PSEUDO-LINEAR ALGEBRA OVER A DIVISION RING

Cédric Milliet

PSEUDO-LINEAR ALGEBRA OVER A DIVISION RING

CÉDRIC MILLIET

ABSTRACT. We consider an analogue of the Zariski topology over a division ring (D, σ, δ) equipped with a ring morphism σ, a σ-derivation δ, and a pseudo-linear transformation θ as introduced by Ore and Jacobson. A basic closed subset of D^n, which we call θ-affine, is the zero set of a (finite) family of linear combinations of $\left\{\theta^{i_1}(x_1), \ldots, \theta^{i_n}(x_n), 1 \colon (i_1, \ldots, i_n) \in \mathbf{N}^n\right\}$ having left coefficients in D. This enables to define elementary notions of algebraic geometry: θ-affine sets, θ-morphisms, a Zariski dimension, and a notion of comorphism that witnesses a duality between the category of θ-affine sets and the category of $D[t; \sigma, \delta]$-modules. Using results of P. Cohn, we show that when σ and δ commute, (D, σ, δ) has an extension in which each nonzero polynomial $a_0 x + a_1\theta(x) + \cdots + a_n\theta^n(x)$ is surjective. In such an extension, using Baur-Monk's quantifier elimination, we show that Chevalley's projection Theorem holds, as well as a Nullstellensatz that provides an equivalence between the category of θ-affine sets having no proper θ-affine subset of the same Zariski dimension, and the category of torsion-free finitely generated $D[t; \sigma, \delta]$-modules. These results are applied in a further paper to division rings that do not have Shelah's independence property.

Given a division ring $(D, \sigma, \delta, \theta)$ equipped with a ring morphism $\sigma \colon D \to D$, a σ-derivation $\delta \colon D \to D$ and a pseudo-linear transformation $\theta \colon D \to D$ as defined by Jacobson [20], the purpose of the paper is the study of the subsets of D^n defined by a system of linear equations

$$\gamma(x_1, \ldots, x_n) = 0 \tag{0.1}$$

where the map $\gamma \colon D^n \to D$ has the form

$$\gamma_1(x_1) + \cdots + \gamma_n(x_n) + c, \tag{0.2}$$

the element c being in D and each $\gamma_i \colon D \to D$ being a linear operator

$$a_{i,0}\mathrm{id} + a_{i,1}\theta + \cdots + a_{i,n}\theta^n \tag{0.3}$$

with left coefficients in D. We write $D[\theta]$ for the set of maps (0.3), $D[\theta, n]$ for the set of maps (0.2) and $\mathrm{C}^{\sigma,\delta}(\theta)$ for the generalised centraliser of θ defined in [26, p. 314] by the formula $\theta(x) = \theta(1) \cdot x$. When $\theta = \sigma$, we recover the usual linear difference operators and the generalised centraliser is $\mathrm{Fix}(\sigma)$, and when $\theta = \delta$, we recover the usual linear differential operators, and the generalised centraliser is $\mathrm{Const}(\delta)$.

With addition and composition, $D[\theta]$ is a ring, isomorphic to the left Ore domain $D[t; \sigma, \delta]$ when the right dimension $[D : \mathrm{C}^{\sigma,\delta}(\theta)]$ is infinite. Since $D[\theta, n]$ is a $D[t; \sigma, \delta]$-module, we begin by elementary considerations about modules over a left Ore domain in Section 1, and study the basic properties of $D[\theta]$ and $D[\theta, n]$ in Section 2. In Section 3, we call a set defined by a system of equations like (0.1) a *θ-affine* set, and a map between θ-affine sets whose coordinate maps are in $D[\theta, n]$ a *θ-morphism*, and we point at a functor between the category of θ-affine sets and the

2010 *Mathematics Subject Classification.* 14R99, 14A22, 12E15, 03C45, 03C60.

Key words and phrases. Division ring, ring morphism, derivation, model theory.

Many thanks to the `http://MathOverflow.net/` community for a rich exchange of ideas. In particular to Tom De Medts for pointing at [30], leading to [24], which were a starting point for the present work. The author is also grateful to the referees for suggestions leading to a clearer version of the paper, and for pointing at pseudo-linear transformations.

category of finitely generated $D[t;\sigma,\delta]$-modules. In Section 4, we call (D,σ,δ,θ) *linearly surjective* if every nonzero $\gamma \in D[\theta]$ is surjective. Using results of P. Cohn on division ring extensions having sufficiently many roots, we show that if either σ or δ are inner, or if σ annd δ commute, then D has a linearly surjective extension $(E,\sigma',\delta',\theta')$. In such an extension, using Baur-Monk's quantifier elimination up to prime positive formulas for theories of modules, we show that Chevalley's Theorem for constructible sets holds, as well as a Nullstellensatz. Section 5 is devoted to defining and calculating the *Zariski dimension* of a θ-affine set V when $[D : \mathrm{C}^{\sigma,\delta}(\theta)]$ is infinite and σ surjective. By a diagonalisation argument due to Wedderburn, we show that the Zariski dimension of V is the unique $d \in \mathbf{N}$ such that V is θ-isomorphic to $D^d \times U$, where U is θ-affine of finite right $\mathrm{C}^{\sigma,\delta}(\theta)$-dimension. In Section 6, we study the θ-affine sets that do not have proper θ-affine subsets of the same Zariski dimension; we call such sets *radical*, and we provide a criterion inspired of [22, Lemma 2.8] and [19, Lemme 5.3] for certain θ-affine sets to be radical.

The paper is originally motivated by questions coming from model theory, aiming at understanding the complexity of the first-order theory $\mathrm{T}(D)$ of a division ring D in the ring language. Among these questions, (1) if $\mathrm{T}(D)$ has countably many pure types, is D commutative (from [41, Problem 12.6])? (2) Does $\mathrm{T}(D)$ satisfy Vaught's conjecture? (3) If $\mathrm{T}(D)$ does not have the independence property (see [35, Definition 4.1]), is the dimension $[D : \mathrm{Z}(D)]$ finite? The restricted setting presented in the paper, considering left modules (instead of bimodules) and almost forgetting about the role of the ring multiplication but reducing it to scalar left multiplication seems to be all that is needed to get a positive answer to (3) in characteristic p, presented in a further paper. But this setting is probably not enough to get an answer to (1), (2) or (3) in characteristic zero.

1. Linear Algebra in a Module over a left Ore domain

Throughout this Section, R is a *left Ore* domain (for any a, b in $R \setminus \{0\}$, the left ideal $Ra \cap Rb$ is nonzero), and M a left R-module. All modules considered in the paper are left modules.

1.1. **Basis and algebraicity.** A family $(v_1,\dots,v_n)$ in M is *dependent* if there is a nonzero tuple $(r_1,\dots,r_n)$ in R such that $r_1v_1+\cdots+r_nv_n=0$. It is a *basis* if it is independent and maximal such.

Lemma 1.1 (incomplete basis)**.** *Any independent family extends to a (possibly empty) basis.*

For all $S \subset M$, we write (S) for the R-submodule generated by S. If $\bar{b}$ is a basis of M, for every $v \in M \setminus \bar{b}$, the set $\bar{b} \cup \{v\}$ is dependent, and there is a nonzero $r \in R$ such that $rv \in (\bar{b})$.

Definition 1.2. We say that v *is algebraic over* S if there is a nonzero $r \in R$ such that $rv \in (S)$. For $A \subset M$, we say that A *is algebraic over* S if every $v \in A$ is algebraic over S.

Lemma 1.3 (transitivity of algebraicity)**.** *If A is algebraic over B and B is algebraic over C, then A is algebraic over C.*

Proof. Let a in A. By assumption, there are $r, r_1,\dots,r_n$ in $R \setminus \{0\}$ and a tuple $\bar{b}$ in B^n such that one has $ra \in (\bar{b})$ and $r_ib_i \in (C)$ for all $i \in \{1,\dots,n\}$. In particular, there is an expression of the form $sa \in (C) + \sum_{i\in I} s_ib_i$, with $s \in R \setminus \{0\}$, and one may choose the set $I \subset \{1,\dots,n\}$ of minimal cardinality. We claim that I is empty. Otherwise I contains some j. By Ore's condition, there are (u,v) in $R \setminus \{0\}$ such that $us_j = vr_j$ hence $us_jb_j \in (C)$, and one has $(us)a \in (C) + \sum_{i\in I\setminus\{j\}} us_ib_i$ with us nonzero as u and s are nonzero, a contradiction with the minimality of I. □

1.2. **Dimension.**

Theorem 1.4 (after Steinitz)**.** *All bases of M have the same cardinality.*

Proof. We treat the case where M has a finite basis $\bar{b} = (b_1, \dots, b_n)$. Let $(c_1, \dots, c_m, \dots)$ be another basis. By maximality of $\bar{b}$, one can write $rc_1 = \sum r_i b_i$ for some nonzero $r \in R$. As c_1 is independent, r_1 say is nonzero, so b_1 is algebraic over $(c_1, b_2, \dots, b_n)$. As M is algebraic over $\bar{b}$, by Lemma 1.3, M is algebraic over $(c_1, b_2, \dots, b_n)$. In a similar way, M is algebraic over $(c_1, c_2, b_3, \dots, b_n)$, and iterating, one can add every c_i. If $m > n$, one concludes that c_m is algebraic over its predecessors, a contradiction, so $m \leqslant n$, and all bases of M are finite. By symmetry, one has $n = m$. □

Definition 1.5. We write $\dim_R M$ and call *R-dimension* of M the cardinal of any basis of M.

Lemma 1.6 (sum)**.** *Let N be another R-module. One has*

$$\dim_R M \oplus N = \dim_R M + \dim_R N.$$

Proof. If $\bar{b}$ is a basis of M and $\bar{c}$ of N, then $\bar{b} \cup \bar{c}$ is an independent family of $M \oplus N$. If $u+v \in M \oplus N$, then u is algebraic over $\bar{b}$, as well as v over $\bar{c}$, so there are (s,t) in $R \setminus \{0\}$ such that $su \in (\bar{b})$ and $tv \in (\bar{c})$. By Ore's condition, there is $r \in R \setminus \{0\}$ such that $r(u+v) \in (\bar{b}, \bar{c})$, so $\bar{b} \cup \bar{c}$ is a basis. □

Lemma 1.7 (quotient)**.** *Let $N \subset M$ be a submodule. One has*

$$\dim_R M/N + \dim_R N = \dim_R M.$$

Proof. Let $\bar{b} + N$ be a basis for M/N and $\bar{c}$ a basis for N. Let us show that $\bar{b} \cup \bar{c}$ is a basis for M. If there is a linear combination $\gamma(\bar{x}) + \gamma'(\bar{y})$ vanishing in $(\bar{b}, \bar{c})$, one has $\gamma(\bar{b} + N) \in N$, so $\gamma = 0$ and $\gamma'(\bar{c}) = 0$, whence $\gamma' = 0$. The family $\bar{b} \cup \bar{c}$ is thus independent. If $v \in M$, by maximality of $\bar{b} + N$, there is $r \in R \setminus \{0\}$ and a linear combination γ such that $rv - \gamma(\bar{b}) \in N$. By maximality of $\bar{c}$, there is $s \in R \setminus \{0\}$ such that $srv - s\gamma(\bar{b}) \in (\bar{c})$. As sr is nonzero, v is algebraic over $\bar{b} \cup \bar{c}$. □

Definition 1.8. For any $S \subset M$, we write $\mathrm{cl}(S)$ for the set of algebraic elements over S.

