Pseudo-linear algebra over a division ring

Cédric Milliet

First paper, not a submission to the JSL.

LINEAR ALGEBRA OVER A DIVISION RING

CÉDRIC MILLIET

ABSTRACT. We consider an analogue of the Zariski topology over a division ring D equipped with a ring morphism $\sigma : \mathrm{D} \to \mathrm{D}$. A basic closed subset of D^n is given by the zero set of a (finite) family of linear combinations of $\{\sigma^{i_1}(x_1), \ldots, \sigma^{i_n}(x_n) : (i_1, \ldots, i_n) \in \mathbb{N}^n\}$ having left coefficients in D. This enables us to define elementary notions of algebraic geometry: algebraic sets, σ-morphisms and comorphisms, a notion of Zariski dimension, a notion of radical component of an algebraic set. We classify the algebraic sets over D up to σ-isomorphisms when σ is onto D and $[\mathrm{D} : \mathrm{Fix}(\sigma)]$ infinite (and as a by-product, the additive algebraic groups over a perfect field), and show that any division ring with infinite $[\mathrm{D} : \mathrm{Fix}(\sigma)]$ has an extension in which each affine polynomial $r + r_0 x + r_1 \sigma(x) + \cdots + r_n \sigma^n(x)$ has a root. In such an extension, Chevalley's projection Theorem for constructible sets holds, as well as affine Nullstellensätze. These results are intended to be applied in a further paper to division rings that do not have Shelah's independence property.

The paper is motivated by this question coming from model theory: is a division ring without the independence property a finite dimensional algebra over its centre? With this aim, our guiding idea is to mimic I. Kaplan and T. Scanlon's proof of [KSW11, Theorem 4.3], where it is shown that if F is an infinite field of characteristic p and without the independence property, then the Artin-Schreier map $\mathrm{Froeb} - \mathrm{id}$ is onto F. By mimic we mean consider a division ring D with infinite $[\mathrm{D} : \mathrm{Fix}(\sigma)]$ instead of the infinite field F replacing Froeb with any ring morphism $\sigma : \mathrm{D} \to \mathrm{D}$, and show that $\sigma - \mathrm{id}$ is onto D whenever D does not have the independence property.

Section 1 presents some basic linear algebra in a module M over a *left-Ore* domain and shows that the cardinality of a maximal independent subset of M defines a well-behaved notion of *dimension* for M. In Section 2, defining a *Euclidean ring* to be any ring R endowed with a Euclidean function $\phi : \mathrm{R} \to \mathbb{N} \cup \{-\infty\}$ for which R is both right- and left-Euclidean, we derive from a diagonalisation argument that in the language of R-modules, the theory of divisible modules over a Euclidean ring R eliminates quantifiers, just as in the case where R is commutative, which will allow transfer arguments. Section 3 presents polynomials that corresponds to our problem, namely one-variable polynomials $r_0 x + \cdots + r_n \sigma^n(x)$ in σ having left coefficients in D. As they are right $\mathrm{Fix}(\sigma)$-linear, we call such polynomials *linear twists*. The ring of linear twists in one variable is written $\mathrm{D}(\sigma)$, and the set of linear twists in n variables $\mathrm{D}(\sigma, n)$, namely linear combinations of $\{\sigma^{i_1}(x_1), \ldots, \sigma^{i_n}(x_n) : (i_1, \ldots, i_n) \in \mathbb{N}^n\}$ having left coefficients in D; $\mathrm{D}(\sigma, n)$ is a left $\mathrm{D}(\sigma)$-module, and we point out that $\mathrm{D}(\sigma)$ is Euclidean when σ is onto D. After introducing elementary notions of algebraic geometry over D^n in Section 4, we define in Section 5 the Zariski dimension of an algebraic subset

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

Key words and phrases. Division ring, model theory.

Thanks to the Mathoverflow community `http://mathoverflow.net/`. In particular to Tom De Medts for pointing at [Mei61] and [Lae61].

of D^n and classify the algebraic subsets of D^n up to σ-isomorphisms when σ is onto D and $[\mathrm{D} : \mathrm{Fix}(\sigma)]$ infinite. The last Section is devoted to *linearly-closed* division rings, that is division rings in which every affine twist $r + r_0x + r_1\sigma(x) + \cdots + r_n\sigma^n(x)$ has a root. When $[\mathrm{D} : \mathrm{Fix}(\sigma)]$ is infinite, we deduce from a series of results of P. Cohn that D has a linearly-closed extension $\mathbf{D}$, in which Chevalley's projection Theorem on constructible sets holds, as well as affine Nullstellensätze.

We answer our motivating question positively for division rings of characteristic p in a further paper.

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

Let R be a domain (associative, with identity, possibly non-commutative). Throughout the Section, we assume that R satisfies the *left Ore condition*, that is, for any non-zero elements $(a, b) \in \mathrm{R}^2$, one has $\mathrm{R}a \cap \mathrm{R}b \neq (0)$. Let M be a left R-module. All modules considered in the paper are left modules.

1.1. **Basis and algebraicity.**

A family $\bar{v} \in \mathrm{M}^n$ is *dependent* if there is a non-zero $\bar{r} \in \mathrm{R}^n$ such that $r_1v_1 + \cdots + r_nv_n = 0$, or *independent* otherwise. It is a *basis* if it is independent and maximal with this property.

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

Proof. An increasing union of independent families is independent. □

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

Lemma 1.2 (transitivity of algebraicity)**.** *Let A, B, C be subsets of* M*. 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 $r, r_1, \ldots, r_n$ in $\mathrm{R} \setminus \{0\}$, tuples $\bar{b} \in B^n$ and $\bar{c} \in C^m$ such that for all $i \in \{1, \ldots, n\}$,

$$ra \in (\bar{b}) \quad \text{and} \quad r_ib_i \in (\bar{c}).$$

In particular, there is an expression of the form $sa \in (\bar{c}) + \sum_{i\in I} s_ib_i$, with $s \in \mathrm{R} \setminus \{0\}$, and one may assume that the set $I \subset \{1, \ldots, n\}$ has minimal cardinality. We claim that I is empty. Otherwise $1 \in I$ say. Let $J = I \setminus \{1\}$. By Ore's condition, there are non-zero $(u, v) \in \mathrm{R}^2$ such that $us_1 = vr_1$ hence $us_1b_1 \in (\bar{c})$, and one has $(us)a \in (\bar{c}) + \sum_{i\in J} us_ib_i$ with us non-zero as u and s are non-zero, a contradiction with the minimality of I. □

1.2. **Dimension.**

Theorem 1.3 (after Steinitz)**.** *All basis of* M *have the same cardinality.*

Proof. Treat the particular case where M has a finite basis $\bar{b} = (b_1, \dots, b_n)$. Let $(c_1, \dots, c_m, \dots)$ be another basis of M. By maximality of $\bar{b}$, one can write $rc_1 = \sum r_i b_i$ for some non-zero $r \in \mathrm{R}$. As c_1 is free, r_1 say is non-zero. 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 $(c_1, b_2, \dots, b_n)$. One concludes in a similar way that M is algebraic over $(c_1, c_2, b_3, \dots, b_n)$, and iterating, one can add every c_i. If $m > n$, we conclude that c_m is algebraic over its predecessors, a contradiction, so $m \leqslant n$, and all basis of M are finite. By symmetry, one has $n = m$. □

We write $\dim_{\mathrm{R}}\mathrm{M}$ and call R-*dimension* of M this number.

Lemma 1.4 (sum)**.** *Let* N *be another* R*-module. One has*

$$\dim_{\mathrm{R}}\mathrm{M} \oplus \mathrm{N} = \dim_{\mathrm{R}}\mathrm{M} + \dim_{\mathrm{R}}\mathrm{N}.$$

Proof. Let $\bar{b}$ and $\bar{c}$ be basis of M and N respectively. Then $\bar{b} \cup \bar{c}$ is an independent family of $\mathrm{M} \oplus \mathrm{N}$. We claim that it is maximal such. If $v + u \in \mathrm{M} \oplus \mathrm{N}$, then v is algebraic over $\bar{b}$, as well as u over $\bar{c}$, so there are non-zero $(s, t) \in \mathrm{R}^2$ such that $sv \in (\bar{b})$ and $tu \in (\bar{c})$. By Ore's condition, there is a non-zero $r \in \mathrm{R}$ such that $r(u + v) \in (\bar{b}, \bar{c})$. □

Lemma 1.5 (quotient)**.** *Let* $\mathrm{N} \subset \mathrm{M}$ *be a submodule. One has*

$$\dim_{\mathrm{R}}\mathrm{M/N} + \dim_{\mathrm{R}}\mathrm{N} = \dim_{\mathrm{R}}\mathrm{M}.$$

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

Lemma 1.6 (algebraic closure)**.** *For all* $S \subset \mathrm{M}$*, the subset* $\mathrm{cl}(S) \subset \mathrm{M}$ *of algebraic elements over* S *is a submodule and*

$$\dim_{\mathrm{R}}\mathrm{cl}(S) = \dim_{\mathrm{R}}(S).$$

Proof. Let a and b be in $\mathrm{cl}(S)$. For all $r \in \mathrm{R}$, the element $a + rb$ is algebraic over $\{a, b\}$, which is algebraic over S, so $a + rb$ is algebraic over S by Lemma 1.2, and $\mathrm{cl}(S)$ is a submodule. A base $\bar{b}$ for (S) is also a base for $\mathrm{cl}(S)$ since $\mathrm{cl}(S)$ is algebraic over (S), hence over $\bar{b}$. □

Lemma 1.7. *Let* $f : \mathrm{M} \to \mathrm{N}$ *be a morphism of* R*-modules. Then*

$$\dim_{\mathrm{R}} \mathrm{Ker} f + \dim_{\mathrm{R}} \mathrm{Im} f = \dim_{\mathrm{R}} \mathrm{M}.$$

Proof. Considering the induced bijection $\mathrm{M/Ker}f \to \mathrm{Im}f$ and in view of Lemma 1.5, we may assume 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. □

2. Quantifier elimination in modules over a Euclidean ring

Modulo the first-order theory of modules over a commutative Euclidean ring, a prime positive formula is equivalent to a conjunction of prime positive formulas of quantifier complexity 1 (see [Pre88, Theorem 2.$\mathbb{Z}$.1]). It follows that the theory of divisible modules over a commutative Euclidean ring eliminates the quantifiers of prime positive formulas. We point out that this also holds when the ring R is non-commutative. In this case, we call R a *Euclidean* ring if there is a Euclidean function $\phi : \mathrm{R} \to \mathbb{N} \cup \{-\infty\}$ for which R is both right- and left-Euclidean. In the Section, R stands for a Euclidean ring.

Lemma 2.1. *Let* $\mathrm{A} \in \mathrm{M}_n(\mathrm{R})$. *Then* $\mathrm{A} = \mathrm{PDQ}$ *where* D *is diagonal and* $\mathrm{P}, \mathrm{Q} \in \mathrm{GL}_n(\mathrm{R})$.

