Some model theory of Bezout difference rings- a survey

Françoise Point*

1 Introduction

This survey article is based on a joint work with Ehud Hrushovski on some Bezout difference rings ([19]). We study in a model-theoretic point of view certain classes of difference rings, namely rings with a distinguished endomorphism and more particularly rings of sequences over a field with a shift.

First we will recall some results on difference fields. A difference field is a difference ring which is a field (in this case, the endomorphism is necessarily injective); and one can show that any difference field can be embedded in an inversive difference field, namely a field with an automorphism ([5]). The model theory of difference fields started in the nineties; one motivation was to understand the model-theory of non principal ultraproducts of the algebraic closure $\mathbb{F}_p^a$ of the prime fields endowed with the Frobenius maps. The existence of a model-companion for the theory of difference fields was shown by L. van den Dries and A. Macintyre ([27]). Here, we will recall the geometric axiomatization $ACFA$ of the class of existentially closed difference fields given by Z. Chatzidakis and E. Hrushovski ([7]); they identified the different completions of $ACFA$, and deduce its decidability. The proofs that the non principal ultraproducts of the $\mathbb{F}_p^a$ endowed with the Frobenius maps, are models of $ACFA$, are much more difficult ($\star$).

An easy consequence of the decidability of $ACFA$ is the decidability of some von Neumann commutative regular difference rings. Indeed, these are Boolean products of fields and whenever the endomorphism σ fixes the prime spectrum of the ring, we may apply transfer results due to S. Burris and H. Werner in these products ([4]). More generally we will consider Bezout difference rings in the point of view

*Senior Research Associate at the "Fonds National de la Recherche Scientifique".
1991 *Mathematics Subject Classification :* 03C60, 03B25, 12H10, 13L05.
Key words and phrases : difference rings, existentially closed, (un)decidability.

of (un)decidability of their theories; this will depend on whether σ has unbounded orbits on the maximal spectrum of the ring. In the case we obtain undecidable theories, we will still describe some existentially closed (non elementary) classes of such difference rings.

Finally, we will recall some results on inversive difference valued fields. One reason being that they do occur in a proof of $(\star)$ ([18]). In this case, one knows by previous negative results of S. Shelah and H. Kikyo ([26]) that in order to get first-order axiomatizable classes of existentially closed models, one has put some constraints on the automorphism. In the case of valued difference fields, there are basically two classes of such existentially closed fields, those where the automorphism induces a rapidly increasing automorphism on the value group ([8], [18]) and those where the automorphism leaves this group fixed and acts non-trivially on the residue field ([36], [1]). A model of this last theory is, for instance, the field of Witt vectors over $\mathbb{F}_p^a$ with the Frobenius map.

In the following section, besides recalling the above results on $ACFA$, in order to make this paper accessible to a non-model-theorist, we give some basic definitions and references.

2 Difference fields

Let (K, σ) be a field with a distinguished endomorphism (respectively automorphism) σ; we will call such a field a *difference* (respectively *inversive* difference) field. We will denote by $Fix(\sigma) := \{x \in K : \sigma(x) = x\}$ the subfield of K consisting of the elements fixed by σ.

Notation 2.1. Let $K[X]_\sigma$ be the σ-polynomial ring, namely the polynomial ring in infinitely many indeterminates: $X, X^\sigma, \cdots, X^{\sigma^n}, \cdots$, $n \in \omega$, where X is a finite tuple of indeterminates: $X = (X_1, \cdots, X_m)$. We denote by X^σ the tuple $(X_1^\sigma, \cdots, X_m^\sigma)$. If for some $1 \leq j \leq m$, $X_j^{\sigma^n}$ occurs non trivially, we will say that P is of order greater than or equal to n. As usual we can write $P(X) \in K[X]_\sigma$ of order n, as $P^*(X_1, \cdots, X_m, X_1^\sigma, \cdots, X_m^{\sigma^n})$ for some element $P^*(Y_1, \cdots, Y_{m.(n+1)}) \in K[Y_1, \cdots, Y_{m.(n+1)}]$ and we define $\frac{\partial}{\partial X_i^{\sigma^j}} P := (\frac{\partial}{\partial Y_{i.(j+1)}} P^*)(X_1, \cdots, X_m^{\sigma^n})$.

Let $\mathcal{L}_{rings} := \{+, -, ., 0, 1\}$, one can express by a set of universal-existential sentences in the language $\mathcal{L}_{rings_\sigma} := \mathcal{L}_{rings} \cup \{\sigma\}$ that a field is an inversive difference field. (By sentence, we mean formula without free variables).

Therefore, any difference field K embeds into an *existentially closed* (e.c.) inversive difference field $\tilde{K}$ ([16] Theorem 8.2.1), namely one endowed with an automorphism and where any *existential* formula with parameters in $\tilde{K}$ which has a solution in some extension of $\tilde{K}$ has already a solution in $\tilde{K}$.

Let $f_1(X, Y), \cdots, f_n(X, Y), g(X, Y)$ belonging to $\mathbb{Z}[X, Y]_\sigma$ and of order $\leq k$, for some $k \in \omega$.

An existential $\mathcal{L}_{rings_\sigma}$-formula $\phi(\bar{y})$ is a formula of the form:

$$\begin{aligned} \exists x_1 \cdots \exists x_m \quad & f_1^*(x_1, \cdots, x_m, \sigma(x_1), \cdots, \sigma^k(x_m), \bar{y}) = 0 \ \& \\ & \cdots \ \& \\ & f_n^*(x_1 \cdots, x_m, \sigma(x_1), \cdots, \sigma^k(x_m), \bar{y}) = 0 \ \& \\ & g^*(x_1 \cdots, x_m, \sigma(x_1), \cdots, \sigma^k(x_m), \bar{y}) \neq 0. \end{aligned}$$

Theorem 2.1. (1.1 in [7]). The class of existentially closed models of the theory of difference fields is axiomatizable, by the following set of axioms called $ACFA$, that express the following properties of a field K.

1. (K, σ) is an inversive difference field,
2. K is an algebraically closed field,
3. For every absolutely irreducible variety U and every absolutely irreducible 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 first-order (namely can be expressed by formulas with quantifiers varying over elements of K); L. van den Dries and K. Schmidt showed how to express *in a first-order way* that a variety is irreducible ([15]).

Rephrasing the above theorem: the theory $ACFA$ is the *model companion* of the theory of difference fields.

Namely that any difference field embeds in a model of $ACFA$ and $ACFA$ is *model-complete* i.e. for any two models $\mathcal{A}$, $\mathcal{B}$ of $ACFA$: $\mathcal{A} \subseteq \mathcal{B}$ implies that $\mathcal{A} \subseteq_{ec} \mathcal{B}$, namely any existential formula in parameters in A and true in B, is also true in A.

In a model-complete theory, every formula is equivalent to an existential formula ([16] Theorem 8.3.1). A theory admits *quantifier-elimination* (q.e.) iff every formula is equivalent to a quantifier-free formula.