Lemma 1.9 (algebraic closure)**.** *For all $S \subset M$, the set $\mathrm{cl}(S)$ is an R-module and*

$$\dim_R \mathrm{cl}(S) = \dim_R(S).$$

Proof. Let a and b in $\mathrm{cl}(S)$. For all $r \in R$, the element $a + rb$ is algebraic over $\{a, b\}$, which is algebraic over S, so $a + rb$ is algebraic over S by Lemma 1.3, and $\mathrm{cl}(S)$ is a submodule. A basis $\bar{b}$ for (S) is also a basis for $\mathrm{cl}(S)$ since $\mathrm{cl}(S)$ is algebraic over (S), hence over $\bar{b}$. □

Lemma 1.10 (Rank-Nullity)**.** *Let $f \colon M \to N$ be a morphism of R-modules. Then*

$$\dim_R \ker f + \dim_R \mathrm{im}\, f = \dim_R M.$$

Proof. Considering the induced bijection $M/\ker f \to \mathrm{im}\, f$ and in view of Lemma 1.7, we may assume without loss of generality that f is a bijection. In this case, it is straightforward that $(b_1, \dots, b_n)$ are independent in M if and only if $(f(b_1), \dots, f(b_n))$ are independent in N. □

Corollary 1.11. *Let $f \colon M \to N$ and $g \colon S \to M$ be morphisms of R-modules. Then*

$$\dim_R \ker f \circ g = \dim_R(\ker f \cap \mathrm{im}\, g) + \dim_R \ker g.$$

Proof. Usual proof using the Rank-Nullity Lemma. □

2. Twists over division rings

Our initial setting is the one introduced in [32], which provides a uniform framework to deal with difference and differential equations. Let D be a division ring and $\sigma\colon D \to D$ a nonzero ring morphism. Let $\delta\colon D \to D$ be a σ-*derivation*, that is, satisfying

$$\delta(x+y) = \delta(x) + \delta(y) \qquad \text{and} \qquad \delta(xy) = \sigma(x)\delta(y) + \delta(x)y \quad \text{for any } (x,y) \in D^2.$$

We write $D[t;\sigma,\delta]$ for the Ore domain of left polynomials $a_0 + a_1 t + \cdots + a_n t^n$ with usual addition, and skew multiplication induced by the rule

$$t \cdot a = \sigma(a)t + \delta(a). \tag{2.1}$$

When δ is zero, we simply write $D[t;\sigma]$.

2.1. 1-Twists.

Let $\theta\colon D \to D$ be a *pseudo-linear transformation* in the sense of [20], that is,

$$\theta(x+y) = \theta(x) + \theta(y) \qquad \text{and} \qquad \theta(xy) = \sigma(x)\theta(y) + \delta(x)y \quad \text{for any } (x,y) \in D^2. \tag{2.2}$$

For any element a in D, the map $\theta_a = \sigma \cdot a + \delta$ is a pseudo-linear transformation, and conversely, a pseudo-linear θ satisfies $\theta(x) = \sigma(x) \cdot \theta(1) + \delta(x)$, so that $\theta = \theta_a$ for $a = \theta(1)$ (from [7, Lemma 3]). We sometimes write θ_a instead of θ when we want to stress on the element $a = \theta(1)$.

We define the set $D[\theta]$ of 1-*twists* by

$$D[\theta] = \left\{ \sum_{i=0}^{n} a_i \theta^i \colon \bar{a} \in D^{n+1},\ n \in \mathbf{N} \right\}.$$

By (2.2), one has the equality $\theta \circ a\theta^n = \sigma(a)\theta^{n+1} + \delta(a)\theta^n$, so that $(D[\theta], +, \circ)$ is a unitary ring, with the convention $\theta^0 = \mathrm{id}$. One can show that the map $a_0 + \cdots + a_n t^n \mapsto a_0\mathrm{id} + \cdots + a_n\theta^n$ is a ring morphism from $D[t;\sigma,\delta]$ to $D[\theta]$. In particular, any pseudo-linear transformation θ defines a structure of $D[t;\sigma,\delta]$-module on D by

$$(g(t), a) \mapsto g(t) \cdot a = g(\theta)(a).$$

Conversely any structure of $D[t;\sigma,\delta]$-module on D (that extends the natural structure of D-module of D) is induced by the action $a \mapsto t \cdot a$, which is a pseudo-linear transformation since, by (2.1),

$$t \cdot a = (t \cdot a) \cdot 1 = (\sigma(a)t + \delta(a)) \cdot 1 = \sigma(a)(t \cdot 1) + \delta(a) = \theta_{t\cdot 1}(a).$$

Any nonzero $\gamma \in D[\theta]$ has a (possibly non unique) expression of the form $a_0\mathrm{id} + a_1\theta + \cdots + a_n\theta^n$ with $a_n \neq 0$. We call a minimal such n the *degree* of γ, written $\deg(\gamma)$, and also define $\deg(0) = -\infty$.

Lemma 2.1 (Euclidean division)**.** *For all nonzero $\rho \in D[\theta]$ and all $\gamma \in D[\theta]$,*

1. *there is $(q,r) \in D[\theta] \times D[\theta]$ such that $\gamma = q\rho + r$ and $\deg(r) < \deg(\rho)$.*
2. *if σ is onto, there is $(q,r) \in D[\theta] \times D[\theta]$ such that $\gamma = \rho q + r$ and $\deg(r) < \deg(\rho)$.*

Proof. This follows from Ore's [32, Theorem 6] stating that the skew polynomial ring $D[t;\sigma,\delta]$ is right Euclidean, and when σ is onto also left Euclidean, and from the fact that the map $\sum a_i t^i \mapsto \sum a_i\theta^i$ is a ring morphism from $D[t;\sigma,\delta]$ to $D[\theta]$ (see [7, Theorem 1] or [28, Corollary 1.3]). □

Lemma 2.2 (factorisation)**.** *Let $\gamma \in D[\theta]$ of degree $n+1$ having a nonzero root b. There is $q \in D[\theta]$ of degree n such that $\gamma = q(\theta - \theta(b)b^{-1}\mathrm{id})$.*

Proof. Since γ has degree $n+1$, the map θ cannot be a left homothety. It follows that $\theta - \theta(b)b^{-1}\mathrm{id}$ is nonzero and has degree 1. By Lemma 2.1.1, there are $q \in D[\theta]$ and $r \in D$ such that γ equals $q(\theta - \theta(b)b^{-1}\mathrm{id}) + r \cdot \mathrm{id}$. Since $\gamma(b) = 0$, one must have $r = 0$. □

Following the notation in [26, p. 314], we define the *generalised centraliser* $\mathrm{C}^{\sigma,\delta}(\theta)$ by

$$\mathrm{C}^{\sigma,\delta}(\theta) = \{x \in D \colon \theta(x) = \theta(1) \cdot x\}\,.$$

In the particular case when $\theta(x) = x \cdot a$, then $\mathrm{C}^{\sigma,\delta}(\theta)$ is the usual centraliser of a. When $\theta = \sigma$, then $\mathrm{C}^{\sigma,\delta}(\sigma)$ is the *division ring fixed by* σ, defined by $\sigma(x) = x$, and in the case $\theta = \delta$, then $\mathrm{C}^{\sigma,\delta}(\delta)$ is the *division ring of constants of* δ, defined by $\delta(x) = 0$. From [26, Lemma 3.2.(1)], one has:

Lemma 2.3. *The centraliser $\mathrm{C}^{\sigma,\delta}(\theta)$ is a division ring, and any $\gamma \in D[\theta]$ is right $\mathrm{C}^{\sigma,\delta}(\theta)$-linear.*

Proof. For any $c \in \mathrm{C}^{\sigma,\delta}(\theta)$, one has $\theta_a(c) = a \cdot c$. By (2.2), for any $x \in D$, one has

$$\theta_a(xc) = \sigma(x)\theta_a(c) + \delta(x)c = \sigma(x)a \cdot c + \delta(x)c = \theta_a(x)c. \tag{2.3}$$

It follows from (2.3) that $\mathrm{C}^{\sigma,\delta}(\theta)$ is a ring, and that any $\gamma \in D[\theta]$ is right $\mathrm{C}^{\sigma,\delta}(\theta)$-linear. The formula $\delta(x^{-1}) = -\sigma(x^{-1})\delta(x)x^{-1}$ also provides us with

$$\theta_a(x^{-1}) = \sigma(x^{-1})\Big(a \cdot x - \delta(x)\Big)x^{-1}, \tag{2.4}$$

from which follows that $\mathrm{C}^{\sigma,\delta}(\theta)$ is a division ring. □

Lemma 2.4 (kernel of a twist)**.** *The kernel of a 1-twist of degree $n \in \mathbf{N}$, is a right $\mathrm{C}^{\sigma,\delta}(\theta)$-vector space of dimension at most n. Conversely, a right $\mathrm{C}^{\sigma,\delta}(\theta)$-vector subspace of D of dimension $n \in \mathbf{N}$ is the kernel of a 1-twist of degree n (or $-\infty$).*

Proof. The first statement of Lemma 2.4 can probably be derived from [26, Theorem 4.2]. Here is a short alternative proof by induction on n, beginning with a twist $\theta - r\mathrm{id}$ of degree 1. If x and y are nonzero roots of $\theta_a - r\mathrm{id}$, one has $rx - \delta(x) = \sigma(x)a$, so by (2.4), $\theta_r(x^{-1}) = ax^{-1}$. By (2.2) follows

$$\theta_a(x^{-1}y) - ax^{-1}y = \sigma(x^{-1})ry + \delta(x^{-1})y - ax^{-1}y = (\theta_r(x^{-1}) - ax^{-1})y = 0,$$

so x and y are right $\mathrm{C}^{\sigma,\delta}(\theta)$-dependent. Now if γ has degree $n+1$ and has a nonzero root, by Lemma 2.2, one has $\gamma = q\gamma'$ where q has degree n and γ' has degree 1. Since γ, q and γ' are right $\mathrm{C}^{\sigma,\delta}(\theta)$-linear maps, by Corollary 1.11 and induction hypothesis, one has $\dim\ker\gamma \leqslant \dim\ker q + \dim\ker\gamma' \leqslant n+1$. For the converse, we consider a right $\mathrm{C}^{\sigma,\delta}(\theta)$-vector subspace of D of dimension n spanned by $(r_1, \ldots, r_n)$. We define $\gamma_n \in D[\theta]$ inductively by putting $\gamma_1 = \theta_a - \theta_a(r_1)r_1^{-1}\mathrm{id}$ and $\gamma_{i+1} = (\theta_a - a \cdot \mathrm{id}) \circ \gamma_i(r_{i+1})^{-1} \cdot \gamma_i$. An immediate induction shows that γ_i has degree at most i, that $\mathrm{span}(r_1, \ldots, r_i) = \ker\gamma_i$ so that $\gamma_i(r_{i+1})$ is nonzero and γ_{i+1} is well defined. □

As in [26, Corollary 4.4], specifying $\theta = \delta$ in Lemma 2.4 yields [11, Theorem 3.7.1] (or Amitsur's [1, Theorem 1] when σ is onto) stating that the kernel of a differential operator $\sum a_i\delta^i$ of degree n has right dimension at most n over the the division ring of constants. Taking $\theta = \sigma$ yields that the kernel of a difference operator $\sum a_i\sigma^i$ of degree n has right dimension at most n over the division ring fixed by σ. Taking $\theta(x) = x \cdot a$ yields that the kernel of the map $a_0x + \cdots + a_nxa^n$ has right dimension at most n over the centraliser of a, and if D is a field of characteristic p, taking $\theta(x) = x^p$ yields that a p-polynomial $a_0x + \cdots + a_nx^{p^n}$ has at most p^n roots.

Corollary 2.5. *The rings $D[t;\sigma,\delta]$ and $D[\theta]$ are isomorphic if and only if $[D : \mathrm{C}^{\sigma,\delta}(\theta)]_{\mathrm{rt}} = +\infty$.*

We call *θ-division ring* any division ring (D, σ, δ) equipped with a ring morphism σ, a σ-derivation δ and a pseudo-linear map θ. We say that D is *strict* if the right dimension $[D : \mathrm{C}^{\sigma,\delta}(\theta)]_{\mathrm{rt}}$ is infinite.

Corollary 2.6. *If D is a strict θ-division ring, then $D[\theta]$ is a left Noetherian and left Ore domain.*

2.2. **n-Twists and twisted Zariski topology.** We write $D[\theta, n]$ for the set of maps $\gamma\colon D^n \to D$ of the form $\gamma_1(x_1) + \cdots + \gamma_n(x_n) + c$ where $\gamma_1, \ldots, \gamma_n$ are in $D[\theta]$ and c in D.