Proof. We slightly modify the diagonalisation algorithm of [HH70, 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 ring 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

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

If $\mathrm{A} = (a_{ij})$ is non-zero, 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 $\mathrm{B} = (b_{ij})$ satisfying

(€)
$$\phi(b_{11}) < \phi(a_{11})$$

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 an entry a_{j1} in the first column such that a_{11} does not right-divide a_{j1}, hence we can write $a_{j1} = qa_{11} + r$ with $\phi(r) < \phi(a_{11})$ and $r \neq 0$. Add $-q$ times row 1 to row j and interchange row 1 and j replaces the leading entry a_{11} by r and so achieves (€).
Case 2. There is an entry a_{1j} in the first row such that a_{11} does not left-divide a_{1j}, hence we can write $a_{1j} = a_{11}q + r$ with $\phi(r) < \phi(a_{11})$ and $r \neq 0$. Add column 1 times $-q$ to column j and interchange column 1 and j replaces the leading entry a_{11} by r and so achieves (€).
Case 3. a_{11} right-divides every entry in the first column, and left-divides every entry in the

first row. Adding suitable left multiples of the first row to the other rows, we can replace all the entries in the first column, other than a_{11}, by zeros. Adding suitable right multiples of the first column to the other columns, we can replace all the entries in the first row, other than a_{11}, by zeros. This brings us to (£). □

We consider the first-order language $\mathcal{L}_{\mathrm{R}} = (+, -, 0, \hat{r} : r \in \mathrm{R})$ of left R-modules where $\hat{r}$ is a unary function symbol. We write DM(R) for the $\mathcal{L}_{\mathrm{R}}$-theory of *divisible* R*-modules* axiomatised by

(D) the axioms $\forall y \exists x (\hat{r}x = y)$ for all non-zero $r \in \mathrm{R}$,
(M) the axioms of left R-modules.

A formula is an *equation* if it is given by equality of two terms. 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.

Theorem 2.2 (quantifier elimination for p.p.-formulas)**.** *For all* p.p.*-formula* $\exists \bar{x} \varphi(\bar{x}, \bar{y})$*, there is a finite conjunction* $\bigwedge \varphi_i(\bar{y})$ *of equations such that*

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

Proof. Same proof as in [Pre88, Theorem 2.ℤ.1]. Write $\varphi(\bar{x}, \bar{y})$ in the form $A\bar{x} = B\bar{y}$, where A and B are square matrices over R. By Lemma 2.1, $\exists \bar{x}(A\bar{x} = B\bar{y})$ is equivalent modulo the theory of R-modules, to $\exists \bar{x}(D\bar{x} = C\bar{y})$ for some diagonal matrix D and matrix C over R, hence to a finite conjunction of formulas of the form $\exists x_i(d_i x_i = c_i(\bar{y}))$ where d_i is the ith diagonal term of D and $c_i(\bar{y})$ the ith entry of $C\bar{y}$. But in a divisible module, $\exists x_i(d_i x_i = c_i(\bar{y}))$ is always true if $d_i \neq 0$ or it is equivalent to $c_i(\bar{y}) = 0$ if $d_i = 0$. □

Corollary 2.3 (p.p.-completeness)**.** *For any boolean combination* φ *of* p.p.*-sentences, one either has* $\mathrm{DM(R)} \models \varphi$ *or* $\mathrm{DM(R)} \models \neg\varphi$*.*

Proof. Let $\mathcal{M}, \mathcal{N} \models \mathrm{DM(R)}$. By Theorem 2.2, if φ holds in $\mathcal{M}$, it is equivalent modulo DM(R) to the sentence $0 = 0$, which holds in $\mathcal{N}$. So φ holds in $\mathcal{N}$. □

Corollary 2.4 (p.p.-closeness)**.** *Let* $\mathcal{M} \models \mathrm{DM(R)}$ *and* Σ *a finite set of equations. If* Σ *has a solution in a left* R*-module* $\mathcal{N}$ *extending* $\mathcal{M}$*, it has a solution in* $\mathcal{M}$*.*

Proof. By [Lam99, Theorem 3.20], there is a divisible left R-module $\boldsymbol{\mathcal{N}}$ extending $\mathcal{N}$. Having a solution for Σ is expressible by a p.p.-sentence $\exists \bar{x} \varphi(\bar{x})$. But $\boldsymbol{\mathcal{N}} \models \exists \bar{x} \varphi(\bar{x})$ so $\mathcal{M} \models \exists \bar{x} \varphi(\bar{x})$ by Corollary 2.3. □

3. Twists over division rings

3.1. **Linear twists.** Let D be a division ring, σ a unary function symbol and $\sigma_{\mathrm{D}} : \mathrm{D} \to \mathrm{D}$ a ring morphism. We consider the ring of *linear twists*

$$\mathrm{D}(\sigma) = \left\{ \sum_{i=0}^{n} r_i \sigma^i \ : \bar{r} \in \mathrm{D}^{n+1},\ n \in \mathbb{N} \right\},$$

equipped with the sum

$$\sum_{i=0}^{n} r_i \sigma^i + \sum_{j=0}^{n} s_j \sigma^j = \sum_{k=0}^{n} (r_k + s_k) \sigma^k$$

and composition law

$$\left(\sum_{i=0}^{n} r_i\sigma^i\right)\left(\sum_{j=0}^{n} s_j\sigma^j\right) = \sum_{i=0}^{n}\left(\sum_{j=0}^{n} r_i\sigma_{\mathrm{D}}^i(s_j)\sigma^{i+j}\right).$$

It is a unitary (we also write id for σ^0) associative integral domain. The *degree* of a linear twist is the greatest power of σ appearing with a non-zero coefficient, or $-\infty$ for the zero twist.

Lemma 3.1 (Euclidean division)**.** *Let* $(\delta,\gamma)\in \mathrm{D}(\sigma)\times\big(\mathrm{D}(\sigma)\setminus\{0\}\big)$.

(1) *There is a unique* $(q,r)\in \mathrm{D}(\sigma)\times\mathrm{D}(\sigma)$ *such that* $\delta = q\gamma + r$ *and* $\deg r < \deg\gamma$.
(2) *If* σ_{D} *is onto, there is a unique* (q,r) *such that* $\delta = \gamma q + r$ *and* $\deg r < \deg\gamma$.

Proof. By induction on $\deg\delta$. Let $r_{n+1}\sigma^{n+1}$ and $s_d\sigma^d$ be the leading terms of δ and γ. For $n+1<d$, we put $q=0$ and $r=\delta$. Assume $n+1\geqslant d$.
(1) Let $q_1 = (r_{n+1}\sigma^{n+1-d})(s_d^{-1}\mathrm{id})$. As $\deg(\delta - q_1\gamma) < n+1$, by induction hypothesis, there are (q_2,r) such that $\deg r < d$ and $\delta - q_1\gamma = q_2\gamma + r$. We put $q = q_1+q_2$.
(2) Let $q_1 = \sigma_{\mathrm{D}}^{-d}(s_d^{-1}r_{n+1})\sigma^{n+1-d}$, such that one has $\deg(\delta-\gamma q_1) < n+1$. □

By Lemma 3.1.(1), $\mathrm{D}(\sigma)$ is a left-principal, left-Noetherian and left-Ore ring.

3.2. **Evaluating and factorising in** D. Given a linear twist $\delta = r_0\mathrm{id}+\cdots+r_n\sigma^n$, we define the map $\delta_{\mathrm{D}}:\mathrm{D}\to\mathrm{D}$ by putting $\delta_{\mathrm{D}}(r) = r_0r+\cdots+r_n\sigma_{\mathrm{D}}^n(r)$. We also write r^δ for $\delta_{\mathrm{D}}(r)$. For all linear twists δ and γ one has $(\delta+\gamma)_{\mathrm{D}} = \delta_{\mathrm{D}}+\gamma_{\mathrm{D}}$ and $(\delta\gamma)_{\mathrm{D}} = \delta_{\mathrm{D}}\circ\gamma_{\mathrm{D}}$, so that the evaluation operator $eval:\mathrm{D}(\sigma)\to\mathrm{D}^{\mathrm{D}},\ \delta\mapsto\delta_{\mathrm{D}}$ is a ring morphism.

Lemma 3.2 (factorisation)**.** *Let* δ *be a linear twist of degree* $n+1$. *If* a *is a non-zero root of* δ_{D}, *there is a twist* γ *of degree* n *such that*

$$\delta = \gamma(\sigma - a^\sigma a^{-1}\mathrm{id}).$$

Proof. There is $\gamma\in\mathrm{D}(\sigma)$ and $r\in\mathrm{D}$ such that $\delta = \gamma(\sigma-a^\sigma a^{-1}\mathrm{id})+r\mathrm{id}$. As δ_{D} and $\sigma_{\mathrm{D}} - a^\sigma a^{-1}\mathrm{id}_{\mathrm{D}}$ vanish in a, and as $eval$ is a ring morphism, r must be zero. □

Lemma 3.3 (structure of the zero set)**.** *Let* δ *be a twist of degree* n. *The zero set of* δ_{D} *is a right* $\mathrm{Fix}(\sigma_{\mathrm{D}})$*-vector space having dimension at most* n.

Proof. Let us assume $\delta = r_1\sigma + r_0\mathrm{id}$ and $r_1\neq 0$. If a and b are non-zero roots of δ_{D}, one must have $a^\sigma a^{-1} = b^\sigma b^{-1}$. It follows that $a^{-1}b\in\mathrm{Fix}(\sigma_{\mathrm{D}})$ so a and b are right $\mathrm{Fix}(\sigma_{\mathrm{D}})$-bound. One concludes by induction on n thanks to Lemma 3.2 knowing that δ_{D} is right $\mathrm{Fix}(\sigma_{\mathrm{D}})$-linear; indeed, if $\delta=\alpha\beta$ then $\dim\mathrm{Ker}\delta_{\mathrm{D}}$ cannot exceed $\dim\mathrm{Ker}\alpha_{\mathrm{D}} + \dim\mathrm{Ker}\beta_{\mathrm{D}}$. □

3.3. n**-Linear twists.** Define the left $\mathrm{D}(\sigma)$-module $\mathrm{D}(\sigma,n)$ by putting $\mathrm{D}(\sigma,1) = \mathrm{D}(\sigma)$ and

$$\mathrm{D}(\sigma,n+1) = \mathrm{D}(\sigma,n)\oplus\mathrm{D}(\sigma).$$

$\mathrm{D}(\sigma,n)$ is a finitely generated left module over a left-Noetherian ring, hence a left-Noetherian $\mathrm{D}(\sigma)$-module by [Bou58, Proposition 7 p. 26]. Given $\delta=\delta_1+\cdots+\delta_n\in\mathrm{D}(\sigma,n)$, we define its evaluation by $\delta_{\mathrm{D}}(\bar r) = \delta_{1\mathrm{D}}(r_1)+\cdots+\delta_{n\mathrm{D}}(r_n)$. The map $eval:\mathrm{D}(\sigma,n)\to\mathrm{D}^{\mathrm{D}^n},\ \delta\mapsto\delta_{\mathrm{D}}$ is a morphism of left $\mathrm{D}(\sigma)$-modules, injective as soon as $[\mathrm{D}:\mathrm{Fix}(\sigma_{\mathrm{D}})]$ is infinite, by Lemma 3.3.