A theory is *complete* if all its models satisfy the same set of sentences. In the case of $ACFA$, its completions are obtained by specifying the characteristic of the field K and the action of the automorphism on the algebraic closure of the prime field $\mathbb{F}_p$ or $\mathbb{Q}$ (see 1.4 in [7]).

Finally, let us say some rather informal words on decidability. A useful reference is the article of Michael O. Rabin on "Decidable theories" in "Handbook of Mathematical logic", edited by J. Barwise ([32]).

A theory T is *decidable* if there is a fixed *algorithm* which, given a property P expressed in the language of T, determines whether P is a theorem of T.

- To show *decidability* of a theory T, one can determine a set of recursively enumerable axioms for it and show it is complete (or determine in an "effective" way its completions) (see [32], Theorems 1 and 2) or one may interpret T in a (known) decidable theory. In order to identify the completions of a theory, one strategy is to show that the definable subsets D in A^n, $n \in \omega$, where $\mathcal{A}$ is any model of T, have a manageable description.

- Often, to show that a theory is *undecidable*, one interprets in it well-known undecidable theories, like *Peano arithmetic* PA, or the theory of a finitely presented group with undecidable word problem.

  Recall PA describes addition, multiplication and the induction scheme in the natural numbers. Note that a theory that interprets PA is necessarily unstable.

Corollary 2.2. (1.4, 1.6 in [7]) The theory $ACFA$ is decidable.

Let p be a prime number, let q be a power of p and let $\Phi_q(x) := x^q$ be the q-Frobenius automorphism. Let (F_q, Φ_q) be an algebraically closed field of characteristic p endowed with Φ_q.

Let T_∞ be the set of sentences θ such that for all sufficiently large q, θ is true in (F_q, Φ_q).

Theorem 2.3. ([18]) T_∞ is decidable; it coincides with $ACFA$.

In particular, denotting by $\mathbb{F}_p^a$ the algebraic closure of $\mathbb{F}_p$, a sentence holds in $(\mathbb{F}_p^a, \Phi_p)$ for almost all prime p, iff it is true in a model of $ACFA$ of characteristic 0.

3 Difference rings

A difference ring is a commutative ring R with 1 and a distinguished ring endomorphism σ. Let $Fix(\sigma)$ be the subring of R consisting of the elements fixed by σ.

1. Let R_0 be any commutative ring; then we form the difference ring of infinite two-sided sequences: $R{=}(R_0^{\mathbb{Z}}, +, ., \sigma_t)$, where $\sigma_t(a_i)_{i\in\mathbb{Z}} = (a_{i+1})$; and $Fix(\sigma) \cong R_0$.

2. Consider the ring of sequences over $\mathbb{Z}$ with the left shift sending $(z_n)_{n\in\omega}$ to $(z_{n+1})_{n\in\omega}$ or with the right shift sending $(z_0, z_1, z_2, \cdots)$ to $(0, z_0, z_1, z_2, \cdots)$. Denote the first difference ring by $(\mathbb{Z}^\omega, \sigma_\ell)$ and the second one by $(\mathbb{Z}^\omega, \sigma_r)$.

3. Let K be a perfect field of characteristic p, p a prime number.
Then, set $R{=}(K^{\mathbb{Z}}, +, ., \sigma)$, where $\sigma((a_i)_{i\in\mathbb{Z}}) := (\Phi_p(a_i))_{i\in\mathbb{Z}}$.

An *inversive* difference ring is a difference ring where $\sigma \in Aut(R)$; for instance $(\mathbb{Z}^\omega_{\mathcal{F}}, \sigma_\ell)$, where $\mathcal{F}$ is the Frechet filter on ω.

A difference ring (R, σ) is *well-mixed* if $\forall a \forall b\ (a.b = 0 \implies a.b^\sigma = 0)$. For instance, the third example is well-mixed, whereas the first two are not well-mixed. Note that any subdirect product of difference fields is well-mixed and any difference ring which is a domain is well-mixed.

The examples above are instances of commutative difference *von Neumann regular* rings, namely commutative rings satisfying in addition:

$$\forall a \exists b\ \ (a^2.b = a\ \&\ \ b^2.a = b).$$

In a *well-mixed* commutative von Neumann regular difference ring, the Boolean algebra of idempotents $\mathcal{B}(R)$ is fixed by σ (namely, if $e^2 = e$, then $e^\sigma = e$) and so the maximal (or prime) spectrum $MSpec(R)$ of such ring R is fixed by σ.

Let R be a difference ring, let $Spec(R)$ be the set of prime ideals of R. An ideal I is *transformally prime* (or σ-prime) if it is a prime ideal with the additional property that $(x \in I \leftrightarrow x^\sigma \in I)$. (Note that if I is σ-prime, then σ induces an injective endomorphism on R/I and it can be extended on the field of fractions of R/I which can be then viewed as a difference field.)

Summary of our main results on difference rings $(R, +, ., \sigma)$

- First, assuming that R is a K-algebra, where K is a difference field containing the subfield $Fix(\sigma)$, we will view R as a module over a skew polynomial ring of the form $K[t; \sigma]$. Under certain conditions on K, we will show that the module theory of R has a model-companion.

- Second, we will consider R with its full ring structure.

  In particular, for R a ring of infinite sequences indexed by ω over a *finite* field F, we will get *decidability results*; whereas if F is an *infinite* field, we will get *undecidability results.*

- Then, we will get *decidability* results for difference rings of the form $(\mathbb{C}^n, +, ., \sigma_n)$, where n is a natural number. Such rings occur in the theory of Picard-Vessiot extensions.

- For commutative difference Bezout rings R with an automorphism having an infinite orbit on $MSpec(R)$, we get *undecidability results.*

- We prove the existence of a model companion for well-mixed von Neumann regular commutative rings, namely certain Boolean products of fields which are models of $ACFA$.

- Finally, we will give some *amalgamation* results for von Neumann commutative regular difference rings and for von Neumann commutative regular *lattice-ordered* difference rings.

3.1 The theory of modules of difference rings.

Let (K, σ) be a difference field. One considers the theory of K in the reduct of the difference field language consisting of an expansion by definition of the module language over a non commutative skew polynomial ring $K[t; \sigma]$ where the action of "t" on the field K is interpreted by the action of the endomorphism σ.

Recall that $K[t; \sigma]$ is the skew polynomial ring where the commutation rule is: $k.t = t.k^\sigma$, for all $k \in K$ ([6]).

In collaboration with Pilar Dellunde and Françoise Delon, we described the theory of modules of separably closed fields of characteristic p and imperfection degree e ($e \in \omega \cup \{\infty\}$) and of non principal ultraproducts of these ([10], [11], [30]).

T. Rohwer in his thesis considered valued difference fields with rapidly increasing automorphism, as valued modules over skew polynomial rings ([34]). He showed in particular that the theory of modules of the field of Laurent series $K := F((X))$ over the skew polynomial ring $K[t; \Phi_p]$, augmented with extra unary predicates for additive subgroups of K in particular for the zero subgroup $\{0\}$, is model-complete whenever the theory of F over the skew polynomial ring $K[t; \sigma]$ is model-complete. Moreover, K is decidable whenever F is decidable. (See chapter 8 in [34].)