Definition 2.7. Let the *twisted Zariski topology* on D^n be the topology whose basic closed sets are of the form $\{(x_1, \ldots, x_n) \in D^n\colon \gamma(x_1, \ldots, x_n) = 0 \text{ for all } \gamma \in S\}$ where S is a subset of $D[\theta, n]$.

Since $D[\theta, n]$ is a finitely generated module over the left Noetherian ring $D[\theta]$, it is a Noetherian module by [6, Proposition 7 p. 26], and the twisted Zariski topology is Noetherian.

Lemma 2.8. *A basic Zariski closed subset of D is a right $\mathrm{C}^{\sigma,\delta}(\theta)$-affine subspace of finite dimension.*

Proof. This follows from Lemma 2.4. □

Lemma 2.9. *A basic Zariski closed subset of D^n meets a right D-line either trivially or in a right $\mathrm{C}^{\sigma,\delta}(\theta)$-affine space of finite dimension.*

Proof. It suffices to consider a basic closed set V defined by a single equation $\gamma(x_1, \ldots, x_n) = 0$. Let L be a right D-line given by $\{x_1 = a_1 x_j + b_1, \ldots, x_n = a_n x_j + b_n\}$ for some $j \in \{1, \ldots, n\}$ and tuples $\bar{a}, \bar{b}$ in D. Replacing every x_i by $a_i x_j + b_i$ in the equation $\gamma(\bar{x}) = 0$ yields an equation of the form $\gamma'(x_j) = 0$ for some $\gamma' \in D[\theta, 1]$ and one concludes with Lemma 2.4. □

Lemma 2.10. *If $\mathrm{C}^{\sigma,\delta}(\theta)$ is infinite, the irreducible closed subsets of D^n are the basic closed sets.*

Proof. Let V be a nonempty basic closed set covered by a finite union $V_1 \cup \cdots \cup V_q$ of basic closed subsets. Translating V, we may assume that V is an additive group. By Neumann's [31, Lemma 4.1], one V_i is a subgroup of V of finite index. Since V/V_i is a right $C^{\sigma,\delta}(\theta)$-vector space, one must have $V = V_i$, so V is irreducible. Conversely, an irreducible closed set is a basic closed set. □

3. Elementary θ-algebraic geometry

Throughout this Section, we consider a θ-division ring D and introduce basic notions directly inspired from classical algebraic geometry.

Definition 3.1. We call *θ-affine set* the zero set of a family S of n-twists, which we write

$$\mathrm{V}(S) = \{(x_1, \ldots, x_n) \in D^n\colon \gamma(x_1, \ldots, x_n) = 0 \text{ for all } \gamma \in S\}\,.$$

Definition 3.2. Given $\Delta \subset D^n$, we call *module of* Δ and write $\mathrm{I}(\Delta)$ the set defined by

$$\mathrm{I}(\Delta) = \{\gamma \in D[\theta, n]\colon \gamma(x_1, \ldots, x_n) = 0 \text{ for all } (x_1, \ldots, x_n) \in \Delta\}\,.$$

Any θ-affine set is right $C^{\sigma,\delta}(\theta)$-affine, and any module $\mathrm{I}(\Delta)$ is a left $D[\theta]$-submodule of $D[\theta, n]$. Since $D[\theta, n]$ is a Noetherian module, a θ-affine set is the zero set of a finite family of twists.

Remark 3.3. Given a polynomial $g \in D[t; \sigma, \delta]$, the map $D[t; \sigma, \delta] \to D[\theta]$ suggests to define $\mathrm{V}(g) = \mathrm{V}(g(\theta)) = \{x \in D\colon g(\theta)(x) = 0\}$. In [27, (2.7) p.46], another definition of $\mathrm{V}(g)$ is introduced, defined (with our notation $\theta_a = \sigma \cdot a + \delta$) by $\mathrm{V}(g) = \{a \in D\colon g(\theta_a)(1) = 0\}$. These definitions are not the same. If $g(t) = \sum b_i t^i$ and in the particular case $(\sigma, \delta) = (\mathrm{id}, 0)$, the former gives the linear subset $\left\{x \in D\colon \sum b_i x a^i = 0\right\}$, whereas the later gives the more usual $\left\{a \in D\colon \sum b_i a^i = 0\right\}$.

We push on the analogy with classical algebraic geometry and define the corresponding notions of morphisms: *θ-morphisms* for θ-affine sets, and usual morphisms of $D[\theta]$-modules for modules.

Definition 3.4. We call *θ-morphism* a map between θ-affine sets whose coordinates are twists. We call *θ-isomorphism* a bijective θ-morphism whose inverse is also a θ-morphism.

In classical algebraic geometry, there is a functor between the category of affine algebraic sets over a field k and the category of finitely generated k-algebras, which witnesses a duality between these two categories (see *e.g.* [18, p. 19]). In our case, there is a functor Γ between the category of θ-affine sets, and the category of finitely generated $D[\theta]$-modules.

Definition 3.5. Given a θ-affine subset V of D^n, we let $\Gamma(V)$ be the $D[\theta]$-module defined by

$$\Gamma(V) = D[\theta, n]/\mathrm{I}(V).$$

Given a θ-morphism $f\colon U \to V$, we let $\Gamma(f)$ be the morphism $\Gamma(f)\colon \Gamma(V) \to \Gamma(U)$ defined by

$$\Gamma(f)\colon \gamma + \mathrm{I}(V) \mapsto \gamma \circ f + \mathrm{I}(U).$$

Given two θ-affine sets U and V, we write $\mathrm{Hom}(U, V)$ for the set of θ-morphisms from U to V, and $\mathrm{Hom}(\Gamma(V), \Gamma(U), 1)$ for the set of morphisms of $D[\theta]$-modules from $\Gamma(V)$ to $\Gamma(U)$ fixing 1.

Lemma 3.6. *The map* $\Gamma : \mathrm{Hom}(U, V) \to \mathrm{Hom}(\Gamma(V), \Gamma(U), 1)$ *is bijective.*

Proof. Γ is injective, and we show that it is surjective as in [18, Proposition 1.33]. If $\phi : \Gamma(V) \to \Gamma(U)$ is a given morphism of $D[\theta]$-modules that fixes 1, where $U \subset D^n$ and $V \subset D^m$, there is a morphism of $D[\theta]$-modules $\bar{\phi}$ such that $\bar{\phi}(1) = 1$ and such that the following diagram commutes.

$$\begin{array}{ccc} D[\theta, m] & \xrightarrow{\bar{\phi}} & D[\theta, n] \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ \Gamma(V) & \xrightarrow{\phi} & \Gamma(U) \end{array}$$

We define a θ-morphism $f\colon D^n \to D^m$ putting $f = \left(\bar{\phi}(x_1), \ldots, \bar{\phi}(x_m)\right)$. Since $\bar{\phi}$ is a morphism of $D[\theta]$-modules and since $\bar{\phi}(1) = 1$, for any m-twist $\gamma = \gamma_1(x_1) + \cdots + \gamma_m(x_m) + r$, one has

$$\bar{\phi}(\gamma) = \bar{\phi}(\gamma_1(x_1) + \cdots + \gamma_m(x_m) + r) = \gamma_1(\bar{\phi}(x_1)) + \cdots + \gamma_m(\bar{\phi}(x_m)) + r = \gamma \circ f,$$

and according to the above diagram, one has $\phi \circ \pi_1(\gamma) = \pi_2(\gamma \circ f)$. This shows that $\gamma \in \mathrm{I}(V)$ implies $\gamma \circ f \in \mathrm{I}(U)$, so that f maps U to V. This also shows that $\phi = \Gamma(f)$, so Γ is surjective. □

Corollary 3.7. *A θ-morphism f is a θ-isomorphism if and only if $\Gamma(f)$ is an isomorphism.*

Proof. As in [36, Corollary 11.4.5], if $f\colon U \to V$ is a θ-isomorphism then the inverse of $\Gamma(f)$ is $\Gamma(f^{-1})$. Conversely, if $\phi \in \mathrm{Hom}(\Gamma(U), \Gamma(V))$ satisfies $\Gamma(f) \circ \phi = \mathrm{id}_{\Gamma(U)}$ and $\phi \circ \Gamma(f) = \mathrm{id}_{\Gamma(V)}$, then ϕ fixes 1, so $\phi = \Gamma(g)$ for some θ-morphism $g\colon V \to U$ by Lemma 3.6. One thus has $\Gamma(f) \circ \Gamma(g) = \Gamma(g \circ f) = \Gamma(\mathrm{id}_U)$, whence $g \circ f = \mathrm{id}_U$ and symmetrically $f \circ g = \mathrm{id}_V$. □

We call a θ-morphism $f\colon U \to V$ *dominant* if $f(U)$ is dense in V for the twisted Zariski topology, and a *closed immersion* if $f(U)$ is Zariski closed in V and $f\colon U \to f(U)$ is a θ-isomorphism. One has the analogue of [17, Theorem 4.88]:

Lemma 3.8. *Let $f\colon U \to V$ be a θ-morphism with U irreducible. Then,*

1. *$\Gamma(f)$ is injective if and only if f is dominant,*
2. *$\Gamma(f)$ is surjective if and only if f is a closed immersion.*

Proof. Towards point (1), since $\Gamma(f)$ sends $\gamma + \mathrm{I}(V)$ to $\gamma \circ f + \mathrm{I}(U)$, the statement $\Gamma(f)$ is injective is equivalent to $\gamma \in \mathrm{I}(V) \iff \gamma \circ f \in \mathrm{I}(U)$. Since $\gamma \circ f \in I(U)$ is equivalent to $\gamma \in \mathrm{I}(f(U))$, one has that $\Gamma(f)$ is injective if and only if $\mathrm{I}(V) = \mathrm{I}(f(U))$, which holds if and only if $\mathrm{VI}\,(f(U)) = V$. But f is continuous for the twisted Zariski topology, so $f(U)$ is irreducible, and the Zariski closure of $f(U)$ is precisely $\mathrm{VI}\,(f(U))$. For point (2) if f is a closed immersion, then there is a θ-morphism $f^{-1}\colon f(U) \to U$ with $f^{-1} \circ f = \mathrm{id}_U$. But f^{-1} is the restriction of some θ-morphism $g\colon V \to D^n$, so $\Gamma(f)$ is surjective. Conversely, if $\Gamma(f)$ is surjective, let $\bar{f}$ denote the restriction $\bar{f}\colon U \to \overline{f(U)}$. Then also $\Gamma(\bar{f})$ is surjective. By point (1), $\Gamma(\bar{f})$ is bijective, and by Corollary 3.7, $\bar{f}$ is a θ-isomorphism, so f is a closed immersion. □

4. Linearly surjective θ-division rings

In classical algebraic geometry, over an algebraically closed field k, Hilbert's Nullstellensatz makes the duality between affine algebraic sets and reduced finitely generated k-algebras an equivalence of categories, where irreducible algebraic sets correspond to integral finitely generated k-algebras. In our case, the analogue of irreducible sets is the one of *radical* sets, and analogue of algebraically closed fields seem to be *linearly surjective* division rings, over which the category of radical θ-affine sets is equivalent to the category of torsion-free finitely generated $D[\theta]$-modules.

Extending the definition in [2, p. 215] given for differential fields, although the terminology *linearly-closed* exists for difference fields (see *e.g.* [34, Lemma 9.1 p. 17] or [33, Definition 4.3 p. 15]), we suggest

Definition 4.1. We call a θ-division ring D *linearly surjective* if every nonzero $\gamma \in D[\theta]$ is surjective, or equivalently if D, as a $D[\theta]$-module, is divisible.

Remark 4.2. If D is linearly surjective, then $\theta_a - a \cdot \mathrm{id}$ is surjective but not injective. By the Rank-Nullity Theorem, D must be strict.

4.1. Linearly surjective extensions.

Following [14, p. 58],

Definition 4.3 (θ-extension)**.** Given a θ-division ring (D, σ, δ) considered with a pseudo linear transformation $\theta_a = \sigma \cdot a + \delta$, we call *$\theta$-extension* of D any division ring (E, σ', δ') extending D and equipped with a ring morphism $\sigma'\colon E \to E$ extending $\sigma\colon D \to D$ and with σ'-derivation $\delta'\colon E \to E$ extending $\delta\colon D \to D$, and considered with the pseudo-linear $\sigma' \cdot a + \delta'$ that extends θ_a.