3.4. **Twisted Zariski topology over D^n.**

Definition 3.4. We define the *twisted Zariski topology* on D^n, whose basic closed sets are zero-sets of linear twists. This defines a Noetherian topology.

Lemma 3.5. *A right* $\mathrm{Fix}(\sigma_\mathrm{D})$*-vector subspace of* D *of finite dimension is a basic closed subset.*

Proof. A basic closed subset of D has finite left $\mathrm{Fix}(\sigma_\mathrm{D})$-dimension by Lemma 3.3. Conversely, let $C_n = r_1\mathrm{Fix}(\sigma_\mathrm{D}) \oplus \cdots \oplus r_n\mathrm{Fix}(\sigma_\mathrm{D})$. Define $\delta^{r_1,\dots,r_n} \in \mathrm{D}(\sigma)$ inductively by putting $\delta^{\emptyset} = \mathrm{id}$ and

$$\delta^{r_1,\dots,r_{i+1}} = \delta_\mathrm{D}^{r_1,\dots,r_i}(r_{i+1})^{-\sigma}(\delta^{r_1,\dots,r_i})^\sigma - \delta_\mathrm{D}^{r_1,\dots,r_i}(r_{i+1})^{-1}\delta^{r_1,\dots,r_i}.$$

An immediate induction shows that $\delta^{r_1,\dots,r_i}$ has degree i and vanishes in C_i, so C_i is precisely the zero-set of $\delta_\mathrm{D}^{r_1,\dots,r_i}$ by Lemma 3.3 hence $\delta_\mathrm{D}^{r_1,\dots,r_i}(r_{i+1}) \neq 0$ and $\delta^{r_1,\dots,r_{i+1}}$ is well-defined. □

Lemma 3.6. *A closed subset of* D^n *meets a right* D*-line trivially or in a finite union of right* $\mathrm{Fix}(\sigma_\mathrm{D})$*-vector spaces of finite dimension.*

Proof. Let $V = \{\bar{x} \in \mathrm{D}^n : \delta_\mathrm{D}(\bar{x}) = 0\}$ be a basic closed set with $\delta \in \mathrm{D}(\sigma, n)$, and L a right D-line given by $\{x_1 = s_1x_j, \dots, x_n = s_nx_j\}$ for some $j \in \{1, \dots, n\}$ and $\bar{s} \in \mathrm{D}^n$. Replacing x_i by s_ix_j in the equation $\delta_\mathrm{D}(\bar{x}) = 0$, we get an equation of the form $\gamma_\mathrm{D}(x_j) = 0$ for some $\gamma \in \mathrm{D}(\sigma)$, which either is the trivial equation (hence $L \subset V$) or shows that $L \cap V$ has finite right $\mathrm{Fix}(\sigma_\mathrm{D})$-dimension by Lemma 3.3. □

4. Elementary algebraic geometry over D^n

4.1. **Algebraic set, module of a set.**

Definition 4.1. An *algebraic set* is the zero set in D^n of a family S of n-linear twists, written

$$\mathrm{V}(S) = \Big\{\bar{x} \in \mathrm{D}^n : \delta_\mathrm{D}(\bar{x}) = 0 \text{ for all } \delta \in S\Big\}.$$

Definition 4.2. Given $V \subset \mathrm{D}^n$, we call *module of* V and write $\mathrm{I}(V)$ the set of n-linear twists that vanish on V,

$$\mathrm{I}(V) = \Big\{\delta \in \mathrm{D}(\sigma, n) : \delta_\mathrm{D}(\bar{x}) = 0 \text{ for all } x \in V\}.$$

Lemma 4.3. *If* $\mathrm{Fix}(\sigma_\mathrm{D})$ *is infinite, the irreducible closed subsets of* D^n *are precisely the algebraic sets.*

Proof. Let $\mathrm{V}(S)$ be an algebraic set. If $\mathrm{V}(S) = \mathrm{V}(S_1) \cup \cdots \cup \mathrm{V}(S_m)$, as $\mathrm{V}(S_i)$ are $\mathrm{Fix}(\sigma_\mathrm{D})$-vector spaces, $\mathrm{V}(S)$ is a subset of some $\mathrm{V}(S_i)$ so $\mathrm{V}(S)$ is irreducible. □

Definition 4.4. We define the *closure* of a module I of $\mathrm{D}(\sigma, n)$ by

$$\mathrm{cl}(I) = \Big\{\delta \in \mathrm{D}(\sigma, n) : \exists \gamma \in \mathrm{D}(\sigma) \setminus \{0\}\ \gamma\delta \in I\Big\}.$$

One has $I \subset \mathrm{cl}(I)$. We say that I is *closed* if $\mathrm{cl}(I) = I$ and that $\mathrm{V}(I)$ is *radical* if I is closed.

Lemma 4.5. *For every* $\mathrm{D}(\sigma)$*-module* I*, its closure* $\mathrm{cl}(I)$ *is a closed* $\mathrm{D}(\sigma)$*-module.*

Proof. Follows from Corollary 1.6. □

4.2. **σ-morphisms and comorphisms.** Let $V \subset \mathrm{D}^m$ an algebraic set. We define the $\mathrm{D}(\sigma)$-module

$$\Gamma(V) = \mathrm{D}(\sigma, m)/\mathrm{I}(V).$$

Definition 4.6. Given algebraic sets $U \subset \mathrm{D}^n$ and $V \subset \mathrm{D}^m$, a map $f : U \to V$ whose coordinate maps are n-linear twists is a *σ-morphism*.

A bijective σ-morphism $f : U \to V$ such that $f^{-1} : V \to U$ is a σ-morphism is called a *σ-isomorphism*, in which case we write $U \simeq_\sigma V$.

Definition 4.7. The *comorphism of f* is the morphism of $\mathrm{D}(\sigma)$-modules $f^* : \Gamma(V) \to \Gamma(U)$

$$f^* : \delta + \mathrm{I}(V) \mapsto \delta \circ f + \mathrm{I}(U)$$

A σ-morphism $f : U \to V$ is *dominant* if $f(U)$ is dense in V for the Zariski topology.

Lemma 4.8. *If U is irreducible, f is dominant if and only if its comorphism is injective.*

Proof. If $f : U \to V$ is a σ-morphism with $U \subset \mathrm{D}^n$ and $V \subset \mathrm{D}^m$ algebraic, one has

$$\begin{aligned}\mathrm{I}\Big(f(U)\Big) &= \Big\{\gamma \in \mathrm{D}(\sigma, m) : \gamma_{\mathrm{D}}(f(U)) = 0\Big\} \\ &= \Big\{\gamma \in \mathrm{D}(\sigma, m) : \gamma \circ f \in I(U)\Big\},\end{aligned}$$

hence $\mathrm{Ker} f^* = \mathrm{I}\Big(f(U)\Big)/\mathrm{I}(V)$. It follows that f^* is injective if and only if $\mathrm{I}\Big(f(U)\Big) \subset \mathrm{I}(V)$, if and only if $\mathrm{VI}\left(f(U)\right) = V$. But $\overline{f(U)} = \mathrm{VI}\left(f(U)\right)$ since $f(U)$ is irreducible. □

5. Zariski dimension

We assume $[\mathrm{D} : \mathrm{Fix}(\sigma_{\mathrm{D}})]$ infinite throughout the section.

Definition 5.1. We define the *Zariski dimension of an algebraic set* $\mathrm{V}(S) \subset \mathrm{D}^n$ by

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

Note that the dimension of $\mathrm{V}(S)$ *à priori* depends on the set S of twists chosen to define it. We shall see that is does not when D is *perfect*, that is σ_{D} is onto D. The following generalises [Hum75, Theorem 20.5] and provides in particular a classification of additive algebraic groups over a perfect field.

Theorem 5.2. *Assume that* D *is perfect. Let* $\mathrm{V}(S) \subset \mathrm{D}^n$ *be an algebraic set. One has*

$$V \simeq_\sigma \mathrm{D}^{\dim V} \times F_1 \times \cdots \times F_{n-\dim V},$$

where $F_1, \ldots, F_{n-\dim V}$ are $\mathrm{Fix}(\sigma_{\mathrm{D}})$*-vector subspaces of* D *of finite dimension. In particular,* $\dim V$ *does not depend on S.*

Proof. The first assertion follows from Lemma 2.1. For the second assertion, a σ-isomorphism $\mathrm{D}^p \times F_1 \times \cdots \times F_{n-p} \simeq_\sigma \mathrm{D}^q \times F_1 \times \cdots \times F_{n-q}$ induces, via its comorphism, an isomorphism of $\mathrm{D}(\sigma)$-modules $\mathrm{D}(\sigma, n)/I \simeq \mathrm{D}(\sigma, n)/J$ with $\dim_{\mathrm{D}(\sigma)} \mathrm{D}(\sigma, n)/I = p$ and $\dim_{\mathrm{D}(\sigma)} \mathrm{D}(\sigma, n)/J = q$. By Lemma 1.7, one has $p = q$. □

Corollary 5.3 (vectorial Nullstellensatz)**.** *Assume that* D *is perfect. For any module* I*,*

$$\mathrm{IV}(I) \subset \mathrm{cl}(I).$$

Proof. Since $\mathrm{V}(I) = \mathrm{V}(\mathrm{IV}(I))$, one has $\dim_{\mathrm{D}(\sigma)} I = \dim_{\mathrm{D}(\sigma)} \mathrm{IV}(I)$ by Theorem 5.2. It follows that $\mathrm{IV}(I) \subset \mathrm{cl}(I)$. □

Lemma 5.4 (cut by a hypersurface)**.** *Let* $\mathrm{V}(S) \subset \mathrm{D}^n$ *be an algebraic set and* $\delta \in \mathrm{D}(\sigma, n)$*.*

(1) *If* $\delta \in \mathrm{cl}(S)$*, one has* $\dim \mathrm{V}(S, \delta) = \dim V$*.*
(2) *If* $\delta \notin \mathrm{cl}(S)$*, one has* $\dim \mathrm{V}(S, \delta) = \dim V - 1$*.*
(3) *If* $\delta \neq 0$*, then* $\dim \mathrm{V}(\delta) = n - 1$*.*

Proof. (1) If $\delta \in \mathrm{cl}(S)$, then $\dim_{\mathrm{D}(\sigma)}(S, \delta) = \dim_{\mathrm{D}(\sigma)}(S)$ by Lemma 1.6. (2) If $\delta \notin \mathrm{cl}(S)$, then $\dim_{\mathrm{D}(\sigma)}(S, \delta) = \dim_{\mathrm{D}(\sigma)}(S) + 1$. (3) As $[\mathrm{D} : \mathrm{Fix}(\sigma_{\mathrm{D}})]$ is infinite, one has $\mathrm{I}(\mathrm{D}^n) = (0)$ by Lemma 3.3, and $\mathrm{cl}(0) = (0)$. One concludes applying point (2) to $V = \mathrm{D}^n$. □

Corollary 5.5. *Assume that* D *is perfect. Let* $U \subsetneq V$ *be algebraic subsets of* D^n*. If* V *is radical, one has* $\dim U < \dim V$*.*

Proof. Since $U \subset V$ is proper, the inclusion $\mathrm{I}(V) \subset \mathrm{I}(U)$ is proper. Since $\mathrm{I}(V)$ is closed, one has $\dim U < \dim \mathrm{VI}(V)$ by Lemma 5.4.2, whence $\dim U < \dim V$. □