Throughout this section, (R, σ) will be a difference ring which is K-algebra, with (K, σ) a difference field containing $Fix(\sigma)$.

Let $A := K[t;\sigma]$, we endow R with a structure of a right A-module by defining the action of t as $s.t := s^\sigma$, $s \in R$. Under an addition assumption on K, we will show that the "module" theory of R has a model-companion.

Let $\mathcal{L}_A = \{+, -, 0, .r; r \in A\}$, where $.r$ denotes right multiplication by r and let T_A be the theory of all right A-modules.

In the theory of modules, one has the following relative quantifier elimination result. Recall that a *positive primitive* (p.p.) formula is a formula expressing that a system of linear equations has a solution.

Then, any $\mathcal{L}_A$-formula is equivalent in T_A to a Boolean combination of p.p. formulas and *index* sentences, namely sentences telling the index of p.p. definable subgroups in one another ([31]).

Assume now that σ is an automorphism and that (K, σ) is an inversive difference field. Then, A is right and left Euclidean ([6]), namely for all $p(t),\ p_1(t)$, there exist $q(t),\ q'(t)$ and $r(t),\ r'(t)$ of degree strictly smaller than the degree of $p_1(t)$ such that $p(t) = p_1(t).q(t) + r(t) = q'(t).p_1(t) + r'(t)$. The next proposition will describe the p.p. $\mathcal{L}_A$-formulas.

Proposition 3.1. (See [20]). *Let A be a right and left Euclidean domain and B be matrix $m \times n$ with coefficients in A. Then there exist invertible matrices P, Q such that $P.B.Q$ is diagonal. Moreover, if $d_1, \cdots, d_k$ are the non zero coefficients occurring on the diagonal, then d_i divides d_{i+1}, $1 \leq i \leq k$.*

In particular, any p.p. formula $\phi(v)$ with one free variable is equivalent in T_A to:

$$\bigwedge_i \exists w_i\ w_i.s_i = v.r_i, \quad s_i, r_i \in A.$$

Let T_m be the following theory:

1. T_A the theory of all right A-modules,
2. $\forall g\ \exists f\ (f.t = g)\ \&\ \forall g\ \ (g.t = 0 \rightarrow\ g = 0)$, "the action of "t" is surjective and injective"
3. $\forall g\ \exists f\ (f.p(t) = g)$, where $p(t)$ is ranging over the irreducible polynomials of A, "divisibility"
4. $\exists v \neq 0\ v.p(t) = 0$, with $p(t) \in A$ and $p(0) \neq 0$, "torsion"

Observe that one can embed R into a model of axiom scheme 3. Indeed, 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 $r_i \in R$. Then R embeds into the difference ring $R^\omega_{\mathcal{F}}$ of sequences modulo the Frechet filter $\mathcal{F}$, sending $r \rightarrow (r)_{\mathcal{F}}$ and $(R^\omega_{\mathcal{F}}, \tilde{\sigma})$ satisfies axiom scheme 3.

From now on, we will make the following *additional* assumptions on the difference ring R: recall that it is a K-algebra and assume that $C := Fix(\sigma) \subset K$ is algebraically closed and that the algebraic closure of K is included in $C^\omega_{\mathcal{F}}$; moreover in characteristic p that K is perfect. These assumptions will insure that as a $K[t;\sigma]$-module, R embeds into a model of T_m. To prove this, we will use the theory of Picard-Vessiot extensions developed by M. Singer and M. van der Put ([37]).

First, observe that to the p.p. $\mathcal{L}_A$-formula of the form:

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

one can associate the difference equation:

$$\sigma V = V.B,$$

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

$$\begin{pmatrix} \sigma v & \sigma^2 v & . & . & \sigma^n v \end{pmatrix} = \begin{pmatrix} v & \sigma v & . & . & \sigma^{n-1} v \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & ... & -a_0 \\ 1 & 0 & 0 & ... & -a_1 \\ & & & & \\ & & & & \\ 0 & 0 & ... & 1 & -a_{n-1} \end{pmatrix}$$

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

Then a ring S is a *Picard-Vessiot ring w.r.to the equation* $\sigma Y = Y.B$, where $B \in GL_n(K)$, if the following conditions hold:

1. One may extend σ to the ring S.
2. S has no non trivial two-sided ideals.
3. There exists a matrix U in $GL_n(S)$ such that $\sigma U = U.B$.
4. This extension is minimal.

Theorem 3.2. ([37]) *Under the hypothesis above, let $\sigma Y = Y.B$ be a difference equation with $B \in GL_n(K)$, then the Picard-Vessiot ring associated to this equation 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.*

Using the above theorem, one shows that our ring R embeds into a model of T_m. Our main result in this section is the following (see [19]).

Proposition 3.3. *As a $K[t;\sigma]$-module, R embeds into a model of T_m. The theory T_m is complete and admits quantifier elimination in $\mathcal{L}_A$.*

Corollary 3.4. *Let K_0 be a recursively presented subfield of K with a splitting algorithm* ([33]). *Let R_0 be the corresponding skew polynomial ring and denote by $T_{m,0}$ the corresponding theory of modules. Then, $T_{m,0}$ is decidable.*

Now, we will enrich the language of modules by adding a predicate for $Fix(\sigma) \cap K$ and so obtain a two-sorted language: one sort for the module elements and another sort for the field (or ring) elements (see for instance [22] chapter 9).

In this framework, T. Pheidas and K. Zahidi considered the polynomial ring $F[X]$ in one indeterminate X over a perfect field F of characteristic p and they showed that its theory of modules over the skew polynomial ring $F[t;\Phi_p]$, with an additional unary predicate for F, is model-complete, whenever the theory of F as an F-vector-space is model-complete (see Theorem 2 in [28]). Recently, M.

Kaminski considered two-sorted modules over polynomial rings in several commuting indeterminates ([24]).

Denote by $\mathcal{L}$ the language of $\mathcal{L}_A$ together with the field language $\mathcal{L}_f$, a predicate C for the fixed subfield of K under σ and new relation symbols $\{D_n(.,\cdots,.); n \in \omega\}$, $\{T_{n,\theta}(\bar{v};\bar{w}); n \in \omega; \theta$ where θ is an open $\mathcal{L}_f$-formula $\}$.

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

1. the theory T_m,

2. C is an algebraically closed field included in $Fix(\sigma)$,

3. $\forall m_1 \in M \cdots \forall m_k \in M \forall c_1 \in C \cdots \forall c_k \in C - \{0\}$
$(\sum_{i=1}^{k} m_i.c_i = 0 \rightarrow D_k(m_1,\cdots,m_k)\ )$, $k \geq 2$, $k \in \omega$,

4. $\forall v_0 \in M \cdots \forall v_n \in M\ \forall w_0 \in M \cdots \forall w_n \in M\ [\ \neg D_n(v_1,\cdots,v_n)$ or
$\neg D_n(w_1,\cdots,w_n)] \rightarrow [T_{n,\theta}(v_0,v_1,v_2,\cdots,v_n;w_0,w_1,w_2,\cdots,w_n)$ iff
$(\exists k_1 \neq 0 \cdots \exists k_n \neq 0\ \in C\ \exists l_1 \neq 0 \cdots \exists l_n \neq 0\ \in C\ \theta(k_1,\cdots,k_n,l_1,\cdots,l_n)$ 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.

