Pseudo-linear algebra over a division ring

Cédric Milliet

PSEUDO-LINEAR ALGEBRA OVER A DIVISION RING

CÉDRIC MILLIET

Abstract. On considère un analogue de la topologie de Zariski sur un corps gauche K muni d'une transformation pseudo-linéaire T, et l'on y définit une géométrie algébrique élémentaire : ensembles T-affines, T-morphismes, et une notion de comorphisme qui témoigne d'une dualité entre la catégorie des ensembles T-affines et celle des $K[t;\sigma,\delta]$-modules. En s'appuyant sur des résultats de P. Cohn, on montre, lorsque σ et δ commutent, que K a une extension $\overline{K}$ sur laquelle chaque fonction de $\overline{K}[\mathrm{T}]$ est surjective. Sur $\overline{K}$, la projection d'un constructible est constructible, et un théorème des zéros est valide. Dans un prochain article, on applique ces résultats aux corps gauches NIP.

Given a division ring D and a one dimensional pseudo-linear transformation T, the purpose of the paper is the study of the subsets of D^n defined by a system of linear equations, each of the form

$$\gamma_1(x_1) + \cdots + \gamma_n(x_n) + c = 0, \tag{0.1}$$

with c being an element of D and for all $i \in \{1, \ldots, n\}$ the map γ_i being a linear operator

$$\gamma_i(x) = a_{i,0}x + a_{i,1}\mathrm{T}(x) + \cdots + a_{i,n}\mathrm{T}^m(x) \tag{0.2}$$

with left coefficients $\{a_{i,j} \colon i \in \{1, \ldots, n\},\ j \in \{1, \ldots, m\}\}$ in D. We write $D[\mathrm{T}]$ for the set of maps (0.2), $D[\mathrm{T}, n]$ for the set of maps (0.1) and $C^{\sigma,\delta}(a)$ for the generalised centraliser defined in [30, p. 314]. This setting, taken from [25] and [30], has the following advantage: when $\mathrm{T} = \sigma$, we recover the usual linear difference operators while the general centraliser is $\mathrm{Fix}(\sigma)$, and when $\mathrm{T} = \delta$, we recover the usual linear differential operators while the centraliser is $\mathrm{Const}(\delta)$.

The ring $D[\mathrm{T}]$ is isomorphic to the Ore extension $D[t;\sigma,\delta]$ when the right dimension $[D : C^{\sigma,\delta}(a)]$ is infinite, and $D[\mathrm{T}, n]$ has a structure of $D[t;\sigma,\delta]$-module. We thus begin in **Section 1** by elementary considerations about the dimension of a module over a left Ore domain. In **Section 2**, we recall some basic properties of $D[\mathrm{T}]$ and $D[\mathrm{T}, n]$ which mainly come from [7, 25, 30, 32, 37]. In **Section 3**, we differ from the setting of [31]: instead of considering varieties defined by skew Ore polynomials with an appropriate notion of evaluation as in [31, (2.7) p. 46], we call T-*affine* a set $\mathrm{V}(S)$ defined by a system S of equations like (0.1), and a T-*morphism* a map between T-affine sets whose coordinate maps are in $D[\mathrm{T}, n]$; so in a sense, our objects of study are very restricted, and closer to linear algebra than to algebraic geometry. Still, they encompass the so called "metro equations" $ax - xb = c$ and their (σ,δ)-generalisations defined in [31, (6.5) p. 63]. There is however a pregnant analogy with classical algebraic geometry (we have been much influenced by reading parts of [1, 24, 38, 44, 45]), and we point at a contravariant functor between the category of T-affine sets and the category of finitely generated $D[t;\sigma,\delta]$-modules. In **Section 4**, we call D *linearly surjective*

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/` and `https://math.stackexchange.com/` communities for a rich exchange of ideas [16, 19, 41], in particular to Tom De Medts for pointing at [35] in [23], leading to [28], which were a starting point for the present work, and to rschwieb for answering many of my elementary ring-theoretic questions. The author is also grateful to the referees for their suggestions leading to a clearer version of the paper and for pointing at pseudo-linear transformations "including skew derivations in the game" (an earlier version of the paper dealt with the case of a division ring equipped with a single ring morphism). Part of the research presented here was done during a postdoctoral position within the Mons logic group.

(a notion analogous to the one of algebraically closed fields) if every nonzero $\gamma \in D[\mathrm{T}]$ is surjective. Using results of P. Cohn on the existence of division ring extensions having sufficiently many roots of certain polynomials, we show that if either σ or δ are inner, or if σ and δ commute, then D has a linearly surjective extension. In such an extension, using Baur-Monk's quantifier elimination up to prime positive formulas for theories of modules, we show that Chevalley's projection Theorem for constructible sets holds, as well as a Nullstellensatz. **Section 5** is devoted to defining and calculating the *Zariski dimension* of a T-affine set V when $[D : C^{\sigma,\delta}(a)]$ is infinite and σ surjective. By a diagonalisation argument due to Wedderburn, we show that the dimension of V is the unique natural number d such that V is T-isomorphic to $D^d \times U$, where U is T-affine of finite right $C^{\sigma,\delta}(a)$-dimension. In **Section 6**, we study the T-affine sets that do not have proper T-affine subsets of the same Zariski dimension; we call such sets *radical*, and we end with a criterion inspired of [27, Lemma 2.8] and [22, Lemme 5.3] for certain T-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 $\mathrm{Th}(D)$ of a division ring D in the ring language. Among these questions, (1) if $\mathrm{Th}(D)$ has countably many pure types, is D commutative (from [48, Problem 12.6])? (2) Does $\mathrm{Th}(D)$ satisfy Vaught's conjecture? (3) If $\mathrm{Th}(D)$ does not have the independence property (see [43, Definition 4.1]), is the dimension $[D : Z(D)]$ 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 an R-module (all modules considered in the paper are left modules). This section recalls that M has a *dimension* that shares several properties of the vector-space dimension. As we could not find a reference, we hint at proofs that would fit in an undergraduate algebra course.

Say that a tuple $\bar{v} = (v_1, \ldots, v_n) \in M^n$ is *dependent* if there is a nonzero tuple $(r_1, \ldots, r_n) \in R^n$ such that $r_1 v_1 + \cdots + r_n v_n = 0$. Say that $\bar{v}$ is a *basis* if independent and maximal. Any independent family extends to a (possibly empty) basis. For all $S \subseteq M$, we write (S) for the submodule generated by S. If $\bar{b}$ is a basis, for every $v \in M \setminus \bar{b}$, there is a nonzero $r \in R$ such that $rv \in (\bar{b})$.

Definition 1.1 (algebraicity)**.** We say that v *is algebraic over* S if there is a nonzero $r \in R$ such that $rv \in (S)$. For $A \subseteq M$, we say that A *is algebraic over* S if every $v \in A$ is algebraic over S.

