq F(\bar{s}_0, \bar{s}_1, \bar{s}_3)$, where $\bar{s}_0, \bar{s}_1, \bar{s}_3$ are chosen as in the statement of the Sub-claim 1.

By induction on $1 < k \leqslant n$ suppose that $\bigcap_{l=1}^k \tilde{J}_l = \tilde{J}_1. \cdots .\tilde{J}_k$. This holds for $k = 2$, taking $J_1 = \tilde{J}_1$ and $J_2 = \tilde{J}_2$. Let $w_i \in J_i - \sigma^{k+1}(\pi)$ for $1 \leqslant i \leqslant k$ (this is always possible since J_i and

J_{k+1} are co-maximal and since J_{k+1} is included in $\sigma^{k+1}(\pi)$, we also have that J_i and $\sigma^{k+1}(\pi)$ are co-maximal and so distinct). Moreover, since $\sigma^{k+1}(\pi)$ is prime, $w := w_1.\cdots.w_k \notin \sigma^{k+1}(\pi)$. So, since $\sigma^{k+1}(\pi)$ is maximal, then $(\sigma^{k+1}(\pi), w) = R$, so there exists $w_{k+1} \in \sigma^{k+1}(\pi)$ such that $w_{k+1} + w = 1$. Set $\tilde{J}_{k+1} := (J_{k+1}, w_{k+1})$. We have that still $\tilde{J}_{k+1} \subseteq \sigma^{k+1}(\pi)$ and now since $\tilde{J}_1.\cdots.\tilde{J}_k$ and $\tilde{J}_{k+1}$ are co-maximal, using the induction hypothesis, we get $\bigcap_{l=1}^{k+1} \tilde{J}_l = \tilde{J}_1.\cdots.\tilde{J}_{k+1}$.

After $n-1$ steps, we get that each $\tilde{J}_l \subseteq \sigma^l(\pi)$, $1 \leqslant l \leqslant n$, is finitely generated and so by hypothesis on our ring R, it is generated by less than b elements and now, their intersection being their product it is still finitely generated and so generated by a tuple, say $\bar{s}_1$ of length less than or equal to b. □

Sub-claim 2. Let $\bar{s}_0 \in R^b$ be such $\langle \bar{s}_0 \rangle \subseteq \pi$, let $\bar{s}_1 \in R^b$ be such that $\langle \bar{s}_1 \rangle = \tilde{J}_1 \cap \tilde{J}_2 \cap \cdots \cap \tilde{J}_n \subseteq \bigcap_{i=1}^n \sigma^i(\pi)$ and $\bar{s}_2 \in R^b$ generate $\tilde{J}_n \subseteq \sigma^n(\pi)$. Then $F(\bar{s}_0, \bar{s}_1, \bar{s}_2) \subseteq [0; n]$.

Proof. Let $f \in F(\bar{s}_0, \bar{s}_1, \bar{s}_2)$. Then, there exists $r \in \pi$ such that $(\sigma(r) - r).(\sigma(r) - r + 1) \in \bigcap_{i=1}^n \sigma^i(\pi)$ and $r - f \in \sigma^n(\pi)$.

First we prove by induction on $k \leqslant n$ that $r.(r-1).\cdots.(r-k) \in \sigma^k(\pi)$.

Note that since $r \in \pi$ and $(\sigma(r) - r).(\sigma(r) - r + 1) \in \sigma(\pi)$, then $r(r-1) \in \sigma(\pi)$. Suppose that it holds for k and let us prove it for $k+1$. So, $r(r-1)\cdots(r-k) \in \sigma^k(\pi)$ and $\sigma(r)(\sigma(r)-1)\cdots(\sigma(r)-k) \in \sigma^{k+1}(\pi)$. Since $\sigma^{k+1}(\pi)$ is prime, either $\sigma(r) = r$ modulo $\sigma^{k+1}(\pi)$, so $r(r-1)\cdots(r-k) \in \sigma^{k+1}(\pi)$, or $\sigma(r) = r - 1$ modulo $\sigma^{k+1}(\pi)$, so $(r-1)\cdots(r-k).(r-(k+1)) \in \sigma^{k+1}(\pi)$. Therefore, $r(r-1)\cdots(r-k).(r-(k+1)) \in \sigma^{k+1}(\pi)$ and we get that $r.(r-1).\cdots.(r-n) \in \sigma^n(\pi)$. But $r - f \in \sigma^n(\pi)$. Therefore, $f(f-1)\cdots(f-n) \in \sigma^n(\pi)$; but F is a field, so $\bigvee_{i=0}^n (f-i) = 0$. □

Putting both sub-claims together, we obtain the claim, namely that for every natural number n, there exists a tuple $\bar{s}_0, \bar{s}_1, \bar{s}_2 \in R^{3b}$ such that

$$[0; n] = F(\bar{s}_0, \bar{s}_1, \bar{s}_2).$$

Then we proceed as in the proof of Proposition 5.1.

Let $(\bar{s}_0, \bar{s}_1, \bar{s}_2) \in R^{3b}$, where b is the maximal size of a generating set for the finitely generated ideals of R. For ease of notations, set $\bar{s} := (\bar{s}_0, \bar{s}_1, \bar{s}_2)$.

Let $Ind := \{\bar{s} \in R^{3b}$: $0 \in F(\bar{s})$ & $(\exists! y \in F(\bar{s}))$ $(\forall x \neq y)$ $(x \in F(\bar{s}) \Rightarrow x+1 \in F(\bar{s}))$ & $y+1 \notin F(\bar{s})\}$.

We saw that for every $n \in \mathbb{N}$, there exists $\bar{s} \in Ind$ with $F(\bar{s}) = [0; n]$.

For $\bar{s} \in Ind$, set $y := c_s$.

Let $\psi(f, \bar{s})$ be the following formula: $\bar{s} \in Ind$ & $\pm f \in F(\bar{s})$ & $F(\bar{s}) \models Q_c$ (with c interpreted as c_s)

Let $M_1 = \{f \in F$: $\exists \bar{s}\ \psi(f, \bar{s})\}$. Then $\bigcup_n [0; n] \subseteq M_1$.

Let $M_0 := \{f \in F$: $\exists \bar{s}$ $[\psi(f, \bar{s})$ & $\forall f' \in F(\bar{s})$ $\exists \bar{s}'$ $\psi(f'.f, \bar{s}')$ & $\psi(f' + f, \bar{s}')$ & $\forall f''$ $\exists \bar{s}''$ $\psi(f'', \bar{s}'')$ & $F(\bar{s}'') \subseteq F(\bar{s})$ or $F(\bar{s}) \subseteq F(\bar{s}'')]\}$.

Now, we can check, as in Proposition 5.1, that M_0 is a model of either Q_c or Q. We have that M_0 contains $\bigcup_n [0; n]$ and, either M_0 has an element c such that for $\bar{s}$ such that $\psi(c, \bar{s})$ we have that $\forall f \in M_0$ $(\forall \bar{s}''\ \psi(f'', \bar{s}'') \rightarrow F(\bar{s}'') \subseteq F(\bar{s}))$, or we get a model of Q. □

Examples 5.9. (1) Let $\mathbb{C}\{z^{-1}\}$ be the ring of power series in z^{-1} that converge in a neighborhood of infinity and let σ_1 be the automorphism sending $f(z) \to f(z+1)$, where $f(z) = \sum_n a_n.z^{-n}$. We can embed this ring in $\mathbb{C}^{\omega}_{\mathcal{F}}$ by sending f to $(f(1), f(2), \ldots)_{\mathcal{F}}$. So its fixed subring is a field. The maximal spectrum of this ring contains the maximal ideals of the functions which are zero at some point z_0 and so we meet the hypothesis of the above proposition.

So, the theory of the difference ring $(\mathbb{C}\{z^{-1}\}, +, ., 0, 1, \sigma_1)$ is undecidable.

(2) Let $\mathbb{C}\{z\}$ be the ring of entire functions, and let $c \in \mathbb{C}$ be a complex number of modulus 1 and which is not a root of unity. Let σ_c be the automorphism sending $f(z) \to f(c.z)$, where $f(z) \in \mathbb{C}\{z\}$. We can embed this ring in $\mathbb{C}^{\omega}_{\mathcal{F}}$ by sending f to $(f(1), f(c), f(c^2), \ldots)_{\mathcal{F}}$. Since the disk of unity is compact, the fixed subring is a field. The maximal spectrum of this ring contains the maximal ideals of the functions which are zero at some point z_0 and so we meet the hypothesis of the above proposition.

So, the theory of the difference ring $(\mathbb{C}\{z\}, +, ., 0, 1, \sigma_c)$ is undecidable.

Remark 5.10. In the preceding proposition, instead of working with maximal ideals we may work with prime ideals provided that given n there exists a prime ideal π such that $\pi, \sigma(\pi), \ldots, \sigma^n(\pi)$ are pairwise co-maximal. Then, we may relax the condition that $Fix(\sigma)$ is a field, assuming that $Fix(\sigma) \cap \pi = \{0\}$. (However, this implies that $Fix(\sigma)$ is a domain.)

This entails that the ring of sequences with coefficients in $\mathbb{Z}$ with the shift, modulo the Frechet filter, is undecidable. This last result is also a consequence of the following corollary. First, we recall some facts on localization.

Let R be a ring with an automorphism σ and let M be a multiplicative subset of $Fix(\sigma)$. Denote by $R[M^{-1}]$ the localization of R by M. Recall that the elements of $R[M^{-1}]$ are of the form $r.m^{-1}$ and that $r_1.m_1^{-1} = r_2.m_2^{-1}$ iff $\exists m \in M\ (r_1.m_2 - r_2.m_1).m = 0$.

If no element of M is a zero divisor (a non-zero-divisor is also called a *regular* element), then R embeds in $R[M^{-1}]$.

Then, we may extend σ on this ring by defining $\tilde{\sigma}(r.m^{-1}) := \sigma(r).\sigma(m)^{-1}$. This is well-defined since if $(r_1.m_2 - r_2.m_1).m = 0$, then $(\sigma(r_1).\sigma(m_2) - \sigma(r_2).\sigma(m_1)).\sigma(m) = 0$. So, since $\sigma(M) \subseteq M$, then $\sigma(r_1).\sigma(m_1)^{-1} = \sigma(r_2).\sigma(m_2)^{-1}$. Now, we calculate $Fix(\tilde{\sigma})$. Suppose that $\sigma(r_1).\sigma(m_1)^{-1} = r_1.m_1^{-1}$ which means that there exists $m \in M$ such that $(\sigma(r_1).m_1 - r_1.\sigma(m_1)).m = 0$ iff $\sigma(r_1.m_1.m) = r_1.m_1.m$ iff $r_1.m_1.m \in Fix(\sigma)$ iff $r_1 \in Fix(\sigma).M^{-1}$.