Theorem 5.6. *The Zariski dimension of an algebraic set* $\mathrm{V}(S) \subset \mathrm{D}^n$ *is equal to*

(1) *the maximal length* d *of a chain* $S \subset I_0 \subsetneq I_1 \subsetneq \cdots \subsetneq I_d$ *of closed modules,*
(2) *the minimal number of twists* $\delta_1, \ldots, \delta_d$ *needed to have* $\dim V(S, \delta_1, \ldots, \delta_d) = 0$*.*

If D *is perfect, it is equal to*

(3) *the maximal length* d *of a chain* $V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_d \subset V$ *of radical algebraic sets.*

Proof. (1) We first build a chain of length $m = \dim V$. Let $(\delta_1, \ldots, \delta_n)$ be a basis for $\mathrm{D}(\sigma, n)$ where $(\delta_1, \ldots, \delta_{n-m})$ is a basis for (S). Put $I_i = \mathrm{cl}(\delta_1, \ldots, \delta_{n-m+i})$ for $i \in \{0, \ldots, m\}$. Conversely, given a maximal chain as in (1), we show inductively on i that $\dim_{\mathrm{D}(\sigma)} I_{d-i} = n-i$. For $i = 0$, the module I_d is maximal closed so $I_d = \mathrm{D}(\sigma, n)$. If $\dim_{\mathrm{D}(\sigma)} I_{d-i} = n - i$, one has $\dim_{\mathrm{D}(\sigma)} I_{d-i-1} \leqslant n - i - 1$ since I_{d-i} is closed, and equality holds by maximality of the chain. This shows $\dim V(I_0) = d$, but $\mathrm{cl}(S) = I_0$ by maximality of the chain, hence $\dim V = d$.

(2) If V has dimension d, by Theorem 5.4, one needs at least d twists $\delta_1, \ldots, \delta_d$ to have $\dim \mathrm{V}(S, \delta_1, \ldots, \delta_d) = 0$. One can easily find such twists by completing a basis for S. □

Lemma 5.7 (product)**.** *Assume that* D *is perfect. Let* $U \subset \mathrm{D}^n$ *and* $V \subset \mathrm{D}^m$ *be algebraic sets. Then* $U \times V \subset \mathrm{D}^{n+m}$ *is algebraic and one has* $\dim(U \times V) = \dim U + \dim V$*.*

Proof. One has $= \mathrm{I}(U \times V) = \mathrm{I}(U) \oplus \mathrm{I}(V)$. By Lemma 1.4, one has $\dim_{\mathrm{D}(\sigma)} \mathrm{I}(U \times V) = \dim_{\mathrm{D}(\sigma)} \mathrm{I}(U) + \dim_{\mathrm{D}(\sigma)} \mathrm{I}(V)$, which reads

$$n + m - \dim(U \times V) = n - \dim U + m - \dim V. \quad \square$$

5.1. **Morphisms and dimension.**

Theorem 5.8. *Assume that* D *is perfect. Let* $U \subset \mathrm{D}^n$ *be an irreducible algebraic set and* $f : U \to \mathrm{D}^m$ *a morphism. Then* $\overline{f(U)}$ *is algebraic, given by* $\overline{f(U)} = \mathrm{VI}(f(U))$*, and one has*

$$\dim \overline{f(U)} = \dim U - \dim \mathrm{Ker} f.$$

Proof. Being the continuous image of an irreducible set, $f(U)$ is irreducible, and so is $\overline{f(U)}$, so $\overline{f(U)}$ is algebraic. Consider the comorphism f^*. One has $\mathrm{Ker} f^* = \mathrm{I}(f(U))/\mathrm{I}(\mathrm{D}^m)$ and $\mathrm{Im} f^* = ((f_1, \dots, f_m) + \mathrm{I}(U))/\mathrm{I}(U)$. One thus has $\dim_{\mathrm{D}(\sigma)} \mathrm{Ker} f^* = \dim \mathrm{D}^m - \dim \overline{f(U)}$ and $\dim_{\mathrm{D}(\sigma)} \mathrm{Im} f^* = \dim U - \dim \mathrm{V}(f, \mathrm{I}(U))$, and the result follows from Lemma 1.7. □

5.2. **Radical component.** Given an algebraic set $G = \mathrm{V}(S)$, we write $G^0 = \mathrm{V}(\mathrm{cl}(S))$ which we call the *radical component* of G.

Lemma 5.9. *The group* G^0 *is the intersection of every algebraic subsets of* G *having Zariski dimension* $\dim G$*, one has* $\dim G^0 = \dim G$*, and* G/G^0 *is a right* $\mathrm{Fix}(\sigma_{\mathrm{D}})$*-vector space of finite dimension. If* D *is perfect,* G^0 *does not depend on* S*, and one has* $G^0 \simeq_\sigma \mathrm{D}^{\dim G}$*.*

Proof. The first two assertions follow from Theorem 5.4. For the third assertion, it suffices to show that for all n-linear twist $\delta \in \mathrm{cl}(S)$, the vector-space $V/V \cap \mathrm{V}(\delta)$ has finite $\mathrm{Fix}(\sigma_{\mathrm{D}})$-dimension. Let $\gamma \in \mathrm{D}(\sigma)$ be non-zero of degree ℓ such that $\gamma\delta \in (S)$. Let $g_0, \dots, g_\ell$ in V. One has $\gamma_{\mathrm{D}}(\delta_{\mathrm{D}}(g_i)) = 0$ for all $i \in \{0, \dots, \ell\}$. By Lemma 3.3, there is a non-trivial $\mathrm{Fix}(\sigma_{\mathrm{D}})$-linear combination $\delta_{\mathrm{D}}(g_0)\lambda_0 + \cdots + \delta_{\mathrm{D}}(g_\ell)\lambda_\ell = 0$, so $g_0\lambda_0 + \cdots + g_\ell\lambda_\ell \in V \cap \mathrm{V}(\delta)$. This shows that $\dim_{\mathrm{Fix}(\sigma_{\mathrm{D}})} V/V \cap \mathrm{V}(\delta)$ is at most ℓ. The last two assertions follow from Corollary 5.3 and Theorem 5.2. □

6. Linearly-closed division rings

6.1. **Definition and examples.**

Definition 6.1. A division ring $\mathbf{D}$ is *linearly-closed* if every non-zero $\delta_{\mathbf{D}} \in \mathbf{D}(\sigma_{\mathbf{D}})$ is onto $\mathbf{D}$.

If $\mathbf{D}$ is linearly-closed with non-trivial $\sigma_{\mathbf{D}}$, one must have $[\mathbf{D}, \mathrm{Fix}(\sigma_{\mathbf{D}})] = +\infty$. Otherwise, being $\mathrm{Fix}(\sigma_{\mathbf{D}})$-linear with a dimension one Kernel, $\sigma_{\mathbf{D}} - \mathrm{id}_{\mathbf{D}}$ would not be surjective. Examples include the field $\left(\mathbb{F}_p^{alg}, \mathrm{Froeb}_p^n\right)$. By Łos Theorem, given non-principal ultrafilters $\mathcal{U}$ on $\mathbb{N}$ and $\mathcal{V}$ on the set of prime numbers, the field $\left(\mathbb{F}_p^{alg\mathcal{U}}, \prod_{\mathcal{U}} \mathrm{Froeb}_p^n\right)$ of characteristic p, and the field $\left(\prod_{\mathcal{V}} \mathbb{F}_p^{alg}, \prod_{\mathcal{V}} \mathrm{Froeb}_p\right)$ of characteristic 0 are linearly-closed. From these, one can build non-commutative examples thanks to

Lemma 6.2. *If* $(\mathrm{D}, \sigma_{\mathrm{D}})$ *is linearly closed, so is the ring of skew Laurent series* $\mathrm{D}((x, \sigma_{\mathrm{D}}))$*.*

Proof. One has $\mathrm{D}((x, \sigma_{\mathrm{D}})) = \left\{ \sum_{k=m}^{+\infty} x^k r_k : r_k \in \mathrm{D},\ m \in \mathbb{Z} \right\}$ with multiplication rule $rx = xr^\sigma$ for $r \in \mathrm{D}$. Consider for σ the conjugation map by x, and let us show that the equation

$$y_n \sigma^n(y) + \cdots + y_1 \sigma(y) + y_0 y = y_{-1} \tag{1}$$

with $y_i = \sum_{k=v_i}^{+\infty} x^k r_{k,i}$ and $r_{v_i,i} \neq 0$ for each $i \in \{-1, \dots, n\}$ has a solution $y = \sum_{k=v}^{+\infty} x^k r_k$. For every $i \in \{0, \dots, n\}$, one has

$$y_i \sigma^i(y) = \left(\sum_{\ell=v_i}^{+\infty} x^\ell r_{\ell,i} \right) \left(\sum_{j=v}^{+\infty} x^j r_j^{\sigma^i} \right) = \sum_{k=v+v_i}^{+\infty} x^k \left(\sum_{j+\ell=k} r_{\ell,i}^{\sigma^j} r_j^{\sigma^i} \right).$$

Let $w = \min\{v_1, \dots, v_n\}$ and let $v = v_{-1} - w$. Let $\delta(i,k) = 1$ if $k \geqslant v + v_i$ and $\delta(i,k) = 0$ otherwise. Replacing into (1), we get

$$\sum_{k=v_{-1}}^{+\infty} x^k \sum_{i=0}^{n} \delta(i,k) \left(\sum_{j+\ell=k} r_{\ell,i}^{\sigma^j} r_j^{\sigma^i} \right) = \sum_{k=v_{-1}}^{+\infty} x^k r_{k,-1}.$$

For the first coefficient of minimal valuation $k = v_{-1}$, this yields

$$\sum_{i=0}^{n} \delta(i, v_{-1}) r_{w,i}^{\sigma^v} r_v^{\sigma^i} = r_{v_{-1},-1},$$

which has a solution r_v since there is $q \in \{0, \dots, n\}$ such that $\delta(q, v_{-1}) r_{w,q} \neq 0$ and since D is linearly closed. For the second coefficient $k = v_{-1} + 1$, we get

$$\sum_{i=0}^{n} \delta(i, v_{-1}+1) \left(r_{w,i}^{\sigma^{v+1}} r_{v+1}^{\sigma^i} + r_{w+1,i}^{\sigma^v} r_v^{\sigma^i} \right) = r_{v_{-1}+1,-1},$$

which also has a solution r_{v+1} since $\delta(q, v_{-1}+1) r_{w,q} \neq 0$, and so on inductively. □

Theorem 6.3. *A division ring* D *with infinite* $[\mathrm{D} : \mathrm{Fix}(\sigma_\mathrm{D})]$ *has a linearly-closed extension.*

Proof. Case 1. σ_D *is inner, say conjugation by* $a \in \mathrm{D}$. By [Coh95, Corollary 3.3.9], a is transcendental over $Z(\mathrm{D})$. As the referee notes, the theory of division rings with centre $Z(\mathrm{D})$ extending D is closed by chains of models, hence has an existentially closed model $\mathbf{D}$. By [Coh73, Theorem 2], for all $(b,c) \in \mathbf{D}^2$, the equation $xa - bx = c$ has at least one solution in $\mathbf{D}$. By [Coh95, Theorem 8.5.1], for every $\bar{r} \in \mathbf{D}^n$, the polynomial $x^n + x^{n-1} r_1 + \cdots + x r_n + r_{n+1}$ has a root in $\mathbf{D}$. One concludes with Claim 1 that every twist over $\mathbf{D}$ is onto $\mathbf{D}$.