For any $S \subseteq M$, we write $\mathrm{cl}(S)$ for the set of algebraic elements over S. Algebraicity is transitive:

Lemma 1.2. *If A is algebraic over B and B is algebraic over C, then A is algebraic over C.*

Proof. Let a be in A. By assumption, there are $r, r_1, \ldots, r_n$ in $R \setminus \{0\}$ and a tuple $\bar{b}$ in B^n such that one has $ra \in (\bar{b})$ and $r_i b_i \in (C)$ for all $i \in \{1, \ldots, n\}$. In particular, there is an expression of the form $sa \in (C) + \sum_{i \in I} s_i b_i$, with $s \in R \setminus \{0\}$, and one may choose the set $I \subseteq \{1, \ldots, n\}$ 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 $us_j b_j \in (C)$, and one has $(us)a \in (C) + \sum_{i \in I \setminus \{j\}} us_i b_i$ with us nonzero as u and s are nonzero, a contradiction with the minimality of I. □

Theorem 1.3 (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 1.2, 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 1.4 (dimension)**.** We call *R-dimension* of M the cardinal of any basis of M.

We write $\dim_R M$ for the R-dimension of M, or $\dim M$ when there is no ambiguity about R. It satisfies the properties one would expect from a dimension:

Proposition 1.5. *Let be a subset $S \subseteq M$, and let N, L be two more R-modules.*

(1) *One has* $\dim M \oplus N = \dim M + \dim N$.
(2) *If $N \subseteq M$ holds, one has* $\dim M = \dim M/N + \dim N$.
(3) *The set* $\mathrm{cl}(S)$ *is an R-module and one has* $\dim \mathrm{cl}(S) = \dim(S)$.
(4) *If $M \xrightarrow{f} N$ is a morphism of R-modules, one has* $\dim M = \dim \ker f + \dim \operatorname{im} f$.
(5) *If $L \xrightarrow{g} M \xrightarrow{f} N$ are morphisms, one has* $\dim \ker f \circ g = \dim(\ker f \cap \operatorname{im} g) + \dim \ker g$.

We leave the proof of Proposition 1.5 as an exercise. Urya First tells in [17] that Proposition 1.5 follows from the exactness of Ore localisation and the corresponding linear algebra facts, citing [29, Exercise 18, end of §10]. We did not explore this path further.

2. Twists over a division ring

Our initial setting comes from [25, 30, 37] and has the advantage of providing a uniform framework to deal with both difference and differential linear equations. The notion of pseudo-linear transformation comes from [25]; we also refer to [7] for an introduction to pseudo-linear algebra. The statements presented in this section are well-known and appear in the literature somewhat maybe in a disguised form, as a referee says. We collect them here as a try to make the paper self-contained and hint at proofs when we could not find precise references.

Given D a division ring, σ a nonzero ring morphism and δ a *σ-derivation* (that is, satisfying $\delta(x+y) = \delta(x) + \delta(y)$ and $\delta(xy) = \sigma(x)\delta(y) + \delta(x)y$ for all (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 $t \cdot a = \sigma(a)t + \delta(a)$. Let $\mathrm{T} = \sigma \cdot a + \delta$ be the *pseudo-linear transformation induced* by $a \in D$ (which we sometimes write T_a).

2.1. 1-twists.

Let be the ring

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

the elements of which we call *twists*, or 1-*twists*. Any nonzero twist γ has an expression of the form $a_0\mathrm{id} + a_1\mathrm{T} + \cdots + a_n\mathrm{T}^n$ with $a_n \neq 0$. We call the minimal such n the *degree* of γ, written $\deg(\gamma)$, and define $\deg(0) = -\infty$. From [37, Theorem 6] and [7, Theorem 1] (see also [32, Corollary 1.3]) follows that $D[\mathrm{T}]$ is right Euclidean, and when σ is onto also left Euclidean:

Fact 2.1 (Euclidean division)**.** *For all nonzero $\rho \in D[\mathrm{T}]$ and all $\gamma \in D[\mathrm{T}]$,*

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

Corollary 2.2 (factorisation with a root)**.** *For any $\gamma \in D[\mathrm{T}]$ of degree $n+1$ with a nonzero root $b \in D^\times$, there is $q \in D[\mathrm{T}]$ of degree n such that $\gamma = q(\mathrm{T} - \mathrm{T}(b)b^{-1}\mathrm{id})$.*

Following [30, p. 314], we write $C^{\sigma,\delta}(a)$ for the *generalised centraliser* $\{x \in D\colon \mathrm{T}_a(x) = a \cdot x\}$. This is a division ring, and any twist is a right $C^{\sigma,\delta}(a)$-linear map. The following fact can probably be derived from [30, Theorem 4.2], or be shown by induction over n.

Fact 2.3 (roots of a twist)**.** *The kernel of a nonzero twist of degree n has right $C^{\sigma,\delta}(a)$-dimension at most n. Conversely, a vector subspace of D of dim. n is the kernel of a twist of degree at most n.*

Corollary 2.4. *The rings $D[t;\sigma,\delta]$ and $D[\mathrm{T}]$ are isomorphic if and only if $[D : C^{\sigma,\delta}(a)]_{\mathrm{r}} = +\infty$.*

Definition 2.5 (T-division ring, strictness)**.** We call T-*division ring* any division ring D equipped with a pseudo-linear map T. We say that D is *strict* if the right dimension $[D : C^{\sigma,\delta}(a)]_{\mathrm{r}}$ is infinite.

Corollary 2.6. *If D is strict, then $D[\mathrm{T}]$ is a left Noetherian domain.*

2.2. **n-twists and twisted Zariski topology.** We write $D[\mathrm{T}, n]$ for the set of maps of the form $\gamma_1(x_1) + \cdots + \gamma_n(x_n) + c$ where $\gamma_1, \ldots, \gamma_n$ are in $D[\mathrm{T}]$ and c in D. We call such maps *n-twists*.

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 $D[\mathrm{T}, n]$.

$D[\mathrm{T}, n]$ is a Noetherian $D[\mathrm{T}]$-module by [6, Proposition 7 p. 26], and the twisted Zariski topology is Noetherian. From Fact 2.3 follows that a basic closed subset of D is a right $C^{\sigma,\delta}(a)$-affine space of finite dimension, and that a basic closed subset of D^n meets a right D-line either trivially or in a right $C^{\sigma,\delta}(a)$-affine space of finite dimension.

Fact 2.8. *If $C^{\sigma,\delta}(a)$ is infinite, the irreducible closed subsets of D^n are the basic closed sets.*

Proof. Follows from Neumann's [36, Lemma 4.1]. □

3. Elementary T-algebraic geometry

Throughout this section, we consider a T-division ring D and introduce basic notions directly inspired from classical algebraic geometry over a field.