5. $\exists v_1 \cdots v_d\ \in M\ \bigwedge_i \neg D_d(v_1,\cdots,v_d) \wedge v_i.p(t) = 0$, where $p(t)$ ranging over the irreducible polynomials of R of degree d, $d \in \omega$

Proposition 3.5. (See [19]). *The theory $T_{m,C}$ admits q.e. in $\mathcal{L}$ and it is complete.*

In the next sections, we will work in the full ring language.

3.2 Decidability results for difference rings of sequences over a field F.

Recall that in a *monadic* second-order theory of a structure, one is allowed to quantify over *subsets of the domain of the structure.* Using *automata* operating on infinite ω sequences, J.R. Büchi proved the decidability of the monadic second-order theory of $\mathcal{N} := (\mathbb{N}, S, \leq)$, where S is the successor function ([3]). From this result, one can easily deduce that the Boolean algebra of idempotents of the ring $F_{\mathcal{F}}^{\omega}$, where $\mathcal{F}$ is the Frechet filter on ω and F a finite field, with the shift automorphism is decidable.

Proposition 3.6. ([19]) *The $\mathcal{L}_{rings_\sigma}$-structures $(\mathbb{F}_2^{\omega},+,.,0,1,\sigma_t)$, $(\mathbb{F}_2^{\mathbb{Z}},+,.,0,1,\sigma_t)$ and $({\mathbb{F}_2}^{\omega}{}_{\mathcal{F}},+,.,0,1,\sigma_t)$ are decidable.*

We can easily generalize the above Proposition as follows.

Corollary 3.7. ([19]) *The difference ring of sequences $(F^{\mathbb{Z}},+,.,0,1,\sigma_t)$ over the finite field F, is decidable.*

3.3 Undecidability results for difference rings of sequences over a field F

As soon as the field F is infinite, we get the following undecidability results in both characteristic 0 or p.

Proposition 3.8. ([19]) *Let F be a field of characteristic zero. Then, the existential theory of the difference ring $(F^{\omega}_{\mathcal{F}}, +, ., -, \sigma_t)$ is undecidable. We define the ring $(\mathbb{Z}, +, ., 0, 1)$.*

Proposition 3.9. ([19]) *Let F be a field of characteristic p which is not included in $\mathbb{F}_p^a$. Then, we can interpret the semi-ring $(\mathbb{N}, +, ., 0, 1)$ in the difference ring $(F^{\omega}_{\mathcal{F}}, +, , ., \sigma_t)$.*

3.4 Undecidability results for commutative difference Bezout rings.

After the negative results of the previous section, one can ask: what about the difference rings of finite sequences? One can show that the theories of $(\mathbb{C}^n, +, ., \sigma_n)$ and the theories of $(\tilde{\mathbb{F}_p}^n, +, ., \sigma_n)$, $n \in \omega$ are decidable and model-complete. Note that these rings also arise as total Picard-Vessiot rings attached to a difference equation ([37] Chapter 1). However, we have no uniformity in $n \in \omega$ in the above results as we shall see in Corollary 3.14, below.

This will be a consequence of a more general undecidability result holding for certain classes of von Neumann regular commutative difference rings.

Definition 3.1. 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 sum of two ideals generated by b elements is again generated by b elements; so the class of b-Bezout rings is an elementary class. This generalizes Bezout rings, namely those where every finitely generated ideal is principal.

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 ([25]).

Now, we will use the fact that there are *undecidable finitely axiomatizable* subtheories of Peano arithmetic ([38]). Let Q_c be the theory of the truncated semi-ring of the integers between 0 and n, $n \in \mathbb{N}$. Let M be an infinite model of Q_c and let T_{fin} be its theory. One shows that T_{fin} contains an essentially undecidable finitely axiomatizable subtheory of PA [38] and so, T_{fin} is undecidable.

Proposition 3.10. (*Partial Dichotomy result* [19]) *Let R be a commutative b-Bezout difference ring of characteristic 0. Suppose that $Fix(\sigma)$ is an infinite field. Then, either some power of σ fixes the maximal spectrum of R, or the theory of R is undecidable.*

By localizing, we can slightly weaken the hypothesis on the fixed subring.

Corollary 3.11. ([19]) *Let R be a b-Bezout ring. Suppose that $Fix(\sigma)$ has no zero-divisors and that for all $n \in \omega$, there exists a prime ideal P such that $P \cap Fix(\sigma) = \{0\}$ and $P, \sigma(P), \cdots, \sigma^n(P)$ are pairwise co-maximal. Then $Th(R)$ is undecidable.*

In the characteristic p case, we have to strengthen our hypothesis of "Bezout".

Proposition 3.12. ([19]) *Let R be a commutative von Neumann regular difference ring of characteristic $p > 0$ and assume that $Fix(\sigma)$ is an infinite field. Assume that for each $n \in \omega$, there is an idempotent e_n such that $\{\sigma(e_n), \cdots, \sigma^n(e_n) = e_n\}$ is a partition of 1. Then the theory of R is undecidable.*

The following result improves Proposition 3.9 of the previous section.

Corollary 3.13. ([19]) *The theory of the ring of all sequences with coefficients in $\mathbb{F}_p^a$ with the shift endomorphism is undecidable.*

Corollary 3.14. [Non-uniformity result] ([19]) *The theory of all non principal ultraproducts on ω of of the following structures either, with $n \in \omega$: $(\mathbb{C}^n, +, ., \sigma_n)$ 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.*

Applications:

1. Let $\mathbb{C}\{z^{-1}\}$ be the ring of power series in z^{-1} that converge in a neighbourhood 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 $(f(1), f(2), \cdots)_{\mathcal{F}}$. 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 Proposition 3.10.

   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, let $c \in \mathbb{C}$ 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 $(f(1), f(c), f(c^2), \cdots)_{\mathcal{F}}$. Since the disk of unity is compact, the fixed subring is isomorphic to $\mathbb{C}$. 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 Proposition 3.10.

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

Concerning the first example, using a previous result of R. Robinson ([34]) and the fact that in this structure, in the language $\mathcal{L}_{z^{-1}} := \mathcal{L}_{rings} \cup \{z^{-1}\}$, the field $\mathbb{C}$ is definable, it was observed in section 6 of [29], that the theory of $\mathbb{C}\{z^{-1}\}$ in $\mathcal{L}_{z^{-1}}$ is undecidable.

Concerning the second example, it was shown by J. Denef that the positive existential theory of $(\mathbb{C}\{z\}, +, ., 0, 1, z)$ in the language $\mathcal{L}_z$ is undecidable ([12]).