Claim 1. *For inner* $\sigma_\mathbf{D}$*, a degree* n *twist factorises in products of degree* 1 *twists if every non-constant polynomial* $r_{n+1} + x r_n + \cdots + x^{n-1} r_1 + x^n r_0$ *with* $\bar{r} \in \mathbf{D}^{n+1}$ *has a root in* $\mathbf{D}$.

Proof of the Claim. Let $xa^2 + \alpha x a + \beta x$ be a degree 2 twist. Let c be a root of $x^2 - x\alpha + \beta$ and put $b = \alpha - c$ so as to have $b + c = \alpha$ and $cb = \beta$. One has

$$\begin{aligned}(xa + cx)(xa + bx) &= xa^2 + (b+c)xa + cbx. \\ &= xa^2 + \alpha x a + \beta x\end{aligned}$$

Let $xa^3 + \alpha x a^2 + \beta x a + \gamma x$ a degree 3 twist. Let d be a root of $x^3 - x^2\alpha + x\beta - \gamma$, let c be a root of $x^2 - x(\alpha - d) + \beta + d\alpha - d^2$ and put $b = \alpha - c - d$, so as to have

$$dcb = dc(\alpha - c - d) = d(c(\alpha - d) - c^2) = d(d^2 - d\alpha - \beta) = \gamma, \text{ and}$$

$$cb + db + dc = d(b + c) + cb = d(\alpha - d) + cb = d\alpha - d^2 + d^{-1}\gamma = \beta.$$

One has

$$\begin{aligned}(xa+dx)(xa+cx)(xa+bx) &= xa^3+(b+c+d)xa^2+(cb+db+dc)xa+dcbx\\ &= xa^3+\alpha xa^2+\beta xa+\gamma x.\end{aligned}$$

The case of higher degree twists is similar. □

Case 2. Consider the division ring $\mathrm{D}((x,\sigma))$ of skew Laurent series $\sum_{i=m}^{+\infty} r_i x^i$ with multiplication rule $xr = r^\sigma x$ for all $r \in \mathrm{D}$. We take $\sigma_{\mathrm{D}((x,\sigma))}$ to be the conjugation map by x^{-1}, which extends σ_{D}. As every central Laurent series commutes with x, one has $C(x) \subset \mathrm{Fix}(\sigma_{\mathrm{D}})((x))$, so $[\mathrm{D}((x,\sigma)) : \mathrm{Fix}(\sigma_{\mathrm{D}((x,\sigma))})] = +\infty$ and we may apply Case 1 to $\Big(\mathrm{D}((x,\sigma)), \sigma_{\mathrm{D}((x,\sigma))}\Big)$. □

6.2. **Constructible subsets and Chevalley Theorem.** A subset $C \subset \mathrm{D}^n$ is *constructible* if it is a finite boolean combination of closed sets.

Theorem 6.4. *Let* $\mathbf{D}$ *be linearly-closed and* $f : \mathbf{D}^n \to \mathbf{D}^m$ *a* σ*-morphism.*

(1) *If* $C \subset \mathbf{D}^n$ *is constructible, then* $f(C)$ *is constructible.*
(2) *If* $F \subset \mathbf{D}^n$ *is closed, then* $f(F)$ *is closed.*

Proof. For point (1), one has $f(C) = \{\bar{y} \in \mathbf{D}^m : (\exists \bar{x} \in C)\ f(\bar{x}) = \bar{y}\}$ which is a subset of $\mathbf{D}^m$ definable by a formula $\varphi(\bar{y})$ in the language $\mathcal{L}_{\mathbf{D}(\sigma)}$ of $\mathbf{D}(\sigma)$-modules. By Baur-Monk Theorem, $\varphi(\bar{y})$ is equivalent to a boolean combinations of p.p.-formulas. Since $\mathbf{D} \models \mathrm{DM}(\mathbf{D}(\sigma))$, by Corollary 2.2, there is a quantifier-free $\mathcal{L}_{\mathbf{D}(\sigma)}$-formula $\psi(\bar{y})$, that is, a finite boolean combination of atomic $\mathcal{L}_{\mathbf{D}(\sigma)}$-fomulas, such that $f(C) = \{\bar{y} \in \mathbf{D}^m : \psi(\bar{y})\}$ holds. For point (2), one may assume that F is irreducible, hence given by a conjunction of equations, so $f(F)$ is defined by a p.p.-formula, and the conclusion follows from Corollary 2.2. □

Theorem 6.5 (after Ax-Grothendieck)**.** *Let* $\mathbf{D}$ *be linearly-closed and* $f : \mathbf{D}^n \to \mathbf{D}^n$ *a* σ*-morphism. If* f *has a dimension zero kernel, then* f *is onto.*

Proof. The image $f(\mathbf{D}^n)$ is closed by Theorem 6.4, hence an algebraic subset of $\mathbf{D}^n$. It has dimension n by Theorem 5.8. As $\mathbf{D}^n$ is radical, one has $f(\mathbf{D}^n) = \mathbf{D}^n$ by Corollary 5.5. □

6.3. **Example of radical groups.** We go on using the properties of linearly-closed division ring to show that a group is radical. Given $n \geqslant 2$ and $\bar{b} \in \mathrm{D}^n$, we consider the algebraic subgroup of D^n

$$G_{\bar{b}}^n = \Big\{\bar{x} \in \mathrm{D}^n : b_1(x_1^\sigma - x_1) = \cdots = b_n(x_n^\sigma - x_n)\Big\},$$

and we look for conditions on $\bar{b}$ for $G_{\bar{b}}^n$ to be radical.

Lemma 6.6. *Let* $\mathbf{D}$ *be an extension of* D *and* $\bar{r} \in \mathrm{D}^n$*. One has* $\dim_{\mathrm{Fix}(\sigma_{\mathrm{D}})} \bar{r} = \dim_{\mathrm{Fix}(\sigma_{\mathbf{D}})} \bar{r}$.

Proof. If $\bar{r}$ is $\mathrm{Fix}(\sigma_{\mathbf{D}})$-bound, there are $i \in \{1,\dots,n\}$ and $\{j_1,\dots,j_m\} \subset \{1,\dots,n\}\setminus\{i\}$ such that r_i belongs to $\bigoplus_{k=1}^m \mathrm{Fix}(\sigma_{\mathbf{D}}) r_{j_k}$. By lemma 3.5, the element r_i belongs to $V(\delta^{r_{j_1},\dots,r_{j_m}}) \cap \mathrm{D}$. But $r_{j_1},\dots,r_{j_m}$ are $\mathrm{Fix}(\sigma_{\mathrm{D}})$-free, so $V(\delta^{r_{j_1},\dots,r_{j_m}}) \cap \mathrm{D}$ equals $\bigoplus_{k=1}^m \mathrm{Fix}(\sigma_{\mathrm{D}}) r_{j_k}$ by Lemma 3.3. This shows that $\bar{r}$ is $\mathrm{Fix}(\sigma_{\mathrm{D}})$-bound. □

The following Lemma is inspired from [KSW11, Lemma 2.8] and its improvement [Hem15, Lemme 5.3].

Lemma 6.7. *Assume that* D *is perfect. The group* $G_{\bar{b}}^n$ *is radical if and only if* $\left(b_1^{-1}, \dots, b_n^{-1}\right)$ *is left* $\mathrm{Fix}(\sigma_{\mathrm{D}})$*-free.*

Proof. Let us assume that $G_{\bar{b}}^n$ is radical and let us put $\gamma = \sigma - \mathrm{id}$. If there is a tuple $\bar{r}$ in $\mathrm{Fix}(\sigma_{\mathrm{D}})$ such that $\sum_{i=1}^{n} r_i b_i^{-1} = 0$, one has for every $\bar{x} \in G_{\bar{b}}^n$,

$$\begin{aligned}\gamma_{\mathrm{D}}(r_1x_1 + \cdots + r_nx_n) &= \sum_{i=1}^{n} r_i\gamma_{\mathrm{D}}(x_i)\\ &= \sum_{i=1}^{n} r_i b_i^{-1} b_i\gamma_{\mathrm{D}}(x_i)\\ &= \left(\sum_{i=1}^{n} r_i b_i^{-1}\right) b_1\gamma_{\mathrm{D}}(x_1)\\ &= 0.\end{aligned}$$

It follows that $r_1x_1 + \cdots + r_nx_n$ belongs to $\mathrm{cl}(\mathrm{I}(G_{\bar{b}}^n))$ hence to $\mathrm{I}(G_{\bar{b}}^n)$. This implies that $r_1x_1 + \cdots + r_nx_n$ vanishes on $\mathrm{Fix}(\sigma_{\mathrm{D}}) \times \cdots \times \mathrm{Fix}(\sigma_{\mathrm{D}})$, hence $\bar{r} = 0$, so the family $(b_1^{-1}, \dots, b_n^{-1})$ is left $\mathrm{Fix}(\sigma_{\mathrm{D}})$-free.

For the converse, we proceed by induction on n, beginning with $n = 2$. If $G_{\bar{b}}^2$ is not radical, then $G_{\bar{b}}^2$ is not radical over $\mathbf{D}$ for any LC extension of D by Lemma 6.6. We now look at varietes over $\mathbf{D}$. There is a 2-variable twist $\delta_1(x_1) + \delta_2(x_2) \in \mathrm{cl}_{\mathbf{D}}(I(G^2)) \setminus I(G_{\bar{b}}^2)$. Since $\dim(G_{\bar{b}}^2)^0 = 1$, at least one of the two projections, say the second one

$$\pi_2 : (G_{\bar{b}}^2)^0 \twoheadrightarrow \mathbf{D} \tag{2}$$

must be onto. Replacing inductively x_1^σ by $x_1 + b_1^{-1}b_2\gamma(x_2)$ in the first equation, the system

$$\{\delta_1(x_1) + \delta_2(x_2) = 0,\ b_1\gamma(x_1) = b_2\gamma(x_2)\}$$

is equivalent to one of the form

$$\{r_1x_1 + \delta(x_2) = 0,\ b_1\gamma(x_1) = b_2\gamma(x_2)\},$$

for some $r_1 \in \mathbf{D}$ with $r_1x_1 + \delta(x_2) \in \mathrm{cl}_{\mathbf{D}}(I(G^2)) \setminus I(G_{\bar{b}}^2)$. As $\dim(G_{\bar{b}}^2)^0 = 1$, the twists $r_1x_1 + \delta(x_2)$ and $b_1\gamma(x_1) - b_2\gamma(x_2)$ must be bound, which implies that r_1 and δ are non-zero. We may assume $r_1 = 1$. Composing by γ, we get the equation

$$b_1^{-1}b_2\gamma(x_2) + \gamma\delta(x_2) = 0,$$

which holds for all $x_2 \in \mathbf{D}$ by (2). This yields $\delta(x_2) = r_2x_2$ for some $r_2 \in \mathbf{D}$, hence

$$b_1^{-1}b_2\gamma(x_2) + \gamma(r_2x_2) = 0, \quad \text{for all } x_2 \in \mathbf{D},$$

from which follows $r_2 = r_2^\sigma = b_1^{-1}b_2$, so $r_2 \in \mathrm{D}$ and (b_1^{-1}, b_2^{-1}) are left $\mathrm{Fix}(\sigma_{\mathrm{D}})$-bound.