In the case of a commutative field, by [7, Lemma 1], a pseudo-linear map is either a linear difference operator, or a linear differential operator for a usual derivation, so the two cases of the following Lemma exhaust all the possible pseudo-derivations.

Lemma 4.4. *If k is a commutative field, any difference field (k, σ) or differential field (k, δ) has a linearly surjective commutative extension.*

Proof. In the difference case, this is observed in [8, Lemma 2.11]. In the differential case, we proceed similarly: as the theory of differential fields extending k has $\forall\exists$ axioms (or equivalently is closed under chains of models), it has an existentially closed model K. Now let $\gamma = 1 + a_0\mathrm{id} + a_1\delta + \cdots + a_n\delta^n$ with $a_i \in k$, $a_n \in k^\times$ and $n > 0$. We consider the domain $R = k[x_0, \ldots, x_{n-1}]$, and extend δ to R letting $\delta(x_i) = x_{i+1}$ for $i < n-1$ and $\delta(x_{n-1}) = \gamma(x_0) + \delta^n(x_0)$, so that $\gamma(x_0) = 0$. Then δ extends to a unique derivation of the fraction field $k(x_0, \ldots, x_{n-1})$ by [23, 4 p.10 and Theorem 1.1]. This shows that K is linearly surjective. Another point of view is to consider the domain $k\{x\}$ of *differential polynomials* in one variable x, which is a differential extension of k, and the *differential*

ideal $\{\gamma\}$ generated by γ. One can show that $1 \notin \{\gamma\}$, so $\{\gamma\}$ is contained in a maximal differential proper ideal I. By [2, Corollary 4.6.7], $k\{x\}/I$ is a differential domain, where $x + I$ is a solution of the equation $\gamma = 0$, and the field of fraction of $k\{x\}/I$ is a differential extension of k. □

We write σ_b for the *inner automorphism* $x \mapsto b^{-1}xb$ induced by $b \in D^\times$, and δ_c for the *inner* σ*-derivation* $x \mapsto \sigma(x)c - cx$ induced by $c \in D$.

Theorem 4.5. *Any θ-division ring has a linearly surjective θ-extension provided that either δ and σ commute, or σ be inner, or δ be inner.*

Proof. We split the proof into several cases, beginning with the most elementary one.

Case 1. *$\delta = 0$ and $\sigma = \mathrm{id}$, so that $\theta_a = \mathrm{id} \cdot a$, and a is transcendental over $\mathrm{Z}(D)$.* As a referee says, the theory of division rings with centre $\mathrm{Z}(D)$ extending D has $\forall\exists$ axioms, hence has an existentially closed model $\mathbf{D}$. So a is transcendental over $\mathrm{Z}(D) = \mathrm{Z}(\mathbf{D})$. By [9, Theorem 2], for all $(b, c) \in \mathbf{D}^2$, the equation $xa - bx = c$ has a solution in $\mathbf{D}$. To finish the first case, it is enough to show that, in $\mathbf{D}$, any $\gamma \in \mathbf{D}[\theta]$ factorises in products of 1-twists of degree 1.

Claim 1. *Let D be a division ring. Assume that every polynomial $x^n + x^{n-1}r_1 + \cdots + xr_n + r_{n+1}$ with $(r_1, \ldots, r_{n+1}) \in D^{n+1}$ has a root in D. Denote by*

$$e_i(x_1, \ldots, x_n) = \sum_{1 \leqslant j_1 < \cdots < j_i \leqslant n} x_{j_i} \cdots x_{j_1}$$

the ith elementary (non) symmetric polynomial. For any $(a_1, \ldots, a_n) \in D^n$, the polynomial system

$$\Sigma_n(\bar{a}) = \{e_1(x_1, \ldots, x_n) = a_1, \ldots, e_n(x_1, \ldots, x_n) = a_n\}$$

has a solution $(x_1, \ldots, x_n)$ in D.

Proof of Claim 1. We proceed by induction on n, the case $n = 1$ being trivial. Assume that the conclusion holds for any system Σ_n of n such polynomial equations, and consider the system $\Sigma_{n+1}(\bar{a})$. Putting $\bar{x} = (x_1, \ldots, x_n)$, one has the following equivalences:

$$\begin{cases} a_1 = x_1 + \cdots + x_n + x_{n+1} \\ a_2 = x_{n+1}x_n + \cdots + x_2x_1 \\ \vdots \\ a_{n+1} = x_{n+1}x_n \cdots x_1 \end{cases} \iff \begin{cases} a_1 - x_{n+1} = e_1(\bar{x}) \\ a_2 = x_{n+1}e_1(\bar{x}) + e_2(\bar{x}) \\ a_3 = x_{n+1}e_2(\bar{x}) + e_3(\bar{x}) \\ \vdots \\ a_n = x_{n+1}e_{n-1}(\bar{x}) + e_n(\bar{x}) \\ a_{n+1} = x_{n+1}e_n(\bar{x}) \end{cases}$$

$$\iff \begin{cases} a_1 - x_{n+1} = e_1(\bar{x}) \\ a_2 - x_{n+1}(a_1 - x_{n+1}) = e_2(\bar{x}) \\ a_3 - x_{n+1}(a_2 - x_{n+1}(a_1 - x_{n+1})) = e_3(\bar{x}) \\ \vdots \\ a_n - x_{n+1}(a_{n-1} - x_{n+1}(\cdots x_{n+1}(a_1 - x_{n+1})\cdots)) = e_n(\bar{x}) \\ a_{n+1} = x_{n+1}[a_n - x_{n+1}(a_{n-1} - x_{n+1}(\cdots x_{n+1}(a_1 - x_{n+1})\cdots))] \end{cases}$$

The last line is a one variable nontrivial polynomial equation, which reads

$$a_{n+1} - x_{n+1}a_n + x_{n+1}^2a_{n-1} + \cdots + (-x_{n+1})^n a_1 + (-x_{n+1})^{n+1} = 0,$$

and has a solution $b_{n+1} \in D$ by assumption. Replacing x_{n+1} by b_{n+1} in the n first equations of the last system gives a subsystem $\Sigma_n(\bar{c})$ for some precise tuple $\bar{c} \in D^n$. By induction hypothesis, $\Sigma_n(\bar{c})$ has a solution $(b_1, \ldots, b_n) \in D^n$, so that $(b_1, \ldots, b_{n+1})$ is a solution of $\Sigma_{n+1}(\bar{a})$, as desired. □

We continue the proof of Case 1 of Theorem 4.5, claiming that for any $\gamma \in \mathbf{D}[\theta]$ of the form $xa^n + a_1xa^{n-1} + a_2xa^{n-2} + \cdots + a_nx$, there is $\bar{b} \in \mathbf{D}^n$ such that the following factorisation holds:

$$\gamma(x) = (xa + b_nx) \cdots (xa + b_1x).$$

For every $\bar{x} = (x_1, \ldots, x_n) \in \mathbf{D}^n$, one has

$$(xa + x_nx) \cdots (xa + x_1x) = xa^n + e_1(\bar{x})xa^{n-1} + e_2(\bar{x})xa^{n-2} + \cdots + e_n(\bar{x})x \tag{4.1}$$

By [11, Theorem 8.5.1], the polynomial $x^n + x^{n-1}r_1 + \cdots + xr_n + r_{n+1}$ has a root in $\mathbf{D}$ for every $(r_1, \ldots, r_{n+1}) \in \mathbf{D}^{n+1}$. By Claim 1, the system $\{e_1(\bar{x}) = a_1, \ldots, e_n(\bar{x}) = a_n\}$ has a solution $\bar{b} \in \mathbf{D}^n$. By (4.1), one has $\gamma(x) = (xa + b_nx) \cdots (xa + b_1x)$, as desired.

Case 2. *$\delta = 0$ and $\sigma = \mathrm{id}$, so that $\theta_a = \mathrm{id} \cdot a$.* By Case 1, we may assume that a is algebraic over $\mathrm{Z}(D)$. We first claim that (D, id) has an extension (D_2, σ_t) with centre $\mathrm{Z}(D_2) = \mathrm{Z}(D)$ where t is transcendental over $\mathrm{Z}(D_2)$. Consider the division ring $D_1 = D(x)$ where x is a central indeterminate, and the ring morphism $\tau\colon g(x) \mapsto g(x^2)$. Then no power of τ is inner since τ is not even surjective, and the division subring fixed by τ is D. Consider the (left) Ore domain $D_1[t; \tau]$ with multiplication rule $r \cdot t = t\tau(r)$. Its division ring of (left) fractions, let's call it D_2, has centre $Z(D)$ by [12, Theorem 7.3.6]. It follows that t is transcendental over $\mathrm{Z}(D_2) = \mathrm{Z}(D)$, and t commutes with D, so that (D_2, σ_t) extends (D, id). Now, putting $b = ta$, for each y in (D_2, σ_t), one has

$$\theta_a(y) = \sigma_t(y) \cdot a = t^{-1}xb. \tag{4.2}$$

If $a = 0$, there is nothing to show and if $a \neq 0$, then b is transcendental over $\mathrm{Z}(D_2)$ (it follows indeed from Brauer's Lemma, see *e.g.* [11, Corollary 3.3.9], that the algebraic elements over $\mathrm{Z}(D_2)$ form a division subring of D_2). By Case 1, $(D_2, \mathrm{id}, 0, \mathrm{id} \cdot b)$ has a linearly surjective extension $(D_3, \mathrm{id}, 0, \mathrm{id} \cdot b)$. In particular, from (4.2), $(D_3, \sigma_t, 0, \theta_a)$ is linearly surjective.

Case 3. *Both σ and δ are inner.* Then $\sigma = \sigma_b$ and $\delta = \sigma \cdot c - c \cdot \mathrm{id}$ for some $b \in D^\times$ and $c \in D$. One thus has

$$\theta_a(x) = \sigma(x)a + \sigma(x)c - cx = b^{-1}xb(a + c) - cx. \tag{4.3}$$

By Case 2 the division ring $(D, \mathrm{id}, 0, \mathrm{id} \cdot b(a + c))$, has a linearly surjective extension $(D_1, \sigma_t, 0, \sigma_t \cdot b(a + c))$. It follows that the extension $(D_1, \sigma_{tb}, \sigma_{tb} \cdot c - c \cdot \mathrm{id}, \theta_a)$ of $(D, \sigma, \delta, \theta_a)$ is linearly surjective.

Case 4. *Only σ is inner.* Then $\sigma = \sigma_b$ for some $b \in D^\times$. In the Ore domain $D[t; \sigma, \delta]$, the multiplication rule $\sigma(r)t = tr + \delta(r)$ shows that $\delta_t = \sigma_b \cdot t - t \cdot \mathrm{id}$ extends δ. By [11, Proposition 2.1.2], δ_t extends uniquely to the division ring of fractions of $D[t; \sigma, \delta]$, and we are back to Case 3.

Case 5. *Only δ is inner.* Then $\delta = \sigma \cdot c - c \cdot \mathrm{id}$ for some $c \in D$. In the (left) Ore domain $D[t; \sigma]$, the multiplication rule $r \cdot t = t\sigma(r)$ shows that the conjugation σ_t extends σ, and we extend δ to $D[t; \sigma]$ by $\delta' = \sigma_t \cdot c - c \cdot \mathrm{id}$. By [11, Proposition 2.1.2], δ' extends uniquely to the division ring of (left) fractions of $D[t; \sigma]$, and we are back to Case 3.

Case 6. *The maps σ and δ commute.* In $D[t; \sigma]$ with rule $r \cdot t = t\sigma(r)$, the conjugation σ_t extends σ. Since σ and δ commute, by [40, Theorem 2.3], the map δ extends to a σ_t-derivation of $D[t; \sigma]$ by putting $\delta(t) = 0$ (see also [10, Exercise 2 p.57]), and δ extends uniquely to a σ_t-derivation of the division ring of (left) fractions of $D[t; \sigma]$, so we are back to Case 4. □

4.2. **Constructible subsets and Chevalley's projection Theorem.** Given a θ-division ring D, we call a subset of D^n *constructible* if it is a finite boolean combination of closed sets for the twisted Zariski topology, that is, a boolean combination of θ-affine sets.

