Residues of skew rational functions and linearized Goppa codes

Xavier Caruso

▶ **To cite this version:**

Xavier Caruso. Residues of skew rational functions and linearized Goppa codes. 2019. hal-02268790v1

HAL Id: hal-02268790

https://hal.science/hal-02268790v1

Preprint submitted on 21 Aug 2019 (v1), last revised 16 Jun 2021 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Residues of skew rational functions and linearized Goppa codes

Xavier Caruso

August 21, 2019

Abstract

This paper constitutes a first attempt to do analysis with skew polynomials. Precisely, our main objective is to develop a theory of residues for skew rational functions (which are, by definition, the quotients of two skew polynomials). We prove in particular a skew analogue of the residue formula and a skew analogue of the classical formula of change of variables for residues.

We then use our theory to define and study a linearized version of Goppa codes. We show that these codes meet the Singleton bound (for the sum-rank metric) and are the duals of the linearized Reed–Solomon codes defined recently by Martínez-Peñas. We also design efficient encoding and decoding algorithms for them.

Contents

In 1933, Ore introduced in [24] a noncommutative variant of the ring of polynomials and established its first properties. Since then, Ore's polynomials have become important mathematical objects and have found applications in many domains of mathematics: abstract algebra, semi-linear algebra, linear differential equations (over any field), Drinfel'd modules, coding theory, *etc.* Ore's polynomials have been studied by several authors: first by Ore himself [24], Jacobson [11, 12] and more recently by Ikehata [9, 10], who proved the Ore's polynomial rings are Azumaya algebras in certains cases, by Lam and Leroy [14, 16, 17] who defined and studied evaluation of Ore's polynomials, and by many others. Lectures including detailed discussions on Ore's polynomials also appear in the literature; for instance, one can cite Cohn's book [5] or Jacobson's book [13].

In the classical commutative case, polynomials are quite interesting because they exhibit at the same time algebraic and analytic aspects: typically, the Euclidean structure of polynomials rings has an algebraic flavour, while derivations and Taylor-like expansion formulas are highly inspired by analysis. However, as far as we know, analysis with Ore's polynomials has not been systematically

studied yet. This article aims at laying the first stone of this study. More precisely, our main motivation is to develop a theory of residues for Ore's polynomials and derive applications.

Actually, the setting of this paper does not encompass the whole generality of Ore's polynomials over arbitrary rings. Precisely, we consider a field K equipped with an automorphism of finite order θ and restrict ourselves to the ring of skew polynomials $K[X;\theta]$ in which the multiplication is governed by the rule $Xa = \theta(a)X$ for $a \in K$. We first define Taylor-like expansions in this framework and show that any skew polynomial $f \in K[X;\theta]$ admits infinite Taylor expansions around any point $z \in K$ fixed by θ. When $z \neq 0$, this expansion takes the form:

$$f(X) = \sum_{n=0}^{\infty} a_n \cdot (X^r - z)^n \tag{1}$$

where r denotes the order of θ and the coefficients a_n lie in the quotient ring $K[X;\theta]/(X^r - z)$. Moreover, assuming further that r is coprime with the characteristic of K, we equip $K[X;\theta]$ with a canonical derivation and interpret the coefficients a_n appearing in Eq. (1) as the values at z of the successive divided derivatives of $f(X)$. All the previous results extend without difficulty to skew rational functions, that are elements of the fraction field of $K[X;\theta]$; in this generality, Taylor expansions take the form:

$$f(X) = \sum_{n=v}^{\infty} a_n \cdot (X^r - z)^n \qquad (v \in \mathbb{Z}). \tag{2}$$

These results lead naturally to the notion of residue: by definition, the residue of $f(X)$ at z is the coefficient a_{-1} in the expansion (2). Considering scalar extensions, we extend this definition to any point z in a separable closure of K, including ∞. In the classical commutative setting, the theory of residues is very powerful because we have at our disposal many formulas, allowing for a complete toolbox for manipulating them easily and efficiently. In this article, we shall prove that residues of skew rational functions also exhibit interesting formulas, that are:

- a residue formula, relating all the residues (at all points) of a given skew rational function,
- a formula of change of variables, expliciting how residues behave under an endomomorphism of $\mathrm{Frac}(K[X;\theta])$.

We then move to applications to coding theory. The story starts in 1978 when Delsarte noticed that linearized polynomials over finite fields can be used to define good codes with respect to the rank metric. These codes were rediscovered by Gabidulin in 1985 and Roth in 1991 and are called nowadays *Gabidulin codes*. More recently, Boucher and Ulmer [2] realized, in a slighty different context, that linearized polynomials can be advantageously replaced by skew polynomials. In 2016, Liu [19] proposed in his thesis to define codes using evaluation of skew polynomials, extending then Gabidulin codes to a more general setting. In 2018, Martínez-Peñas [20] extended Liu's construction to arbitrary Ore's algebras and came up with the notion of linearized Reed–Solomon codes. He also introduced the sum-rank distance, which is the relevant metric for studying these codes. In the present paper, we show that, considering residues in place of evaluations, we end up with new interesting codes, that we call *linearized Goppa codes*. We prove that these codes exhibit an optimal minimal distance (they meet the Singleton bound) and we design efficient encoding and decoding algorithms for them. Moreover, a consequence of the skew residue formula is that our linearized Goppa codes appear naturally as the duals of Martínez-Peñas' linearized Reed–Solomon codes.

This article is structured as follows. In §1, we recall several useful algebraic properties of rings of skew polynomials. Special attention is paid to the study of endomorphisms of $K[X;\theta]$ and of its fraction fields. The heart of the article is contained in §2. After a premilinary study of derivations of $K[X;\theta]$ and of its fraction fields, we establish Taylor-like expansion formulas and develop the theory of residues we have outlined rapidly above. Finally, applications to coding theory are addressed in §3. We emphasize that §3 actually uses only a small part of the contents of §2. Therefore, we advise the reader, who is mostly interesting by coding theory, to skip the technicalities of §2 in the first reading and just go back to it for following the few references encoutered while reading §3.

1 Algebra with skew polynomials

Throughout this article, we consider a field K equipped with an automorphism $\theta : K \to K$ of finite order r. We let F be the subfield of K consisting of elements $a \in K$ with $\theta(a) = a$. The extension K/F has degree r and it is Galois with cyclic Galois group generated by θ.