Definition 3.1. We call T-*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 $\Delta \subseteq D^n$, we call *module of* Δ and write $\mathrm{I}(\Delta)$ the set defined by

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

Any T-affine set $\mathrm{V}(S)$ is right $C^{\sigma,\delta}(a)$-affine; any module $\mathrm{I}(\Delta)$ is a submodule of $D[\mathrm{T}, n]$. Since $D[\mathrm{T}, n]$ is a Noetherian module, a T-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 $D[t;\sigma,\delta] \to D[\mathrm{T}]$ suggests to define $\mathrm{V}(g) = \mathrm{V}(g(\mathrm{T})) = \{x \in D\colon g(\mathrm{T})(x) = 0\}$. In [31, (2.7) p. 46], another definition of $\mathrm{V}(g)$ is introduced, defined (with our notation $\mathrm{T}_a = \sigma \cdot a + \delta$) by $\mathrm{V}(g) = \{a \in D\colon g(\mathrm{T}_a)(1) = 0\}$. 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: T-*morphisms* for T-affine sets, and usual morphisms of $D[\mathrm{T}]$-modules for modules.

Definition 3.4. We call T-*morphism* a map between T-affine sets whose coordinate maps are twists. We call T-*isomorphism* a bijective T-morphism whose inverse is also a T-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.* [20, p. 19]). In our case, there is a functor Γ between the category of T-affine sets, and the category of finitely generated $D[\mathrm{T}]$-modules.

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

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

Given a T-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 T-affine sets U and V, we write $\mathrm{Hom}(U, V)$ for the set of T-morphisms from U to V, and $\mathrm{Hom}(\Gamma(V), \Gamma(U), 1)$ for the set of morphisms of $D[\mathrm{T}]$-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 [20, Proposition 1.33]. If $\phi : \Gamma(V) \to \Gamma(U)$ is a given morphism of $D[\mathrm{T}]$-modules that fixes 1, where $U \subseteq D^n$ and $V \subseteq D^m$, there is a morphism of $D[\mathrm{T}]$-modules $\bar{\phi}$ such that $\bar{\phi}(1) = 1$ and such that the following diagram commutes.

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

We define a T-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 $D[\mathrm{T}]$-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* T-*morphism* f *is a* T-*isomorphism if and only if* $\Gamma(f)$ *is an isomorphism.*

Proof. As in [45, Corollary 11.4.5]. □

4. Linearly surjective T-division rings

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 set is the one of *radical* set, and analogue of algebraically closed fields seems to be:

Definition 4.1 (linearly surjective)**.** We call a T-division ring D *linearly surjective* if every nonzero $\gamma \in D[\mathrm{T}]$ is surjective, or equivalently if D, as a $D[\mathrm{T}]$-module, is divisible.

Definition 4.1 extends definition [2, p. 215] given for differential fields; the wording *linearly-closed* exists for difference fields (see *e.g.* [42, Lemma 9.1 p. 17] or [39, Definition 4.3 p. 15]). Note that a linearly surjective division ring must be strict. We begin the Section by showing that most T-division rings have a linearly surjective extension and we show that in such extensions, Chevalley's projection theorem holds, as well as a Nullstellensatz.

4.1. **Linearly surjective extensions.** Following [13, p. 58],

Definition 4.2 (T-extension)**.** Given a T-division ring $(D, \sigma, \delta, \mathrm{T}_a)$, a T-*extension* of D is a T′-division ring (D', σ', δ') extending (D, σ, δ) and considered with $\mathrm{T}' = \sigma' \cdot a + \delta'$.

Theorem 4.3. *Any* T*-division ring has a linearly surjective* T*-extension provided that either δ and σ commute, or σ or δ be inner.*

Proof. Recall that an *inner automorphism* is one of the form $x \mapsto b^{-1}xb$, and an *inner σ-derivation* of the form $x \mapsto \sigma(x)c - cx$. We write σ_b and δ_c respectively for the inner automorphism induced by b and the inner σ-derivation induced by c. We split the proof of Theorem 4.3 into several cases, beginning with the most elementary one.

Case 1. *$\delta = 0$ and $\sigma = \mathrm{id}$, so that $\mathrm{T}_a = \mathrm{id} \cdot a$, and a is transcendental over $Z(D)$.* As a referee says, the theory of division rings with centre $Z(D)$ extending D has $\forall\exists$ axioms, hence has an existentially closed model $\mathbf{D}$. So a is transcendental over $Z(D) = Z(\mathbf{D})$. By [8, 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 $\gamma \in \mathbf{D}[\mathrm{T}]$ 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

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

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 4.3, claiming that for any $\gamma \in \mathbf{D}[\mathrm{T}]$ of the form $xa^n + a_1 x a^{n-1} + a_2 x a^{n-2} + \cdots + a_n x$, there is $\bar{b} \in \mathbf{D}^n$ such that the following factorisation holds:

$$\gamma(x) = (xa + b_n x) \cdots (xa + b_1 x).$$

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

$$(xa + x_n x) \cdots (xa + x_1 x) = xa^n + e_1(\bar{x}) x a^{n-1} + e_2(\bar{x}) x a^{n-2} + \cdots + e_n(\bar{x}) x \tag{4.1}$$

By [10, Theorem 8.5.1], the polynomial $x^n + x^{n-1} r_1 + \cdots + x r_n + r_{n+1}$ 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 $\gamma(x) = (xa + b_n x) \cdots (xa + b_1 x)$, as desired.

Case 2. *$\delta = 0$ and $\sigma = \mathrm{id}$, so that $\mathrm{T}_a = \mathrm{id} \cdot a$.* By Case 1, we may assume that a is algebraic over $Z(D)$. We first claim that (D, id) has an extension (D_2, σ_t) with centre $Z(D_2) = Z(D)$ where t is transcendental over $Z(D_2)$. 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 [11, Theorem 7.3.6]. It follows that t is transcendental over $Z(D_2) = Z(D)$, 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

$$\mathrm{T}_a(y) = \sigma_t(y) \cdot a = t^{-1} x b. \tag{4.2}$$

If $a = 0$, there is nothing to show and if $a \neq 0$, then b is transcendental over $Z(D_2)$ (it follows indeed from Brauer's Lemma, see *e.g.* [10, Corollary 3.3.9], that the algebraic elements over $Z(D_2)$ 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), $(D_3, \sigma_t, 0, \mathrm{T}_a)$ 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

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

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 $(D_1, \sigma_{tb}, \sigma_{tb} \cdot c - c \cdot \mathrm{id}, \mathrm{T}_a)$ of $(D, \sigma, \delta, \mathrm{T}_a)$ 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 [10, 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 [10, 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 [47, Theorem 2.3], the map δ extends to a σ_t-derivation of

$D[t;\sigma]$ by putting $\delta(t)=0$ (see also [9, 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 sets and Chevalley's projection Theorem.**

Definition 4.4 (constructible set)**.** Given a T-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.