Theorem 4.6 (after Chevalley)**.** *Let D be linearly surjective and f a θ-morphism.*

(1) *The image by f of a closed set is closed.*
(2) *The image by f of a constructible set is constructible,*

Proof. The classical version of Chevalley's Theorem is an immediate consequence of Tarski's quantifier elimination in algebraically closed fields, and we proceed similarly by quantifier elimination.

Claim 2. *Given a right Euclidean ring R (in the sense of Lemma 2.1.1) and matrices A, B in $\mathcal{M}_{m,n}(R)$, there is C in $\mathcal{M}_{m,n}(R)$ such that for all divisible R-module M and $\bar{y}$ in M^n, one has*

$$C\bar{y} = 0 \iff \exists \bar{x} \in M^n \, (A\bar{x} = B\bar{y}) \, .$$

Proof of Claim 2. Arguing as in [16, Proposition 6.1], one can find invertible square matrices P and Q (where Q has coefficients in $\{0, 1\}$), and an upper triangular matrix

$$T = \begin{pmatrix} T_1 \\ 0 \end{pmatrix}$$

with T_1 upper triangular having nonzero diagonal coefficients, such that $A = P \cdot T \cdot Q$. The formula $\exists \bar{x} \in M^n \, (A\bar{x} = B\bar{y})$ is equivalent to $\exists \bar{x} \in M^n (T\bar{x} = C\bar{y})$ where $C = P^{-1}Q$. Writing $C = (C_1, C_2)$ by blocks compatible with $T = (T_1, 0)$, the formula $\exists \bar{x} \in M^n (T\bar{x} = C\bar{y})$ reads

$$\exists \bar{x} \in M^n \, (T_1\bar{x} = C_1\bar{y}) \wedge C_2\bar{y} = 0.$$

As M is divisible, the formula $\exists \bar{x} \in M^n \, (T_1\bar{x} = C_1\bar{y})$ is satisfied by any tuple $\bar{y}$ in M, so $\exists \bar{x} \in M^n \, (A\bar{x} = B\bar{y})$ is equivalent to $C_2\bar{y} = 0$. □

Fact 4.7 (Baur-Monk [4])**.** *Given a ring R and an R-module M, any formula $\phi(\bar{y})$ (possibly with parameters, with $|\bar{y}| = n$) in the language $\mathcal{L}_R = (+, -, 0, \{r\cdot \colon r \in R\})$ of R-modules is equivalent in M to a finite boolean combination of formulas $\{\phi_i(\bar{y}) \colon i \in I\}$, each formula $\phi_i(\bar{y})$ being of the form $\exists \bar{x}(A_i\bar{x} = B_i\bar{y} + \bar{a}_i)$ with A_i, B_i in $\mathcal{M}_{m,n}(R)$ and $\bar{a}_i \in M^n$.*

A more recent reference for Baur-Monk Theorem is [29, Corollary 2.6.5]. From Claim 2 and Fact 4.7 follows immediately:

Claim 3. *Given a right Euclidean ring R and a divisible R-module M, any subset of M^n defined by a formula in the language $\mathcal{L}_R$ is definable by a quantifier-free formula in $\mathcal{L}_R$.*

A referee points out the broader class of k-stage Euclidean domains introduced in [15] in the case of commutative domains, but also considered for noncommutative rings, that could possibly lead to quantifier elimination. We note that a k-stage Euclidean domain is Bézout [15, Proposition 14], and that there are domains which are PID and not k-stage Euclidean, or k-stage Euclidean and not PID (see *e.g.* [38, Example 1.1.5] and [38, Example 1.1.10]). It is shown in [39, Theorem 3.1], via a diagonalisation argument, that a divisible torsion-free module over a (commutative) Bézout domain eliminates quantifiers.

We go back to the proof of Theorem 4.6. For point (1), it suffices to show that the image of a basic closed F closed. Since translations are bicontinuous, we may also assume that $0 \in F$ and $f(0) = 0$. Then F is given by a linear system $A'\bar{x} = 0$, and $f(\bar{x}) = \bar{y}$ by the system $A''\bar{x} = \bar{y}$ for some matrices A', A'' with coefficients in the ring $D[\theta]$. Putting $A = (A', A'')$ and $B = (0, \mathrm{id})$, one has

$\bar{y} \in f(F)$ if and only if $\exists \bar{x} \in D^n(A\bar{x} = B\bar{y})$, and one concludes by Lemma 2.1.1 and Claim 2 applied to $M = D$. For point (2), we note that a constructible set is defined by a quantifier-free formula in the language $\mathcal{L}_{D[\theta]}$ and conversely, a quantifier-free formula defines a constructible set. Since a θ-morphism is definable (with parameters) in the language $\mathcal{L}_{D[\theta]}$, the image $f(C)$ of a constructible set C is definable, hence constructible by Claim 3. From (2), one can also derive (1) by a topological argument: $f(F)$ is constructible, and since the topology is Noetherian, $f(F)$ contains a dense open set U of its Zariski closure $\overline{f(F)}$ by [36, Proposition 1.4.6]. $\overline{f(F)}$ is a group, so for any $a \in \overline{f(F)}$, the set $a - U$ is open in $\overline{f(F)}$, so $(a - U) \cap U$ is nonempty, from which follows $a \in U + U$ and $\overline{f(F)} = U + U$. Since $U \subset f(F)$, one has $f(F) = \overline{f(F)}$. □

4.3. **Weak Nullstellensatz.**

Theorem 4.8 (weak Nullstellensatz)**.** *Over a linearly surjective θ-division ring, if I is a module avoiding* 1*, then* $\mathrm{V}(I)$ *is nonempty.*

Proof. Again, the classical weak Nullstellensatz has a short proof derived from quantifier elimination, and we follow this line.

Claim 4. *Let R be a right Euclidean ring, M a divisible R-module, and Σ a linear system $\{A\bar{x} = \bar{b}\}$ with $\bar{b} \in M^m$ and $A \in \mathcal{M}_{m,n}(R)$. If Σ has a solution in an R-module extending M, then Σ has a solution in M.*

Proof of Claim 4. If Σ has a solution in an extension of M, by [25, Theorem 3.20] and [25, Corollary 3.17'], Σ has a solution in a divisible module N extending M. By Claim 2, there is a matrix C such that $C\bar{b} = 0$ holds in N, hence also in M. By Claim 2 again, Σ has a solution in M. □

We are now ready to prove Theorem 4.8. I has finitely many generators $\gamma_1, \ldots, \gamma_r$. We consider the system $\Sigma = \{\gamma_1(\bar{x}) = 0, \ldots, \gamma_r(\bar{x}) = 0\}$ and the $D[\theta]$-module D. Since I does not contain 1, there is an embedding $D \to D[\theta, n]/I$ of $D[\theta]$-modules. But Σ has a solution in $D[\theta, n]/I$, namely $(x_1 + I, \ldots, x_n + I)$. Since D divisible, Σ also has a solution in D by Claim 4. □

Corollary 4.9. *Over a linearly surjective θ-division ring D, for any maximal module I avoiding* 1*, there is $\bar{a} \in D^n$ such that*

$$I = (x_1 - a_1, \ldots, x_n - a_n).$$

Proof. We write $J_{\bar{a}} = (x_1 - a_1, \ldots, x_n - a_n)$ and first claim that $J_{\bar{a}}$ is a maximal module avoiding 1. Assume $J_{\bar{a}}$ is contained in a proper module J. One can write any $\gamma \in J \setminus J_{\bar{a}}$ under the form

$$\gamma = \gamma_1(x_1 - a_1) + \cdots + \gamma_n(x_n - a_n) + b,$$

for some 1-twists $\gamma_1, \ldots, \gamma_n$ and $b \in D$. Since $\gamma \notin J_{\bar{a}}$, one has $b \neq 0$, and $\gamma \in J$ yields $1 \in J$. This shows the claim. By maximality of $J_{\bar{a}}$, from the inclusion $J_{\bar{a}} \subset \mathrm{I}(\bar{a})$ follows the equality $J_{\bar{a}} = \mathrm{I}(\bar{a})$. Now, if I is a maximal module avoiding 1, it contains a point $\bar{a}$ by Theorem 4.8. One thus has $I \subset \mathrm{I}(\bar{a})$, and equality holds by maximality of I. □

4.4. **Closed modules and strong Nullstellensatz.** Following Definition 1.2, when D is strict, we define the closure $\mathrm{cl}(I)$ of a module I as the set of algebraic elements over I:

$$\mathrm{cl}(I) = \{\gamma \in D[\theta, n] \colon \exists \rho \in D[\theta] \setminus \{0\},\ \rho\gamma \in I\}.$$

As D is strict, one has $\mathrm{cl}(0) = D$ and hence $I + D \subset \mathrm{cl}(I)$.

We say that I is a *closed* module if $\mathrm{cl}(I) = I + D$. It follows from Corollary 1.9 and Lemma 2.1.1 that $\mathrm{cl}(I)$ is a closed $D[\theta]$-module. We say that a θ-affine set U is *radical* if its module $\Gamma(U)$ is closed, equivalently, if the $D[\theta]$-torsion of $\Gamma(U)$ is D.

Lemma 4.10. *If U, V are θ-isomorphic θ-affine sets, then U is radical if and only if V is radical.*

Proof. If $f\colon U \to V$ is a θ-isomorphism, its comorphism $\Gamma(f)\colon \Gamma(V) \to \Gamma(U)$ is bijective hence maps the torsion of $\Gamma(V)$ onto the torsion of $\Gamma(U)$, and $\Gamma(f)$ fixes 1. □

Theorem 4.11 (Nullstellensatz)**.** *Over a linearly surjective θ-division ring, for any module J avoiding 1, one has*

$$\mathrm{I}(\mathrm{V}(J)) \subset \mathrm{cl}(J).$$

Proof. Let $\gamma_1, \ldots, \gamma_r$ be a generating family for J, let $\gamma \in \mathrm{IV}(J)$, and let us consider the $D[\theta]$-module $I = (\gamma_1, \ldots, \gamma_r, \gamma + 1)$. If $\bar{x} \in \mathrm{V}(I)$, then $\bar{x} \in \mathrm{V}(J)$, so $\gamma(\bar{x}) = 0$. But one also has $\gamma(\bar{x}) + 1 = 0$, a contradiction, so $\mathrm{V}(I)$ is empty. By Theorem 4.8, the module I contains 1 so there exist $\rho_1, \ldots, \rho_r, \rho$ in $D[\theta]$ such that

$$1 = \rho(\gamma + 1) + \rho_1\gamma_1 + \cdots + \rho_r\gamma_r.$$

The twist ρ is nonzero since J avoids 1. Applying this equality to a point of $\mathrm{V}(J)$ (which is nonempty by Theorem 4.8), we get $\rho(1) = 1$ hence $\rho\gamma \in J$, whence $\gamma \in \mathrm{cl}(J)$. □

Corollary 4.12. *Over a linearly surjective θ-division ring, for any closed J avoiding 1, one has*

$$\mathrm{I}(\mathrm{V}(J)) = J.$$

Proof. By Theorem 4.11, one has $J \subset \mathrm{IV}(J) \subset J + D$. By Theorem 4.8, the set $\mathrm{V}(J)$ is nonempty, so $\mathrm{IV}(J)$ does not contain 1, hence $\mathrm{IV}(J) \subset J$. □

Corollary 4.13. *Over a linearly surjective θ-division ring D, the functor Γ induces an equivalence of categories*

$$\Gamma\colon \{\textit{radical } \theta\textit{-affine sets}\} \to \{\textit{torsion-free finitely generated } D[\theta]\textit{-modules}\}.$$