We denote by $K[X;\theta]$ the Ore algebra of *skew polynomials* over K. By definition elements of $K[X;\theta]$ are usual polynomials with coefficients in K, subject to the multiplication driven by the following rule:

$$\forall a \in K, \quad X \cdot a = \theta(a)X. \tag{3}$$

Similarly, we define the ring $K[X^{\pm 1};\theta]$: its elements consists of Laurent polynomials over K in the variable X and the multiplication on it is given by (3) and its counterpart:

$$\forall a \in K, \quad X^{-1} \cdot a = \theta^{-1}(a)X^{-1}. \tag{4}$$

In what follows, we will write $\mathcal{A} = K[X^{\pm 1};\theta]$. Letting $Y = X^r$, it is easily checked that the centre of $\mathcal{A}$ is $F[Y^{\pm 1}]$; we denote it by $\mathcal{Z}$. We also set $\mathcal{C} = K[Y^{\pm 1}]$; it is a maximal *commutative* subring of $\mathcal{A}$. We shall also use the notations $\mathcal{A}^+$, $\mathcal{C}^+$ and $\mathcal{Z}^+$ for $K[X;\theta]$, $K[Y]$ and $F[Y]$ respectively.

In this section, we review the most important algebraic properties of $\mathcal{A}^+$ and $\mathcal{A}$. A large part of the material presented here is somehow classical and already appears in [24, 9, 10, 14, 16, 17, 5, 13]. However, our presentation might be different on certain points and we spend some time in §1.2 to classify and study the endomorphisms of $\mathcal{A}^+$, $\mathcal{A}$ and some of their quotients as they will play an important role in this article. Besides, the theory of evaluation of skew polynomials we will present in §1.3.2 is developed a bit further than it is in the above references.

1.1 Preliminaries

The ring $\mathcal{A}^+$ was first introduced by Ore in his seminal paper [24]. In this article, Ore proved many important algebraic properties of $\mathcal{A}^+$ that we recall below.

Euclidean division and consequences. As usual polynomials, skew polynomials are endowed with a Euclidean division, which is very useful for elucidating the algebraic structure of the rings $\mathcal{A}^+$ and $\mathcal{A}$. The Euclidean division relies on the notion of degree whose definition is straightforward.

Definition 1.1.1. The *degree* of a nonzero skew polynomial $f = \sum_i a_i X^i \in \mathcal{A}^+$ is the largest integer i for which $a_i \neq 0$.

By definition, the degree of $0 \in \mathcal{A}^+$ is $-\infty$.

Theorem 1.1.2. *Let $A, B \in \mathcal{A}^+$ with $B \neq 0$.*

(i) There exists $Q_{\text{right}}, R_{\text{right}} \in \mathcal{A}^+$, uniquely determined, such that $A = Q_{\text{right}} \cdot B + R_{\text{right}}$ and $\deg R_{\text{right}} < \deg B$.

(ii) There exists $Q_{\text{left}}, R_{\text{left}} \in \mathcal{A}^+$, uniquely determined, such that $A = B \cdot Q_{\text{left}} + R_{\text{left}}$ and $\deg R_{\text{left}} < \deg B$.

We underline that, in general, $Q_{\text{right}} \neq Q_{\text{left}}$ and $R_{\text{right}} \neq R_{\text{left}}$. For example, in $\mathbb{C}[X, \text{conj}]$ (where conj is the complex conjugacy), the Euclidean divisions of aX by $X - c$ (for some $a, c \in \mathbb{C}$) read:

$$aX = a \cdot (X - c) + ac = (X - c) \cdot \bar{a} + \bar{a}c.$$

Actually, without the assumption that θ has finite order, right Euclidean division always exists but left Euclidean division may fail to exist.

The mere existence of Euclidean divisions has the following classical consequence.

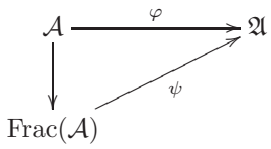
Corollary 1.1.3. *The ring $\mathcal{A}^+$ is left and right principal.*

A further consequence is the existence of left and right gcd and lcm on $\mathcal{A}^+$. They are defined in term of ideals:

$$\mathcal{A}f + \mathcal{A}g = \mathcal{A} \cdot \text{RGCD}(f, g) \quad ; \quad \mathcal{A}f \cap \mathcal{A}g = \mathcal{A} \cdot \text{LLCM}(f, g)$$
$$f\mathcal{A} + g\mathcal{A} = \text{LGCD}(f, g) \cdot \mathcal{A} \quad ; \quad f\mathcal{A} \cap g\mathcal{A} = \text{RLCM}(f, g) \cdot \mathcal{A}$$

for $f, g \in \mathcal{A}^+$. A noncommutative version of Euclidean algorithm is also available and allows for an explicit and efficient computation of left and right gcd and lcm.

Fraction field. For many applications, it is often convenient to be able to manipulate quotient of polynomials, namely rational functions, as well-defined mathematical objects. In the skew case, defining the field of rational functions is more subtle but can be done: using Ore condition [23] (see also [15, §10]), one proves that there exists a unique field $\mathrm{Frac}(\mathcal{A})$ containing $\mathcal{A}$ and satisfying the following universal property: for any noncommutative ring $\mathfrak{A}$ and any ring homomorphism $\varphi : \mathcal{A} \to \mathfrak{A}$ such that $\varphi(x)$ is invertible for all $x \in \mathcal{A}$, $x \neq 0$, there exists a unique morphism $\psi : \mathrm{Frac}(\mathcal{A}) \to \mathfrak{A}$ making the following diagram commutative:



(5)

Under our assumption that θ has finite order the construction of $\mathrm{Frac}(\mathcal{A})$ can be simplified. Indeed, we have the following theorem.

Theorem 1.1.4. *The ring* $\mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}} \mathcal{A} \simeq \mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}^+} \mathcal{A}^+$ *containing* $\mathcal{A}$ *and it satisfies the above universal property,* i.e.*:*

$$\mathrm{Frac}(\mathcal{A}) = \mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}} \mathcal{A} = \mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}^+} \mathcal{A}^+.$$

For the proof, we will need the following lemma.