Theorem 4.5 (after Chevalley)**.** *Let D be linearly surjective and f a* T*-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 left Euclidean domain R (in the sense of Fact 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 [15, 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 4.6 (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 [34, Corollary 2.6.5]. From Claim 2 and Fact 4.6 follows immediately:

Claim 3. *Given a left Euclidean domain 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 $\mathcal{L}_R$.*

We go back to the proof of Theorem 4.5. 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 $D[\mathrm{T}]$. 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 $\mathcal{L}_{D[\mathrm{T}]}$ and conversely, a quantifier-free formula defines a constructible set. Since a T-morphism is definable (with parameters) in the language $\mathcal{L}_{D[\mathrm{T}]}$, 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 [45, 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 $U \subseteq f(F)$, one has $f(F) = \overline{f(F)}$. □

4.3. **Weak Nullstellensatz.**

Theorem 4.7 (weak Nullstellensatz)**.** *Over a linearly surjective* T*-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 (see *e.g.* [18]), and we follow this line.

Claim 4. *Let R be a right Euclidean domain, 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 [29, Theorem 3.20] and [29, 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 4.7. I has finitely many generators $\gamma_1, \dots, \gamma_r$. We consider the system $\Sigma = \{\gamma_1(\bar{x}) = 0, \dots, \gamma_r(\bar{x}) = 0\}$ and the $D[\mathrm{T}]$-module D. Since I does not contain 1, there is an embedding $D \to D[\mathrm{T}, n]/I$ of $D[\mathrm{T}]$-modules. But Σ has a solution in $D[\mathrm{T}, n]/I$, namely $(x_1 + I, \dots, x_n + I)$. Since D divisible, Σ also has a solution in D by Claim 4. □

Corollary 4.8. *Over a linearly surjective* T*-division ring D, for any maximal module I avoiding* 1*, there is $\bar{a} \in D^n$ such that*

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

Proof. We write $J_{\bar{a}} = (x_1 - a_1, \dots, x_n - a_n)$ 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 $\gamma_1, \dots, \gamma_n$ 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 $J_{\bar{a}} \subseteq \mathrm{I}(\bar{a})$ 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 4.7. One thus has $I \subseteq \mathrm{I}(\bar{a})$, and equality holds by maximality of I. □

4.4. **Strong Nullstellensatz, closed modules and radical sets.** Following Definition 1.1, when D is strict, we define the closure $\mathrm{cl}(I)$ of a module I to be the set of algebraic elements over I:

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

Theorem 4.9 (Nullstellensatz)**.** *If D is linearly surjective, for any module J avoiding* 1*, one has*

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

Proof. Let $\gamma_1, \dots, \gamma_r$ be a generating family for J, let $\gamma \in \mathrm{IV}(J)$, and let us consider the $D[\mathrm{T}]$-module $I = (\gamma_1, \dots, \gamma_r, \gamma + 1)$. 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 4.7, the module I contains 1 so there exist $\rho_1, \ldots, \rho_r, \rho$ in $D[\mathrm{T}]$ 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 4.7), we get $\rho(1) = 1$ hence $\rho\gamma \in J$, whence $\gamma \in \mathrm{cl}(J)$. □

Note that D being strict implies $I + D \subseteq \mathrm{cl}(I)$ for every module I. We say that I is a *closed* module if $\mathrm{cl}(I) = I + D$. It follows from Proposition 1.5.3 that $\mathrm{cl}(I)$ is a closed $D[\mathrm{T}]$-module.

Definition 4.10 (radical set)**.** We say that a T-affine set U is *radical* if its module $\mathrm{I}(U)$ is closed.

Note that U is radical if and only if the $D[\mathrm{T}]$-torsion of $\Gamma(U)$ is D.

Lemma 4.11. *If U, V are* T*-isomorphic* T*-affine sets, then U is radical if and only if V is radical.*

Proof. If $f\colon U \to V$ is a T-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. □

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

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

Proof. By Theorem 4.9, one has $J \subseteq \mathrm{IV}(J) \subseteq J + D$. By Theorem 4.7, the set $\mathrm{V}(J)$ is nonempty, so $\mathrm{IV}(J)$ does not contain 1, hence $\mathrm{IV}(J) \subseteq J$. □

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

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

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 $D[\mathrm{T}]$-module. Considering U up to a translation, which preserves the notion of radicality by Lemma 4.11, we may assume that U contains 0. It follows that $\mathrm{I}(U) \subseteq (x_1, \ldots, x_n)$ 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 $D[\mathrm{T}]$-module M, let us show that $M \oplus D$ is isomorphic to some $\Gamma(U)$ for a T-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 $D[\mathrm{T}]$-module $(x_1, \ldots, x_n)$. Since M is torsion-free, one has $\mathrm{cl}(N) = N$. If we set $U = \mathrm{V}(N) \subseteq D^n$, one has that U is radical, and hence $N = \mathrm{IV}(N)$ by Corollary 4.12, so $M \oplus D$ is isomorphic to $(x_1, \ldots, x_n)/\mathrm{I}(U) \oplus D = D[\mathrm{T}, n]/\mathrm{I}(U) = \Gamma(U)$. 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 [10, Section 2.3 p. 66] and [26, 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 [10, Proposition 2.3.3]). When D is countable, the fraction field of $D[t;\sigma]$ is countable, whereas $D((t,\sigma))$ is uncountable.

5. The Zariski dimension

This section introduces an analogue of the classical Zariski dimension of an algebraic variety. We still call this dimension Zariski as it coincides with the usual Zariski dimension for an algebraic group defined by p-polynomials, and shares many other geometric features, as well as (Krull-like and topological-like) definitions in terms of length of certain chains. Throughout the section, D is a strict T-division ring, and we also assume that σ is surjective.

Definition 5.1 (Zariski dimension)**.** For a T-affine set V, we define the *Zariski dimension of* V to be the dimension of the $D[\mathrm{T}]$-module $\Gamma(V)$.

We write $\dim V$ for this dimension and hope there cannot be any confusion with the dimension of V as a right $C^{\sigma,\delta}(a)$ affine space, which is most of the time simply infinite. Note that if $V \subseteq D^n$ holds, one has the equality $\dim V = n - \dim_{D[\mathrm{T}]} \mathrm{I}(V)$. It follows that D^n has dimension n, and that the empty set, a single point, or $C^{\sigma,\delta}(a)$ all have dimension zero. From Proposition 1.5 also follow:

Lemma 5.2. *For any two* T*-isomorphic* T*-affine* U *and* V*, one has* $\dim U = \dim V$.

Lemma 5.3. *For any two nonempty* T*-affine* U *and* V*, one has* $\dim(U \times V) = \dim U + \dim V$.