Now, if every non-zero element of $Fix(\sigma)$ is regular, then we take $M = Fix(\sigma) - \{0\}$ and we get that $Fix(\tilde{\sigma})$ is a field.

Corollary 5.11. *Let R be a commutative b-Bezout ring of characteristic* 0. *Suppose that $Fix(\sigma) - \{0\}$ is infinite, that it consists of regular elements and for every n, $n \in \omega$, that there exists a prime ideal π such that $\pi \cap Fix(\sigma) = \{0\}$ and $\pi, \sigma(\pi), \ldots, \sigma^n(\pi)$ are pairwise co-maximal. Then $Th((R, \sigma))$ is undecidable.*

Proof. Let $M = Fix(\sigma) - \{0\}$ and consider $R[M^{-1}]$. From the above discussion, we know that we can extend σ on $R[M^{-1}]$ by say $\tilde{\sigma}$ and that $Fix(\tilde{\sigma})$ is a field. We use the fact that the theory of $(R[M^{-1}], +, ., 0, 1, \sigma)$ is interpretable in the theory of R and we check that it satisfies the hypothesis of the proposition above. So, let us check that $R[M^{-1}]$ is b-Bezout. Given k elements $r_1.m_1^{-1}, \ldots, r_k.m_k^{-1}$ generating an ideal I, then the elements $r_1, \ldots, r_k$ also generate I. Since R is b-Bezout, there exist $s_1, \ldots, s_b$ such that there exist $t_j \in R$, $1 \leqslant j \leqslant b$ such that for $1 \leqslant i \leqslant k$, we have $r_i = \sum_{j=1}^{b} s_j.t_j$. So, I is also generated by $s_1, \ldots, s_b$. □

Question 1. Let $\tilde{\mathbb{Z}}$ be the ring of algebraic integers and let σ be a non-trivial element of the absolute Galois group $G(\mathbb{Q})$ of $\mathbb{Q}$. Then, $(\tilde{\mathbb{Z}}, \sigma)$ does not satisfy the hypothesis of the above Corollary. Is the theory of $(\tilde{\mathbb{Z}}, \sigma)$ undecidable?

Recall that G. Cherlin and M. Jarden [9] showed that the theory consisting of the set of sentences true in almost all $(\mathbb{Q}, \sigma_1, \ldots, \sigma_e)$, for $(\sigma_1, \ldots, \sigma_e) \in G(\mathbb{Q})^e$ and $e \geqslant 2$, is undecidable. They left the question open for $e = 1$.

6. Boolean products of models of *ACFA*

In the previous section, we showed undecidability results for von Neumann regular commutative rings for which the automorphism had an infinite orbit on the maximal spectrum. In this section, we will consider von Neumann regular commutative difference rings R, satisfying the following hypothesis on the automorphism σ: the orbits of σ on the maximal spectrum of R, are finite of the same cardinality. We will apply a transfer result due to Burris and Werner on Boolean products.

First, let us recall the definition of a Boolean product of $\mathcal{L}$-structures R_x with $x \in X$ (see [5]). It will be denoted by $\Gamma_a(X, \bigcup_{x \in X} R_x)$ and the R_x will be called the stalks of this Boolean product.

Definition 6.1. First, we define the truth value of a formula $\phi(u, \bar{a})$ in a subdirect product included in $\prod_{x \in X} R_x$ as $\{x \in X\colon R_x \models \phi(u(x), \bar{a}(x))\}$ and we denote this subset by $[\phi(u, \bar{a})]$. Then, R is a Boolean product of $\mathcal{L}$-structures R_x with $x \in X$ if

(1) R is a subdirect product of the R_x, $x \in X$,
(2) the set X is a Boolean space i.e. X has a basis of clopen sets (both open and closed),
(3) for every atomic formula, its truth value is a clopen subset of X,
(4) R has the *patchwork property* i.e. for any $f, g \in R$ and N a clopen subset of X, the element h of the product $\prod_{x \in X} R_x$ defined by

$$h(x) = \begin{cases} f(x) & \text{if } x \in N, \\ g(x) & \text{if } x \in X - N, \end{cases}$$

belongs to R.

If all the structures R_x are equal to some R_{x_0}, we will denote the corresponding Boolean product by $\Gamma_a(X, R_{x_0})$. (The domain of this Boolean product is the set of locally constant functions from X to R_{x_0}.)

Recall that any commutative von Neumann regular ring R can be represented as a Boolean product of fields (see [12], [6, p. 163]), namely $\Gamma_a(X, \bigcup_{x \in X} R_x)$ where $X = MSpec(R)$, x is a maximal ideal of R and R_x is the field R/x. If b is an element of R, then e_b denotes the idempotent $b.c$, where c is such that $b = b^2.c$ and $c = c^2.b$. Such element c is uniquely determined and will be called the pseudo-inverse of b.

In the above Boolean product representation, one can view e_b as the characteristic function of the support of b i.e. $\{x \in X\colon 1 - e_b \in x\} = \{x \in X\colon b \notin x\}$; and it will be called the idempotent associated with b.

Recall that the Boolean algebra of idempotents of R is denoted by $\mathcal{B}(R)$, and that this structure is 0-definable in R. The Stone space of $\mathcal{B}(R)$ is homeomorphic to X.

We add to the ring language $\mathcal{L}_{\text{rings}}$ a unary function symbol $*$, the corresponding language is denoted by $\mathcal{L}_{\text{rings},*}$ and we add the following defining *universal* axiom: $\forall x\ (x.(x.x^*) = x\ \&\ x^*.(x^*.x) = x^*)$. In the language $\mathcal{L}_{\text{rings},*}$, the theory of commutative von Neumann regular rings is universally axiomatized. Using the function *, we have that $c = b^*$ and $e_b = b.b^*$.

Lemma 6.2. *Let R be commutative von Neumann regular ring and let σ be a ring endomorphism. Then,*

(1) *σ is an Boolean algebra endomorphism of $\mathcal{B}(R)$. Moreover, if it is injective on $\mathcal{B}(R)$, it is injective on R.*
(2) *σ preserves the equality between the supports of the elements.*
(3) *If $\mathcal{B}(R) \cap Fix(\sigma) = \{0, 1\}$, then $Fix(\sigma)$ is a field.*

Proof. (1) The first part follows from the fact that $\mathcal{B}(R)$ is 0-definable in R. Then, suppose that $\sigma(a) = 0$. Then, $\sigma(e_a) = 0$ and so $e_a = 0$ by hypothesis, which implies that $a = 0$.

(2) First, note that $\sigma(a^*) = \sigma(a)^*$ (indeed the function * is definable in the ring language), for any element $a \in R$. Now, let a, b be two elements with the same supports. So $e_a = a.a^* = e_b = b.b^*$, and $\sigma(e_a) = \sigma(a).\sigma(a^*) = \sigma(e_b) = \sigma(b).\sigma(b^*)$. But, $\sigma(a^*) = \sigma(a)^*$ (respectively $\sigma(b^*) = \sigma(b)^*$), so $e_{\sigma(a)} = \sigma(e_a)$. Therefore, $\sigma(a)$ and $\sigma(b)$ have the same supports.

(3) Let $r \in Fix(\sigma) - \{0\}$, then $r^* \in Fix(\sigma)$. So, $r.r^* \in Fix(\sigma) \cap \mathcal{B}(R)$, by hypothesis, $r.r^* = 1$, namely r is invertible. □

Remark 6.3. If (R, σ) is a von Neumann commutative regular difference ring, then the hypothesis of $Fix(\sigma)$ *is an infinite field* is equivalent to $Fix(\sigma)$ *infinite and* $Fix(\sigma) \cap \mathcal{B}(R) = \{0, 1\}$.

Definition 6.4. Given an $\mathcal{L}$-theory T and a unary function symbol σ, we define the language $\mathcal{L}_\sigma$ to be the language $\mathcal{L} \cup \{\sigma, \sigma^{-1}\}$ and the $\mathcal{L}_\sigma$-theory T_σ to be the theory T together the scheme of axioms expressing that σ is an automorphism in the class of models of T and that σ^{-1} is its inverse. Note that if T is an $\forall\exists$-theory, then so is T_σ.

From now on in this section, let $\mathcal{L}$ be $\mathcal{L}_{\text{rings}} := \{0, 1, +, -, .\}$ and T be the $\mathcal{L}$-theory of commutative von Neumann regular rings (respectively T_σ the $\mathcal{L}_\sigma$-theory of commutative von Neumann regular difference rings).

In a von Neumann commutative regular ring, one can define a binary function symbol $p(.,.)$ as follows: $p(a, b) = d \leftrightarrow \exists c\ (b = b.c^2 \wedge d = a.(1 - b.c))$. Alternatively using the function *, we get that $p(a, b) = a.(1 - b.b^*)$. The support of an element a is equal to $1 - p(1, a) = a.a^*$. (Note that the relation "the support of a is included in the support of b" is definable by $p(a, b) = 0$ without referring to the supports of each element. Indeed, $p(a, b) = 0 \leftrightarrow a = a.e_b \rightarrow a.a^* = a.e_b.a^* \rightarrow e_a = e_a.e_b$. Conversely, assume that $e_a = e_a.e_b$, then $a.e_a = e_a.e_b.a \rightarrow a = a.e_b \rightarrow a = a.b.b^* \leftrightarrow p(a, b) = 0$.)

Since $p(.,.)$ is definable in the ring language, σ remains an automorphism for the $\mathcal{L} \cup \{p(.,.)\}$ language (and similarly for $\mathcal{L}_*$). Also, if we show a model-completeness result in $\mathcal{L} \cup \{p(.,.)\}$, then it still holds in $\mathcal{L}$ since the graph of $p(.,.)$ is existentially definable.

Let T_{vac} be the $\mathcal{L}$-theory T augmented by the axioms expressing that the Boolean algebra of idempotents is atomless and that any monic polynomial has a root.

Recall that this theory has been shown to be the model companion of the theory T_{nn} of non-trivial commutative rings with unity and without non-zero nilpotent elements (see [24] and [5]). Later in this section, we will prove an analogous result in a subclass of the class of difference semi-simple rings (see Proposition 6.8).