Lemma 1.1.5. *Any skew polynomial* $f \in \mathcal{A}$ *has a left multiple and a right multiple in* $\mathcal{Z}$*.*

Proof. If $f = 0$, the lemma is obvious. Otherwise, the quotient $\mathcal{A}/f\mathcal{A}$ is a finite dimension vector space over F. Hence, there exists a nontrivial relation of linear dependence of the form:

$$a_0 + a_1 Y + a_2 Y^2 + \cdots + a_n Y^n \in f\mathcal{A} \qquad (a_i \in F).$$

In other words, there exists $g \in \mathcal{A}$ such that $fg = N$ with $N = a_0 + \cdots + a_n Y^n$. In particular $fg \in \mathcal{Z}$, showing that f has a right multiple in $\mathcal{Z}$. Multiplying the relation $fg = N$ by g on the left, we get $gfg = Ng = gN$. Simplifying now by g on the left, we are left with $gf = N$, showing that f has a left mutiple in $\mathcal{Z}$ as well. □

Proof of Theorem 1.1.4. Clearly $\mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}} \mathcal{A}$ contains $\mathcal{A}$. Let us prove now that it is a field. Reducing to the same denominator, we remark that any element of $\mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}} \mathcal{A}$ can be written as $D^{-1} \otimes f$ with $D \in \mathcal{Z}$ and $f \in \mathcal{A}$. We assume that $f \neq 0$. By Lemma 1.1.5, there exists $f \in \mathcal{A}$ such that $fg \in \mathcal{Z}$. Letting $N = fg$, one checks that $N^{-1} \otimes gD$ is a multiplicative inverse of $D^{-1} \otimes f$.

Consider now a noncommutative ring $\mathfrak{A}$ together with a ring homomorphism $\varphi : \mathcal{A} \to \mathfrak{A}$ such that $\varphi(x)$ is invertible for all $x \in \mathcal{A}$, $x \neq 0$. If $\psi : \mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}} \mathcal{A} \to \mathfrak{A}$ is an extension of φ, it must satisfy:

$$\psi\big(D^{-1} \otimes f\big) = \varphi(D)^{-1} \cdot \varphi(f). \tag{6}$$

This proves that, if such an extension exists, it is unique. On the other hand, using that $\mathcal{Z}$ is central in $\mathcal{A}$, one checks that the formula (6) determines a well-defined ring homomorphism $\mathrm{Frac}(\mathcal{A}) \to \mathfrak{A}$ making the diagram (5) commutative. □

The notion of degree extends with difficulty to skew rational functions: if $f = \frac{g}{D} \in \mathrm{Frac}(\mathcal{A})$ with $g \in \mathcal{A}^+$ and $D \in \mathcal{Z}^+$, we define $\deg f = \deg g - \deg D$. This definition is not ambiguous because an equality of the form $\frac{g}{D} = \frac{g'}{D'}$ implies $gD' = g'D$ (since D and D' are central) and then $\deg g + \deg D' = \deg g' + \deg D$, that is $\deg g - \deg D = \deg g' - \deg D'$.

1.2 Endomorphisms of skew polynomial rings

The aim of this subsection is to classify and derive interesting structural properties of the endomorphisms of various rings of skew polynomials.

Classification. Given an integer $n \in \mathbb{Z}$ and a Laurent polynomial $C \in \mathcal{C}$ written as $C = \sum_i a_i X^i$, we define $\theta(C) = \sum_i \theta(a_i) X^i$. The obtained morphism θ extends to $\mathrm{Frac}(\mathcal{C})$. For $n \geq 0$ and $C \in \mathrm{Frac}(\mathcal{C})$, we set:

$$\mathrm{N}_n(C) = C \cdot \theta(C) \cdots \theta^{n-1}(C)$$

and, when $C \neq 0$, we extend the definition of N_n to negative n by:

$$\mathrm{N}_n(C) = \theta^{-1}(C^{-1}) \cdot \theta^{-2}(C^{-1}) \cdots \theta^{n}(C^{-1})$$

We observe that $\mathrm{N}_0(C) = 1$ and $\mathrm{N}_1(C) = C$ for all $C \in \mathcal{C}$. Moreover, when $n = r$, the mapping N_r is the norm from $\mathrm{Frac}(\mathcal{C})$ to $\mathrm{Frac}(\mathcal{Z})$. In particular $\mathrm{N}_r(C) \in \mathrm{Frac}(\mathcal{Z})$ for all $C \in \mathrm{Frac}(\mathcal{C})$.

Theorem 1.2.1. *Let $\gamma : \mathcal{A}^+ \to \mathcal{A}^+$ (resp. $\gamma : \mathcal{A} \to \mathcal{A}$, resp. $\gamma : \mathrm{Frac}(\mathcal{A}) \to \mathrm{Frac}(\mathcal{A})$) be a morphism of K-algebras. Then there exists a uniquely determined element $C \in \mathcal{C}^+$ (resp. invertible[1] element $C \in \mathcal{C}$, resp. nonzero element $C \in \mathrm{Frac}(\mathcal{C})$) such that*

$$\gamma\Big(\sum_i a_i X^i\Big) = \sum_i a_i (CX)^i = \sum_i a_i \mathrm{N}_i(C) X^i. \tag{7}$$

Conversely any element of C as above gives rise to a well-defined endomorphism of $\mathcal{A}^+$ (resp. $\mathcal{A}$, resp. $\mathrm{Frac}(\mathcal{A})$).

Remark 1.2.2. An endomorphism of $\mathrm{Frac}(\mathcal{A})$ is entirely determined by Eq. (7). Indeed, by definition, the datum of $\gamma : \mathrm{Frac}(\mathcal{A}) \to \mathrm{Frac}(\mathcal{A})$ is equivalent to the the datum of a morphism $\tilde{\gamma} : \mathcal{A} \to \mathrm{Frac}(\mathcal{A})$ with the property that $\tilde{\gamma}(f) \neq 0$ whenever $f \neq 0$. Moreover, in the above equivalence, $\tilde{\gamma}$ appears as the restriction of γ to $\mathcal{A}$. This shows, in particular, that γ is determined by its restriction to $\mathcal{A}$.

Proof of Theorem 1.2.1. Unicity is obvious since C can be recovered thanks to the formula $C = \gamma(X)X^{-1}$.