5.1. **Main result.** Theorem 5.5 bellow classifies T-affine sets up to isomorphism, and has a surprisingly simple proof via a diagonalisation argument using the following fact:

Fact 5.4 (see Cohn [12, Theorem 1.4.7 p. 80])**.** *Let* R *be a both left and right principal domain and* A *an* $m \times n$ *matrix with coefficients in* R*. Then the row and column rank of* A *are the same; denoting the common value by* r*, we can find* $P \in GL_m(R)$ *and* $Q \in GL_n(R)$ *such that* $PAQ^{-1} = \mathrm{diag}(e_1, \dots, e_r, 0, \dots, 0)$*, with* $e_i || e_{i+1}$ *and* $e_r \neq 0$.

As an editor tells, Fact 5.4 also appears in [2, Theorem 5.3.3 p. 226] for Euclidean domains and is attributed in this case in [2, p. 229] to Wedderburn [49, Theorem 10.1 p. 139] and Jacobson [25].

Theorem 5.5. *Let* V *be nonempty* T*-affine. There is a* T*-isomorphism* $V \simeq D^d \times U$*, where* U *is a right* $C^{\sigma,\delta}(a)$*-vector space of finite dimension, and* $d = \dim V$.

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

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

By Fact 5.4, one has $A = PBQ$ for invertible square matrices P, Q with coefficients in $D[\mathrm{T}]$ and $B = \mathrm{diag}(0, \dots, 0, \beta_{d+1}, \dots, \beta_n)$ where $\beta_{d+1}, \dots, \beta_n$ are nonzero elements of $D[\mathrm{T}]$ and d is the

number of zero entries on the diagonal of B (hence independent of any T-extension of D). One has the equivalence $(x_1,\dots,x_n)\in V \iff BQ(x_1,\dots,x_n)=0$. The map $(x_1,\dots,x_n)\mapsto Q(x_1,\dots,x_n)$ induces a T-isomorphism $V\simeq\{\bar{y}\in D^n\colon B\bar{y}=0\}$, from which follows $V\simeq D^d\times \mathrm{V}(\beta_{d+1})\times\cdots\times \mathrm{V}(\beta_n)$, as desired. Next we show $d=\dim V$. 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 5.2, also $d=\dim V$. □

In the case of an infinite perfect field k of characteristic p equipped with the Frobenius $\mathrm{T}(x)=x^p$, one recovers from Theorem 5.5 the classical counterpart that a connected algebraic subgroup of k^n defined by p-polynomials is T-isomorphic to k^d (see *e.g.* [46, Corollary 3.3.15]). Note that D need not be linearly surjective in Theorem 5.5.

Corollary 5.6. *Given a fixed set S of twists with coefficients in D, if $\mathrm{V}(S)$ is nonempty, then $\dim \mathrm{V}(S)$ does not depend on the* T*-extension of D in which $\mathrm{V}(S)$ is considered.*

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

Lemma 5.7. *Let $\mathrm{V}(S)\subseteq D^n$ be nonempty* T*-affine. One has $\dim \mathrm{V}(S)=n-\dim_{D[\mathrm{T}]}(S)$.*

Proof. By Theorem 4.9, one has $S\subseteq \mathrm{IV}(S)\subseteq \mathrm{cl}(S)$. Conclude with Proposition 1.5. 3. □

Theorem 5.8 (cut by a T-hypersurface)**.** *Let $\mathrm{V}(S)\subseteq D^n$ be* T*-affine and γ an n-twist.*

1. *If γ is algebraic over S and $\mathrm{V}(S,\gamma)$ nonempty, one has $\dim \mathrm{V}(S,\gamma)=\dim \mathrm{V}(S)$.*
2. *If γ is not algebraic over S and $\mathrm{V}(S,\gamma)$ is nonempty, one has $\dim \mathrm{V}(S,\gamma)=\dim \mathrm{V}(S)-1$.*

Proof. Point (1) follows from Proposition 1.5. 3 and Lemma 5.7. For point (2), if γ is not algebraic over S, then one has the equality $\dim_{D[\mathrm{T}]}(S,\gamma)=\dim_{D[\mathrm{T}]}(S)+1$. □

Corollary 5.9. *If $U\subsetneq V$ are nonempty* T*-affine and V is radical, one has $\dim U<\dim V$.*

Proof. Since $U\subseteq V$ is a proper inclusion, $\mathrm{I}(V)\subseteq \mathrm{I}(U)$ is also 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 5.8.2. □

We end the subsection by characterizing the dimension in terms of length of certain chains.

Theorem 5.10. *The Zariski dimension of a nonempty* T*-affine $\mathrm{V}(S)\subseteq D^n$ is equal to*

1. *the maximal length d of a chain $S\subseteq I_0\subsetneq I_1\subsetneq\cdots\subsetneq I_d$ of proper closed submodules of $D[\mathrm{T},n]$ avoiding 1 and containing S,*
2. *the maximal length d of a chain $V_0\subsetneq V_1\subsetneq\cdots\subsetneq V_d\subseteq \mathrm{V}(S)$ of nonempty proper radical* T*-affine subsets of $\mathrm{V}(S)$,*
3. *the minimal number d 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 length $m=\dim \mathrm{V}(S)$ chain of closed modules avoiding 1. 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 be a closed module containing 1, let $K\subseteq I$ be a submodule avoiding 1, and J a maximal module avoiding 1 such that $K\subseteq J\subseteq I$. Then J is closed.*

Proof of Claim 5. Let $\alpha \in \mathrm{cl}(J)$. Since D is divisible, there is a nonzero $\gamma \in D[\mathrm{T}]$ 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 $\deg(\gamma) \geqslant 1$ for a contradiction, then $\alpha + d \in I \setminus J$, so $(\alpha + d, J)$ contains 1 by maximality of J, and there is $\varepsilon \in D[\mathrm{T}]$ 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. □

We continue the proof of Theorem 5.10.1. 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 $\dim_{D[\mathrm{T}]} I_{d-i} = n - i$. For $i = 0$, the module I_d is maximal so has dimension n. If $\dim_{D[\mathrm{T}]} I_{d-i} = n - i$, one has $\dim_{D[\mathrm{T}]} I_{d-i-1} \leqslant n - i - 1$ since I_{d-i} is closed, and equality holds by maximality of the chain. This shows $\dim \mathrm{V}(I_0) = d$, but $\mathrm{cl}(S) = I_0 + D$ by maximality of the chain, hence $\dim V = d$. For (2), by Corollary 4.12, there is a one-to-one order reversing correspondence between closed modules avoiding 1 and nonempty radical T-affine sets, so (2) is equivalent to (1). For point (3), if $\mathrm{V}(S)$ has dimension d, by Theorem 5.8, 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). □

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

Theorem 5.11. *Let U be an irreducible* T*-affine set and $f\colon U \to D^m$ a* T*-morphism. 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 T-affine by Theorem 4.5.1. 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 5.7, the Zariski dimension of $\mathrm{V}(J)$ is $n - \dim_{D[\mathrm{T}]} J$. Since $\mathrm{V}(J)$ equals $\ker f$, one has

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

and the conclusion follows from the Rank-Nullity Proposition 1.5. 4 applied to $\Gamma(f)$. □

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

Proof. $\operatorname{im} f$ has Zariski dimension n by Theorem 5.11, and f is surjective by Corollary 5.9. □

6. Radical sets

We defined the notion of a *radical* set over a strict T-division ring D in Section 4.4. This last section gives this notion a closer look, and provides a criterion for certain T-affine sets to be radical. This criterion plays a central role in a forthcoming paper.