Let (R, σ) be a commutative difference ring without nilpotent elements. Suppose that σ leaves *MSpec*(R) invariant, then R is a subdirect product of difference fields, each of which can be embedded into a model of *ACFA*. In the following, we will axiomatize the Boolean products of such structures. There is a general procedure for doing so, described by Burris and Werner [5]. One expands the language of the structures by adding a discriminator function, namely $t(a,b,c) = d \leftrightarrow ((a = b \;\&\; t(a,b,c) = c)$ or $(a \neq b \;\&\; t(a,b,c) = a))$, where t is a term of the language. In our case, one can take for $t(a,b,c)$ the term $p(c-a, a-b) + a$. Then, whenever a class of structures is $\forall\exists$-axiomatizable, the class of Boolean products of elements of that class is $\forall\exists$-axiomatizable in the expansion (see Lemma 9.4, Corollary 9.5 in [5]).

Definition 6.5. Let R be a commutative von Neumann regular difference ring and let $X = MSpec(R)$. Then, $R \cong \Gamma_a(X, \bigcup_{x\in X} R_x)$, where $R_x \cong R/x$.

A subset U of R^n is said to be an *algebraic variety on an idempotent e* if it is the set of all solutions of a finite conjunction of polynomial equations where the support of each non-zero coefficient is equal to the idempotent e.

We will denote by $U(x)$ the subset of elements $\bar{s}$ in ${R_x}^n$ such that there exists $\bar{r} \in R^n \cap U$ such that $\bar{s} = \bar{r}(x)$. Recall that the property for a variety U for being irreducible (respectively absolutely irreducible) is a first-order property of the set of coefficients, which can be expressed by a quantifier-free formula (see [14]). We define the property of being *irreducible* (respectively *absolutely irreducible*) for a variety U on an idempotent e as the property that for each $x \in e$, $U(x)$ is irreducible (respectively absolutely irreducible). This last property can be expressed in $\mathcal{L}_\sigma$ by a quantifier-free formula in the coefficients and the idempotent e.

We will denote by $\sigma(U)$ the set of $\{\sigma(\bar{r}).e\colon \bar{r} \in U\}$.

Let U be an irreducible variety on e and let V be a variety included in $U \times \sigma(U)$, then V projects generically onto U, if for every $x \in e$, $V(x)$ projects generically onto $U(x)$.

Notation 6.1. On the set of idempotents of a model of T, we will use the relation symbol $\leqslant$ defined by $e \leqslant u$ whenever $e.u = e$.

6.1. Let $T_{\mathrm{atm},1,\sigma}$ be the following $\mathcal{L}_\sigma$-theory.

(1) R is a von Neumann regular commutative difference ring without minimal idempotents satisfying $T_{\mathrm{vac},\sigma}$,
(2) The Boolean algebra of idempotents is included in the set of fixed points of σ,
(3) For each idempotent e, for every absolutely irreducible variety U on e and every variety $V \subset U \times \sigma(U)$ projecting generically onto U and $\sigma(U)$ and every algebraic set W properly contained in V, there is $a \in U(R)$ such that $(a, \sigma(a)) \in V - W$.

The fact that the list of the above properties are $\forall\exists$-axiomatizable in $\mathcal{L}_\sigma$ follows from the fact that *ACFA* is $\forall\exists$ axiomatizable and that we work in the expansion of $\mathcal{L}_\sigma$ by $p(.,.)$ (see Lemma 9.4 and Corollary 9.5 in [5]).

Using the construction of bounded Boolean powers, one can exhibit models of $T_{\mathrm{atm},1,\sigma}$ (see [5, p. 274]). Let X_0 be a Cantor space, namely a Boolean space without isolated points. Let

(F, σ) be a model of *ACFA*, let $\Gamma_a(X_0, F)$ be the set of locally constant functions from X_0 to F. Any element $\Gamma_a(X_0, F)$ is of the form $\sum_{i\in I} e_i.f_i$, where I is a finite set, $f_i \in F$ and e_i is a characteristic function of a clopen subset of X_0. Then, $\Gamma_a(X_0, F)$ is a model of $T_{\mathrm{atm},1,\sigma}$.

Proposition 6.6. *The theory $T_{\mathrm{atm},1,\sigma}$ is model-complete and decidable.*

Proof. First, to show model-completeness, we apply a transfer result of Burris and Werner (Theorem 9.13 in [5]), using the model-completeness of *ACFA*. So, we obtain that $T_{\mathrm{atm},1,\sigma}$ is model-complete in the expanded language $\mathcal{L}_\sigma \cup \{p(.,.)\}$. Then we note that the function $p(.,.)$ is existentially definable in the ring language. (We could have used directly a result of A. Macintyre on sheaves of positively model-complete theories (see Corollary 10.9 in [5]).) For the decidability result, apply Theorem 4.5 in [5] and the decidability of *ACFA* (see [11]). (To show this last result, one identifies the completions of *ACFA* and notes that they are recursively axiomatizable.) □

Recall that in a commutative ring R, the Jacobson radical $J(R)$ is the intersection of all its maximal ideals; it is equal to $\{z \in R\colon \forall a\ \exists u\ (1-a.z).u = 1\}$. In his paper [13] on the decidability of the theory of the ring of algebraic integers, L. van den Dries introduced the binary relation

$$a_1 \in rad(a),$$

expressing (in the class of all commutative rings) that every maximal ideal containing a also contains a_1. (One expresses that $a_1 \in J(R/(a))$.) This relation $a_1 \in rad(a)$ is first-order definable by:

$$\forall x\ \exists y\ (1 - a_1.x).y \in 1 + (a).$$

Definition 6.7. Let $T_{ss,\sigma}$ be the following $\mathcal{L}_\sigma$-theory expressing the following properties of a difference ring R.

(1) (R, σ) is a commutative difference ring,
(2) $\forall z\ (\forall a\ \exists u\ (1 - a.z).u = 1 \to z = 0)$ (R is semi-simple),
(3) $\forall a\ \forall x\ \exists y\ \exists z\ (1 - \sigma(a).x).y = 1 + a.z$.

Proposition 6.8. *The theory $T_{\mathrm{atm},1,\sigma}$ is the model-companion of $T_{ss,\sigma}$.*

Proof. First, note that a model R of $T_{\mathrm{atm},1,\sigma}$ satisfies $T_{ss,\sigma}$. Let us check axiom (3). Let M be a maximal ideal of R, suppose that $a \in M$, then $e_a(M) = 0$. Since σ is the identity on the Boolean algebra of idempotents of R, $\sigma(e_a) = e_a$. In particular, $\sigma(e_a)(M) = 0$, but $\sigma(e_a) = \sigma(a.a^*) = \sigma(a).\sigma(a)^* = e_{\sigma(a)}$, so $\sigma(a) \in M$.

Then, let (R, σ) be a model of $T_{ss,\sigma}$, let us show that we can embed it into a model $(\tilde{R}, \tilde{\tilde{\sigma}})$ of $T_{\mathrm{atm},1,\sigma}$. The hypothesis (2) on R that $J(R) = \{0\}$ is equivalent to R being a subdirect product of fields. Moreover, since R satisfies $\forall a\ \sigma(a) \in rad(a)$ by (3), these fields are difference fields. Indeed, for any maximal ideal M, we have $a \in M$ implies that $\sigma(a) \in M$. So, for any $a \in R$, we may define $\sigma(a + M) := \sigma(a) + M$. Then we use the previous result as follows.

Since R embeds into $\prod_{M_i \in MSpec(R)} R/M_i$, we have that $\prod_{M_i \in MSpec(R)} R/M_i \hookrightarrow \prod_{M_i \in MSpec(R)} F_i$, where F_i is a model of *ACFA* into which R/M_i embeds [11].

Let X_0 be the Cantor space and let $\Gamma_a(X_0, F_i)$ be the Boolean product of locally constant functions from X to F_i. We extend σ to $\Gamma_a(X_0, F_i)$ as follows: $\tilde{\sigma}(\sum_j e_j.f_j) := \sum_j e_j.\sigma(f_j)$, where e_j is the characteristic function of a clopen subset of X_0 and $f_j \in F_i$. Now, each $\Gamma_a(X_0, F_i)$ is a model of $T_{\mathrm{atm},1,\sigma}$ (see [5, p. 274]).

Set $\tilde{R} = \prod_{M_i \in MSpec(R)} \Gamma_a(X_0, F_i)$. Then, $\tilde{R}$ is a model of T_{vac}. We extend $\tilde{\sigma}$ to $\tilde{R}$ as follows: $\tilde{\tilde{\sigma}}(r_i)_{M_i \in MSpec(R)} := (\tilde{\sigma}(r_i))_{M_i \in MSpec(R)}$. As a direct product of models of $T_{\mathrm{atm},1,\sigma}$, $(\tilde{R}, \tilde{\tilde{\sigma}})$ is also a model of $T_{\mathrm{atm},1,\sigma}$, which is model-complete by the preceding proposition. Since $R \hookrightarrow \tilde{R}$, we get the result. □

6.2. Let R be a commutative von Neumann regular difference ring. Assume that there exists a natural number $n > 1$ such that σ^n acts as the identity on $X(R) = MSpec(R)$.

For each divisor d of n, let X_d be the set $\{x \in X(R)\colon \sigma^d(x) = x\}$. Note that $X_d^\sigma = X_d$ and $X(R) = X_n$. Let $1 \leqslant d_0, d_1 \leqslant d$ be two divisors of d. Then if $d_0 \mid d_1$, $X_{d_0} \subseteq X_{d_1} \subseteq X_n$, and if $(d_0, d_1) = 1$, then $X_{d_0} \cap X_{d_1} = X_1$.

The subspaces of the form X_d are closed subsets of $X(R)$. Indeed, $\{y \in X(R)\colon \sigma^d(y) \neq y\}$ is an open subset of $X(R)$ since we can find an idempotent e such that e belongs to y and with disjoint image under σ^d. On $X(R)$, we put the following equivalence relation $\sim$: $x_0 \sim x_1$ iff x_0, x_1 belong to the same orbit. Note that each X_d is a union of equivalence classes. Above each element $[x]_\sim$ of $Y_d := X_d/\sim$, we put a direct product of n/d copies of the difference field $(R/x, \sigma^d)$, namely $(R/x \times \cdots \times R/x, \sigma)$.

From now on, we will assume that the automorphism σ has all its orbits of size n on $X(R)$, namely for any divisor d of n strictly smaller than n we have

$$X_d = \emptyset \quad \text{and} \quad X_n = X(R). \tag{$\star$}$$

Note that for the Boolean algebra of subsets of a finite set X on which σ acts, property $(\star)$ of X is equivalent to the following property of the Boolean algebra: $\exists e\ (\bigwedge_{i=1}^{n-1} e.e^{\sigma^i} = 0\ \&\ \sum_{i=0}^{n-1} e^{\sigma^i} = 1)$.