Let $\tilde{\mathbb{Z}}$ be the ring of all algebraic integers. The theory of this ring has been shown to be decidable by L. van den Dries ([13]), using a local-global principle due to R. Rumely. Its maximal spectrum coincides with the prime spectrum and it is a totally disconnected topological space.

Let τ be a non-trivial element of the absolute Galois group $G(\mathbb{Q})$ of $\mathbb{Q}$. Then every prime ideal has a non trivial intersection with $Fix(\tau)$. Is the theory of this ring $Th((\tilde{\mathbb{Z}}, \tau))$ with this distinguished automorphism (un)decidable?

G. Cherlin and M. Jarden have shown that the theory consisting of the set of sentences true in almost all $(\mathbb{Q}, \tau_1, \cdots, \tau_e)$ for $(\tau_1, \cdots, \tau_e) \in G(\mathbb{Q})^e$, $e > 1$, is undecidable ([9]).

3.5 Boolean products of models of $ACFA$

Because of our undecidability result for commutative difference von Neumann regular rings of characteristic zero, with a distinguished automorphism σ having an infinite orbit on $Spec(R)$, we will now consider the class of difference von Neumann regular rings where the orbits of the automorphism on $Spec(R)$, are of cardinality 1 (the well-mixed case). Since in this case, it is a Boolean product of commutative inversive difference fields, we will transfer positive results due to Z. Chatzidakis and E. Hrushovski on $ACFA$.

First, let us recall the definition of a Boolean product (see [4]) of $\mathcal{L}$-structures R_x with $x \in X$.

The *truth value of a formula* $\phi(u, \bar{a})$ in a subdirect product $\prod_{x\in X} R_x$ is

$$[\phi(u, \bar{a})] := \{x \in X : R_x \models \phi(u(x), \bar{a}(x))\}.$$

R is a (atomeless) Boolean product of $\mathcal{L}$-structures R_x, $x \in X$, if

$$R = \Gamma_a(X, \bigcup_{x\in X} R_x)$$

1. R is a subdirect product of the R_x, $x \in X$,
2. The set X is a (atomeless) Boolean space i.e. X has a basis of clopen sets (namely both open and closed) (and no isolated points),
3. For every atomic formula, its truth value in 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.

To the language of rings, we add a *pseudo-inverse* * defined as follows:

$$\forall r \;\; r^2.r^* = r \& \; (r^*)^2.r = r^*.$$

Let $\mathcal{L}_0 := \mathcal{L}_{rings} \cup \{\sigma, \sigma^{-1}\} \cup \{^*\}$ and $T_{atm,\sigma}$ be the following $\mathcal{L}_0$-theory of difference commutative rings R:

1. R is von Neumann regular without minimal idempotents, σ is an automorphism of R and every monic polynomial has a root,
2. The Boolean algebra of idempotents is included in the set of fixed points of σ,
3. For each idempotent e of R, for every irreducible variety U on e and every irreducible 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 $(a, \sigma(a)) \in V - W$.

Applying Burris-Werner's transfer results ([4]) to atomeless Boolean products of models of $ACFA$ and Theorem 2.1 and Corollary 2.2, we get the following Proposition.

Proposition 3.15. ([19]) *The theory $T_{atm,\sigma}$ is model-complete in $\mathcal{L}_0$ and decidable.*

Recall that in a commutative ring R, the Jacobson radical $J(R)$ is the intersection of its maximal ideals; it is equal to $\{z \in R : \forall a \exists u \ \ (1 - a.z).u = 1\}$. One can define the binary relation

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

meaning that every maximal ideal containing a also contains a_1, by the first-order formula:

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

Proposition 3.16. ([19]) *Let T_{rad} be the theory of commutative inversive difference rings in which $J(R) = \{0\}$, satisfying the sentence $\forall a \ \ \sigma(a) \in rad(a)$. Then T_{rad} has a model-companion.*

Proof: Since $J(R) = \{0\}$, R is a subdirect product of fields and these fields are difference fields, since R satisfies $\forall a \ \ \sigma(a) \in rad(a)$. Then, one embeds R in an atomeless Boolean product of difference fields, applies the fact that $ACFA$ is the model companion of the theory of difference fields and the above Proposition on atomeless Boolean products. ∎

3.6 Amalgamation

Let $\mathcal{C}$ be the class of von Neumann regular commutative inversive difference rings. Let $R_0 \subseteq R_1, \ R_2$ be commutative von Neumann regular inversive difference rings of characteristic zero or perfect of characteristic p.

We show that we can embed them in a functorial way in a von Neumann regular ring. In particular, since these are inversive difference rings, this embedding will commute with each automorphism.

Lemma 3.17. *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 $Spec(R_2)$) be such that $x_1 \cap x_2 \in Spec(R_0)$.

Then, $R_1/x_1 \otimes_{R_0/x_0} R_2/x_2$ embeds in a canonical way in a von Neumann regular commutative ring R_x, $x := (x_1, x_2)$ containing both R_1/x_1 and R_2/x_2.

Recall that a *Robinson* theory ([17]) is a *universal* theory with *amalgamation*, namely any two models can be embedded in a third one. So, the class $\mathcal{C}^{ec}$ of its existentially closed models is well-behaved, in particular any existential formula is equivalent to an infinitary quantifier-free formula ([16]). Such theory has *universal* domains ([17]).

Let T_0 be the theory of von Neumann commutative inversive difference regular rings of characteristic zero in the language $\mathcal{L}_0$. Note that in this language $\mathcal{L}_0$, the theory T_0 is universal.

Proposition 3.18. ([19]) *The theory T_0 is a Robinson theory in the language $\mathcal{L}_0$.*

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 $\forall r \exists s \;\; r = s^p$). Let $\mathcal{L}_p := \mathcal{L}_0 \cup \{(.)^{1/p}\}$, where the new unary symbols are defined by $(x)^{1/p} = y$ iff $x^p = y$, $p \in \mathcal{P}$, where $\mathcal{P}$ denotes the set of prime numbers. In this language $\mathcal{L}_p$, the theory T_p is universal.

Proposition 3.19. ([19]) *The theory T_p is a Robinson theory in the language $\mathcal{L}_p$.*

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

Let $\mathcal{L}_{\infty,p} := \mathcal{L}_p \cup \{e_n;\;\; n \in \omega\}$, where $p \in \mathcal{P} \cup \{0\}$.

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

1. for each n, the axiom: $e_n^2 = e_n$ and $\sum_{i=0}^{n-1} \sigma^i(e_n) = 1$ & $\bigwedge_{i \neq j} \sigma^i(e_n).\sigma^j(e_n) = 0$ & $\sigma^n(e_n) = e_n$,
2. the theory T_p.

Proposition 3.20. ([19]) *The theory $T_{\infty,p}$ is a Robinson theory in the language $\mathcal{L}_{\infty,p}$.*

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

Finally, we will consider the class of lattice-ordered commutative rings (ℓ-rings) with an automorphism. (For a reference on ℓ-rings and their properties, see for instance [2]). Recall that those rings R are partially ordered rings where $(R, \wedge, \vee)$ form a lattice. Let $\mathcal{L}_\ell$=$\mathcal{L}_{rings} \cup \{\wedge, \vee\}$ the language of lattice-ordered rings.