Now assume that the Lemma is proved for $n-1$ and suppose that $G_{\bar{b}}^n$ is not radical. Then it is not radical over $\mathbf{D}$ either, and there is some $\delta_1(x_1) + \cdots + \delta_n(x_n) \in \mathrm{cl}_{\mathbf{D}}(I(G_{\bar{b}}^n)) \setminus I(G_{\bar{n}}^n)$. We may assume that $G_{\bar{b}}^{n-1}$ is radical over $\mathbf{D}$ for otherwise the conclusion follows by induction

hypothesis and Lemma 6.6. As $\dim(G_{\bar{b}}^n)^0 = 1$, one of the n main projections of $(G_{\bar{b}}^n)^0$, say the one on the first coordinate, is onto $\mathbf{D}$,

$$\pi_1 : (G_{\bar{b}}^n)^0 \twoheadrightarrow \mathbf{D}. \tag{3}$$

By Theorem 6.4, the projection on the first $n-1$ coordinates $\pi_{n-1} : G_{\bar{b}}^n \to G_{\bar{b}}^{n-1}$ is onto and has a Zariski dimension 0 kernel so

$$\pi_{n-1} : (G_{\bar{b}}^n)^0 \twoheadrightarrow G_{\bar{b}}^{n-1} \tag{4}$$

is onto since $G_{\bar{b}}^{n-1}$ is radical, by Theorem 6.4, Theorem 5.8, and Corollary 5.5. If δ_n is zero, then $\delta_1(x_1) + \cdots + \delta_{n-1}(x_{n-1})$ belongs to $I(G_{\bar{b}}^{n-1})$ by (4), hence to $I(G_{\bar{b}}^n)$, a contradiction. So δ_n is non-zero. From the system $\{\delta_1(x_1) + \cdots + \delta_n(x_n) = 0,\ b_n\gamma(x_n) = \cdots = b_1\gamma(x_1)\}$, we derive one equation of the form

$$x_n = \alpha(x_1) + r_2x_2 + \cdots + r_{n-1}x_{n-1}.$$

Composing by γ, we get

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

which holds in $G_{\bar{b}}^{n-1}$ by (4). For any $j \in \{2, \ldots, n-1\}$, taking some non-zero $x_j \in \mathrm{Fix}(\sigma_{\mathbf{D}})$ and $x_i = 0$ for any $i \in \{2, \ldots, n-1\} \setminus \{j\}$ yields $r_j \in \mathrm{Fix}(\sigma_{\mathbf{D}})$, hence

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

which holds for all $x_1 \in \mathbf{D}$ by (3). It follows that $\alpha(x_1) = r_1x_1$ for some $r_1 \in \mathbf{D}$, which yields

$$r_1^\sigma = r_1 = b_n^{-1}b_1 + \sum_{i=2}^{n-1} r_ib_i^{-1}b_1,$$

so $(b_1^{-1}, \ldots, b_n^{-1})$ are left $\mathrm{Fix}(\sigma_{\mathbf{D}})$-bound, hence left $\mathrm{Fix}(\sigma_{\mathrm{D}})$-bound by Lemma 6.6, as desired. □

6.4. **Affine Nullstellensätze.** (Useless for the next paper) Given a linearly-closed division ring $\mathbf{D}$, we consider the $\mathbf{D}(\sigma)$-module $\mathbf{D}_{\mathrm{aff}}(\sigma, n)$ of affine twists, and define similarly an affine algebraic set $\mathrm{V}(S)$ for a set S of affine twists, and a module $\mathrm{I}(V)$ for any $V \subset \mathbf{D}^n$.

Theorem 6.8 (weak Nullstellensatz)**.** *If I is a module with $1 \notin I$, then $\mathrm{V}_{\mathbf{D}}(I)$ is non-empty.*

Proof. $\mathbf{D}_{\mathrm{aff}}(\sigma, n)$ is a module of finite type over left-Noetherian $\mathbf{D}(\sigma)$, so I has finitely many generators $\delta_1, \ldots, \delta_m$. Let us show that the system

$$\mathcal{S} = \{\delta_1(\bar{x}) = 0, \ldots, \delta_m(\bar{x}) = 0\}.$$

has a solution in $\mathbf{D}$. Consider the left $\mathbf{D}(\sigma)$-module $\mathbf{D}$. Since I does not contain 1, there is an embedding $\mathbf{D} \to \mathbf{D}_{\mathrm{aff}}(\sigma, n)/I$ of left $\mathbf{D}(\sigma)$-modules. But $\mathbf{D}_{\mathrm{aff}}(\sigma, n)/I$ has a solution for $\mathcal{S}$. Since $\mathbf{D} \models \mathrm{DM}(\mathbf{D}(\sigma))$ holds, $\mathbf{D}$ also has a solution for $\mathcal{S}$ by Corollary 2.4. □

Corollary 6.9. *For any maximal module I satisfying $1 \notin I$, there is $\bar{a} \in \mathbf{D}^n$ such that*

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

Proof. We first claim that $(x_1 - a_1, \dots, x_n - a_n)$ is a maximal module avoiding 1. Assume that $I \subset J$ is proper for some module J and let $\delta \in J \setminus I$. One can write δ under the form

$$\delta = \delta_1(x_1 - a_1) + \cdots + \delta_n(x_n - a_n) + b,$$

for some 1-variable twists $\delta_1, \dots, \delta_n$ and some $b \in \mathbf{D}$. Note that b is non-zero since $\delta \notin I$, but $\delta \in J$ yields $b \in J$. This shows the claim. Now, if I is a maximal module avoiding 1, then it contains a point $\bar{a}$ by Theorem 6.8. Hence $I \subset \mathrm{I}(\bar{a})$. But $(x_1 - a_1, \dots, x_n - a_n) \subset \mathrm{I}(\bar{a})$, so equality holds by maximality of $(x_1 - a_1, \dots, x_n - a_n)$. This yields $I \subset (x_1 - a_1, \dots, x_n - a_n)$, and equality holds by maximality of I. □

Theorem 6.10 (Nullstellensatz)**.** *If J is a module that does not contain* 1*, one has*

$$\mathrm{IV}(J) \subset \mathrm{cl}_{\mathrm{aff}}(J).$$

Proof. Let $\delta_1, \dots, \delta_r$ be a generating family for J. Let $\delta \in \mathrm{IV}(J)$. Consider the module $L = (\delta_1, \dots, \delta_r, \delta + 1)$. If $\bar{x} \in \mathrm{V}(L)$, then $\bar{x} \in \mathrm{V}(J)$, so $\delta(\bar{x}) = 0$. But one also has $\delta(\bar{x}) + 1 = 0$, a contradiction, so $\mathrm{V}(L)$ is empty. By Theorem 6.8, the module L contains 1 so there exist $h_1, \dots, h_r$ and h in $\mathbf{D}(\sigma)$ such that

$$1 = h(\delta + 1) + h_1\delta_1 + \cdots + h_r\delta_r.$$

h is non-zero since $1 \notin J$. Applying this equality to a point of $\mathrm{V}(J)$ (which is non-empty by Theorem 6.8), we get $h(1) = 1$ hence $h\delta \in J$, whence $\delta \in \mathrm{cl}_{\mathrm{aff}}(J)$. □

This provides that $\mathrm{IV}(I) = I$ if I is a *closed* module (that is $\mathrm{cl}_{\mathrm{aff}}(I) = I + \mathbf{D}$) not containing 1.

End of first paper.

Second paper.

NIP DIVISION RINGS OF CHARACTERISTIC p

CÉDRIC MILLIET

Abstract. We provide a non-trivial example of NIP division ring of characteristic p for every prime number p and show that a NIP division ring of characteristic p has finite dimension over its centre.

It is known that a stable division ring of characteristic p is a finite dimensional algebra over its centre. Whereas the only known stable division rings are fields, Hamilton's Quaternions over the real or 2-adic numbers are non-trivial examples of NIP division rings of characteristic zero. The paper provides a non-trivial example of NIP division ring of characteristic p (Theorem 1.1), a new simple proof of the particular stable case (Fact 4.1) and shows that every NIP division ring of characteristic p has finite dimension over its centre (Theorem 4.2). The proofs of Theorem 4.2 and Fact 4.1 closely follow ideas of and use Kaplan and Scanlon's result that an infinite NIP field does not have any proper Artin-Schreier extension [KSW11], as well as a Zariski dimension theory for subgroups of $(\mathrm{D}^n, +)$ defined over a division ring D by linear equations involving a ring morphism $\sigma : \mathrm{D} \to \mathrm{D}$.

Definition 0.11 (Shelah)**.** An L-structure M is *NIP* if for every L-formula $\varphi(x, \bar{y})$ there are $n \in \mathbb{N}$, tuples $(a_1, \ldots, a_n)$ and $(\bar{b}_J)_{J\subset\{1,\ldots,n\}}$ in M such that $M \models \varphi(a_i, \bar{b}_J)$ if and only if $i \in J$.

1. Examples

Theorem 1.1. *There are non-trivial NIP division rings of every characteristic.*

Proof. Let p be a prime number, $\Gamma = \left\langle \frac{1}{p^i} : i \in \mathbb{N} \right\rangle$ the ordered subgroup of $(\mathbb{R}, +)$ and $H = \mathbb{F}_p^{alg}((\Gamma))$ the field of formal Hahn series

$$\sum_{\gamma\in\Gamma} a_\gamma t^\gamma$$

having a well ordered support in Γ and coefficients $a_\gamma \in \mathbb{F}_p^{alg}$. With its natural valuation v maping a series to the minimum of it support, the valued field (H, v) is maximal, *i.e.* has no proper valued field extension having both same residue field and same valuation group (see [Kru32] or [EP05, Exercise 3.5.6]). Its residue field $\mathbb{F}_p^{alg}$ is infinite, perfect and does not have the independence property. Its valuation group Γ is p-divisible, so the pure field H does not have the independence property by [KSW11, Theorem 5.9]. If $p \neq 2$, the cyclic extension $H(\sqrt{t})/H$ is Galois, with Galois group generated by the automorphism $\sigma \in Aut(H(\sqrt{t})/H)$ switching $\sqrt{t}$ and $-\sqrt{t}$. Consider the left $H(\sqrt{t})$-vector space of dimension 2

$$\mathrm{D} = H(\sqrt{t}) \oplus H(\sqrt{t}) \cdot x$$

with internal multiplication defined by the rules

$$x^2 = t^{1/p} \quad \text{and} \quad x \cdot k = \sigma(k)x \quad \text{for all } k \in H(\sqrt{t}).$$

D is an H-algebra of centre H and dimension 4, interpretable in H, so D does not have the independence property. Since the norm $N_{H(\sqrt{t})/H}$ of the extension $H(\sqrt{t})/H$ is defined by

$$N_{H(\sqrt{t})/H}(a + b\sqrt{t}) = a^2 + b^2 t,$$

it is not difficult to verify that one has

$$t^{1/p} \notin N_{H(\sqrt{t})/H}(H(\sqrt{t})),$$

so D is a division ring by [Lam91, Corollary 14.8]. If $p = 2$, one can do a similar construction with the cyclic Galois extension $H(\sqrt[3]{t})/H$. □

Note that the above division ring is not stable since its centre is Henselian (see [Efr06, Corollary 18.4.2]) and has a non-trivial definable valuation (see [KJ15b, Theorem 5.2] or [KJ15a, Theorem 3.10]).