Let $B_0 := \{e \in \mathcal{B}(R)\colon e, \sigma(e), \ldots, \sigma^{n-1}(e)$ are pairwise disjoint$\}$. Note that if $e \in B_0$ and $u \leqslant e$, then $u \in B_0$. Recall that the notation $[e = 1] = \{x \in X(R)\colon 1 - e \in x\}$ denotes the truth value of the atomic formula $e = 1$ in the Boolean product representation. By $(\star)$, we have that $X(R) = \bigcup_{e \in B_0} [e = 1]$ and we extract a finite disjoint minimal subcovering $\{[e_1 = 1], \ldots, [e_m = 1]\}$. Let $\mathcal{B}_0$ be the difference Boolean algebra generated by $e_1, \ldots, e_m$. Since $\mathcal{B}_0$ is finite and has no ultrafilters with orbits of order strictly less than n, it contains an idempotent e such that $(\bigwedge_{i=1}^{n-1} e.e^{\sigma^i} = 0\ \&\ \sum_{i=0}^{n-1} e^{\sigma^i} = 1)$; let $X_0 := [e = 1]$.

Now, we can proceed in two ways. Either, above each point x of X_0, we define the fiber to be equal to the direct product $R/x \times \cdots \times R/x^{\sigma^{n-1}}$, or we decompose R as the finite direct product $R.e \times \cdots \times R.\sigma^{n-1}(e)$.

We will choose the first approach.

Let $\mathcal{O}$ be the set of orbits of σ. Each orbit contains exactly one element of X_0, so we identify it with this element. So, the set of orbits becomes a Boolean space and for $O \in \mathcal{O}$, we write $R_O := R/\pi \times \cdots \times R/\pi^{\sigma^{n-1}}$, where O contains π. We get that R is isomorphic to a subdirect product of the R_O, $O \ni x$, $x \in X_0$. For an element $r \in R$, denote by r_O the n-tuple $(r + x, \ldots, \sigma^{n-1}(r) + \sigma^{n-1}(x))$ with $x \in O$. Indeed, let f be the map sending r to $((r_O)_{O \in \mathcal{O}})$. The map f is injective: let $r \neq s$ and let $x \in [r - s \neq 0]$. Then there exists i such that $\sigma^i(x) \in X_0$ and $\sigma^i(r - s) \notin \sigma^i(x)$. Then, given an element $(r_0 + x, \ldots, r_{n-1} + \sigma^{n-1}(x))$ with $r_0, \ldots, r_{n-1} \in R$, we can choose an element u in B_0 such that $x \in u$. So, letting $r := \sum_{i=0}^{n-1} r_i.\sigma^i(u)$, we have that $r_O = (r_0 + x, \ldots, \sigma^{-n+1}(r_{n-1}) + \sigma^{n-1}(x))$.

Properties 3 and 4 of a Boolean product (see Definition 6.1) follow from the fact that R is a Boolean product.

The automorphism σ acts as the identity on $\mathcal{O}$. Therefore, R is a Boolean product of models of $T^f_{n,\sigma}$ (see Section 4). So, we obtained the following result.

Lemma 6.9. *Suppose that there exists n such that σ^n fixes $\mathcal{B}(R)$ and such that $\mathcal{B}(R)$ satisfies $\exists e\ (\bigwedge_{i=1}^{n-1} e.e^{\sigma^i} = 0\ \&\ \sum_{i=0}^{n-1} e^{\sigma^i} = 1)$. Then, R is a Boolean product of difference rings $R_O \models T^f_{n,\sigma}$, when O ranges over the orbits of σ on the corresponding Boolean space X_0. Also, σ acts as the identity on X_0.*

Let $T_{\mathrm{atm},n,\sigma}$ be the following $\mathcal{L}_\sigma$-theory.

(1) R is a von Neumann commutative regular difference ring satisfying $T_{\mathrm{vac},\sigma}$,
(2) the Boolean algebra of idempotents is included in the set of fixed points of σ^n,
(3) the Boolean algebra of idempotents satisfies the following sentence*:* $\exists e\ (\bigwedge_{i=1}^{n-1} e.e^{\sigma^i} = 0\ \&\ \sum_{i=0}^{n-1} e^{\sigma^i} = 1)$.
(4) for each idempotent e, for every absolutely irreducible variety U on e and every variety $V \subset U \times \sigma^n(U)$ projecting generically onto U and $\sigma^n(U)$ and every algebraic set W properly contained in V, there is $a \in U(R)$ such that $(a, \sigma^n(a)) \in V - W$.

Proposition 6.10. *The theory $T_{\mathrm{atm},n,\sigma}$ is model-complete in $\mathcal{L}_\sigma$ and decidable. It is the model-companion of the theory of von Neumann commutative regular difference rings satisfying axiom* (2) *above.*

Proof. For the first part, apply Proposition 4.3 and Theorems 9.13, 4.5 in [5]. For the second part, note that in any existentially closed von Neumann commutative regular difference ring R where $\sigma^n = 1$, all the orbits of σ in $X(R)$ are of cardinality n and so axiom (3) holds (see the discussion at the beginning of Section 6.2). Then, apply Proposition 4.5 and Lemma 6.9. □

7. Amalgamation

Let $\mathcal{C}$ be the class of von Neumann regular difference commutative rings. We work here in the language $\mathcal{L}_{\mathrm{rings}} \cup \{p(.,.)\}$ of rings with the binary function symbol $p(.,.)$ defined in the previous section or in the language $\mathcal{L}_* := \mathcal{L}_{\mathrm{rings},*}$ with the unary function symbol (pseudo-inverse) *, expanded with extra symbols for the automorphism and its inverse, denote this last language by $\mathcal{L}_{*,\sigma}$. Recall that in these languages, $\mathcal{C}$ has a universal axiomatization T_σ (see Section 6, above Lemma 6.2).

Let $\mathcal{C}_0$ be the subclass of $\mathcal{C}$ consisting of the rings of characteristic 0 and $\mathcal{C}_p$ of the perfect rings of characteristic p, namely those satisfying $\forall r\ \exists s\ r = s^p$. Note that $\mathcal{C}_0$ (respectively $\mathcal{C}_p$) have a $\forall\exists$-axiomatization and so any element of $\mathcal{C}_0$ (respectively $\mathcal{C}_p$) embeds in an existentially closed element. We will denote by $\mathcal{C}_0^{\mathrm{ec}}$ (respectively $\mathcal{C}_p^{\mathrm{ec}}$) the class of the existentially closed elements of $\mathcal{C}_0$ (respectively $\mathcal{C}_p$). We will show in both cases that $\mathcal{C}_0$ and $\mathcal{C}_p$ have the amalgamation property (in the characteristic p case, we will need this hypothesis of being perfect). Let T_0 be a universal axiomatization of $\mathcal{C}_0$ in $\mathcal{L}_{*,\sigma}$. Then this will entail that T_0 is a Robinson theory (see

Proposition 7.6); Robinson theories were introduced in [18] (see also [1]), these are universal theories whose class of models has the amalgamation property. So, the class $\mathcal{C}_0^{\mathrm{ec}}$ is well-behaved, in particular, it has a universal domain and any existential formula is equivalent to an infinitary quantifier-free formula (see [16, Theorem 8.1.3]).

Expanding $\mathcal{L}_{*,\sigma}$, we will get a universal axiomatization T_p of $\mathcal{C}_p$ and analogous results for this class (see Proposition 7.7).

We will end this section by giving a proof that the classes of existentially closed models of elementary subclasses of elements of $\mathcal{C}_0$, where σ has orbits of unbounded sizes, (respectively of $\mathcal{C}_p$) are not first-order axiomatizable (see Proposition 7.11).

In this section, we will use sheaf constructions (see [30] and the Appendix in [5]).

Let $R_0 \subseteq R_1, R_2$ be commutative von Neumann regular rings of characteristic zero or perfect of characteristic p. Let X_0, X_1, X_2 be their spectrum (or equivalently maximal spectrum). As usual with von Neumann regular rings, we will identify the spectrum of the ring and the Stone space of the corresponding Boolean algebra of idempotents. We will show in this section that we can embed them in a functorial way in a von Neumann regular ring. In particular, since these are difference rings, this embedding will commute with each automorphism.

Let $\pi_1 : X_1 \to X_0$ and $\pi_2 : X_2 \to X_0$ be the maps sending $x_1 \in X_1$ (respectively $x_2 \in X_2$) to $x_1 \cap \mathcal{B}(R_0)$ (respectively $x_2 \cap \mathcal{B}(R_0)$). These maps are surjective since given any $x \in X_0$ one can extend it to a maximal ideal of $\mathcal{B}(R_1)$ (respectively $\mathcal{B}(R_2)$). Note also that $R_0/\pi_1(x_1)$ embeds in R_1/x_1 (respectively in R_2/x_2).

Define $X := \{(x_1, x_2) \in X_1 \times X_2\colon\ \pi_1(x_1) = \pi_2(x_2)\}$. We endow the space $X_1 \times X_2$ with the product topology and so this is a Hausdorff, compact, totally disconnected topological space. On X, we define a basis $\mathcal{U}$ of open sets as the sets of the form $X \cap (U_1 \times U_2)$, where U_1 is a clopen subset of X_1 and U_2 is a clopen subset of X_2. One can show that X is a Hausdorff, compact, totally disconnected topological space.

Lemma 7.1. *Let R_0, R_1, R_2 be commutative von Neumann regular rings either of characteristic* 0 *or perfect of characteristic p, with $R_0 = R_1 \cap R_2$. Let x_1* (*respectively x_2*) *belong to Spec*(R_1) (*respectively Spec*(R_2)) *and suppose that $x_0 := x_1 \cap x_2 \in$ Spec(R_0). Then, there is a free construction, described below, of a von Neumann commutative regular ring that we will denote by R_x, $x := (x_1, x_2)$ containing both R_1/x_1 and R_2/x_2 and in which $R_1/x_1 \otimes_{R_0/x_0} R_2/x_2$ embeds. Moreover, R_x will be either of characteristic* 0 *or perfect of characteristic p.*

Proof. (See Chapter 8, Section 18 in [20].) It suffices to prove it for finitely generated rings R_1, R_2 and from now on, we will work under this hypothesis. Since R_0, R_1 and R_2 are von Neumann regular, the corresponding quotients are fields and since we are either in characteristic zero or perfect of characteristic p, the extension say R_1/x_1 of R_0/x_0 is a separable extension and so by Theorem 8.48 of [20], the tensor product has no non-zero nilpotent elements. Since we have assumed that the extension R_1/x_1 of R_0/x_0 is finitely generated, we reduce to the case where it is a separable algebraic extension of a purely transcendental extension. In the case where the extension R_1/x_1 of R_0/x_0 is purely transcendental, we get a domain (see Theorem 8.47 in [20]) and in the case where the extension R_1/x_1 of R_0/x_0 is separably algebraic, we obtain a direct product of fields (see Theorem 8.46 in [20]). Denote R_1/x_1 by F_1, R_2/x_2 by F_2 and R_0/x_0 by F_0, then write F_1 as a separable algebraic extension of $F_0(B_0)$, where B_0 is a transcendence basis of F_1 over F_0. So, we get $F_1 \otimes_{F_0} F_2 = F_1 \otimes_{F_0(B_0)} (F_0(B_0) \otimes_{F_0} F_2)$. Let Q_2 be the fraction field of $F_0(B_0) \otimes_{F_0} F_2$; so $F_1 \otimes_{F_0} F_2$ embeds in $F_1 \otimes_{F_0(B_0)} Q_2$. This last ring, that we will denote by R_x, is a direct product of fields (since F_1 is a separable algebraic extension of $F_0(B_0)$) and so is von Neumann regular.