Lemma 6.1. *Let $U \subseteq V$ be nonempty* T*-affine sets. Then U and V have the same Zariski dimension if and only if the $C^{\sigma,\delta}(a)$ dimension of V/U is finite.*

Proof. Let us assume that U and V have the same dimension. It suffices to show that for any $\gamma \in \mathrm{I}(U)$, the quotient $V/V \cap \mathrm{V}(\gamma)$ has finite right $C^{\sigma,\delta}(a)$-dimension. As $\mathrm{I}(U)$ and $\mathrm{I}(V)$ have the same dimension, γ is algebraic over $\mathrm{I}(V)$. Let $\rho \in D[\mathrm{T}]$ 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 $C^{\sigma,\delta}(a)$-dependent.

As $\gamma(\bar{g}_1), \ldots, \gamma(\bar{g}_n)$ are roots of ρ, by Fact 2.3, there is a nontrivial $C^{\sigma,\delta}(a)$-linear combination with $\gamma(\bar{g}_0)\lambda_0 + \cdots + \gamma(\bar{g}_n)\lambda_n = 0$, 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 $C^{\sigma,\delta}(a)$-dimension at most n, as desired. Conversely, assume that V/U has finite $C^{\sigma,\delta}(a)$-dimension, and let $\gamma \in \mathrm{I}(U)$. Then $V/V \cap \mathrm{V}(\gamma)$ has a finite basis $(\bar{g}_1, \ldots, \bar{g}_n) + V \cap \mathrm{V}(\gamma)$. By Fact 2.3, there is $\rho \in D[\mathrm{T}]$ 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.**

Definition 6.2. Given a T-affine set V and a point $a \in V$, the *radical component of a in V* is the intersection of all T-affine subsets of V that contain a and have the same Zariski dimension as V.

We write $V^0(a)$ for the radical component of a in V.

Lemma 6.3. *For any* T*-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* T*-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 $C^{\sigma,\delta}(a)$-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 $V^0(a) \subseteq \mathrm{V}(\gamma')$. 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 5.5 and Lemma 4.11. □

6.2. **An example of a radical group.** Given a strict T-division ring D where T is induced by a, a natural number $n \geqslant 1$ and a tuple $\bar{b} = (b_1, \ldots, b_n)$, we consider the T-affine set

$$G_{\bar{b}} = \{(x_1, \ldots, x_n) \in D^n \colon b_1(\mathrm{T}x_1 - ax_1) = b_i(\mathrm{T}x_i - ax_i) \text{ for all } 1 \leqslant i \leqslant n\},$$

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

Lemma 6.4. *Given any tuple $(r_1, \ldots, r_n) \in D^n$, the right dimension of $(r_1, \ldots, r_n)$ over $C^{\sigma,\delta}(a)$ does not vary when computed in a* T*-extension of D.*

Proof. By Fact 2.3, right $C^{\sigma,\delta}(a)$-dependence of a tuple $(r_1, \ldots, r_n)$ 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 $C^{\sigma,\delta}(a)$-dependence of $(r_1, \ldots, r_n)$ does not depend on the T-extension of D. □

Lemma 6.5 bellow is inspired by [27, Lemma 2.8] and its linearised version [22, Lemma 5.3]. It plays a crucial role in [27] and [22] in the particular case when (D, T) is an algebraically closed field (k, σ_p) of characteristic p equipped with the Frobenius σ_p. In that particular case, if $\left(b_1^{-1}, \ldots, b_n^{-1}\right)$ are $\mathbf{F}_p$-linearly independent, [22, Lemma 5.3] states that, $G_{\bar{b}}$ is *connected* as an algebraic group, whereas Lemma 6.5 only states that $G_{\bar{b}}$ has no subgroup of finite index defined by p-polynomials. But one recovers the conclusion of [22, Lemma 5.3] knowing that $G_{\bar{b}}$ is σ_p-isomorphic to $(k, +)$ by Theorem 5.5, and $(k, +)$ is connected, so that $G_{\bar{b}}$ is connected as well.

Lemma 6.5. *Assume that a is central, and σ and δ commute. Given $\bar{b} = (b_1, \ldots, b_n)$ in $D^\times$, the set $G_{\bar{b}}$ is radical if and only if $\left(b_1^{-1}, \ldots, b_n^{-1}\right)$ are left $C^{\sigma,\delta}(a)$-linearly independent.*

Proof. We first assume that $G_{\bar{b}}$ is radical and put $\gamma = \mathrm{T} - a\mathrm{id}$. If there are $(r_1, \dots, r_n)$ in $C^{\sigma,\delta}(a)$ such that $r_1 b_1^{-1} + \cdots + r_n b_n^{-1} = 0$, one has for every $(x_1, \dots, x_n) \in G_{\bar{b}}$,

$$\gamma(r_1 x_1 + \cdots + r_n x_n) = \sum_{i=1}^{n} r_i \gamma(x_i) = \sum_{i=1}^{n} r_i b_i^{-1} b_i \gamma(x_i) = \left(\sum_{i=1}^{n} r_i b_i^{-1} \right) b_1 \gamma(x_1) = 0.$$

It follows that $r_1 x_1 + \cdots + r_n x_n$ is algebraic over $\mathrm{I}(G_{\bar{b}})$, so belongs to $\mathrm{I}(G_{\bar{b}})$ by assumption. This implies that $r_1 x_1 + \cdots + r_n x_n$ vanishes on $C^{\sigma,\delta}(a) \times \cdots \times C^{\sigma,\delta}(a)$, 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 T-extension (E, T') of (D, T). We chose (E, T') linearly surjective by Theorem 4.3 and we look at T′-varieties over E. By induction hypothesis and Lemma 6.4 (since T still defines a pseudo-linear transformation in the opposite division ring), 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 5.8, 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 6.3, 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 $\pi \left(G^0_{b_1,\dots,b_n} \right)$ is σ'-affine and has dimension 1 by Theorem 5.11. Since $G_{b_1,\dots,b_{n-1}}$ is radical, by Corollary 5.9, 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 $\gamma' \in \mathrm{cl}\left(\mathrm{I}\left(G_{b_1,\dots,b_n}\right)\right) \setminus \mathrm{I}\left(G_{b_1,\dots,b_n}\right)$ with coefficients in D. Replacing inductively $\mathrm{T}'(x_i)$ by $a x_i + b_i^{-1} b_1 \gamma(x_1)$ 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

$$\{\alpha(x_1) + r_2 x_2 + \cdots + r_n x_n = 0,\ b_1\gamma(x_1) = \cdots = b_n\gamma(x_n)\},$$