2. Preliminaries on NIP division rings of characteristic p

2.1. **Fields.** Little is known on NIP fields. In addition to the Baldwin-Saxl chain condition, we use the following result (see [KSW11, Theorem 4.3]). If F is a field of characteristic p, a proper field extension $\mathrm{F}(a)/\mathrm{F}$ is *Artin-Schreier* if a is a root of $x^p - x + b$ for some $b \in \mathrm{F}$.

Fact 2.1 (Kaplan and Scanlon)**.** *An infinite NIP field has no Artin-Schreier extension.*

The proof of Fact 2.1 relies on the classification of irreducible closed subgroups of $\mathbf{G}_a^n$ having dimension 1. As an immediate Corollary, using the result of Duret on weakly algebraically closed non separably closed fields (see [Dur79, Théorème 6.4] and [KSW11, Corollary 4.5]),

Fact 2.2 (Kaplan and Scanlon)**.** *An infinite NIP field of characteristic p contains $\mathbb{F}_p^{alg}$.*

2.2. **Metro equation.** Let D be a division ring of characteristic p. We refer to [Her96, Lemma 3.1.1] and [Lam03, Exercises 13.8 and 16.11] for the following results.

Fact 2.3 (Herstein)**.** *Let $a \in \mathrm{D} \setminus Z(\mathrm{D})$ have finite order. There is some $b \in \mathrm{D}$ and a natural number $i > 0$ such that*

$$a^b = a^i \neq a.$$

Fact 2.4 (Lam)**.** *Let $a \in \mathrm{D} \setminus Z(\mathrm{D})$ with $a^{p^n} \in Z(\mathrm{D})$. There is some $b \in \mathrm{D}$ such that*

$$b^a = b + 1.$$

Fact 2.5 (Lam)**.** *Let $a \in \mathrm{D}$ be algebraic over $Z(\mathrm{D})$. The equation $ax - xa = 1$ has a solution $x \in \mathrm{D}$ if and only if a is not separable over $Z(\mathrm{D})$.*

We assume from now on that D is infinite and does not have the independence property.

Theorem 2.6. *The centre of* D *is infinite.*

Proof. If every element of D have finite order, we show that D is commutative, for if $a \in \mathrm{D} \setminus Z(\mathrm{D})$, by Fact 2.3, there is some $b \in \mathrm{D}$ (having finite order) such that $a^b = a^i \neq a$. It follows that the division ring generated by a et b is finite, a contradiction to Wedderburn Theorem. So we may assume that there is some $c \in \mathrm{D}$ having infinite order. The field

$Z\left(C(c)\right)$ is infinite and contains a copy of $\mathbb{F}_p^{alg}$ by Fact 2.2. We claim that $Z(\mathrm{D})$ contains every p^nth-root of 1. Assume for a contradiction that there is $a \in \mathrm{D} \setminus Z(\mathrm{D})$ with $a^{p^n} = 1$. By Fact 2.4 there is $b \in \mathrm{D}$ such that

$$b^a = b + 1. \tag{5}$$

Rising to the power p we get $(b^p)^a = b^p + 1$. Substracting (5),

$$(b^p - b)^a = b^p - b. \tag{6}$$

If $(b^p - b)$ has finite order, say $(b^p - b)^{p^m} = b^p - b$, one has for every $q \in \mathbb{N}$,

$$(b^p - b)^{p^{qm}} = b^p - b, \quad \text{hence} \quad (b^{p^{qm}})^p - b^{p^{qm}} = b^p - b.$$

In the field generated by b, the polynomial $x^p - x - (b^p - b)$ has finitely many roots, so b must have finite order. By (5), a and b generate a finite division ring, a contradiction. So $(b^p - b)$ has infinite order and the field $Z\left(C(b^p - b)\right)$ is infinite. As b commutes with $Z\left(C(b^p - b)\right)$, the extension $Z\left(C(b^p - b)\right)(b)$ is Artin-Schreier. By Fact 2.1, one has $b \in Z\Big(C(b^p - b)\Big)$, so a and b commute by (6), contradicting (5). □

Theorem 2.7 (metro equation)**.** *For $a \in \mathrm{D}$, the equation $ax - xa = 1$ has no solution in* D.

Proof. We first claim that for every $b \in \mathrm{D}$, one has $C(b^p - b) = C(b)$. As b commutes with $Z\left(C(b^p - b)\right)$, the field $Z\left(C(b^p - b)\right)(b)$ is an Artin-Schreier extension. The division ring $C(b^p - b)$ is infinite by [Lam91, Theorem 13.10], so $Z\left(C(b^p - b)\right)$ is infinite by Theorem 2.6. By Fact 2.1, one has $b \in Z\left(C(b^p - b)\right)$ and thus $C(b^p - b) \subset C(b)$. To show the Theorem, assume for a contradiction that there be some $b \in \mathrm{D}$ with $b^a = b+1$. We deduce $(b^p)^a = b^p+1$. Substracting the identities, we get $(b^p-b)^a = b^p-b$, a contradiction with the above claim. □

Corollary 2.8. *For every $a \in \mathrm{D}$, one has $C(a^p) = C(a)$.*

Proof. The element a is algebraic over the field $ZC(a^p)$. Since $ax - xa = 1$ has no solution in $C(a^p)$, by Fact 2.5, a is separable over $ZC(a^p)$ so $a \in ZC(a^p)$ and $C(a^p) \subset C(a)$. □

3. Preliminaries on division rings

The results of this Section can be found in **??**. Let D be a division ring, σ a unary function symbol and $\sigma_{\mathrm{D}} : \mathrm{D} \to \mathrm{D}$ a surjective ring morphism with $[\mathrm{D} : \mathrm{Fix}(\sigma_{\mathrm{D}})]$ infinite.

3.1. **Linear twists.** Define the ring of *linear twists*

$$\mathrm{D}(\sigma) = \left\{ \sum_{i=0}^{n} r_i \sigma^i \ : \bar{r} \in \mathrm{D}^{n+1},\ n \in \mathbb{N} \right\},$$

equipped with the sum

$$\sum_{i=0}^{n} r_i \sigma^i + \sum_{j=0}^{n} s_j \sigma^j = \sum_{k=0}^{n} (r_k + s_k)\sigma^k$$

and composition law

$$\left(\sum_{i=0}^{n} r_i \sigma^i\right)\left(\sum_{j=0}^{n} s_j \sigma^j\right) = \sum_{i=0}^{n}\left(\sum_{j=0}^{n} r_i \sigma_{\mathrm{D}}^i(s_j)\sigma^{i+j}\right).$$

$\mathrm{D}(\sigma)$ is a unitary (we also write id for σ^0) associative integral domain. Since the map sending a twist $r_0\mathrm{id}+\cdots+r_n\sigma^n$ to the map $\delta_{\mathrm{D}}:\mathrm{D}\to\mathrm{D},\ x\mapsto r_0x+\cdots+r_n\sigma^n_{\mathrm{D}}(x)$ is an injective ring morphism, we may identify a twist δ and the evaluation map δ_{D} induced by δ.

Fact 3.1. *Let $\delta\in\mathrm{D}(\sigma)$ and $a\in\mathrm{D}^\times$ a root. There is $\gamma\in\mathrm{D}(\sigma)$ such that $\delta=\gamma(\sigma-a^\sigma a^{-1}\mathrm{id})$.*

Fact 3.2. *Any division ring with infinite $[\mathrm{D}:\mathrm{Fix}(\sigma_{\mathrm{D}})]$ has a linearly-closed extension, i.e. an extension in which every affine twist $r+r_0x+\cdots+r_n\sigma^n(x)$ has a root.*

3.2. **Algebraic sets and morphisms.** An *n-linear twist* is a linear combination of

$$\left\{\sigma^{i_1}(x_1),\dots,\sigma^{i_n}(x_n):(i_1,\dots,i_n)\in\mathbb{N}^n\right\}$$

having left coefficients in D. We write $\mathrm{D}(\sigma,n)$ for the $\mathrm{D}(\sigma)$-module of n-linear twists. Again, we often identify an n-linear twist $\delta(x_1,\dots,x_n)$ and the induced evaluation map $\delta_{\mathrm{D}}:\mathrm{D}^n\to\mathrm{D}$. An *algebraic set* is the zero set $V(S)$ in D^n of a family S of n-linear twists. A map $f:U\to V$ between algebraic sets $U\subset\mathrm{D}^n$ and $V\subset\mathrm{D}^m$ is a *σ-morphism* if its coordinate maps are n-linear twists. It is a *σ-isomorphism* if bijective and if f and f^{-1} are σ-morphisms.

3.3. **Zariski dimension.** Given a subset $V\subset\mathrm{D}^n$, we write $\mathrm{I}(V)$ for the set of n-linear twists that vanish on V. This is a $\mathrm{D}(\sigma)$-submodule of $\mathrm{D}(\sigma,n)$. We define the quotient module

$$\Gamma(V)=\mathrm{D}(\sigma,n)/\mathrm{I}(V),$$

and the *Zariski dimension of V* by

$$\dim V=\dim_{\mathrm{D}(\sigma)}\Gamma(V).$$

For any submodule $I\subset\mathrm{D}(\sigma,n)$, we define its closure $\mathrm{cl}(I)$ by

$$\mathrm{cl}(I)=\left\{\delta\in\mathrm{D}(\sigma,n):\exists\gamma\in\mathrm{D}(\sigma)\setminus\{0\},\ \gamma\delta\in I\right\}.$$

We say that V is a *radical* set if $\mathrm{cl}(\mathrm{I}(V))=\mathrm{I}(V)$.

Fact 3.3. *For any algebraic $V\subset\mathrm{D}^n$ and $\delta\in\mathrm{D}(\sigma,n)$, one has $\dim\left(V\cap\mathrm{V}(\delta)\right)\geqslant\dim V-1$.*

Fact 3.4. *Every algebraic $V\subset\mathrm{D}^n$ has a radical component $V^0\subset V$ with $\dim V=\dim V^0$.*

Fact 3.5. *Let $V\subset\mathrm{D}^n$ be a radical algebraic set. Then V is σ-isomorphic to $\mathrm{D}^{\dim V}$.*

Fact 3.6. *Let $U\subset\mathrm{D}^n$ and $V\subset\mathrm{D}^m$ be algebraic sets. Then $\dim(U\times V)=\dim U+\dim V$.*

Fact 3.7. *Let $U\subset\mathrm{D}^n$ be an irreducible algebraic set and $f:U\to\mathrm{D}^m$ a σ-morphism. One has $\dim\mathrm{VI}(f(U))=\dim U-\dim\mathrm{Ker}f$.*

3.4. **A particular radical group.** The following result uses Fact 3.2 and Chevalley's projection Theorem for constructible sets over a linearly-closed division ring.