For the last assertion, assume that R_1 and R_2 are perfect rings of characteristic p and take an element in $r \in F_1 \otimes_{F_0(B_0)} Q_2$, with $r = \sum_i f_{1i} \otimes (\sum_j f'_{1ij} \otimes f_{2ij})$, with $f_{1i} \in F_1$, $f'_{1ij} \in F_0(B_0)$ and $f_{2ij} \in F_2$. W.l.o.g., we may assume that there exist $g_{1i}, g_{1ij} \in F_1$ and $g_{2ij} \in F_2$ such that $g_{1i}^p = f_{1i}$, $g_{1ij}^p = f'_{1ij}$ and $g_{2ij}^p = f_{2ij}$. Since, $f'_{1ij} \in F_0(B_0)$ and F_1 is separable algebraic over $F_0(B_0)$, we have that $g_{1ij} \in F_0(B_0)$. Since we are in characteristic p, $\sum_j (g_{1ij} \otimes g_{2ij})^p = (\sum_j g_{1ij} \otimes g_{2ij})^p$ and $r = [\sum_i g_{1i} \otimes (\sum_j g'_{1ij} \otimes g_{2ij})]^p$. □

Remark 7.2. Suppose F_0 is not a perfect field and it is included in two perfect closures F_1, F_2. So there exist $s \in F_0$ and $r \in F_1$ such that $r^p = s$ and $r' \in F_2$ such that $r'^p = s$. But then the element $(r \otimes 1 - 1 \otimes r')$ is nilpotent (and non-zero).

Now, we are going to define a sheaf of von Neumann regular rings such that R_1 and R_2 embed in the ring of global sections of the associated sheaf space.

To each $U \in \mathcal{U}$, we associate a commutative von Neumann regular ring $F(U)$ as follows. First, we define a map ϕ from $R_1 \times R_2$ to $\prod_{x \in U} R_x$, where $x = (x_1, x_2)$, as follows: $(r_1, r_2) \to ((r_1 + x_1) \otimes_{R_0/x_0} (r_2 + x_2))_{(x_1,x_2) \in U}$. We define $F(U)$ as the subring generated by the image of ϕ in this product of von Neumann regular rings. A typical element of $F(U)$ has the form: $((\sum_{i \in I} (r_{1,i} + x_1) \otimes_{R_0/x_0} (r_{2,i} + x_2))_{(x_1,x_2) \in U})$ with $r_{1,i}, r_{2,i} \in R$ and I a finite set.

Lemma 7.3. *Using the notations above, the data*

$$\mathcal{F} := \{F(U) \colon U \in \mathcal{U}\}$$

together with the restriction maps determine a unique sheaf $\mathcal{G}$ on X of commutative von Neumann regular rings such that for any $U \in \mathcal{U}$, $F(U) = \Gamma(U, \mathcal{G})$.

Proof. First, we have to show that each $F(U)$ is a von Neumann commutative ring. Note that each of R_1, R_2 and R_x are von Neumann regular rings; recall that we denote by $*$ the pseudo-inverse. Let $x = (x_1, x_2) \in U$, and $x_0 = x_1 \cap x_2$.

So, we have

$$\begin{aligned}\phi(r_1, r_2)^2.\phi(r_1^*, r_2^*) &= \big((r_1 + x_1)^2.(r_1^* + x_1) \otimes_{R_0/x_0} (r_2 + x_2)^2.(r_2^* + x_2)\big)_{x \in U}\\ &= \big((r_1 + x_1) \otimes_{R_0/x_0} (r_2 + x_2)\big)_{x \in U} = \phi(r_1, r_2).\end{aligned}$$

Also,

$$\phi(r_1^*, r_2^*)^2.\phi(r_1, r_2) = \phi(r_1^*, r_2^*).$$

Moreover, if we consider

$$\sum_i \phi(r_{1i}, r_{2i}) = \left(\left(\sum_{i \in I} (r_{1,i} + x_1) \otimes_{R_0/x_0} (r_{2,i} + x_2)\right)_{x \in U}\right)$$

and we define

$$\Big(\sum_i \phi(r_{1i}, r_{2i})\Big)^* = \Big(\Big(\sum_{i\in I}(r_{1,i}+x_1)\otimes_{R_0/x_0}(r_{2,i}+x_2)^*\Big)_{x\in U}\Big).$$

Then, we check that

$$\begin{aligned}
&\Big(\sum_i \phi(r_{1i}, r_{2i})\Big)^2 . \Big(\sum_i \phi(r_{1i}, r_{2i})\Big)^* \\
&\quad = \Big(\Big(\Big(\sum_{i\in I}(r_{1,i}+x_1)\otimes_{R_0/x_0}(r_{2,i}+x_2)\Big)^2 . \Big(\sum_{i\in I}(r_{1,i}+x_1)\otimes_{R_0/x_0}(r_{2,i}+x_2)\Big)^*\Big)_{x\in U}\Big) \\
&\quad = \Big(\Big(\sum_{i\in I}(r_{1,i}+x_1)\otimes_{R_0/x_0}(r_{2,i}+x_2)\Big)_{x\in U}\Big) = \Big(\sum_i \phi(r_{1i}, r_{2i})\Big).
\end{aligned}$$

Let $V \subseteq U$. Define

$$\pi_V^U : F(U) \to F(V):$$
$$\Big(\Big(\sum_i (r_{1,i}+x_1)\otimes_{R_0/x_0}(r_{2,i}+x_2)\Big)_{x\in U}\Big) \to \Big(\Big(\sum_i (r_{1,i}+x_1)\otimes_{R_0/x_0}(r_{2,i}+x_2)\Big)_{x\in V}\Big).$$

It is clear that:

(1) $\pi_U^U = 1_U$,
(2) whenever $W \subseteq V \subseteq U \in \mathcal{U}$ $\pi_W^U = \pi_W^V \circ \pi_U^V$.

So, $\mathcal{F}$ is a presheaf.

To show that this data determines an unique sheaf, we have to check an equalizer condition for two coverings by basic open subsets (see [30, Lemma 2.6, p. 83, Chapter 4]).

So, consider a covering of a basic open set U by a family of basic open subsets U_j.

To check that the map from $F(U)$ to $\prod_{U_j} F(U_j)$ sending r_U to $(\pi_{U_j}^U(r_U))$ is injective, is easy. If $r_U \neq r'_U$, then there exists $x \in U$ such that $r(x) \neq r'(x)$; so there exists j such that $x \in U_j$. Therefore, $\pi_{U_j}^U(r_U) \neq \pi_{U_j}^U(r'_U)$.

Let $\{r_{U_j}\}_j$ be a family of elements of $F(U_j)$ such that for every pair $\{i, j\}$ we have $\pi_{U_j\cap U_i}^{U_i}(r_{U_i}) = \pi_{U_j\cap U_i}^{U_j}(r_{U_j})$. We have to find an element r_U of $F(U)$ such that $\pi_{U_j}^U(r_U) = r_{U_j}$, for each U_j. Let $U = (U_1, U_2)$ where U_1 (respectively U_2) is a clopen subset of X_1 (respectively X_2) and similarly let $U_j = (U_{j1}, U_{j2})$ where U_{j1} (respectively U_{j2}) are clopen subsets of X_1 (respectively X_2). Note that we get a covering of U_1 (respectively U_2) by the U_{1j} (respectively U_{2j}). By compactness of the spaces X_1, X_2, we can extract a finite subcovering from which we construct a finite disjoint covering, say $V_{1,\ell}$ (respectively $V_{2,k}$). Let V_n, $n < N$, be a corresponding open finite disjoint covering of X; each V_n is of the form $(V_{1,\ell}, V_{2,k})$ for some tuple of indices (ℓ, k). Now for each n, we associate an index $j(n)$ such that V_n is contained in $U_{j(n)}$. Set $r_U := (\pi^{U_{j(n)}}_{V_n}(r_{U_j}))_{x\in\bigcup V_n}$. The compatibility condition implies that this is well defined. It remains to check that $\pi^U_{U_j}((\pi^{U_{j(n)}}_{V_n}(r_{U_j}))_{x\in\bigcup V_n}) = r_{U_j}$. □

Lemma 7.4. *Let $x \in X$, let $\mathcal{U}$ be the set of clopen subsets U of X containing x. Then $R_x = \varinjlim_{U\in\mathcal{U}} F(U)$.*

Proof. By definition, $\varinjlim_{U\in\mathcal{U}} F(U) = \coprod_{U\in\mathcal{U}} F(U)/\sim$; where $\sim$ is the equivalence relation defined as follows: $r \sim s$ with $r \in F(V_1)$ and $s \in F(V_2)$ if there exists $W \subset V_1 \cap V_2$, $W \in \mathcal{U}$ such that $\pi^{V_1}_W(r) = \pi^{V_2}_W(s)$.

Let $r_x \in R_x$. Then $r_x = \sum_i (r_{1,i} + x_1) \otimes_{R_0/x_0} (r_{2,i} + x_2)$ with $r_{1,i} \in R_1$ and $r_{2,i} \in R_2$. Let U_{1i} (respectively U_{2i}) be the truth values $[r_{1,i} \neq 0] := \{y_1 \in X_1\colon r_{1,i} \notin y_1\}$ (respectively $[r_{2,i} \neq 0] := \{y_2 \in X_2\colon r_{2,i} \notin y_2\}$), it is a clopen subset of X_1 (respectively in X_2) containing x_1 (respectively x_2). Let $U_1 := \bigcap_{i\in I} U_{1i}$ (respectively $U_2 := \bigcap_{i\in I} U_{2i}$) and let $U = U_1 \times U_2$. Then, we send r_x to the equivalence class of the following element:

$$r_U := \sum_i \left(r_{1,i} + x'_1\right) \otimes_{R_0/x'_1\cap x'_2} \left(r_{2,i} + x'_2\right)_{x'=(x'_1,x'_2)\in U}.$$

Let us show this is well defined. Namely, assume that $s_{1i} + x_1 = r_{1i} + x_1$ for some $s_{1i} \in R_1$ (respectively $s_{2i} + x_2 = r_{2i} + x_2$ for some $s_{2i} \in R_2$), with $i \in I$. Then, these equalities remain true on the truth values of $[s_{1i} - r_{1i}]$ (respectively $[s_{2i} - r_{2i}]$), $i \in I$, in X_1 (respectively in X_2). Let U'_1 (respectively U'_2) be the intersection of these truth values over $i \in I$ in X_1 (respectively in X_2). So, U'_1 (respectively U'_2) is a clopen subset of X_1 (respectively X_2) containing x_1 (respectively x_2). Set $U' := (U'_1, U'_2)$. So the element $s_{U'} := \sum_{i\in I}(s_{1i} + x'_1) \otimes_{R_0/x'_1\cap x'_2} (s_{2i} + x'_2)_{x'=(x'_1,x'_2)\in U'}$ is equivalent for the relation $\sim$ to r_U.