We first consider the case of an endomorphism of $\mathcal{A}^+$. Write $\gamma(X) = \sum_i c_i X^i$ with $c_i \in K$. Applying γ to the relation (3), we obtain:

$$\sum_i c_i \theta^i(a) \cdot X^{i+1} = \sum_i c_i \theta(a) \cdot X^{i+1}$$

for all $a \in K$. Identifying the coefficients, we end up with $c_i \theta^i(a) = c_i \theta(a)$. Since this equality must hold for all a, we find that c_i must vanish as soon as $i \not\equiv 1 \pmod{r}$. Therefore, $\gamma(X) = CX$ for some element $C \in \mathcal{C}^+$. An easy induction on i then shows that $\gamma(X^i) = \mathrm{N}_i(C) X^i$ for all i, implying eventually (7). Conversely, it is easy to check that Eq. (7) defines a morphism of K-algebras.

For endomorphisms of $\mathcal{A}$, the proof is exactly the same, except that we have to justify further that C is invertible. This comes from the fact that $X\,\gamma(X^{-1})$ has to be an inverse of C.

We now come to the case of endomorphisms of $\mathrm{Frac}(\mathcal{A})$. Writing $\gamma(X) = fD^{-1}$ with $f \in \mathcal{A}^+$ and $D \in \mathcal{Z}^+$ and repeating the proof above, we find that $fX^{-1} \in \mathcal{C}$. Thus $\gamma(X) = CX$ with $C \in \mathrm{Frac}(\mathcal{C})$. As before, C cannot vanish because it admits $X\,\gamma(X^{-1})$ as an inverse. From the fact that γ is an endomorphism of K-algebras, we deduce that $\gamma_{|\mathcal{A}}$ is given by Eq. (7). Conversely, we need to justify that the morphism γ defined by Eq. (7) extends to $\mathrm{Frac}(\mathcal{A})$. After Remark 1.2.2, it is enough to check that $\gamma(f) \neq 0$ when $f \neq 0$, which can be seen by comparing degrees. □

For $C \in \mathrm{Frac}(\mathcal{C})$, $C \neq 0$, we let $\gamma_C : \mathrm{Frac}(\mathcal{A}) \to \mathrm{Frac}(\mathcal{A})$ denote the endomorphism of Theorem 1.2.1 ($X \mapsto CX$). When C lies in $\mathcal{C}^+$ (resp. when C is invertible in $\mathcal{C}$), γ_C stabilized $\mathcal{A}^+$ (resp. $\mathcal{A}$); when this occurs, we will continue to write γ_C for the endomorphism induced on $\mathcal{A}^+$ (resp. on $\mathcal{A}$). We observe that γ_C takes Y to:

$$\mathrm{N}_r(C) \cdot Y = \mathrm{N}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C) \cdot Y \in \mathrm{Frac}(\mathcal{Z})$$

and, therefore, maps $\mathrm{Frac}(\mathcal{Z})$ to itself. In other words, any endomorphism of K-algebra of $\mathrm{Frac}(\mathcal{A})$ stabilizes the centre. This property holds similarly for endomorphism of $\mathcal{A}^+$ and endomorphisms of $\mathcal{A}$.

[1] We notice that the invertible elements of $\mathcal{C}$ are exactly those of the form aY^n with $a \in K$, $a \neq 0$ and $n \in \mathbb{Z}$.

Proposition 1.2.3. *For $C \in \mathrm{Frac}(\mathcal{C})$, the following assertions are equivalent:*

(i) γ_C *is a morphism of* $\mathcal{C}$*-algebras,*

(ii) $\mathrm{N}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C) = 1$,

(iii) there exists $U \in \mathrm{Frac}(\mathcal{C})$, $U \neq 0$ *such that* $\gamma_C(f) = U^{-1}fU$ *for all* $f \in \mathrm{Frac}(\mathcal{A})$.

Proof. If γ_C is an endomorphism of $\mathcal{C}$-algebras, it must act trivially on $\mathcal{Z}$, implying then (ii). By Hilbert's Theorem 90, if $C \in \mathrm{Frac}(\mathcal{C})$ has norm 1, it can be written as $\frac{\theta(U)}{u}$ for some $U \in \mathrm{Frac}(\mathcal{C})$, $U \neq 0$; (iii) follows. Finally it is routine to check that (iii) implies (i). □

For endomorphisms of $\mathcal{A}^+$ and $\mathcal{A}$, Proposition 1.2.3 can be made more precise.

Proposition 1.2.4. *For $C \in \mathcal{C}$, the following assertions are equivalent:*

(i) γ_C *is a morphism of* $\mathcal{C}$*-algebras,*

(ii) $\mathrm{N}_{\mathcal{C}/\mathcal{Z}}(C) = 1$,

(ii') $C \in K$ *and* $\mathrm{N}_{K/F}(C) = 1$,

(iii) there exists $u \in K$, $u \neq 0$ *such that* $\gamma_C(f) = u^{-1}fu$ *for all* $f \in \mathrm{Frac}(\mathcal{A})$.

Proof. The proof is the same as that of Proposition 1.2.3, except that we need to justify in addition that any element $C \in \mathcal{C}$ of norm 1 needs to be a constant. This follows by comparing degrees. □

Corollary 1.2.5. *Any endomorphism of* $\mathcal{C}$*-algebras of* $\mathcal{A}^+$ *(resp.* $\mathcal{A}$*, resp.* $\mathrm{Frac}(\mathcal{A})$*) is an isomorphism.*

Proof. The case of $\mathcal{A}^+$ (resp. $\mathcal{A}$) follows directly from Proposition 1.2.4. For $\mathrm{Frac}(\mathcal{A})$, we check that if γ_C is an endomorphism of $\mathcal{C}$-algebra then $\gamma_{C^{-1}}$ is also (it is a consequence of Proposition 1.2.3) and $\gamma_C \circ \gamma_{C^{-1}} = \gamma_{C^{-1}} \circ \gamma_C = \mathrm{id}$. □