Proof. Given a nonempty radical U, let us show that $\Gamma(U)$ is isomorphic to $M \oplus D$ where M is a torsion-free finitely generated $D[\theta]$-module. Considering U up to a translation, which preserves the notion of radicality by Lemma 4.10, we may assume that U contains 0. It follows that $\mathrm{I}(U) \subset (x_1, \ldots, x_n)$ and one has $\Gamma(U) = (x_1, \ldots, x_n)/\mathrm{I}(U) \oplus D$, and $M = (x_1, \ldots, x_n)/\mathrm{I}(U)$ is torsion-free. Conversely, given a torsion-free finitely generated $D[\theta]$-module M, let us show that $M \oplus D$ is isomorphic to some $\Gamma(U)$ for a θ-affine set. Since M is finitely generated, it is isomorphic to some $(x_1, \ldots, x_n)/N$ where N is a submodule of the free $D[\theta]$-module $(x_1, \ldots, x_n)$. Since M is torsion-free, one has $\mathrm{cl}(N) = N$. If we set $U = \mathrm{V}(N) \subset D^n$, one has that U is radical, and hence $N = \mathrm{IV}(N)$ by Corollary 4.12, so $M \oplus D$ is isomorphic to $(x_1, \ldots, x_n)/\mathrm{I}(U) \oplus D = D[\theta, n]/\mathrm{I}(U) = \Gamma(U)$. One concludes with Lemma 3.6. □

4.5. **Examples.** Examples of linearly surjective difference fields include (k_p, σ_p) where k_p is a field of characteristic p with no finite algebraic extension divisible by p (such as $\bigcup \mathbf{F}_{p^{p^n}}$ or $\mathbf{F}_p^{alg}$) and σ_p the Frobenius map. By Łos Theorem, given nonprincipal ultrafilters $\mathcal{U}$ on $\mathbf{N}$ and $\mathcal{V}$ on the set of prime numbers, the field $\prod_{n\to\mathcal{U}} \left(k_p, \sigma_p^n\right)$ of characteristic p, and the field $\prod_{p\to\mathcal{V}} (k_p, \sigma_p)$ of characteristic 0 are also linearly surjective. By [5, Corollary 2.10], the field $\mathrm{W}(k_p)$ of Witt vectors over k_p with the Witt Frobenius is linearly surjective, and so is the field $k_p((t))$ of formal Laurent series over k_p with the ring morphism $\sigma_t\colon \sum r_i t^i \mapsto \sum r_i^p t^i$. It is also noticed in [3, Lemma 4.6] that a contractive

and σ-henselian *valued difference field* is linearly surjective. From these examples, one can build noncommutative examples using:

Lemma 4.14. *If (D,σ) is a linearly surjective difference division ring, and $\tau\colon D \to D$ a nonzero ring morphism that commutes with σ, then*

1. *the division ring of fractions of $D[t;\tau]$ with $\sigma_t\colon \sum r_i t^i \mapsto \sum \sigma(r_i)t^i$ is linearly surjective,*
2. *the division ring of Laurent series $D((t,\tau))$ with $\sigma_t\colon \sum r_i t^i \mapsto \sum \sigma(r_i)t^i$ is lin. surjective.*

We leave the proof of Lemma 4.14 as an exercise. Possible references for twisted Laurent series are [11, Section 2.3 p. 66] and [21, Section 1.10 p 37]. We note that the division ring of fractions of $D[t;\sigma]$ is a proper subring of $D((t,\sigma))$ since series $\sum t^{f(i)}$ where $f\colon \mathbf{N} \to \mathbf{N}$ has a positive acceleration, are not rational (see also the rationality criterion in [11, Proposition 2.3.3]). When D is countable, the fraction field of $D[t;\sigma]$ is countable, whereas $D((t,\sigma))$ is uncountable.

5. Zariski dimension

We consider a strict θ-division ring D, and assume in addition that σ is surjective. Since $D[\theta]$ is a left Ore domain, from Section 1, any $D[\theta]$-module M has a well-defined dimension which we write $\dim_{D[\theta]} M$.

Definition 5.1. We define the *Zariski dimension of a θ-affine set V* by

$$\dim V = \dim_{D[\theta]} \Gamma(V).$$

Examples 5.2. From Lemma 1.7, if $V \subset D^n$, one has $\dim V = n - \dim_{D[\theta]} \mathrm{I}(V)$.

- The whole space D^n has dimension n since $\mathrm{I}(D^n)$ is zero.
- The empty set has dimension zero since $\mathrm{I}(\emptyset)$ equals $D[\theta,n]$.
- A single point $\bar{a} = (a_1,\dots,a_n)$ has dimension zero since $\mathrm{I}(\bar{a}) = (x_1 - a_1,\dots,x_n - a_n)$.
- The division ring $\mathrm{C}^{\sigma,\delta}(\theta)$ has dimension zero since $\mathrm{I}(\mathrm{C}^{\sigma,\delta}(\theta)) = (\theta - \theta(1)\cdot \mathrm{id})$.

Lemma 5.3. *Two θ-isomorphic θ-affine sets have the same Zariski dimension*

Proof. If $f\colon U \to V$ is a θ-isomorphism, by Corollary 3.7, its comorphism $\Gamma(f)\colon \Gamma(V) \to \Gamma(U)$ is an isomorphism, hence $\dim U$ equals $\dim V$ by Lemma 1.10. □

5.1. Main result.

Theorem 5.4. *Let $V \subset D^n$ be a nonempty θ-affine set. Then V is θ-isomorphic to*

$$D^d \times F_{d+1} \times \cdots \times F_n,$$

where $F_{d+1},\dots,F_n$ are right $\mathrm{C}^{\sigma,\delta}(\theta)$-vector subspaces of D of finite dimension, and $d = \dim V$.

Proof. Let $\mathrm{I}(V) = (\gamma_1,\dots,\gamma_m)$. Translating V, we may assume that V contains zero. We write $\gamma_i = \gamma_{i1}(x_1) + \cdots + \gamma_{in}(x_n)$ with $\gamma_{ij} \in D[\theta]$, and consider the $m \times n$ matrix

$$A = \begin{pmatrix} \gamma_{11} & \cdots & \gamma_{1n} \\ \vdots & & \vdots \\ \gamma_{m1} & \cdots & \gamma_{mn} \end{pmatrix}$$

Since σ is surjective, by Lemma 2.1, $D[\theta]$ is a left and right Euclidean ring. By [42, Theorem 10.1] (see also [13, Theorem 1.4.7]), one has $A = P \cdot B \cdot Q$ for some invertible matrices P and Q with

coefficients in $D[\theta]$ and a diagonal $B = \mathrm{diag}(0, \dots, 0, \beta_{d+1}, \dots, \beta_n)$ where $\beta_{d+1}, \dots, \beta_n \in D[\theta]$ are nonzero. Writing $\bar{x} = (x_1, \dots, x_n)$, one has

$$\bar{x} \in \mathrm{V}(\gamma_1, \dots, \gamma_m) \iff A\bar{x} = 0 \iff BQ\bar{x} = 0.$$

One also has, via $\bar{x} \mapsto Q\bar{x}$, the θ-isomorphism

$$V \simeq \{\bar{y} \in D^n \colon B\bar{y} = 0\} = D^d \times \mathrm{V}(\beta_{d+1}) \times \cdots \times \mathrm{V}(\beta_n),$$

where d is the number of zero entries on the diagonal of B, hence independent of any θ-extension of D. One concludes by Lemma 2.4 that each $\mathrm{V}(\beta_i)$ has finite right $\mathrm{C}^{\sigma,\delta}(\theta)$-dimension.

Putting $U = D^d \times \mathrm{V}(\beta_{d+1}) \times \cdots \times \mathrm{V}(\beta_n)$, and choosing $\beta_{d+1}, \dots, \beta_n$ having minimal degrees, one can show using the right Euclidean division that $\mathrm{I}(U) = (\beta_{d+1}(x_{d+1}), \dots, \beta_n(x_n))$. One thus has $d = \dim U$, and by Lemma 5.3, also $d = \dim V$. □

In the case of an infinite perfect field k of characteristic p equipped with the Frobenius $\theta(x) = x^p$, one recovers from Theorem 5.4 the classical counterpart that a connected algebraic subgroup of k^n defined by p-polynomials is θ-isomorphic to k^d (see *e.g.* [37, Corollary 3.3.15]).

Corollary 5.5. *Given a fixed set S of twists, if $\mathrm{V}(S)$ is nonempty, $\dim \mathrm{V}(S)$ does not depend on the θ-extension of D in which $\mathrm{V}(S)$ is considered.*

5.2. **Calculation rules.** Let D be linearly surjective. As a Corollary of the Nullstellensatz, the dimension of $\mathrm{V}(S)$ does not depend on the set S chosen:

Lemma 5.6. *Let $\mathrm{V}(S) \subset D^n$ be a nonempty θ-affine set. One has*

$$\dim \mathrm{V}(S) = n - \dim_{D[\theta]}(S).$$

Proof. By Theorem 4.11, one has $S \subset \mathrm{IV}(S) \subset \mathrm{cl}(S)$. By Lemma 1.9, the modules $\mathrm{IV}(S)$ and (S) have the same $D[\theta]$-dimension. □

In particular, it is now easy to give the dimension of a cut by a θ-hypersurface:

Theorem 5.7. *Let $\mathrm{V}(S) \subset D^n$ be a θ-affine set and $\gamma \in D[\theta, n]$.*

1. *If $\gamma \in \mathrm{cl}(S)$ and $\mathrm{V}(S, \gamma) \neq \emptyset$, one has $\dim \mathrm{V}(S, \gamma) = \dim \mathrm{V}(S)$.*
2. *If $\gamma \notin \mathrm{cl}(S)$ and $\mathrm{V}(S, \gamma) \neq \emptyset$, one has $\dim \mathrm{V}(S, \gamma) = \dim \mathrm{V}(S) - 1$.*
3. *If γ is not constant, then $\dim \mathrm{V}(\gamma) = n - 1$.*

Proof. For point (1), if $\gamma \in \mathrm{cl}(S)$, then (S, γ) and (S) have the same $D[\theta]$-dimension by Lemma 1.9, and one concludes with Lemma 5.6. For point (2), if $\gamma \notin \mathrm{cl}(S)$, then $\dim_{D[\theta]}(S, \gamma) = \dim_{D[\theta]}(S) + 1$. For point (3), as $[D : \mathrm{C}^{\sigma,\delta}(\theta)]_{\mathrm{right}}$ is infinite, one has $\mathrm{I}(D^n) = (0)$ by Lemma 2.4, and $\mathrm{cl}(0) = D$. One concludes applying point (2) to $V = D^n$. □

Corollary 5.8. *Let $U \subsetneq V$ be nonempty θ-affine sets. If V is radical, then $\dim U < \dim V$.*

Proof. Since $U \subset V$ is proper, the inclusion $\mathrm{I}(V) \subset \mathrm{I}(U)$ is proper. For any $\gamma \in \mathrm{I}(U) \setminus \mathrm{I}(V)$, since $\mathrm{I}(V)$ is closed and U nonempty, one has $\gamma \notin \mathrm{cl}(\mathrm{I}(V))$ hence $\dim U < \dim V$ by Theorem 5.7.2. □

Theorem 5.9. *The Zariski dimension of a nonempty θ-affine set $\mathrm{V}(S) \subset D^n$ is equal to*

1. *the maximal length d of a chain $S \subset I_0 \subsetneq \cdots \subsetneq I_d$ of closed modules avoiding 1,*
2. *the maximal length d of a chain $V_0 \subsetneq \cdots \subsetneq V_d \subset \mathrm{V}(S)$ of nonempty radical θ-affine sets,*
3. *the minimal number of n-twists $\gamma_1, \dots, \gamma_d$ needed for $\mathrm{V}(S, \gamma_1, \dots, \gamma_d)$ to be nonempty and have dimension 0.*

Proof. Towards point (1), we first build a chain of submodules of $D[\theta, n]$ of length $m = \dim \mathrm{V}(S)$. Let $(\gamma_1, \dots, \gamma_{n-m})$ be a basis for (S). Since $\mathrm{V}(S)$ is nonempty, (S) does not contain 1, and one can build a chain of modules avoiding 1 of the form $(\gamma_1, \dots, \gamma_i)$ choosing inductively $\gamma_i \notin \mathrm{cl}(\gamma_1, \dots, \gamma_{i-1})$ for $i > n - m$.