Conversely, suppose that $r \in F(V_1)$ and $s \in F(V_2)$ with $V_1, V_2 \in \mathcal{U}$ and $r \sim s$. So there exists $W \in \mathcal{U}$ with $W \subset V_1 \cap V_2$ such that for any $(x'_1, x'_2) \in W$, $\sum_{i\in I}(r_{1,i} + x'_1) \otimes_{R_0/x_0} (r_{2,i} + x'_2) = \sum_{j\in J}(s_{1,j} + x'_1) \otimes_{R_0/x'_1\cap x'_2} (s_{2,j} + x'_2)$. Therefore the map sending the equivalence class of r to the element $\sum_{i\in I}(r_{1,i} + x_1) \otimes_{R_0/x_0} (r_{2,i} + x_2)$ is well defined. □

Let $\Gamma L\mathcal{F}$ be the sheafification of $\mathcal{F}$, where $L\mathcal{F}$ is the sheaf space associated to $\mathcal{F}$. Recall that $L\mathcal{F} := \coprod_{x\in X} R_x$, and we take for a basis of the topology, the sets:

$$\{r_x \in L\mathcal{F};\ r_x \in R_x\ \&\ x \in U\}.$$

$\Gamma(U, L\mathcal{F}) := \{$continuous maps $f: U \to L\mathcal{F}\colon p \circ f = 1_U\}$, where $p: L\mathcal{F} \to X$. We have that $\mathcal{F}$ is isomorphic to $\Gamma L(\mathcal{F})$ (see Lemma 4.3, p. 23 in [30]).

Lemma 7.5. *The rings R_1, R_2 embed over R_0 in the ring $\Gamma L(\mathcal{F})$ of global sections over X defined above.*

Proof. The rings R_1 and R_2 embed in $\Gamma L(\mathcal{F})$ and this embedding commutes on R_0. Let 1_{x_1} (respectively 1_{x_2}) be the identity elements of the rings R_1/x_1 (respectively R_2/x_2), where $x = (x_1, x_2) \in X$. Send $r \in R_1$ to $((r + x_1) \otimes_{R_0/x_0} 1_{x_2})_{x\in X}$ (respectively $r' \in R_2$ to $(1_{x_1} \otimes_{R_0/x_0} (r' + x_2))_{x\in X}$.) □

Let T_0 be the theory of von Neumann commutative regular difference rings of characteristic zero (i.e. $\forall r\ (n.r = 0 \to r = 0)$ where $n \in \mathbb{N} - \{0\}$). Let $\mathcal{C}_0$ be the class of its models. Note that in the language $\mathcal{L}_0 := \mathcal{L}_{*,\sigma}$, the theory T_0 is universal.

Proposition 7.6. *T_0 is a Robinson $\mathcal{L}_0$-theory.*

Proof. The proof consists in showing that $\mathcal{C}_0$ has the amalgamation property, which follows from the preceding lemma. □

Now we will describe the characteristic p case, where p is a prime number.

Let T_p be the theory of perfect von Neumann commutative regular difference rings of characteristic p (i.e. $\forall r\ p.r = 0$ and $\forall r\ \exists s\ r = s^p$), expressed in the language $\mathcal{L}_p := \mathcal{L}_{*,\sigma} \cup \{(.)^{1/p};\ p \in \mathcal{P}\}$, where the new unary symbols are defined by $(x)^{1/p} = y$ iff $x = y^p$. In this language $\mathcal{L}_p$, the theory T_p is universal.

Proposition 7.7. *T_p is a Robinson $\mathcal{L}_p$-theory.*

Now, we want to add constraints on the automorphism σ, namely that every orbit of σ is infinite, which can be expressed by the following scheme: for each $n \in \omega$, there is an idempotent e_n such that $\{\sigma(e_n), \ldots, \sigma^n(e_n) = e_n\}$ is a partition of 1.

In the following, we will make the convention that p is either a prime number, or that it is equal to 0.

In order to have a universal theory, we add to the language $\mathcal{L}_p$ a countable set of constants c_n, $n \in \omega$, to obtain a new language $\mathcal{L}_{\infty,p}$.

Let $T_{\infty,p}$ be the following $\mathcal{L}_{\infty,p}$-theory consisting of:

(1) for each n, the axiom:

$$c_n^2 = c_n \quad \& \quad \sum_{i=0}^{n-1} \sigma^i(c_n) = 1 \quad \& \quad \bigwedge_{i \neq j} \sigma^i(c_n).\sigma^j(c_n) = 0 \quad \& \quad \sigma^n(c_n) = c_n,$$

(2) the $\mathcal{L}_p$-theory T_p.

Note that for $p = 2$, the Boolean algebra $(2^{\omega}_{\mathcal{F}}, \sigma_t)$ is a model of $T_{\infty,2}$.

Proposition 7.8. *$T_{\infty,p}$ is a Robinson $\mathcal{L}_{\infty,p}$-theory.*

Proof. Here we have to check if R_0, R_1 and R_2 satisfy axiom scheme (1), then the embedding we described above in the von Neumann regular ring $\Gamma L(\mathcal{F})$ also satisfies this scheme (Lemma 7.5). Since this scheme consists in existential sentences, this is straightforward. □

We will end this section by proving that the class of existentially closed models of $T_{\infty,p}$ (respectively T_p) (with p a prime number or 0) cannot be elementary.

Let $T_{nn,\sigma}$ be the theory of commutative difference rings without nilpotent elements, namely the $\mathcal{L}_\sigma$-theory described by the first two axioms in Definition 6.7. Let $T_{0,nn,\sigma}$ be the theory $T_{nn,\sigma}$ plus the axiom stating that the characteristic is equal to 0 (namely its prime ring is $\mathbb{Z}$ [19, p. 106]).

Lemma 7.9. *The theory $T_{0,nn,\sigma}$ has no model-companion.*

Proof. Let R be a model of $T_{nn,\sigma}$, in particular it is a model of T_{nn} and so it embeds in a von Neumann commutative regular ring [24], say $\tilde{R}$ that we may consider as an $\mathcal{L}_*$-structure. Let R_* be the $\mathcal{L}_*$-substructure generated by the image of R in $\tilde{R}$. We extend σ on R_* in $\tilde{R}$ as follows: $\sigma_*(a^*) = \sigma(a)^*$. Now (R_*, σ_*) is a von Neumann regular difference ring.

Let (A, σ) be any existentially closed, $\aleph_1$-saturated von Neumann commutative regular difference ring. Note that in such a model, the automorphism σ always has orbits of unbounded sizes.

Now, let us assume that the characteristic of A is 0.

The ring A is isomorphic to a Boolean product of fields: $\Gamma_a(X, \bigcup_{x\in X} A_x)$, where X is the Stone space of the Boolean algebra $\mathcal{B}$ of idempotents of A and $A_x := A/x$, (equivalently to the ring of global sections of the sheaf space $L := \coprod_{x\in X} A_x$). We will identify the elements of A with their images in that representation; moreover we identify the idempotents of A with the clopen subsets of X. Note that for every $x \in X$, A_x is isomorphic to A_{x^σ}, sending $a + x$ to $a^\sigma + x^\sigma$; this is well-defined by Lemma 6.2(b).

Note that in the Boolean representation of A, the truth value (see Definition 6.1) $[f = g]$ of the atomic formula $(f = g)$ is equal to the support of the idempotent $1 - (f - g)^*$.

Denote by B the domain of $\mathcal{B}$, by $B' = B \setminus (0)$; let $Fix(\sigma) := \{a \in A\colon \sigma(a) = a\}$.

Define

$$P := \bigl\{(f, e_0, e) \in A \times B \times B\colon e_0 \leqslant e \in B,\ [f = 1] \geqslant e_0,\ \bigl[f = \sigma(f) + 1\bigr] \geqslant e\bigr\},$$
$$P' := \bigl\{(f, e_0, e) \in P\colon (\forall f')\ \bigl((f', e_0, e) \in P \to [f = f'] \geqslant e\bigr)\bigr\}.$$

Note that if $e_0, \sigma(e_0), \ldots, \sigma^n(e_0)$ are disjoint idempotents, $e = \bigvee_{i=0}^n \sigma^i(e_0)$, and $[f = i] \geqslant \sigma^i(e_0)$, then $(f, e_0, e) \in P'$.

Let

$$Q_1 = \bigl\{(e_1, \alpha) \in B \times Fix(\sigma)\colon \exists (f, e_0, e) \in P'\ \bigl(e_1 \leqslant e\ \&\ [f = \alpha] \geqslant e_1\bigr)\bigr\}.$$

It follows that for $n \in \mathbb{N}$, $(e_1, n) \in Q_1$ for any sufficiently small idempotent e_1.

Let

$$Q = \bigl\{\alpha \in Fix(\sigma)\colon \forall e \in B'; \exists e_1 \in B'\ \bigl((e_1 \leqslant e)\ \&\ (e_1, \alpha) \in Q_1\bigr)\bigr\}.$$

So for any $n \in \mathbb{N}$ we have $n \in Q$.

Now let us use that A is an existentially closed model of T_0.

Claim. *If $(f, e_0, e) \in P'$ then for some $n \in \mathbb{N}$, $e \leqslant \bigvee_{i=0}^n \sigma^i(e_0)$.*

Proof. Suppose otherwise. Then, $e \nsubseteq U$, where $U := \bigcup_{i=0}^\infty \sigma^i(e_0)$. We embed A in a von Neumann commutative regular difference ring A', containing an element f' such that $(f', e_0, e) \in P$ but with e not included in $[f = f']$. Since $A \subseteq_{\mathrm{ec}} A'$, we can find such element in A, which contradicts the fact that $(f, e_0, e) \in P'$.