Morphisms between quotients. Let $N \in \mathcal{Z}^+$ be a nonconstant polynomial with a nonzero constant term. The principal ideals generated by N in $\mathcal{A}^+$ and $\mathcal{A}$ respectively are two-sided, so that the quotients $\mathcal{A}^+/N\mathcal{A}^+$ and $\mathcal{A}/N\mathcal{A}$ inherit a structure of K-algebra. By our assumptions on N, they are moreover isomorphic. We consider in addition a commutative algebra $\mathcal{Z}'$ over $\mathcal{Z}$. We let θ act on $\mathcal{Z}^+ \otimes_{\mathcal{Z}} \mathcal{C}$ by $\mathrm{id} \otimes \theta$ and we extend the definition of γ_C to all elements $C \in \mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{C}$. Precisely, for C as above, we define $\gamma_C : \mathcal{A}^+ \to \mathcal{Z}^+ \otimes_{\mathcal{Z}} \mathcal{A}$ by

$$\gamma_C\Big(\sum_i a_i X^i\Big) = \sum_i a_i (CX)^i = \sum_i a_i \mathrm{N}_i(C) X^i.$$

Theorem 1.2.6. *Let $N_1, N_2 \in \mathcal{Z}^+$ be two nonconstant polynomials with nonzero constant terms. Let $\gamma : \mathcal{A}/N_1\mathcal{A} \to \mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{A}/N_2\mathcal{A}$ be a morphism of K-algebras. Then $\gamma = \gamma_C \mod N_2$ for some element $C \in \mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{C}$ with the property that N_2 divides $\gamma_C(N_1)$. Such an element C is uniquely determined modulo N_2.*

Moreover, the following assertions are equivalent:

(i) γ *is a morphism of* $\mathcal{C}$*-algebras,*

(ii) $\mathrm{N}_{\mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{C}/\mathcal{Z}'}(C) \equiv 1 \pmod{N_2}$.

(iii) there exists $U \in \mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{C}/N_2\mathcal{C}$, U *invertible such that* $\gamma(f) = U^{-1}fU$ *for all* $f \in \mathcal{A}/N_1\mathcal{A}$.

Proof. The proof is entirely similar to that of Theorem 1.2.1 and Proposition 1.2.3. Note that, for the point (iii), Hilbert's Theorem 90 applies because the extension $\mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{C}/N_2\mathcal{C}$ of $\mathcal{Z}'/N_2\mathcal{Z}'$ is a cyclic Galois covering. □

As an example, let us have a look at the case where $\mathcal{Z}' = \mathcal{Z}$ and N_1 and N_2 have Y-degree 1. Write $N_1 = Y - z_1$ and $N_2 = Y - z_2$ with $z_1 \neq 0$ and $z_2 \neq 0$. By Theorem 1.2.6, any morphism $\gamma : \mathcal{A}/N_1\mathcal{A} \to \mathcal{A}/N_2\mathcal{A}$ has the form $X \mapsto cX$ for an element $c \in K$ with the property that:

$$z_1 = \mathrm{N}_{K/F}(c) \cdot z_2. \tag{8}$$

Obviously, Eq. (8) implies that c does not vanish. Hence, any morphism γ as above is automatically an isomorphism. Moreover, Eq. (8) again shows that $\frac{z_1}{z_2}$ must be a norm in the extension K/F. Conversely, if $\frac{z_1}{z_2}$ is the norm of an element $c \in K$, the morphism γ_C induces an isomorphism between $\mathcal{A}/N_1\mathcal{A}$ to $\mathcal{A}/N_2\mathcal{A}$. We have then proved the following proposition.

Proposition 1.2.7. *Let z_1 and z_2 be two nonzero elements of F. There exists a morphism $\mathcal{A}/(Y-z_1)\mathcal{A} \to \mathcal{A}/(Y-z_2)\mathcal{A}$ if and only if $\frac{z_1}{z_2}$ is a norm in the extension K/F. Moreover, when this occurs, any such morphism is an isomorphism.*

The section operators. For $j \in \mathbb{Z}$, we define the *section operator* $\sigma_j : \mathcal{A} \to \mathcal{C}$ by the formula:

$$\sigma_j\Big(\sum a_i X^i\Big) = \sum_i a_{j+ir} Y^i.$$

For $0 \leq j < r$ and $f \in \mathcal{A}$, we notice that $\sigma_j(f)$ is the j-th coordinate of f in the canonical basis $(1, X, X^2, \ldots, X^{r-1})$ of $\mathcal{A}$ over $\mathcal{C}$. When $j \geq 0$, we observe that σ_j takes $\mathcal{A}^+$ to $\mathcal{C}^+$ and then induces a mapping $\mathcal{A}^+ \to \mathcal{C}^+$ that, in a slight abuse of notations, we will continue to call σ_j.

Lemma 1.2.8. *For $f \in \mathcal{A}$, $C \in \mathcal{C}$ and $j \in \mathbb{Z}$, the following identities hold:*

(i) $f = \sum_{j=0}^{p-1} \sigma_j(f) X^j$,

(ii) $\sigma_j(fC) = \sigma_j(f) \cdot \theta^j(C)$ *and* $\sigma_j(fX) = \sigma_{j-1}(f)$,

(iii) $\sigma_j(Cf) = C \cdot \sigma_j(f)$ *and* $\sigma_j(Xf) = \theta(\sigma_{j-1}(f))$,

(iv) $\sigma_{j-r}(f) = Y \cdot \sigma_j(f)$.

Proof. It is an easy checking. □

Lemma 1.2.8 ensures in particular that σ_0 is $\mathcal{C}$-linear and the σ_j's are $\mathcal{Z}$-linear for all $j \in \mathbb{Z}$. Consequently, for any integer j, the operator σ_j induces a $\mathrm{Frac}(\mathcal{C})$-linear mapping $\mathrm{Frac}(\mathcal{A}) \to \mathrm{Frac}(\mathcal{C})$. Similarly, for any $N \in \mathcal{Z}$ and any integer j, it also induces a $(\mathcal{Z}/N\mathcal{Z})$-linear mapping $\mathcal{A}/N\mathcal{A} \to \mathcal{C}/N\mathcal{C}$. Tensoring by a commutative $\mathcal{Z}$-algebra $\mathcal{Z}'$, we find that σ_j induces also a $(\mathcal{Z}'/N\mathcal{Z}')$-linear mapping $\mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{A}/N\mathcal{A} \to \mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{C}/N\mathcal{C}$. In a slight abuse of notations, we will continue to denote by σ_j all the extensions of σ_j defined above.