Claim 5. *Let I a module with $\mathrm{cl}(I) = I$, and J a maximal submodule avoiding 1. Then J is closed.*

Proof of Claim 5. Let $\alpha \in \mathrm{cl}(J)$. Since D is divisible, there is a nonzero $\gamma \in D[\theta]$ of minimal degree such that there is $d \in D$ with $\gamma(\alpha + d) \in J$. We claim that γ has degree 0, so $\alpha \in J + D$, as desired. Assume for a contradiction that $\deg(\gamma) \geqslant 1$, then $\alpha + d \in I \setminus J$, so $(\alpha + d, J)$ contains 1 by maximality of J, and there is $\varepsilon \in D[\theta]$ such that $\varepsilon(\alpha + d) \in J + 1$. Dividing ε by γ by Lemma 2.1.1, one has $\varepsilon = q\gamma + r$ with $\deg(r) < \deg(\gamma)$, hence $r(\alpha + d) \in J + 1$. Since $1 \notin J$, one has $r \neq 0$. Since $r(d') = 1$ for some $d' \in D$, one has $r(\alpha + d - d') \in J$, which contradicts the minimality of γ. □

For each $i \in \{0, \dots, m\}$, setting $I_{-1} = (\gamma_1, \dots, \gamma_{n-m})$, there is a maximal submodule I_i of $\mathrm{cl}(\gamma_1, \dots, \gamma_{n-m+i})$ that avoids 1 and contains I_{i-1}. By Claim 5, the chain $I_0 \subsetneq \cdots \subsetneq I_m$ has the desired properties. Conversely, given a maximal chain as in (1), we show inductively that $\dim_{D[\theta]} I_{d-i} = n - i$. For $i = 0$, the module I_d is maximal so has dimension n. If $\dim_{D[\theta]} I_{d-i} = n - i$, one has $\dim_{D[\theta]} I_{d-i-1} \leqslant n - i - 1$ since I_{d-i} is closed, and equality holds by maximality of the chain. This shows that $\dim \mathrm{V}(I_0)$ is d, but $\mathrm{cl}(S) = I_0 + D$ by maximality of the chain, hence $d = \dim V$. For point (2), by Corollary 4.12, there is a one-to-one order reversing correspondence between closed modules avoiding 1 and nonempty radical θ-affine sets, so that (2) is equivalent to (1). For point (3), if $\mathrm{V}(S)$ has dimension d, by Theorem 5.7, one needs at least d twists $\gamma_1, \dots, \gamma_d$ to have $\dim \mathrm{V}(S, \gamma_1, \dots, \gamma_d) = 0$. One can find such twists by completing a basis of (S). □

Lemma 5.10 (product)**.** *Let U, V be θ-affine sets. Then* $\dim(U \times V) = \dim U + \dim V$.

Proof. One has $\mathrm{I}(U \times V) = \mathrm{I}(U) \oplus \mathrm{I}(V)$, and the conclusion follows from Lemma 1.6. □

5.3. **θ-Morphisms and dimension.** D still denotes a linearly surjective θ-division ring.

Theorem 5.11. *Let U be an irreducible θ-affine set and $f\colon U \to D^m$ a θ-morphism. Then* $\operatorname{im} f$ *is a θ-affine set and one has*

$$\dim \operatorname{im} f + \dim \ker f = \dim U.$$

Proof. Being the continuous image of an irreducible set, $\operatorname{im} f$ is irreducible hence θ-affine by Theorem 4.6.1. Considering the comorphism $\Gamma(f)\colon \Gamma(D^m) \to \Gamma(U)$, one has

$$\ker \Gamma(f) = \mathrm{I}(\operatorname{im} f) \quad \text{and} \quad \operatorname{im} \Gamma(f) = (f_1, \dots, f_m, \mathrm{I}(U))\,/\mathrm{I}(U).$$

Putting $J = (f_1, \dots, f_m, \mathrm{I}(U))$, by Corollary 5.6, the Zariski dimension of $\mathrm{V}(J)$ is $n - \dim_{D[\theta]} J$. Since $\mathrm{V}(J)$ equals $\ker f$, one has

$$\dim_{D[\theta]} \ker \Gamma(f) = m - \dim \operatorname{im} f \quad \text{and} \quad \dim_{D[\theta]} \operatorname{im} \Gamma(f) = \dim U - \dim \ker f,$$

and the conclusion follows from the Rank-Nullity Lemma 1.10 applied to $\Gamma(f)$. □

Theorem 5.12 (after Ax-Grothendieck)**.** *Let $f\colon D^n \to D^n$ be a θ-morphism whose fibers have Zariski dimension zero. Then f is surjective.*

Proof. As D^n is irreducible, the image of f is a θ-affine set of Zariski dimension n by Theorem 5.11. As D^n is radical, f is surjective by Corollary 5.8. □

6. Radical sets

Throughout this Section, D is a strict θ-division ring.

Lemma 6.1. *Let $U \subset V$ be nonempty θ-affine sets. Then $\dim U = \dim V$ if and only if V/U has finite right $\mathrm{C}^{\sigma,\delta}(\theta)$-dimension.*

Proof. Assume that U and V have the same Zariski dimension. By Noetherianity, it suffices to show that for any $\gamma \in \mathrm{I}(U)$, the vector-space $V/V \cap \mathrm{V}(\gamma)$ has finite right $\mathrm{C}^{\sigma,\delta}(\theta)$-dimension. As $\mathrm{I}(U)$ and $\mathrm{I}(V)$ have the same $D[\theta]$-dimension, γ is algebraic over $\mathrm{I}(V)$. Let $\rho \in D[\theta]$ be nonzero of degree n such that $\rho\gamma \in \mathrm{I}(V)$. Let $\bar{g}_0, \dots, \bar{g}_n$ in V, and let us show that their images in $V/V \cap \mathrm{V}(\gamma)$ are right $\mathrm{C}^{\sigma,\delta}(\theta)$-dependent. As $\gamma(\bar{g}_1), \dots, \gamma(\bar{g}_n)$ are all roots of ρ, by Lemma 2.4, there is a nontrivial $\mathrm{C}^{\sigma,\delta}(\theta)$-linear combination

$$\gamma(\bar{g}_0)\lambda_0 + \cdots + \gamma(\bar{g}_n)\lambda_n = 0,$$

so $\bar{g}_0\lambda_0 + \cdots + \bar{g}_n\lambda_n$ belongs to $V \cap \mathrm{V}(\gamma)$. This shows that $V/V \cap \mathrm{V}(\gamma)$ has $\mathrm{C}^{\sigma,\delta}(\theta)$-dimension at most n, as desired. Conversely, assume that V/U has finite $\mathrm{C}^{\sigma,\delta}(\theta)$-dimension, and let $\gamma \in \mathrm{I}(U)$. Then $V/V \cap \mathrm{V}(\gamma)$ has a finite basis $(\bar{g}_1, \dots, \bar{g}_n) + V \cap \mathrm{V}(\gamma)$. By Lemma 2.4, there is $\rho \in D[\theta]$ of degree at most n which vanishes on every $\gamma(\bar{g}_i)$, so in particular ρ is nonzero and $\rho\gamma \in \mathrm{I}(V)$. This shows that $\mathrm{I}(U)$ is algebraic over $\mathrm{I}(V)$, so U and V have the same dimension. □

6.1. **Radical components.** Given a θ-affine set V and a point $a \in V$, we define the *radical component of a in V* to be the intersection of all θ-affine subsets of V that contain a and have the same Zariski dimension as V. We write it $V^0(a)$.

Lemma 6.2. *For any θ-affine set V and $a \in V$, the sets V and $V^0(a)$ have the same Zariski dimension d, and $V^0(a)$ is a radical set. If σ is surjective, $V^0(a)$ is θ-isomorphic to D^d.*

Proof. The first assertion follows from Lemma 6.1 and the fact that the topology is Noetherian. To show that $V^0(a)$ is radical, let γ be algebraic over $\mathrm{I}(V^0(a))$. Then also $\gamma' = \gamma - \gamma(a)$ is algebraic over $\mathrm{I}(V^0(a))$. By the argument used in the proof of Lemma 6.1, the $\mathrm{C}^{\sigma,\delta}(\theta)$-dimension of $V^0(a)/V^0(a) \cap \mathrm{V}(\gamma')$ is finite. By Lemma 6.1, $V^0(a) \cap \mathrm{V}(\gamma')$ has the same Zariski dimension as V, so $V^0(a) \subset \mathrm{V}(\gamma')$. This shows that γ' belongs to $\mathrm{I}(V^0(a))$, and that $\mathrm{I}(V^0(a))$ is closed. The last assertion follows from Theorem 5.4 and Lemma 4.10. □

6.2. **An example of a radical group.** Given a strict difference division ring (D, σ) and a tuple $\bar{b} = (b_1, \dots, b_n)$, we consider the σ-affine set

$$G_{\bar{b}} = \{(x_1, \dots, x_n) \in D^n \colon b_1(\sigma x_1 - x_1) = b_i(\sigma x_i - x_i) \text{ for all } 1 \leqslant i \leqslant n\},$$

and we look for conditions for $G_{\bar{b}}$ to be radical. We shall need the following Lemma.

Lemma 6.3. *Given any tuple $(r_1, \dots, r_n) \in D^n$, the left dimension of $(r_1, \dots, r_n)$ over $\mathrm{Fix}(\sigma)$ does not vary when computed in a σ-extension of D.*

Proof. By lemma 2.4, right $\mathrm{Fix}(\sigma)$-dependence of a tuple $(r_1, \dots, r_n)$ is expressible by a quantifier-free formula stating that the r_i are all roots of a certain 1-twist of degree less than n with coefficients in D, so right $\mathrm{Fix}(\sigma)$-dependence of $(r_1, \dots, r_n)$ does not depend on the σ-extension of D. The corresponding 'left' statement is obtained considering D with the opposite multiplication $a * b = b \cdot a$ since σ is still a ring morphism of $(D, +, *)$. □

Lemma 6.4 is inspired by [22, Lemma 2.8] and its improved version [19, Lemme 5.3]. It plays a crucial role in [22] and [19] in the particular case when (D,σ) is an algebraically closed field (k,σ_p) of characteristic p equipped with the Frobenius σ_p. In that particular case, if $\left\{b_1^{-1},\dots,b_n^{-1}\right\}$ are $\mathbf{F}_p$-linearly independent, [19, Lemme 5.3] states that, $G_{\bar{b}}$ is *connected* as an algebraic group, whereas Lemma 6.4 only states that $G_{\bar{b}}$ has no subgroup of finite index defined by p-polynomials. But one recovers the conclusion of [19, Lemme 5.3] knowing that $G_{\bar{b}}$ is σ_p-isomorphic to $(k,+)$ by Theorem 5.4, and $(k,+)$ is connected, so that $G_{\bar{b}}$ is connected as well.

Lemma 6.4. *Given a natural number $n \geqslant 1$ and a tuple $\bar{b} = (b_1,\dots,b_n)$ in $D^\times$, the set $G_{\bar{b}}$ is radical if and only if $\left(b_1^{-1},\dots,b_n^{-1}\right)$ are left $\mathrm{Fix}(\sigma)$-linearly independent.*

Proof. We first assume that $G_{\bar{b}}$ is radical and put $\gamma = \sigma - \mathrm{id}$. If there are $(r_1,\dots,r_n)$ in $\mathrm{Fix}(\sigma)$ such that $r_1b_1^{-1} + \cdots + r_nb_n^{-1} = 0$, one has for every $(x_1,\dots,x_n) \in G_{\bar{b}}$,

$$\gamma(r_1x_1 + \cdots + r_nx_n) = \sum_{i=1}^{n} r_i\gamma(x_i) = \sum_{i=1}^{n} r_ib_i^{-1}b_i\gamma(x_i) = \left(\sum_{i=1}^{n} r_ib_i^{-1}\right) b_1\gamma(x_1) = 0.$$

It follows that $r_1x_1 + \cdots + r_nx_n$ is algebraic over $\mathrm{I}\,(G_{\bar{b}})$, so belongs to $\mathrm{I}\,(G_{\bar{b}})$ by assumption. This implies that $r_1x_1 + \cdots + r_nx_n$ vanishes on $\mathrm{Fix}(\sigma) \times \cdots \times \mathrm{Fix}(\sigma)$, hence $(r_1,\dots,r_n)$ is zero.