We construct A' as follows. Let $\bar{U}$ be the closure of U in X. Note that U and $\bar{U}$ are invariant under σ. We partition $\bar{U} - U$ into disjoint orbits and we choose a representative x_i in each orbit. Let $\{x_i\colon\ i \in I\}$ be the set of these representatives. We will denote by $Orb(x)$ the orbit of x under σ. Set $A|_U := \pi^X_U(A)$ (respectively $A|_{X-\bar{U}} := \pi^X_{X-\bar{U}}(A)$). We define σ on $A|_U$ by $\sigma(\pi^X_U(r)) := \pi^X_U(\sigma(r))$ and similarly for $A|_{X-\bar{U}}$, it is still an isomorphism since U and $X - \bar{U}$ are invariant under σ. Then we define σ on the direct product $A_{Orb(x)} := \prod_{z\in\mathbb{Z}} A_{\sigma^z(x)}$ as follows: let $a_x \in A_x$, then there exists $a \in A$ such that $a + x = a_x$ and we define $\sigma(a_x) := \sigma(a) + \sigma(x)$ (this is well defined (see Lemma 6.2)). Thus, $A_{Orb(x)}$ is a difference ring.

Let $A' := A|_U \times A|_{X-\bar{U}} \times \prod_{i\in I} A_{Orb(x_i)}$. As a direct product of von Neumann commutative difference rings, A' is a von Neumann regular commutative difference ring and A embeds in A' as a difference ring.

For the claim, it remains to construct f'. Let $x \in e - U$, and let $\beta \in Fix(A)$ such that $f(x) \neq \beta$. Let $i \in I$ be such that $x \in Orb(x_i)$ and w.l.o.g. $x_i = x$. We first define the following sequences $g_i \in \prod_{z\in\mathbb{Z}} A_{\sigma^z(x)}$ by setting $g_i(x_i) = \beta$ and $g_i(\sigma^z(x_i)) = \alpha + z$. Let $g := (g_i)_{i\in I}$. Then, we define f' as follows: $f' := (\pi^X_U(f), g, \pi_{X-\bar{U}}(f))$. Then $(f', e_0, e) \in P$, but $e \nleqslant [f = f']$, completing the proof of the claim. □

Let $(e_1, \alpha) \in Q_1$. Then there exists $(f, e_0, e) \in P'$ with $e_1 \leqslant e$ and $[f = \alpha] \geqslant e_1$. Hence, by the claim, for some $n \in \mathbb{N}$, $e \leqslant \bigvee_{i=0}^n \sigma^i(e_0)$. Since $\alpha \in Fix(\sigma)$, for some $m \in \mathbb{N}$, $[\alpha = m] \geqslant e_1$. Thus if $\alpha \in Q$ then for any $e \in B'$, for some $e_1 \in B'$ with $e_1 \leqslant e$, and some $m \in \mathbb{N}$, we have $[\alpha = m] \geqslant e_1$.

Now, by $\aleph_1$-saturation of A, for some integer N, for all $\alpha \in Q$ and $e \in B'$, for some $m \leqslant N$, $([\alpha = m] \wedge e) \neq 0$. It follows that $\bigcup_{i=0}^N [\alpha = i] = X$. But this contradicts the fact that $\mathbb{Z}$ can be embedded in A and consequently that $\mathbb{N} \subseteq Q$. □

Corollary 7.10. *The theory $T_{nn,\sigma}$ has no model-companion.*

An easy adaptation of the above proof gives us the following proposition. We keep the same notations.

Proposition 7.11. *The theories T_p and $T_{\infty,p}$ have no model-companion, p a prime number or* 0.

Proof. Note that in any model of T_p, $Fix(\sigma)$ contains the closure under pth -roots of $\mathbb{F}_p$ and so is infinite. Thus, in an $\aleph_1$-saturated model A of T_p, there exists a non-algebraic element $\mu \in Fix(\sigma)$ over $\mathbb{F}_p$.

In a similar way as before, we will show that if A is in addition existentially closed, we reach a contradiction since this implies that then this element μ is algebraic over $\mathbb{F}_p$. Let

$$P_\mu = \bigl\{(f, e_0, e)\colon\ f \in A,\ e_0 \leqslant e \in B,\ [f = 1] \geqslant e_0,\ \bigl[f = \mu.\sigma(f)\bigr] \geqslant e\bigr\},$$
$$P'_\mu = \bigl\{(f, e_0, e) \in P_\mu\colon\ (\forall f')\ \bigl((f', e_0, e) \in P_\mu \Rightarrow [f = f'] \geqslant e\bigr)\bigr\}.$$

Note that if $e_0, \sigma(e_0), \ldots, \sigma^n(e_0)$ are disjoint idempotents, and $e = \bigcup_{i=0}^n \sigma^i(e_0)$, and $[f - \mu^i] \geqslant \sigma^i(e_0)$, then $(f, e_0, e) \in P'_\mu$.

Let

$$Q_{1,\mu} = \bigl\{(e_1, \alpha)\colon\ \bigl(\exists (f, e_0, e) \in P'_\mu\bigr)\ (e_1 \leqslant e)\ \&\ [f = \alpha] \geqslant e_1\bigr\}.$$

It follows that for $n \in \mathbb{N}$, $(e_1, \mu^n) \in Q_{1,\mu}$ for any sufficiently small idempotent e_1.

Let

$$Q_\mu = \bigl\{\alpha \in Fix(\sigma)\colon (\forall e \in B')\,(\exists e_1 \in B')\,(e_1 \leqslant e)\ \&\ (e_1, \alpha) \in Q_{1,\mu}\bigr\}.$$

So for any $n \in \mathbb{N}$ we have $\mu^n \in Q_\mu$.

The following claim is proven as before.

Claim. *If $(f, e_0, e) \in P'_\mu$ then for some $n \in \mathbb{N}$, $e \subseteq \bigcup_{i=0}^{n} \sigma^i(e_0)$.*

Hence if $(e_1, \alpha) \in Q_{1,\mu}$ then for some $n \in \mathbb{N}$, $[\alpha = \mu^n] \geqslant e_1$. Thus if $\alpha \in Q_\mu$ then for any $e \in B'$, for some $e_1 \in B'$ with $e_1 \leqslant e$, and some $n \in \mathbb{N}$, we have $[\alpha = \mu^n] \geqslant e_1$. By $\aleph_1$-saturation, for some integer N, for all $\alpha \in Q_\mu$ and $e \in B'$, for some $n \leqslant N$, $([\alpha = \mu^n] \wedge e) \neq 0$. It follows that $\bigcup_{i=0}^{N}[\alpha = \mu^i] = X$. But this contradicts the fact that $\{\mu^n\colon n \in \omega\} \subseteq Q_\mu$ and the assumption that μ is algebraic. □

So, the only case where σ has orbits of unbounded sizes and where we could have a model-companion is when $Fix(\sigma)$ is finite. In Section 3, we examined a special case: we showed that the ring of sequences over a finite field F, indexed by the positive integers and quotiented out by the Frechet filter, with the shift automorphism, belongs to a first-order axiomatizable, model-complete class of difference rings (see Proposition 3.4).

8. Sequences with coefficients in $\mathbb{R}$

In this section, we will consider the class of lattice-ordered commutative rings, in short ℓ-rings, endowed with an automorphism.

First, we will recall a few facts on ℓ-rings [2]. An ℓ-ring R is a commutative ring with two additional operations: $\{\wedge, \vee\}$ such that

(1) $(R, \wedge, \vee)$ is a lattice and
(2) $\forall a\, \forall b\, \forall c\ (a \leqslant b \rightarrow (a + c \leqslant b + c))$,
(3) $\forall a\, \forall b\, \forall c\ ((a \leqslant b\ \&\ c \geqslant 0) \rightarrow (a.c \leqslant b.c))$,

where $\leqslant$ is the lattice order, namely $a \leqslant b$ iff $a \wedge b = a$. In this section, R will always denote such a ring.

Let $\mathcal{L} := \mathcal{L}_{\text{rings}}$, $\mathcal{L}_{\leqslant} := \mathcal{L} \cup \{\leqslant\}$ the language of ordered rings and $\mathcal{L}_\ell = \mathcal{L} \cup \{\wedge, \vee\}$ the language of ℓ-rings.

An ℓ-ideal I of R is a (ring) ideal which has the following property: $\forall a \in I\ \forall x \in R\ (|x| \leqslant |a| \rightarrow x \in I)$. In an ℓ-ring, any finitely generated ℓ-ideal is principal (see Corollary 8.2.9 in [2]).

First let us state a corollary of the undecidability result of Proposition 5.8.

Corollary 8.1. *Let R be an ℓ-ring with an automorphism σ which has an infinite orbit on the set of its maximal ℓ-ideals. Assume that $Fix(\sigma)$ is an infinite field. Then, the theory of $(R, +, ., \wedge, \vee, \sigma)$ is undecidable.*

Now, we will consider the subclass of ℓ-rings which can be represented as a subdirect product of totally-ordered commutative rings; it is the subclass of so-called f-rings. An f-ring is an ℓ-ring where $\forall a, b, c > 0\ (a \wedge b = 0 \rightarrow (a \wedge b.c = 0 \text{ and } a \wedge c.b = 0))$.

Note that in the case where R is an f-ring, the proof of the above corollary can be simplified, since the intersection of a finite number of principal ℓ-ideals is again a principal ℓ-ideal (see Proposition 9.1.8 in [2]) .

Let R be an f-ring. We will denote by $Spec(R)$ the set of irreducible ℓ-ideals of R with the spectral topology; namely an open set is the set of ideals which do not contain a given element (Chapter 10 in [2]).

Recall that an ℓ-ideal I of R is irreducible if whenever $a, b \in R$ are such that $\langle a\rangle \cap \langle b\rangle \subset I$, then $a \in I$ or $b \in I$.

An f-ring without nilpotent elements can be represented as a subdirect product of totally-ordered integral domains (see Corollary 9.2.5 in [2]) and in von Neumann regular f-ring, any irreducible ideal contains no non-trivial idempotents and so the quotient of such a ring by an irreducible ℓ-ideal is a field.

Recall that the theory of $\mathbb{R}$ is the theory of real-closed fields, it is model-complete in $\mathcal{L}$ and admits quantifier elimination in $\mathcal{L}_{\leqslant}$.

A *real-closed* von Neumann regular f-ring is a von Neumann regular f-ring where every monic polynomial of odd order has a root and every positive element is a square.

A. Macintyre proved that the theory T_f of commutative f-rings with no non-zero nilpotent elements has a model-companion T_{vrc}, namely the theory of commutative real-closed von Neumann regular f-rings with no minimal idempotents (see [25]). This latter theory admits quantifier elimination in the language of lattice-ordered rings augmented with the projector $p(.,.)$ (or with the pseudo-inverse *).