It worths remarking that the section operators satisfy special commutation relations with the morphisms γ_C introduced above, namely:

Lemma 1.2.9. *For $C \in \mathrm{Frac}(\mathcal{C})$ (resp. $C \in \mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{C}$) and $j \in \mathbb{Z}$, we have the relation $\sigma_j \circ \gamma_C = \mathrm{N}_j(C) \cdot (\gamma_C \circ \sigma_j)$.*

Proof. Let $f \in \mathcal{A}^+$ and write $f = \sum_{i=0}^{r-1} \sigma_i(f) X^i$. Applying γ_C to this relation, we obtain:

$$\gamma_C(f) = \sum_{i=0}^{r-1} \gamma_C \circ \sigma_i(f) \cdot \mathrm{N}_j(X)\, X^i.$$

Applying now σ_j, we end up with $\sigma_j \circ \gamma_C(f) = \gamma_C \circ \sigma_j(f) \cdot \mathrm{N}_j(X)$. This proves the lemma. □

From Lemma 1.2.9, it is possible to construct some quantities that are invariant under all γ_C, that is, after what we have achieved before, under all morphisms of K-algebras. Precisely, for a tuple of integers $(j_1, \ldots, j_m) \in \mathbb{Z}^m$, we define:

$$\sigma_{j_1,\ldots,j_m} = \sigma_{j_1} \cdot (\theta^{j_1} \circ \sigma_{j_2}) \cdot (\theta^{j_1+j_2} \circ \sigma_{j_3}) \cdots (\theta^{j_1+\cdots+j_{m-1}} \circ \sigma_{j_m}) \ : \ \mathrm{Frac}(\mathcal{A}) \to \mathrm{Frac}(\mathcal{C}).$$

Proposition 1.2.10. *Let $\gamma : \mathcal{A}^+ \to \mathcal{A}^+$ (resp. $\gamma : \mathcal{A} \to \mathcal{A}$, resp. $\gamma : \mathrm{Frac}(\mathcal{A}) \to \mathrm{Frac}(\mathcal{A})$, resp. $\gamma : \mathcal{A}/N_1\mathcal{A} \to \mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{A}/N_2\mathcal{A}$ with $\mathcal{Z}'$, N_1, N_2 as in Theorem 1.2.6). Let $(j_1, \ldots, j_m) \in \mathbb{Z}^m$.*

(i) If γ is a morphism of K-algebras, then γ commutes with $\sigma_{j_1,\ldots,j_m}$ as soon as $j_1 + \cdots + j_m = 0$.

(ii) If γ is a morphism of $\mathcal{C}$-algebras, then γ commutes with $\sigma_{j_1,\ldots,j_m}$ as soon as $j_1 + \cdots + j_m \equiv 0 \pmod{r}$.

Proof. By Theorem 1.2.1 or 1.2.6, it is enough to prove the Proposition when $\gamma = \gamma_C$ for some C. By Lemma 1.2.9, combined with the relation $\mathrm{N}_{j+j'}(C) = \mathrm{N}_j(C) \cdot \theta^j\big(\mathrm{N}_{j'}(C)\big)$ (for $j, j' \in \mathbb{Z}$), we find:

$$\sigma_{j_1,\ldots,j_m} \circ \gamma_C = \mathrm{N}_{j_1+\cdots+j_m}(C) \cdot \big(\gamma_C \circ \sigma_{j_1,\ldots,j_m}\big).$$

The first assertion follows while the second is a direct consequence of the caracterisation of morphisms of $\mathcal{C}$-algebras given by Proposition 1.2.4 or Theorem 1.2.6. □

1.3 Evaluation of skew polynomials

Defining nice evaluation maps for skew polynomials is not a straightforward task because the most natural map one thinks at, namely:

$$K[X;\theta] \to K, \quad \textstyle\sum_i a_i X^i \mapsto \sum_i a_i c^i$$

(for a given element $c \in K$) is *not* a ring homomorphism: it does not preserve multiplication. This subsection aims at getting around this issue and define a good notion of evaluation for skew polynomials.

1.3.1 Evaluation at semi-linear morphisms

One option for defining good evaluation maps consists in evaluating skew polynomial at other types of arguments. Precisely, instead of scalars, we are going to consider semi-linear endomorphisms of K. Let us recall briefly that a semi-linear endomorphism φ of a K-vector space V is an additive mapping $\varphi : V \to V$ satisfying the following axiom:

$$\forall \lambda \in K,\ \forall x \in V, \quad \varphi(\lambda x) = \theta(\lambda)\varphi(x). \tag{9}$$

We observe in particular that semi-linear endomorphisms are F-linear.

Definition 1.3.1. Given $P = \sum_i a_i X^i \in \mathcal{A}^+$ and a semi-linear morphism $\varphi : V \to V$ (where V is a K-vector space), we define $P(\varphi) = \sum_i a_i \varphi^i$.

Note that $P(\varphi)$ is a F-linear endomorphism to V. In other words, Definition 1.3.1 leads to a function:

$$\varepsilon_\varphi : \mathcal{A}^+ \to \mathrm{End}_F(V)$$

where $\mathrm{End}_F(V)$ denotes the ring of F-linear endomorphisms of V. The latter is naturally a K-algebra since V is, by definition, a vector space over K. Besides, we observe that when φ is invertible, the mapping ε_φ extends to $\mathcal{A}$. Regarding our objective to define nice evaluation maps, the relevance of the above construction is summarized in the next lemma.

Lemma 1.3.2. *The mapping ε_φ is a morphism of K-algebras.*

Proof. For $c \in K$, let $m_c : V \to V$, $x \mapsto cx$. It is enough to check that $\varphi \circ m_c = m_{\theta(c)} \circ \varphi$, which is a direct reformulation of the axiom (9). □

Besides, semi-linear endomorphisms of K are easy to classify, as shown by the next proposition.

Proposition 1.3.3. *(i) For all $c \in K$, $c\,\theta$ is a semi-linear endomorphism of K.*

(ii) All the semi-linear endomorphisms of K are of this form.