We show the converse by induction on n. If $n = 1$, then G_{b_1} equals D, so G_{b_1} is radical. Let us assume that the Lemma is proved for $n-1$ and that $G_{b_1,\dots,b_n}$ is not radical over D. Then $G_{b_1,\dots,b_n}$ is not radical over any difference extension (E,σ') of (D,σ). We chose (E,σ') linearly surjective by Theorem 4.5 and we look at σ'-varieties over E. By induction hypothesis and Lemma 6.3, we may assume that $G_{b_1,\dots,b_{n-1}}$ is radical over E. One has $\dim G_{b_1,\dots,b_n} \geqslant 1$ by Theorem 5.7, and, since the kernel of the first projection $\pi_1 \colon G_{b_1,\dots,b_n} \to E$ has dimension 0, one also has $\dim G_{b_1,\dots,b_n} \leqslant 1$ by Theorem 5.11. Writing $G^0_{b_1,\dots,b_n}$ for the radical component of 0 in $G_{b_1,\dots,b_n}$, one has $\dim\left(G^0_{b_1,\dots,b_n}\right) = 1$ by Lemma 6.2, so one of the n main projections of $G^0_{b_1,\dots,b_n}$, say on the first coordinate, is onto,

$$\pi_1 \colon G^0_{b_1,\dots,b_n} \longrightarrow\!\!\!\!\!\rightarrow E. \tag{6.1}$$

Consider the projection on the first $n-1$ coordinates $\pi \colon G_{b_1,\dots,b_n} \to G_{b_1,\dots,b_{n-1}}$. Since $\ker\pi$ has dimension 0, the image $\pi\left(G^0_{b_1,\dots,b_{n-1}}\right)$ is σ'-affine and has dimension 1 by Theorem 5.11. Since $G_{b_1,\dots,b_{n-1}}$ is radical, by Corollary 5.8, the following restriction is onto

$$\pi \colon G^0_{b_1,\dots,b_n} \longrightarrow\!\!\!\!\!\rightarrow G_{b_1,\dots,b_{n-1}}. \tag{6.2}$$

By assumption, there is a linear $\gamma' \in \mathrm{cl}\,(\mathrm{I}\,(G_{b_1,\dots,b_n})) \setminus \mathrm{I}\,(G_{b_1,\dots,b_n})$ with coefficients in D. Replacing inductively $\sigma'(x_i)$ by $x_i + b_i^{-1}b_1\gamma(x_1)$ for all $i \in \{2,\dots,n\}$ in the equation $\gamma'(\bar{x}) = 0$, the system $\{\gamma'(\bar{x}) = 0,\ b_1\gamma(x_1) = \cdots = b_n\gamma(x_n)\}$ is equivalent to one of the form

$$\{\alpha(x_1) + r_2x_2 + \cdots + r_nx_n = 0,\ b_1\gamma(x_1) = \cdots = b_n\gamma(x_n)\},$$

with $r_2,\dots,r_n$ in D. Since $G_{b_1,\dots,b_{n-1}}$ is radical, we may assume $r_n = 1$. Composing by γ, we get

$$\gamma\alpha(x_1) + \gamma(r_2x_2) + \cdots + \gamma(r_{n-1}x_{n-1}) + b_n^{-1}b_1\gamma(x_1) = 0,$$

which holds for all $(x_1,\dots,x_{n-1}) \in G_{b_1,\dots,b_{n-1}}$ by (6.2). Taking $x_2 = 1$ and else $x_j = 0$ yields $r_2 \in \mathrm{Fix}(\sigma') \cap D = \mathrm{Fix}(\sigma)$, and symmetrically $r_2,\dots r_{n-1} \in \mathrm{Fix}(\sigma)$, hence

$$\gamma\alpha(x_1) + r_2b_2^{-1}b_1\gamma(x_1) + \cdots + r_{n-1}b_{n-1}^{-1}b_1\gamma(x_1) + b_n^{-1}b_1\gamma(x_1) = 0,$$

which holds for all $x_1 \in E$ by (6.1). It follows that $\alpha(x_1) = r_1x_1$ for some $r_1 \in \mathrm{Fix}(\sigma)$, which yields

$$r_1b_1^{-1} + r_2b_2^{-1} + \cdots + r_{n-1}b_{n-1}^{-1} + b_n^{-1} = 0,$$

so $(b_1^{-1},\dots,b_n^{-1})$ are left $\mathrm{Fix}(\sigma)$-dependent, and the induction is proved. □

Given a strict differential division ring (D, δ), since δ is still a derivation on the opposite division ring $(D, +, *)$, one has with a similar proof:

Lemma 6.5. *Given a natural number $n \geqslant 1$ and a tuple $\bar{b} = (b_1, \ldots, b_n)$ in $D^\times$, the set*

$$\{(x_1, \ldots, x_n) \in D^n \colon b_1\delta(x_1) = b_i\delta(x_i) \text{ for all } 1 \leqslant i \leqslant n\}$$

is radical if and only if $\left(b_1^{-1}, \ldots, b_n^{-1}\right)$ are left $\mathrm{Const}(\delta)$-linearly independent.

References

[1] Shimshon Amitsur. A generalization of a theorem on linear differential equations. *Bulletin of the American Mathematical Society*, 54:937–941, 1948.

[2] Matthias Aschenbrenner, Lou van den Dries, and Joris van der Hoeven. *Asymptotic differential algebra and Model theory of transseries*. Princeton University Press, 2017.

[3] Salih Azgin. Valued fields with contractive automorphism and Kaplansky fields. *Journal of Algebra*, 324:2757–2785, 2010.

[4] Walter Baur. Quantifier elimination for modules. *Israel Journal of Mathematics*, 25:64–70, 1976.

[5] Luc Bélair and Françoise Point. Quantifier elimination in valued Ore modules. *The Journal of Symbolic Logic*, 75:1007–1034, 2010.

[6] Nicolas Bourbaki. *Algèbre, chapitre 8, Modules et anneaux semi-simples*. Hermann, 1958.

[7] Manuel Bronstein and Marko Petkovšek. An introduction to pseudo-linear algebra. *Theoretical Computer Science*, 157:3–33, 1996. Algorithmic complexity of algebraic and geometric models (Créteil, 1994).

[8] Artem Chernikov and Martin Hils. Valued difference fields and NTP_2. *Israel Journal of Mathematics*, 204:299–327, 2014.

[9] Paul Moritz Cohn. The range of derivations on a skew field and the equation $ax - xb = c$. *Journal of the Indian Mathematical Society*, 37:61–69, 1973.

[10] Paul Moritz Cohn. *Free rings and their relations*, volume 19 of *London Mathematical Society Monographs*. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London, second edition, 1985.

[11] Paul Moritz Cohn. *Skew fields, Theory of general division rings*, volume 57 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1995.

[12] Paul Moritz Cohn. *Further Algebra and Applications*. Springer, 2003.

[13] Paul Moritz Cohn. *Free ideal rings and localization in general rings*, volume 3 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.

[14] Richard Cohn. *Difference Algebra*. Interscience Publishers, 1965.

[15] George Cooke. A weakening of the euclidean property for integral domains and applications to algebraic number theory. I. *Journal für die reine und angewandte Mathematik*, 282:133–156, 1976.

[16] Pilar Dellunde, Françoise Delon, and Françoise Point. The theory of modules of separably closed fields 1. *The Journal of Symbolic Logic*, 67:997–1015, 2002.

[17] Walter Ricardo Ferrer Santos and Alvaro Rittatore. *Actions and invariants of algebraic groups*. Monographs and Research Notes in Mathematics. CRC Press, Boca Raton, FL, second edition, 2017.

[18] Ulrich Görtz and Torsten Wedhorn. *Algebraic geometry I*. Advanced Lectures in Mathematics. Vieweg + Teubner, Wiesbaden, 2010. Schemes with examples and exercises.

[19] Nadja Hempel. On n-dependent groups and fields. *Mathematical Logic Quarterly*, 62:215–224, 2016.

[20] Nathan Jacobson. Pseudo-linear transformations. *Annals of Mathematics*, 38:484–507, 1937.

[21] Nathan Jacobson. *Finite-dimensional division algebras over fields*. Springer-Verlag, Berlin, Corrected 2nd printing, 2010.

[22] Itay Kaplan, Thomas Scanlon, and Frank Wagner. Artin-Schreier extensions in NIP and simple fields. *Israel Journal of Mathematics*, 185:141–153, 2011.

[23] Irving Kaplansky. *An introduction to differential algebra*. Publications de l'Institut Mathématique de l'Université de Nancago, V. Hermann, Paris, 1957.

[24] Earl Laerson. Onto inner derivations in division rings. *Bulletin of the American Mathematical Society*, 67:356–358, 1961.

[25] Tsit Yuen Lam. *Lectures on Modules and Rings*, volume 189 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.

[26] Tsit Yuen Lam and André. Leroy. Vandermonde and Wronskian matrices over division rings. *Journal of Algebra*, 119:308–336, 1988.

[27] Tsit Yuen Lam and André Leroy. Wedderburn polynomials over division rings. I. *Journal of Pure and Applied Algebra*, 186:43–76, 2004.

[28] André Leroy. Noncommutative polynomial maps. *Journal of Algebra and its Applications*, 11:1250076, 16, 2012.

[29] Annalisa Marcja and Carlo Toffalori. *A guide to classical and modern model theory*, volume 19 of *Trends in Logic—Studia Logica Library*. Kluwer Academic Publishers, Dordrecht, 2003.

[30] Gary Meisters. On the equation $ax - xb = c$ in division rings. *Proceedings of the American Mathematical Society*, 12:428–432, 1961.

[31] Bernhard Hermann Neumann. Groups covered by permutable subsets. *Journal of the London Mathematical Society*, 29:236–248, 1954.

[32] Oystein Ore. Theory of non-commutative polynomials. *Annals of Mathematics. Second Series*, 34:480–508, 1933.

[33] Françoise Point. Some model theory of Bezout difference rings-a survey. *Bulletin of the Belgian Mathematical Society Simon Stevin*, 13:807–826, 2006.

[34] Thomas Scanlon. Quantifier elimination for the relative Frobenius. In *Valuation Theory and Its Applications Volume II, Conference proceedings of the International Conference on Valuation Theory (Saskatoon, 1999)*, Fields Institute Communications Series, (AMS, Providence), pages 323–352. Franz-Viktor Kuhlmann, Salma Kuhlmann, and Murray Marshall, eds., 2003.

[35] Saharon Shelah. Stability, the f.c.p., and superstability; model theoretic properties of formulas in first order theory. *Annals of Mathematical Logic*, 3:271–362, 1971.

[36] Patrice Tauvel and Rupert Yu. *Lie Algebras and Algebraic groups*. Springer Monographs in Mathematics, 2005.

[37] Jacques Tits. Lectures on algebraic groups, Yale university, fall 1966. In *Jacques Tits Collected Works volume IV*, pages 657–740. European Mathematical Society, Francis Buekenhout & al. eds., 2013.

[38] Vandy Jade Tombs. *Euclidean domains*. Master Thesis, Brigham Young University. `https://scholarsarchive.byu.edu/etd/6918`, 2018.

[39] Lou van den Driess and Jan Holly. Quantifier elimination for modules with scalar variables. *Annals of Pure and Applied Logic*, 57:161–179, 1992.

[40] Michael Voskoglou. Extending derivations and endomorphisms to skew polynomials rings. *Publications de l'Institut Mathématique (Beograd)*, 53:79–82, 1986.

[41] Frank Wagner. Small fields. *Journal of Symbolic Logic*, 63(3):995–1002, 1998.

[42] Joseph Weddeburn. Noncommmutative domains of integrity. *J. Reine Angew. Math.*, 167:129–141, 1932.

Département de mathématiques, Université de Mons,
Le Pentagone, 20, Place du Parc,
B-7000 Mons, Belgique

Email address: `cedric.milliet@umons.ac.be`