Note that in an ℓ-ring, a finitely generated ℓ-ideal is principal. So, we may apply our undecidability result for Bezout rings. Namely, given an ℓ-ring R with an automorphism σ which has an infinite orbit on the set of its ℓ-ideals and such that $Fix(\sigma)$ is an infinite field, then the theory of $(R, +, ., \wedge, \vee, \sigma)$ is undecidable.

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

Again, the key lemma is the following.

Lemma 3.21. ([19]) *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 $x_1 \cap x_2 \in Spec(R_0)$. 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.*

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

1. the $\mathcal{L}_\ell$-theory of von Neumann commutative regular f-rings with a pseudo-inverse $\{^*\}$,

2. σ is an morphism of ℓ-rings and σ^{-1} is its inverse.

Note that T_f is a universal theory: the axioms axiomatizing the class of f-rings are universal and we have already seen that the other ones were universal.

Proposition 3.22. ([19]) *Let T_f is a Robinson theory in $\mathcal{L}^*$.*

Can we describe in some ways the universal domains?

4 Topological difference fields

In this section, we will consider topological difference fields. Let (K, v, σ) be an inversive difference valued field, namely a valued field endowed with a distinguished field automorphism σ satisfying $\forall a\ v(\sigma(a)) \geq v(a)$ (*). This kind of structures was considered on one hand by L. Bélair, A. Macintyre and T. Scanlon ([1], [36]), requiring in addition that $v(a) = v(\sigma(a))$ for all $a \in K^\times$ and on the other hand by E. Hrushovski and Z. Chatzidakis requiring that σ induces a rapidly increasing automorphism on the value group of K ([7], [18]).

Note that H. Kikyo and S. Shelah showed that *in general* given a model-complete theory T, the theory T_σ of the class of the models of T endowed with a distinguished automorphism σ does not have a model-companion (see [26]). In particular, when T is not stable which is the case here. So, in order to obtain a first-order theory, one has to put additional constraints on the automorphism σ.

Throughout this section, K is a valued field of characteristic zero with valuation v, the valuation ring $O_K := \{x \in K : v(x) \geq 0\}$, the maximal ideal $M_K := \{x \in K : v(x) > 0\}$, $k \cong O_K/M_K$ is the residue field and Γ is the value group of v. We will denote the residue map from K to k by $a \to \overline{a} := a + M_K$. Because of the relation (*) between the valuation and the distinguished automorphism σ, σ induces an endomorphism $\bar{\sigma}$ on the residue field k, namely $\bar{\sigma}(\bar{a}) := \sigma(a) + M_K$.

Note that these fields can also be seen in the formalism of valued D-fields introduced by T. Scanlon ([36]). Indeed, one defines a map D in the following way: $D(a) := (\sigma(a) - a)/p$, which is additive, $D(x.y) = D(x).y + x.D(y) + p.D(x).D(y)$ and $D(1) = 0$.

In the case where $\bar{\sigma}$ is the usual Frobenius on the residue field, one can also use the following p-derivation, defined as follows $\delta_1(a) := (\sigma(a) - a^p)/p$ (see [23] and [1]).

4.1 σ acts on the residue field

Let A be a commutative ring of characteristic p. One can define for each m, the Witt ring $W_m[A]$ whose domain is included in A^m, the direct product of m copies of A with the shift $\sigma_r : W_m[A] \to W_{m+1}[A]$ and the Frobenius map Φ_p acting pointwise. For the definition of addition and multiplication (see section 8.10 [21]); for these operations the right shift is only a morphism of the additive group structure. The ring $W[A]$ is defined as the inverse limit of the rings $W_m[A]$. If A is a perfect field, then $W[A]$ is a domain and we will denote its field of fractions by $W(A)$. The ring $W[A]$ is endowed with the valuation v sending a sequence $(a_n)_{n\in\omega}$ to m if a_m is the

first non zero coefficient and with the endomorphism σ sending (a_n) to $(\Phi_p(a_n))_{n\in\omega}$. Then, we extend these two maps to $W(A)$.

L. Belair, A. Macintyre and T. Scanlon have identified and studied the theory of $W(\mathbb{F}_p^a)$ as a valued difference field, as well as the theory of the non principal ultraproducts of these, varying p ([1], [36]). The fixed subfield of $W(\mathbb{F}_p^a)$ is isomorphic to $\mathbb{Q}_p \cong W(\mathbb{F}_p)$, the field of p-adic numbers and $W(\mathbb{F}_p^a)$ is the completion of the maximal unramified extension of $\mathbb{Q}_p$.

Definition 4.1. ([1]]) Let $P[Z] \in \mathcal{O}_K[Z]_\sigma$ of order n with Z one indeterminate. Let $\bar{X} := (X_0, \cdots, X_n)$, $\bar{\ell} = (\ell_0, \cdots, \ell_n)$, $|\bar{\ell}| = \ell_0 + \cdots + \ell_n$ and $\bar{Y}^{\bar{\ell}} := (Y_0^{\ell_0}, \cdots, Y_n^{\ell_n})$. Write $P^*[\bar{X} + \bar{Y}]$ as $P^*[\bar{X}] + \sum_{\bar{\ell}\geq 1} P^*_{\bar{\ell}}[\bar{X}].\bar{Y}^{\bar{\ell}}$.

One says that $\tilde{a} := (a, a^\sigma, \cdots, a^{\sigma^n})$ and P are in σ-Hensel configuration if

$$v(P^*(\tilde{a})) = \gamma + min_{|\bar{\ell}|=1} v(P^*_{\bar{\ell}}(\tilde{a}))$$

$$< j.\gamma + v(P^*_{\bar{\ell}}(\tilde{a})),$$

whenever $j = |\bar{\ell}| > 1$.

Definition 4.2. Let T_w be the following theory of difference valued fields (K, k, Γ, v).

1. (K, v) is a valued field of characteristic 0,
2. σ is an automorphism of the field K,
3. $\forall a \in K\ v(a) = v(\sigma(a))$,
4. density of the fixed field: $\forall a \in K\ \exists x \in Fix(\sigma)\ v(x) = v(a)$,
5. every inhomogeneous non-trivial linear $\bar{\sigma}$-equation over k has a solution in k,
6. every equation $\bar{\sigma}(x) = \lambda.x$, with $\lambda \neq 0$ has a non-trivial solution in k.
7. σ-Hensel Lemma: for any $P[X_1] \in O_K[X_1]_\sigma$, and $a \in O_K$ in σ-Hensel configuration, there exists $b \in O_K$ such that $P(b) = 0$ and $v(a - b) = \gamma$.

Definition 4.3. Let (F, σ) be a difference field. Then F is linearly difference closed if the linear difference operators $\sum_{i=0}^m a_j \sigma^j$, $m \in \omega$ and $a_j \in F$, are surjective on F.

Note that the above definition exactly expresses that F is a divisible $F[t; \sigma]$-module.