Proof. The first assertion is an easy checking. For the second assertion, consider a semi-linear morphism $\varphi : K \to K$. Define $c = \varphi(1)$. Axiom (9) applied with $x = 1$ shows that $\varphi(\lambda) = c \cdot \theta(\lambda)$ for all $\lambda \in K$. Therefore $\varphi = c\,\theta$. □

Clearly $c\theta$ is bijective if and only if c does not vanish. For $c \in K$, $c \neq 0$, we set $\varepsilon_c = \varepsilon_{c\theta}$. Coming back to the definition, the morphism ε_c is then explicitely given as follows:

$$\begin{array}{rccc} \varepsilon_c : & \mathcal{A} & \longrightarrow & \mathrm{End}_F(K) \\ & \sum_i a_i X^i & \mapsto & \sum_i a_i (c\theta)^i. \end{array} \tag{10}$$

Artin's theorem on linear independance of characters ensures that the kernel of ε_c is the principal ideal generated by $N = Y - \mathrm{N}_{K/F}(c)$. Comparing dimensions, we find that ε_c induces an isomorphism $\mathcal{A}/N\mathcal{A} \simeq \mathrm{End}_F(K)$.

It is interesting to examine how ε_c changes when c varies. It follows from the definition that $\varepsilon_c = \varepsilon_1 \circ \gamma_c$ where γ_c is the morphism defined in §1.2. Slightly more generally, if c_1 and c_2 are two nonzero elements of K, one has $\varepsilon_{c_1} = \varepsilon_{c_2} \circ \gamma_{c_1/c_2}$. If moreover $N_{K/F}(c_1) = N_{K/F}(c_2)$, Hilbert's Theorem 90 asserts that $\frac{c_1}{c_2} = \frac{\theta(u)}{u}$ for some $u \in K$, $u \neq 0$ and an easy calculation shows that:

$$\varepsilon_{c_1}(f)(x) = u^{-1} \cdot \varepsilon_{c_2}(f)(xu)$$

for all $f \in \mathcal{A}$ and $x \in K$. In other words, $\varepsilon_{c_1}(f)$ and $\varepsilon_{c_2}(f)$ are conjugated in $\mathrm{End}_F(K)$ by the multiplication by u.

Zeros of skew polynomials. In the classical commutative setting, it is a quite standard fact that the number of roots of a polynomial cannot exceed its degree. In the skew case, bounds of this type also exist.

Proposition 1.3.4. *For $c \in K$, $c \neq 0$ and $f \in \mathcal{A}^+$, $f \neq 0$, we have $\dim_F \ker \varepsilon_c(f) \leq \deg f$. Equality holds if and only if f divides $Y - \mathrm{N}_{K/F}(c)$ in $\mathcal{A}$.*

Proof. Set $V = \ker \varepsilon_c(f)$ and let I be the left ideal of $\mathrm{End}_F(K)$ consisting of linear functions vanishing on $\ker V$. The inverse image of I by ε_c is an ideal of $\mathcal{A}^+$. Since the latter is a principal ring, there exists $P \in \mathcal{A}^+$ such that $\varepsilon_c^{-1}(I) = K[X;\theta] \cdot P$. Moreover:

$$\begin{aligned} r \cdot \deg P &= \dim_F \big(K[X;\theta]/K[X;\theta]P\big) = \dim_F \big(K[X;\theta]/\varepsilon_c^{-1}(I)\big) \\ &= \dim_F \big(\mathrm{End}_F(K)/I\big) = r \cdot \dim_F V \end{aligned}$$

the third equality coming from the surjectivity of ε_c while the other equalities are easily checked by hand. We deduce that $\deg P = \dim_F V$. Besides, it is obvious that f lies in $\varepsilon_c^{-1}(I)$. Therefore, f has be to a multiple of P, implying that:

$$\deg f \geq \deg P = \dim_F V = \dim_F \ker \varepsilon_c(f). \tag{11}$$

This first part of the proposition is proved.

Noticing that $\varepsilon_c(f) = \varepsilon_c(\mathrm{RGCD}(f, N))$, we see that the inequality (11) can be an equality only if $\deg f = \deg \mathrm{RGCD}(f, N)$, that is f divides N. Conversely, let us assume that f divides N. We can then write $ff' = N$ for some $f' \in \mathcal{A}^+$. Applying (11) for f and f', we find:

$$r \;=\; \dim_F \ker \varepsilon_c(ff') \;\leq\; \dim_F \ker \varepsilon_c(f) \,+\, \dim_F \ker \varepsilon_c(f') \;\leq\; \deg f + \deg f' \;=\; r.$$

All the above inequalities then have to be equalities, showing in particular that $\dim_F \ker \varepsilon_c(f) = \deg f$. □

There is also an analogue of Lagrange's interpolation theory for skew polynomials.

Proposition 1.3.5. *Let $c \in K$, $c \neq 0$. Let V be a F-linear subspace of K. Then there exists a unique monic skew polynomial $P \in \mathcal{A}^+$ such that $\ker \varepsilon_c(P) = V$ and $\deg P = \dim_F V$.*

Moreover, ε_c induces an isomorphism of K-vector spaces:

$$\mathcal{A}^+/\mathcal{A}^+P \xrightarrow{\sim} \mathrm{Hom}_F(V, K), \quad f \mapsto \varepsilon_c(f)_{|V}.$$

Proof. This is immediate after the proof of Proposition 1.3.4. □

Remark 1.3.6. If V is the line generated by $a \in K$, it is easy to check that the skew polynomial P of Proposition 1.3.5 is $P = X - \frac{c\cdot\theta(a)}{a}$. From this observation, we deduce more generally that, if $(a_1, \dots, a_d)$ is a F-basis of V, the skew polynomial P of Proposition 1.3.5 is given explicitely by:

$$P = \operatorname{LLCM}\left(X - \frac{c\cdot\theta(a_1)}{a_1},\, X - \frac{c\cdot\theta(a_2)}{a_2},\, \dots,\, X - \frac{c\cdot\theta(a_m)}{a_m}\right).$$

Propositions 1.3.4 and 1.3.5 admit a straightforward extension to the case of multiple evaluation points.

Proposition 1.3.7. *Let $c_1, \dots, c_m$ be nonzero elements of K such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct.*

(i) For all $f \in \mathcal{A}^+$, $f \neq 0$, we have:

$$\sum_{i=1}^{m} \dim_F \ker \varepsilon_{c_i}(f) \;\leq\; \deg f \tag{12}$$

and equality holds if and only if f divides $\prod_{i=1}^{m}\big(Y - \mathrm{N}_{K/F}(c_i)\big)$.