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

$$\gamma\alpha(x_1) + \gamma(r_2 x_2) + \cdots + \gamma(r_{n-1} x_{n-1}) + b_n^{-1} b_1 \gamma(x_1) = 0,$$

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 $r_2 \in C^{\sigma',\delta'}(a) \cap D = C^{\sigma,\delta}(a)$, and symmetrically $r_2, \dots, r_{n-1} \in C^{\sigma,\delta}(a)$, hence

$$\gamma\alpha(x_1) + r_2 b_2^{-1} b_1 \gamma(x_1) + \cdots + r_{n-1} b_{n-1}^{-1} b_1 \gamma(x_1) + b_n^{-1} b_1 \gamma(x_1) = 0,$$

which holds for all $x_1 \in E$ by (6.1). It follows that $\alpha(x_1) = r_1 x_1$ for some $r_1 \in C^{\sigma,\delta}(a)$, which yields

$$r_1 b_1^{-1} + r_2 b_2^{-1} + \cdots + r_{n-1} b_{n-1}^{-1} + b_n^{-1} = 0,$$

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

7. Appendix. On ω-stage Euclidean domains

We show here that a matrix with coefficients in an ω-stage Euclidean ring is equivalent to a diagonal one. This generalises the corresponding Theorem [49, 10.1 p. 139] for Euclidean rings in a different direction than the PID case [12, 1.4.7 p. 80]. We also provide a trigonalisation result when coefficients belong to an ω-stage *left* Euclidean ring. Let us recall the definitions adapted from the commutative case [14, p. 135], which appear *e.g.* in [33, Section 7 p. 27]:

Let R be an integral domain, and (a, b) in R^2. A *right k-stage division chain starting from* (a, b) is a sequence of equations $a = bq_1 + r_1$, $b = r_1q_2 + r_2$, $r_1 = r_2q_3 + r_3$, $\dots$, $r_{k-2} = r_{k-1}q_k + r_k$.

Definition 7.1 (ω-stage right Euclidean)**.** Let $N\colon R \to \mathbf{Z}$ be a function with $N(0) = 0$ and $N(a) > 0$ for all $a \neq 0$. The ring R is *ω-stage right Euclidean* if for every pair (a, b) with $b \neq 0$, there is a right k-stage division chain for some $k \in \mathbf{N}$ such that last remainder r_k satisfies $N(r_k) < N(b)$.

An ω-stage *left* Euclidean domain is defined similarly, and we say that a domain is *ω-stage Euclidean* if it is both ω-stage right and left Euclidean with respect to the same function N.

Theorem 7.2. *Let R be an ω-stage Euclidean ring and $A \in M_n(R)$. There exist a diagonal $B \in M_n(R)$ and invertible $P, Q \in GL_n(R)$ such that $A = PBQ$.*

Proof. We slightly modify the diagonalisation algorithm of [21, Theorem 7.10] given for commutative Euclidean rings. For any $i \neq j$, let F_{ij} be the matrix obtained from the identity matrix by interchanging row i and row j, $H_{ij}(r)$ the one obtained from the identity by adding r times row j to row i and $\bar{H}_{ij}(r)$ by adding column j times r to column i. Since each of these matrix have coefficients in a commutative subring and have determinant -1 or 1, they are invertible. The effect of premultiplying a matrix

(a) by F_{ij} is to interchange row i and row j,
(b) by $H_{ij}(r)$ is to add r times row j to row i,

and the effect of postmultiplying a matrix

(c) by F_{ij} is to interchange column i and column j,
(d) by $\bar{H}_{ij}(r)$ is to add column j times r to column i,

Our aim is to reduce the starting matrix A to an equivalent matrix of the form

$$\left(\begin{array}{c|c} r_{11} & 0 \ \cdots \ 0 \\ \hline 0 & \\ \vdots & C \\ 0 & \end{array}\right) \qquad (£)$$

If $A = (a_{ij})$ is nonzero, by a suitable exchange of lines and columns, we may assume $a_{11} \neq 0$. We describe a finite sequence of elementary row and column operations which, when performed on A, either yields a matrix of the form (£) or else leads to a matrix B $= (b_{ij})$ satisfying

$$N(b_{11}) < N(a_{11}) \qquad (€)$$

In the latter case we go back to the beginning and apply the sequence of operations again. The sequence of operations is as follows.

Case 1. There is a second nonzero entry a_{j1} in the first column. Consider a left k-stage division chain $a_{j1} = q_1a_{11} + r_1$, $a_{11} = q_2r_1 + r_2$,..., $r_{k-2} = q_kr_{k-1} + r_k$ with $N(r_k) < N(a_{11})$ starting from (a_{j1}, a_{11}). Adding $-q_1$ times row 1 to row j and interchanging rows 1 and j replaces in the first column the pair (a_{11}, a_{j1}) by (r_1, a_{11}). Then adding $-q_2$ times row 1 to row j and interchanging rows 1 and j replaces (r_1, a_{11}) by (r_2, r_1). Continuing this way k times, we end with a first column in which the initial pair (a_{11}, a_{j1}) has been replaced by (r_k, r_{k-1}). So this achieves (€).

Case 2. There is a second nonzero entry a_{1j} in the first row. We proceed similarly considering a right k-stage division chain starting from (a_{1j}, a_{11}), and also achieve (€).

Case 3. (£) is achieved. □

With a similar argument, we get this generalisation of [15, Proposition 6.2]:

Theorem 7.3. *Let R be an ω-stage left Euclidean ring and $A \in M_n(R)$, there exist invertible $P, Q \in GL_n(R)$ with Q having $\{0,1\}$ coefficients, and an upper triangular $B \in M_n(R)$ of the form*

$$B = \left(\begin{array}{c|c} B_{11} & B_{12} \\ \hline 0 & 0 \end{array}\right)$$

where B_{11} is upper triangular with nonzero diagonal coefficients , such that $A = PBQ$.