Any complete discrete valued difference valued field K satisfying axioms (1) up to (5) with a residue field which is linearly difference closed satisfies the σ-Hensel Lemma ([1] Corollary 4.3).

Definition 4.4. Let $T_{w,p}$ be the following theory of difference valued fields (K, v, k, Γ).

1. K is a model of T_w,
2. the residue field k has characteristic p and $v(p) = 1$,
3. $\forall a \in k\ \ \bar{\sigma}(a) = a^p$.

Definition 4.5. Let $T_{w,0}$ be the following theory of difference valued fields (K, v, k, Γ).

1. K is a model of T_w,
2. the residue field k has characteristic 0,
3. no residual σ-identities: for every $p[X] \in k[X]_{\bar{\sigma}} - \{0\}$, there is an element $a \in k$ with $p(a) \neq 0$,
4. genericity axiom: for any inhomogeneous nontrivial linear $\bar{\sigma}$-equation over k of order n and any nontrivial polynomial $G(X)$ over k of order $m < n$, there is a solution α in k of the linear equation such that $G(\alpha) \neq 0$.

One obtains the following Ax-Kochen-Ershov like theorem:

Theorem 4.1. (Theorems 8.1, 9.1 in [1]) *Let $(K, v, k, \Gamma, \sigma)$ be a model of either $T_{w,0}$ or $T_{w,p}$. Then its theory is determined by the theory T_k of the residue field $(k, \bar{\sigma})$ and the theory T_Γ of value group Γ. Moreover its theory is model-complete whenever the theories T_k and T_Γ are model-complete.*

This theorem implies that the theory WF_p of $(W(\mathbb{F}_p^a), \sigma)$ is axiomatized by $T_{w,p}$ plus the schemes of axioms expressing that the residue field k is algebraically closed (of characteristic p), that the value group is a $\mathbb{Z}$-group with its least strictly positive element equal to $v(p)$. (Note that in this case the valuation is definable in the ring language and so we get a theory of existentially closed difference fields different from $ACFA$).

In addition one can show that WF_p is the model-companion of the theory of p-valued difference fields satisfying $\forall x \in k\ (\bar{\sigma}(x) = x^p)$ (Proposition 9.3 in [1]).

By asymptotic theory of the $(W(\mathbb{F}_p^a), \sigma)$, $p \in \mathcal{P}$, we mean the set of sentences θ true in all but finitely many $(W(\mathbb{F}_p^a), \sigma)$. The above Theorem implies that the asymptotic theories of the $(W(\mathbb{F}_p^a), \sigma)$, and of the $(\mathbb{F}_p^a((t)), \sigma_{p,t})$, $p \in \mathcal{P}$, where $\sigma_{p,t}$ is the Frobenius on $\mathbb{F}_p^a$ and $\sigma_{p,t}(t) = t$ coincide (see Corollary 11.5 in [1]).

4.2 σ acts on the value group.

Let (K_p, Φ_p, v) be an algebraically closed difference field of characteristic p with a non trivial valuation v. The aim here is to describe the theory of the difference non-trivially valued fields of characteristic 0 which are non principal ultraproducts of these structures. Note that if $a_p \in K_p$ with $v(a_p) > 0$, then $v(\Phi(a_p)) = p.v(a)$ and so in the ultraproduct $\prod_U (K_p, \Phi_p, v)$ with U a non principal ultrafilter over the prime numbers, we have that $v(\Phi([a_p]_U) > n.v([a_p]_U)$ for every natural number $n \in \omega$.

Definition 4.6. Let $\mathbb{Z}[T]$ be the polynomial ring in one indeterminate. We extend the order on $\mathbb{Z}$ by setting $\sum_{i=0}^n a_i T^i > 0$, with $a_i \in \mathbb{Z}$ if $a_n > 0$.

Recall that a ball of center c and radius $\gamma \in \Gamma$ in a valued field K is a subset of the form $\{x \in K :\ v(x - c) > \gamma\}$.

Definition 4.7. *Strong approximation:* Let $Q \in K[X_0, \cdots, X_n]$, let $B_0, \cdots, B_n \subset K$ be $n+1$ balls. Then, $v(Q; B_0 \times \cdots \times B_n) := inf\{v(Q(\bar{a})) : \bar{a} \in B_0 \times \cdots \times B_n\}$ and for $B \subset K$ a ball and $P \in K[X]_\sigma$ we have $v(P; B) := v(P^*; B \times B^\sigma \times \cdots \times B^{\sigma^n})$.

We say that $a \in B$ is an approximate solution of P on B if $v(P(a)) > v(P; B)$.

Definition 4.8. Let VFA_0 be the following theory of difference valued fields (K, k, Γ, v) ([8]).

1. σ is an automorphism of the field K.
2. $\forall a \in K\ v(a) \leq v(\sigma(a))$ and $\forall a \in M_K\ v(a) < v(\sigma(a))$.
3. $(k, \bar{\sigma})$ is a difference field of characteristic 0, model of $ACFA$.
4. Γ is a $\mathbb{Z}[\sigma]$-module and for each $\gamma \in \Gamma^{>0}$ and each $f(T) \in \mathbb{Z}[T]^{>0}$, $f(\sigma)(\gamma) > 0$.
5. Γ is a divisible $\mathbb{Z}[\sigma]$-module.
6. σ-S-Hensel Lemma: for any $P(X) \in O_K[X]_\sigma$, for any open ball in O_K such that $P(X)$ has an approximate solution in B and $\frac{\partial}{\partial X_0}P$ has none in B, there exists $c \in B$ such that $P(c) = 0$.

Theorem 4.2. ([8]) The theory VFA_0 is model-complete in $\mathcal{L}_{v,\sigma}$ and coincide with the asymptotic theory of the (K_p, Φ_p, v), $p \in \mathcal{P}$.

The proof of this theorem uses Theorem 2.3 in order to show that the residue fields of non principal ultraproducts of the (K_p, Φ_p, v) are models of $ACFA$ ([18]).

4.3 A real-closed valued difference field

Let us now conclude this section by considering another kind of topological difference fields: real-closed valued difference fields. Let R be a real-closed field and let $(G, ., 1, <)$ be a totally ordered abelian group and τ an increasing automorphism of this group.
Consider the field $R((G)) := \{\sum_{g \in G} r_g.g :\ r_g \in R\ \&\ \{g \in G : r_g \neq 0\}\ \text{is well} - \text{ordered}\}$; the fact that it is indeed a field has been shown by A.I. Mal'cev and B.H. Neumann. One can embed any ordered field in a field of this form with $R = \mathbb{R}$. If G is divisible, then this field is real-closed. One can define a valuation v by setting $v(\sum_{g \in G} r_g.g)$ to be the least g in the support of this element. One defines an automorphism σ by $\sigma(\sum_{g \in G} r_g.g) = \sum_{g \in G} r_g.\tau(g)$; it satisfies axiom 2 of Definition 4.9.