Fact 3.8. *Given $n\geqslant 2$ and $\bar{b}\in\mathrm{D}^n$, we consider the algebraic subgroup of D^n defined by*

$$G_{\bar{b}}=\left\{\bar{x}\in\mathrm{D}^n:b_1\gamma(x_1)=\cdots=b_n\gamma(x_n)\right\},$$

where $\gamma=\sigma-\mathrm{id}$. Then $G_{\bar{b}}$ is radical if and only if $(b_1^{-1},\dots,b_n^{-1})$ are left $\mathrm{Fix}(\sigma_{\mathrm{D}})$-free.

4. Main result

We begin by proposing an alternative proof of the stable case, that does not use the fact that iterates of $\sigma - \mathrm{id}$ are uniformly definable in characteristic p (where σ is a conjugation map). The part of the argument that mimics Scanlon's result has the advantage to be valid in any characteristic.

Fact 4.1. *A stable division ring of characteristic p has finite dimension over its centre.*

Proof. Let D be a stable division ring of characteristic p. By the stable descending chain condition on centralisers, it suffices to show that $[\mathrm{D} : C_{\mathrm{D}}(a)]$ is finite for any $a \in \mathrm{D}$ (this will imply that D has finite dimension over a commutative subfield, hence over its centre). Let us assume for a contradiction that there is $a \in \mathrm{D}$ such that $[\mathrm{D} : C_{\mathrm{D}}(a)]$ is infinite. Let σ_{D} be the conjugation map by a and $\gamma = \sigma - \mathrm{id}$. We shall show that γ_{D} is onto D, a contradiction with Theorem 2.7. We adapt [Sca99]. By the stable descending chain condition, there are a natural number m and elements $b_1, \ldots, b_m$ in $\mathrm{D}^\times$ such that

$$I = \bigcap_{b \in \mathrm{D}^\times} b\gamma_{\mathrm{D}}(\mathrm{D}) = \bigcap_{i=1}^{m} b_i \gamma_{\mathrm{D}}(\mathrm{D}).$$

Let $G_{\bar{b}}$ the algebraic subgroup of D^m defined by

$$G_{\bar{b}} = \{\bar{x} \in \mathrm{D}^m : b_1\gamma_{\mathrm{D}}(x_1) = \cdots = b_m\gamma_{\mathrm{D}}(x_m)\}.$$

This is an intersection of $m-1$ hypersurfaces of D^m, so $\dim G_{\bar{b}} \geqslant 1$ by Fact 3.3. By Facts 3.4 and 3.5, one has $\dim_{\mathrm{Fix}(\sigma_{\mathrm{D}})} G_{\bar{b}} = +\infty$, so I contains a non-zero element. Since I is a left ideal of D, one must have $I = \mathrm{D}$, hence $\gamma_{\mathrm{D}}(\mathrm{D}) = \mathrm{D}$. □

Theorem 4.2. *A NIP division ring of characteristic p has finite dimension over its centre.*

Proof. It suffices to show that for such a division ring D and any $a \in \mathrm{D}$, the index $[\mathrm{D} : C_{\mathrm{D}}(a)]$ is finite (for in that case, the set $\{[\mathrm{D} : C_{\mathrm{D}}(a)] : a \in \mathrm{D}\}$ is bounded by the Compactness Theorem, hence any descending chain of centralisers must stabilise by the NIP chain condition). Let us assume for a contradiction that $[\mathrm{D} : C_{\mathrm{D}}(a)]$ is infinite for some $a \in \mathrm{D}$. Let σ_{D} be the conjugation map by a and $\gamma = \sigma - \mathrm{id}$. We shall show that γ_{D} is onto D, a contradiction with Theorem 2.7.

We adapt [KSW11]. For every natural number $m \geqslant 1$ and tuple $\bar{b} \in \mathrm{D}^{\mathbb{N}}$, let us consider the algebraic subgroup $G^m_{\bar{b}}$ of D^m defined by

$$G^m_{\bar{b}} = \{\bar{x} \in \mathrm{D}^m : b_1\gamma_{\mathrm{D}}(x_1) = \cdots = b_m\gamma_{\mathrm{D}}(x_m)\}.$$

One has $\dim G^m_{\bar{b}} \geqslant 1$ by Fact 3.3. The kernel of the first projection $\pi_1 : G^m_{\bar{b}} \to \mathrm{D}$ equals $\{0\} \times \mathrm{Ker}\gamma_{\mathrm{D}} \times \cdots \times \mathrm{Ker}\gamma_{\mathrm{D}}$ hence has Zariski dimension 0 by Fact 3.6. It follows that $\dim G^m_{\bar{b}} = 1$ by Fact 3.7. Since $[\mathrm{D} : C_{\mathrm{D}}(a)]$ is infinite, by Fact 3.8, one may chose an infinite tuple $\bar{c} \in \mathrm{D}^{\mathbb{N}}$ such that the group $G^m_{\bar{c}}$ is radical for every m. By the NIP chain condition, there are natural numbers n and i such that

$$\bigcap_{j \in \{1,\ldots,n+1\}} c_j\gamma_{\mathrm{D}}(\mathrm{D}) = \bigcap_{j \in \{1,\ldots,n+1\} \setminus \{i\}} c_j\gamma_{\mathrm{D}}(\mathrm{D}).$$

Put $\bar{b} = (c_1, \ldots, c_{i-1}, c_{n+1}, c_{i+1}, \ldots, c_n, c_i) \in \mathrm{D}^{n+1}$, so that the projection $\pi_{\mathrm{D}} : G^{n+1}_{\bar{b}} \to G^n_{\bar{b}}$ on the n first coordinates is onto. Since $G^{n+1}_{\bar{b}}$ and $G^n_{\bar{b}}$ are radical, by Fact 3.5, there are two σ-isomorphisms $\delta_{\mathrm{D}} : G^{n+1}_{\bar{b}} \to \mathrm{D}$ and $\varepsilon_{\mathrm{D}} : G^n_{\bar{b}} \to \mathrm{D}$. The σ-morphism $\rho = \varepsilon\pi\delta^{-1}$ makes the following diagram commute.

$$\begin{array}{ccc} G^{n+1}_{\bar{b}} & \xrightarrow{\ \pi\ } & G^n_{\bar{b}} \\ {\scriptstyle\delta}\downarrow & & \downarrow{\scriptstyle\varepsilon} \\ \mathrm{D} & \xrightarrow[\ \rho\ ]{} & \mathrm{D} \end{array}$$

Let $c \in \mathrm{Ker}\rho_{\mathrm{D}} \setminus \{0\}$, and put $\bar{\rho}(x) = \rho(cx)$. Then $\bar{\rho}_{\mathrm{D}}$ is onto and $\bar{\rho}$, γ have the same kernel in any extension of D. By Fact 3.1, $\bar{\rho}$ factorises in $\bar{\rho} = \beta\gamma$ with $\gamma = \sigma - \mathrm{id}$. If $x \in \mathrm{Ker}\beta_{\mathrm{D}}$, then $x = \gamma_{\mathbf{D}}(\mathbf{x})$ for some $\mathbf{x}$ in a linearly-closed extension $\mathbf{D}$ of D given by Fact 3.2, hence $\mathbf{x} \in \mathrm{Ker}\rho_{\mathbf{D}} = \mathrm{Ker}\gamma_{\mathbf{D}}$ so $x = 0$. It follows that β_{D} is bijective, so γ_{D} is onto, which is the desired contradiction. □

Elbée has a few lines proof, using mainly computational properties of the dp-rank, that a strongly NIP division ring has finite dimension over its centre (in any characteristic).

References

[Bou58] Nicolas Bourbaki, *Algèbre, chapitre 8, modules et anneaux semi-simples*, Hermann, 1958.

[Coh73] Paul Moritz Cohn, *The range of derivations on a skew field and the equation $ax - xb = c$*, Journal of the Indian Mathematical Society **37** (1973), 61–69.

[Coh95] ———, *Skew fields, theory of general division rings*, Encyclopedia of Mathematics and its Applications, vol. 57, Cambridge University Press, Cambridge, 1995.

[Dur79] Jean-Louis Duret, *Les corps faiblement algébriquement clos non séparablement clos ont la propriete d'indépendance*, Model Theory of Algebra and Arithmetic (proc. Karpacz), Lecture Notes in Mathematics, vol. 834, Springer-Verlag, Berlin, 1979, pp. 13–162.

[Efr06] Ido Efrat, *Valuations, orderings, and milnor k-theory*, Mathematical Surveys and Monographs, vol. 124, American Mathematical Society, Providence, RI, 2006.

[EP05] Antonio Engler and Alexander Prestel, *Valued fields*, Springer Monographs in Mathematics, 2005.

[Hem15] Nadja Hempel, *On n-dependent groups and fields*, to appear in Mathematical Logic Quarterly (2015).

[Her96] Israel Herstein, *Noncommtuative rings*, The Mathematical Association of America, fourth edition, 1996.

[HH70] Brian Hartley and Trevor Hawkes, *Rings, modules and linear algebra*, Chapman and Hall, London, 1970.

[Hum75] James Humphreys, *Linear algebraic groups*, Graduate texts in mathematics, Springer-verlag, 1975.

[KJ15a] Jochen Koenigsmann and Franziska Jahnke, *Definable henselian valuations*, The Journal of Symbolic Logic **80** (2015), 85–99.

[KJ15b] ———, *Uniformly defining p-henselian valuations*, Annals of Pure and Applied Logic **166** (2015), 741–754.

[Kru32] Wolfgang Krull, *Allgemeine bewertungstheorie*, Journal für Mathematik **167** (1932), 160–196.

[KSW11] Itay Kaplan, Thomas Scanlon, and Frank O. Wagner, *Artin-Schreier extensions in NIP and simple fields*, Israel J. Math. **185** (2011), 141–153.

[Lae61] Earl Laerson, *Onto inner derivations in division rings*, Bulletin of the American Mathematical Society **67** (1961), 356–358.

[Lam91] Tsit Yuen Lam, *A first course in noncommutative rings*, Graduate Texts in Mathematics, vol. 131, Springer-Verlag, Berlin/Heidelberg, 1991.

[Lam99] ———, *Lectures on modules and rings*, Graduate Texts in Mathematics, vol. 189, Springer-Verlag, New York, 1999.

[Lam03] ———, *Exercises in classical ring theory*, Problem books in Mathematics, Springer-Verlag, New York, 2003, Second Edition.

[Mei61] Gary Meisters, *On the equation $ax - xb = c$ in division rings*, Proceedings of the American Mathematical Society **12** (1961), 428–432.

[Pre88] Mike Prest, *Model theory and modules*, London Mathematical Society Lecture notes, 1988.

[Sca99] Thomas Scanlon, *Infinite stable fields are Artin-Schreier closed*, unpublished (1999).

5, rue Ornano,
69001 Lyon, France

E-mail address: cedric.milliet@gmail.com