Proof. Starting with a nonzero A, our aim is to reduce A to an equivalent matrix of the form

$$\left(\begin{array}{c|ccc} r_{11} & r_{12} & \cdots & r_{1n} \\ \hline 0 & & & \\ \vdots & & C & \\ 0 & & & \end{array}\right), \qquad (\$)$$

where r_{11} is nonzero. Repeating Case 1 of the previous proof eventually leads to a matrix of the form ($) where r_{11} is nonzero since the last but one remainder r_{k-1} of a division chain is nonzero. □

Given an ω-stage left Euclidean domain R, Theorem 7.3 has the following immediate consequences on the first order theory of divisible R-modules. We consider the language $\mathcal{L}_R$ of left R-modules and write DM_R for the $\mathcal{L}_R$-theory of *divisible R-modules* axiomatised by the axioms $\forall y \exists x (rx = y)$ for all nonzero $r \in R$, and the axioms of left R-modules. An *equation* is a formula of the form $r_1 x_1 + \cdots + r_n x_n = 0$. A formula is *prime positive* (p.p. for short) if of the form $\exists \bar{x} \varphi(\bar{x}, \bar{y})$ for some finite conjunction φ of equations. With a proof similar to the one of [40, Theorem 2.$\mathbb{Z}$.1], one has a quantifier elimination result for p.p.-formulas:

Corollary 7.4. *For all p.p.-formula $\exists \bar{x} \varphi(\bar{x}, \bar{y})$, there are finitely many equations $\varphi_i(\bar{y})$ such that*

$$\mathrm{DM}_R \models \forall \bar{y} \left(\bigwedge \varphi_i(\bar{y}) \leftrightarrow \exists \bar{x} \varphi(\bar{x}, \bar{y}) \right).$$

Corollary 7.5. *For a boolean combination φ of p.p.-sentences, one has $\mathrm{DM}_R \models \varphi$ or $\mathrm{DM}_R \models \neg\varphi$.*

Corollary 7.6. *Let M be a divisible R-module and Σ a finite set of equations. If Σ has a solution in a left R-module extending M, then Σ has a solution in M.*

References

[1] Michael Artin. *Algebra*. Pearson, Second Edition, 2010.

[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] 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.

[9] 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.

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

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

[12] Paul Moritz Cohn. *Free ideal rings and localization in general rings*, volume 3 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2006.
[13] Richard Cohn. *Difference Algebra*. Interscience Publishers, 1965.
[14] 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.
[15] 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.
[16] Gérard Duchamp (https://mathoverflow.net/users/25256/duchamp-gérard-h-e). On rings R such that $xR \cap yR$ is non zero whenever x and y are non zero. MathOverflow. `https://mathoverflow.net/q/232420` (version: 2017-12-02).
[17] Uriya First (https://mathoverflow.net/users/86006/uriya-first). Dimension of a module over a left-Ore domain. MathOverflow. `https://mathoverflow.net/q/311966` (version: 2018-10-03).
[18] Nicolas Ford. A model-theoretic proof of Hilbert's Nullstellensatz. *https://www.math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALFULL/Ford.pdf*, 2007.
[19] John Goodrick (https://mathoverflow.net/users/93/john-goodrick). Examples of NIP fields of characteristic p. MathOverflow. `https://mathoverflow.net/q/232448` (version: 2016-02-29).
[20] Ulrich Görtz and Torsten Wedhorn. *Algebraic geometry I*. Advanced Lectures in Mathematics. Vieweg + Teubner, Wiesbaden, 2010. Schemes with examples and exercises.
[21] Brian Hartley and Trevor Hawkes. *Rings, Modules and Linear Algebra*. Chapman and Hall, London, 1970.
[22] Nadja Hempel. On n-dependent groups and fields. *Mathematical Logic Quarterly*, 62:215–224, 2016.
[23] Drike (https://mathoverflow.net/users/18583/drike). Existence of a skew field with surjective inner derivations. MathOverflow. `https://mathoverflow.net/q/229479` (version: 2016-01-28).
[24] James Humphreys. *Linear algebraic groups*. Graduate texts in mathematics. Springer-verlag, 1975.
[25] Nathan Jacobson. Pseudo-linear transformations. *Annals of Mathematics*, 38:484–507, 1937.
[26] Nathan Jacobson. *Finite-dimensional division algebras over fields*. Springer-Verlag, Berlin, Corrected 2nd printing, 2010.
[27] Itay Kaplan, Thomas Scanlon, and Frank Wagner. Artin-Schreier extensions in NIP and simple fields. *Israel Journal of Mathematics*, 185:141–153, 2011.
[28] Earl Laerson. Onto inner derivations in division rings. *Bulletin of the American Mathematical Society*, 67:356–358, 1961.
[29] Tsit Yuen Lam. *Lectures on Modules and Rings*, volume 189 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.
[30] Tsit Yuen Lam and André Leroy. Vandermonde and Wronskian matrices over division rings. *Journal of Algebra*, 119:308–336, 1988.
[31] Tsit Yuen Lam and André Leroy. Wedderburn polynomials over division rings. I. *Journal of Pure and Applied Algebra*, 186:43–76, 2004.
[32] André Leroy. Noncommutative polynomial maps. *Journal of Algebra and its Applications*, 11:1250076, 16, 2012.
[33] Pierre Lezowski. On some Euclidean properties of matrix algebras. *Journal of Algebra*, 486:157–203, 2017.
[34] 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.
[35] Gary Meisters. On the equation $ax - xb = c$ in division rings. *Proceedings of the American Mathematical Society*, 12:428–432, 1961.
[36] Bernhard Hermann Neumann. Groups covered by permutable subsets. *Journal of the London Mathematical Society*, 29:236–248, 1954.
[37] Øystein Ore. Theory of non-commutative polynomials. *Annals of Mathematics. Second Series*, 34:480–508, 1933.
[38] Daniel Perrin. *Géométrie algébrique, une introduction*. EDP Sciences, CNRS Éditions, 2001.
[39] Françoise Point. Some model theory of Bezout difference rings-a survey. *Bulletin of the Belgian Mathematical Society Simon Stevin*, 13:807–826, 2006.
[40] Mike Prest. *Model Theory and Modules*. London Mathematical Society Lecture notes, 1988.
[41] Jeremy Rickard (https://mathoverflow.net/users/22989/jeremy-rickard). Extending an automorphism to an inner one. MathOverflow. `https://mathoverflow.net/q/280651` (version: 2017-09-08).
[42] 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.

[43] 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.
[44] Tonny Springer. *Linear algebraic groups*. Birkhaüser, 1998.
[45] Patrice Tauvel and Rupert Yu. *Lie Algebras and Algebraic groups*. Springer Monographs in Mathematics, 2005.
[46] 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.
[47] Michael Voskoglou. Extending derivations and endomorphisms to skew polynomials rings. *Publications de l'Institut Mathématique (Beograd)*, 53:79–82, 1986.
[48] Frank Wagner. Small fields. *Journal of Symbolic Logic*, 63(3):995–1002, 1998.
[49] 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@gmail.com