If one specialize to the case of $G = t^{\mathbb{Z}}$, one gets the usual field of Laurent series. Finally, let us say a few words on the field $\mathbb{R}((t))^{LE}$ of real exponential-logarithmic series ([14]). Its construction is described in ([14]). One starts with the field $R_0 := \mathbb{R}((x^{-1}))$ of Laurent series ordered by $x > \mathbb{R}$; a typical element $f(x)$ is of the form $r_n x^n + \cdots + r_1.x + r_0 + r_{-1}.x^{-1} + r_{-2}.x^{-2} + \cdots$. It consists of an infinite part: $f_1 := r_n x^n + \cdots + r_1.x$, a standard part r_0 and an infinitesimal part: $f_{-1} := r_{-1}.x^{-1} + r_{-2}.x^{-2} + \cdots$. The field $K := R_0$ can be decomposed as a direct sum of an additive subgroup $K_\infty = K - \mathcal{O}_K$ consisting of its elements of valuation > 1, and a multiplicative (convex) subgroup consisting of its elements of valuation ≤ 1. One defines the exponentiation operation E on finite elements as

follows: $E(r_0 + f_{-1}) := e^{r_0}.\sum_{m=0}^{\infty}(1/m!).(f_{-1})^m$, where e is the usual exponentiation operation on $\mathbb{R}$. Then, taking a strictly increasing homomorphism E_1 from the additive group of K into the multiplicative subgroup of its strictly positive elements, one defines $E(f(x)) := E_1(f_1).E(r_0 + f_{-1})$.

Then, one considers the field $R_1 := R_0((E_1(K_\infty)))$ and iterate this construction in ω steps, obtaining the field $\mathbb{R}((t))^E$ and then we close off by the logarithmic function, obtaining $\mathbb{R}((t))^{LE}$ as a countable union of exponential fields. This last construction uses the substitution map $\Phi : R^E \to R^E$ defined (informally) by $\Phi(f(x)) := f(E(x))$, and so is the identity on $\mathbb{R}$. This is used to define a logarithm operation for the elements in its image (see section 2.6 in [14]).

Then, one can verify that Φ is an automorphism of $\mathbb{R}((t))^{LE}$ and it is is ω-increasing [14].

References

[1] Bélair L., Macintyre A., Scanlon T., Model Theory of Frobenius on Witt vectors, submitted, http://132.208.138.87/belair/.

[2] Bigard A., Keimel K., Wolfenstein S., **Groupes et Anneaux réticulés**, Lecture Notes in Mathematics 608, Springer-Verlag, Berlin Heidelberg New-York 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 Univ. Press, Stanford, California, 1962, pp. 1-11.

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

[5] Cohn P.M., **Difference algebra**, Interscience Tracts in pure and applied Mathematics, Interscience Publishers, John Wiley and Sons, number 17, 1965.

[6] Cohn P.M., **Skew fields**, Encyclopedia of mathematics and its applications, edited by G.-C. Rota, Vol. 57, Cambridge University Press,1995.

[7] Chatzidakis C., Hrushovski E., Model theory of difference fields, Trans. Amer. Math. 351, 1999, 2997-3071.

[8] Chatzidakis C., Hrushovski E., Model theory of difference valued fields, notes spring 2002.

[9] Cherlin G., Jarden M., Undecidability of some elementary theories over PAC fields, Annals of Pure and Applied Logic 30, 1986, 137-163.

[10] Dellunde, P., Delon, F., Point F., The theory of modules of separably closed fields-1, J. Symbolic Logic 67, 2002, no. 3, 997-1015.

[11] Dellunde, P., Delon, F., Point F., The theory of modules of separably closed fields-2, Ann. Pure Appl. Logic 129, 2004, no. 1-3, 181-210.

[12] Denef J., The diophantine problem for polynomial rings and fields of rational functions, Trans. Amer. Math. Soc., 242, 1978, 391-399.

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

[14] van den Dries L., Macintyre A., Marker D., Logarithmic-exponential series, Annals of Pure and Applied Logic 111, 2001, 61-113.

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

[16] Hodges W., **Model theory**, Encyclopedia of Mathematics and its applications, volume 42, Cambridge University Press, 1993.

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

[18] Hrushovski E., The elementary theory of the Frobenius automorphisms, February 2004, Math ArXiv LO/0406514 v1.

[19] Hrushovski E., Point F., On von Neumann regular rings with an automorphism, submitted 2005.

[20] Jacobson N., **Basic Algebra 1**, W.H. Freeman and Compagny, San Francisco, 1974.

[21] Jacobson N., **Basic Algebra 2**, W.H. Freeman and Compagny, San Francisco, 1974.

[22] Jensen C.U., Lenzig H., **Model Theoretic Algebra**, Gordon and Breach Science Publishers, 1989.

[23] Joyal A., δ-anneaux et vecteurs de Witt, C.R. Math. Rep. Acad. Sci. Canada, 7, 1985, 177-182.

[24] Kaminsky M., Two-sorted theory of modules over $K[t_1, \cdots, t_m]$, preprint.

[25] Kaplansky I., **Commutative rings**, The University of Chicago Press, revised edition, 1974.

[26] Kikyo H., Shelah S., The strict order property and generic automorphisms, J. Symbolic Logic 67, 2002, no. 1, 214-216.

[27] Macintyre A.J., Generic automorphisms of fields, Annals of Pure and Applied Logic 88, n2-3, 1997, 165-180.

[28] Pheidas T., Zahidi K., Elimination theory for addition and the Frobenius map in polynomial rings, J. Symbolic Logic 69, 2004, no. 4, 1006-1026.

[29] Pheidas T., Zahidi K., Undecidability of existential theories of rings and fields: a survey, *Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999)*, 49-105, Contemp. Math., 270, Amer. Math. Soc., Providence RI, 2000.

[30] Point F., Asymptotic theory of modules of separably closed fields, J. of Symbolic Logic, 70, 2005, no. 2, 573-592.

[31] Prest M., *Model theory and modules*, L. M. Soc. Lecture Notes Series 130, Cambridge University Press, 1988.

[32] Rabin M.O., Decidable theories in *Handbook of Mathematical Logic*, edited by J. Bairwise, Studies in Logic and the Foundations of Mathematics, vol. 90, North-Holland, 1977, 595-629.

[33] Rabin M., Computable algebra, general theory and theory of computable fields, Trans. Amer. Math. Soc. 95, 1960, 341-360.

[34] Robinson R., Undecidable rings, Trans. Amer. Math. Soc. 70, 1951, 137-159.

[35] Rohwer T., Valued difference fields as modules over twisted polynomial rings, PhD thesis, University of Illinois at Urbana-Champaign, 2003.

[36] Scanlon T., Quantifier elimination for the relative Frobenius, Fields Institute Communications, volume 33, 2003, 323-352.

[37] Singer M., van der Put M., **Galois theory of difference equations**, L.N.M., 1666, Springer, 1997.

[38] Tarski A., Mostowski A., Robinson R., **Undecidable theories**, Studies in Logic and the foundations of Mathematics, North Holland (second printing 1968), 1953.

Institut de Mathématique
Université de Mons-Hainaut, Le Pentagone
6, avenue du Champ de Mars, B-7000 Mons, Belgium
email : point@logique.jussieu.fr