Here, we consider the subclass of existentially closed von Neumann commutative regular f-rings endowed with an automorphism σ. As in Lemma 7.9, in the case where the automorphism σ has an infinite orbit on the set of maximal ℓ-ideals, such a class cannot be elementary, so in a similar way as in Section 7, we want to describe the associated Robinson theory.

First, we show that the class of von Neumann regular difference f-rings has the amalgamation property. The main lemma is as follows.

Lemma 8.2. *Let R_0, R_1, R_2 be commutative von Neumann regular f-rings, with $R_0 = R_1 \cap R_2$. Let x_1 (respectively x_2) belong to $Spec(R_1)$ (respectively $Spec(R_2)$) be such that $x := x_1 \cap x_2 \in Spec(R_0)$. Then, $R_1/x_1 \otimes_{R_0/x_0} R_2/x_2$ embeds in a canonical way in a von Neumann regular f-ring that we will denote by R_x, $x := (x_1, x_2)$ containing both R_1/x_1 and R_2/x_2.*

Proof. (See Chapter 8, Section 18 in [20].) It suffices to prove it for finitely generated rings R_1, R_2. From now on let us work under this hypothesis. Since R_0, R_1 and R_2 are von Neumann regular f-rings the corresponding quotients are totally-ordered fields. Set $F_0 := R_0/x_0$, $F_1 := R_1/x_1$, $F_2 := R_2/x_2$ and F_0^r, F_1^r and F_2^r their respective real-closures. Since we are in characteristic zero, the extension say F_1 of F_0 is a separable extension and so by Theorem 8.48 of [20], the tensor product has no non-zero nilpotent elements. Since we have assumed that the extension F_1 of F_0 is finitely generated, we reduce to the case where it is a separable algebraic extension of a purely transcendental extension. If F_1 is a purely transcendental extension of F_0, we get a domain (see Theorem 8.47 in [20]) and if F_1 is a separable algebraic extension of F_0, we get a direct product of orderable fields (see Theorem 8.46 in [20]).

So, first assume that F_1 is a finite algebraic separable extension of F_0; it is generated by an element a, namely F_1 is of the form $F_0[a]$. Let $p(x)$ the minimal polynomial of a over F_0. Let $f : F_0^r \to F_2^r$ be an embedding of F_0^r into F_2^r, which is the identity on F_0. The polynomial $p(x)$ factorizes in $F_0^r[x]$ as a product of polynomials of degree 2, of the form $x^2 + c$ where c is a positive element in F_0^r, and of degree 1. Let $\tilde{a}_1, \dots, \tilde{a}_m$ be the roots in F_0^r of the polynomial $p(x)$. We consider the subring $F_2[f(\tilde{a}_i)]$ of F_2^r generated by F_2 and $f(\tilde{a}_i)$, $1 \leqslant i \leqslant m$. Note that $F_2[f(\tilde{a}_i)]$ is in fact a subfield.

Let $p_1, \dots, p_m$ be the minimal polynomials of $f(\tilde{a}_1), \dots, f(\tilde{a}_m)$ respectively, over F_2. So, for $1 \leqslant i \leqslant m$, $F_2[f(\tilde{a}_i)] \cong F_2[x]/(p_i(x))$. Since $F_2[f(\tilde{a}_i)]$ is included in a formally real field, it is formally real. Let $p_1, \dots, p_k$, $k \leqslant m$ be the distinct elements among $p_1, \dots, p_m$. Then we have that $p(x) = p_1(x). \cdots .p_k(x)$ in $F_2[x]$ (*) and $F_2[x]/(p(x)) \cong \prod_{i=1}^k F_2[x]/(p_i(x))$ with each $F_2[x]/(p_i(x))$ a formally real field. So, the ring $F_1 \otimes F_2 \cong F_2[x]/(p(x))$ is a von Neumann regular commutative f-ring.

Here, to see (*), we apply the Euclidean algorithm in $F_2[x]$, namely $p(x) = p_1(x).q(x) + r(x)$ with degree of $r(x)$ strictly smaller than degree of $p_1(x)$. So, $p(f(\tilde{a}_1)) = r(f(\tilde{a}_1)) = 0$. But $p(f(\tilde{a}_1)) = f(p((\tilde{a}_1))) = 0$. So, $r(x) = 0$.

In the general case, we write F_1 as a separable algebraic extension of $F_0(B_0)$, where B_0 is a transcendence basis of F_1 over F_0. So, we get $F_1 \otimes_{F_0} F_2 = F_1 \otimes_{F_0(B_0)} (F_0(B_0) \otimes_{F_0} F_2)$. Let Q_2 be the fraction field of $F_0(B_0) \otimes_{F_0} F_2$; so $F_1 \otimes_{F_0} F_2$ embeds in $F_1 \otimes_{F_0(B_0)} Q_2$. This last ring, that we will denote by R_x, is a direct product of orderable fields and so is a von Neumann regular f-ring. □

Let T_f be the following $\mathcal{L}_\ell \cup \{*\} \cup \{\sigma, \sigma^{-1}\}$-theory consisting of:

(1) the $\mathcal{L}_\ell$-theory of von Neumann regular f-rings with a pseudo-inverse $\{*\}$,
(2) σ is an automorphism of l-rings and σ^{-1} is its inverse.

Note that T_f is a universal theory; the axiomatization that we have given, of the class of f-rings is universal and we have already seen that the other axioms were universal.

Proposition 8.3. *T_f is a Robinson theory.*

Now one can ask the following question.

Question 2. When the automorphism σ fixes pointwise the Boolean algebra of idempotents, is it possible to describe a class of Boolean products of existentially closed models of a theory of difference ordered fields?

Further, can one obtain a geometric axiomatization of this class similar to the one obtained in the case of *ACFA* (see [11])? We already know that in order to hope to answer to such question, we necessarily have to put constraints on the automorphism. Indeed, H. Kikyo and S. Shelah showed that if a model-complete theory T has a model whose theory has the strict-order property, then the theory T_σ does not have a model-companion (see [23]).

Acknowledgments

We would like to thank Zoé Chatzidakis for useful discussions. We also thank the referee for his careful reading.

References

[1] I. Ben-Yaacov, Positive model theory and compact abstract theories, J. Math. Log. 3 (1) (2003) 85–118.

[2] A. Bigard, K. Keimel, S. Wolfenstein, Groupes et Anneaux Réticulés, Lecture Notes in Math., vol. 608, Springer-Verlag, Berlin, 1977.

[3] J.R. Büchi, On a decision method in restricted second order arithmetic, in: Logic, Methodology and Philosophy of Science, Proc. 1960 Internat. Congr., Stanford University Press, Stanford, CA, 1962, pp. 1–11.

[4] S. Burris, The first-order theory of Boolean algebras with a distinguished group of automorphisms, Algebra Universalis 15 (1982) 156–161.

[5] S. Burris, H. Werner, Sheaf constructions and their elementary properties, Trans. Amer. Math. Soc. 248 (2) (1979) 269–309.

[6] S. Burris, H.P. Sankappanavar, A Course in Universal Algebra, Grad. Texts in Math., vol. 78, Springer-Verlag, 1981.

[7] P.M. Cohn, Difference Algebra, Intersci. Tracts in Pure and Appl. Math., vol. 17, Interscience Publishers, John Wiley and Sons, 1965.

[8] P.M. Cohn, Skew Fields, G.-C. Rota (Ed.), Encyclopedia Math. Appl., vol. 57, Cambridge University Press, 1995.

[9] G. Cherlin, M. Jarden, Undecidability of some elementary theories over *PAC* fields, Ann. Pure Appl. Logic 30 (1986) 137–163.

[10] Z. Chatzidakis, Model theory of difference fields, in: The Notre Dame Lectures, in: Lect. Notes Log., vol. 18, Assoc. Symbol. Logic, Urbana, IL, 2005, pp. 45–96.

[11] Z. Chatzidakis, E. Hrushovski, Model theory of difference fields, Trans. Amer. Math. Soc. 351 (1999) 2997–3071.

[12] J. Dauns, K. Hofmann, The representation of biregular rings by sheaves, Math. Z. 91 (1966) 103–122.

[13] L. van den Dries, Elimination theory for the ring of algebraic integers, J. Reine Angew. Math. 388 (1988) 189–205.

[14] L. van den Dries, K. Schmidt, Bounds in the theory of polynomial rings over fields. A non-standard approach, Invent. Math. 76 (1984) 77–91.

[15] M. Gromov, Endomorphisms of symbolic algebraic varieties, J. Eur. Math. Soc. (JEMS) 1 (2) (1999) 109–197.

[16] W. Hodges, Model Theory, Encyclopedia Math. Appl., vol. 42, Cambridge University Press, Cambridge, 1993.

[17] B. Hodgson, Décidabilité par automate fini, Ann. Sci. Math. Québec 7 (1) (1983) 39–57.

[18] E. Hrushovski, Simplicity and the Lascar group, preprint, 1997.

[19] N. Jacobson, Basic Algebra 1, W.H. Freeman and Company, San Francisco, 1974.

[20] N. Jacobson, Basic Algebra 2, W.H. Freeman and Company, San Francisco, 1974.

[21] I. Kaplansky, Commutative Rings, revised edition, University of Chicago Press, 1974.

[22] M. Kamensky, The model-completion of the theory of modules over finitely generated commutative algebras, arXiv: math/0607418v2.

[23] H. Kikyo, S. Shelah, The strict order property and generic automorphisms, J. Symbolic Logic 67 (1) (2002) 214–216.

[24] L. Lipshitz, D. Saracino, The model companion of the theory of commutative rings without nilpotent elements, Proc. Amer. Math. Soc. 38 (1973) 381–387.

[25] A.J. Macintyre, Model-completeness for sheaves of structures, Fund. Math. 81 (1) (1973/1974) 73–89.

[26] M. Prest, Model Theory and Modules, London Math. Soc. Lecture Note Ser., vol. 130, Cambridge University Press, 1988.

[27] M. Rabin, Computable algebra, general theory and theory of computable field, Trans. Amer. Math. Soc. 95 (1960) 341–360.

[28] M. Singer, M. van der Put, Galois Theory of Difference Equations, Lecture Notes in Math., vol. 1666, Springer-Verlag, 1997.

[29] A. Tarski, A. Mostowski, R. Robinson, Undecidable Theories, Stud. Logic Found. Math., North-Holland, 1953 (second printing 1968).

[30] B.R. Tennison, Sheaf Theory, London Math. Soc. Lecture Note Ser., vol. 20, Cambridge University Press, 1975.