(ii) Given F-linear subspaces $V_1, \dots, V_m$ of K, there exists a unique monic skew polynomial $P \in \mathcal{A}^+$ such that $\deg P = \dim_F V_1 + \cdots + \dim_F V_m$ and $\varepsilon_{c_i}(P)$ vanishes on V_i for all i. For this particular P, we have an isomorphism:

$$\begin{array}{ccc} \mathcal{A}^+/\mathcal{A}^+P & \xrightarrow{\sim} & \mathrm{Hom}_F(V_1,K) \times \mathrm{Hom}_F(V_2,K) \times \cdots \times \mathrm{Hom}_F(V_m,K) \\ f & \mapsto & \big(\varepsilon_{c_1}(f)_{|V_1},\, \varepsilon_{c_2}(f)_{|V_2},\, \dots,\, \varepsilon_{c_m}(f)_{|V_m}\big). \end{array}$$

Proof. The assumption of the c_i's ensures that the morphism $\varepsilon : \mathcal{A}^+ \to \mathrm{End}_F(K)^m$ taking f to the tuple $(\varepsilon_{c_1}(f), \dots, \varepsilon_{c_m}(f))$ is surjective. Indeed, a skew polynomial f lying in $\ker\varepsilon$ must be a multiple of $Y - \mathrm{N}_{K/F}(c_i)$ for all i. Since these polynomials are pairwise coprime, we deduce that $\ker\varepsilon$ is the principal ideal generated by $\prod_{i=1}^{m}\big(Y - \mathrm{N}_{K/F}(c_i)\big)$. Surjectivity follows by comparing dimensions.

With this input, the proof of the proposition is now absolutely similar to that of Propositions 1.3.4 and 1.3.5. □

1.3.2 Evaluation by Euclidean division

Another option for evaluating skew polynomials is to use Euclidean divisions. Indeed, if P is a usual polynomial, it is well known that $P(a)$ is equal to the reminder of the division of P by the degree 1 polynomial $X - a$ (where X is the variable). Translating this property to the skew context, we introduce the following definition.

Definition 1.3.8. For $f \in \mathcal{A}^+$ and $c \in K$, we define the *evaluation* of f at c, denoted by $\mathrm{ev}_c(f)$, as the remainder of the right Euclidean division of f by $X - c$.

The two types of evaluation we have defined are actually closely related. Indeed, a simple computation shows that:

$$\mathrm{ev}_c(f) = \varepsilon_c(f)(1).$$

It turns out that the value $\mathrm{ev}_c(f)$ has another interesting interpretation in terms of the section operator σ_0 introduced in §1.2. In the next proposition, we denote by $C_{|Y=z}$ the value takes by a polynomial $C \in \mathcal{C}^+ = F[Y]$ at the point $z \in F$.

Proposition 1.3.9. *For $c \in K$ and $f \in \mathcal{A}^+$, we have:*

$$\mathrm{ev}_c(f) = cz^{-1} \cdot \sigma_0(f\, Q_c)_{|Y=z}$$

where $z = \mathrm{N}_{K/F}(c)$ and $Q_c \in \mathcal{A}^+$ is defined by the identity $(X - c)\cdot Q_c = Y - z$.

Proof. A direct computation shows that:

$$Q_c = \sum_{i=1}^{r} \theta^{-1}(c) \cdots \theta^{-i+1}(c) X^{r-i}.$$

By linearity, it is enough to establish the proposition when $f = X^n$. From the formula above, we find:

$$X^n Q_c = \sum_{i=1}^{r} \theta^{n-1}(c) \cdots \theta^{n-i+1}(c) X^{n+r-i}.$$

Only the term corresponding to $i \equiv n \pmod{r}$ contributes to $\sigma_0(X^n Q_c)$. Precisely, if $n = qr + m$ is the Euclidean division of n by r, we obtain:

$$\sigma_0(X^n Q_c) = \theta^{n-1}(c) \cdots \theta^{n-m+1}(c) X^{n+r-m} = \theta(c) \cdots \theta^{m-1}(c) X^{r(q+1)}.$$

Evaluating at $Y = z$, we find:

$$\sigma_0(X^n Q_c)_{|Y=z} = z \cdot \theta(c) \cdots \theta^{n-1}(c) = z c^{-1} \cdot \mathrm{ev}_c(X^n)$$

and the proposition is proved. □

Proposition 1.3.10. *We assume that K is a finite field. For $z \in F$ and $f \in \mathcal{A}^+$, we have:*

$$\sum_{\substack{c \text{ s.t.} \\ \mathrm{N}_{K/F}(c)=z}} \mathrm{ev}_c(f) \;=\; \sigma_0(f)_{|Y=z} \tag{13}$$

Proof. By $\mathcal{C}$-linearity, it is enough to prove the proposition when $f = X^n$ with $0 \leq n < r$. It follows directly from the definition that $\sigma_0(X^n) = 1$ if $n = 0$ and $\sigma_0(X^n) = 0$ if $0 < n < r$. On the other hand, when $f = X^n$, the right hand side of (13) is equal to:

$$s = \sum_{c \in X_z} c \cdot \theta(c) \cdots \theta^{n-1}(c)$$

where X_z denotes the subset of K consisting of elements of norm z. When $n = 0$, $s = \mathrm{Card}\, X_z$. Since the norm map $N_{K/F} : K^\times \to F^\times$ is a surjective group homomorphism, we end up with $s = \frac{\mathrm{Card}\, K - 1}{\mathrm{Card}\, F - 1}$, so $s = 1$ in K. When $0 < n < r$, we choose an element $u \in K$ with $N_{K/F}(u) = 1$ and $u \cdot \theta(u) \cdots \theta^{n-1}(u) \neq 1$. The multiplication by u induces a bijection $X_z \xrightarrow{\sim} X_z$. Hence:

$$s = \sum_{c \in X_z} uc \cdot \theta(uc) \cdots \theta^{n-1}(uc) = u \cdot \theta(u) \cdots \theta^{n-1}(u) \cdot s$$

and then $s = 0$. □

In some special cases, Propositions 1.3.9 and 1.3.10 have a common generalization, providing a nice formula for the sum of $\mathrm{ev}_c(f)$'s for c varying in the set of zeros of another skew polynomial. Precisely, we have the following result.

Proposition 1.3.11. *Let F be a finite field of cardinality q and K be a finite extension extension of F. We endow K with the automorphism $\theta = Frob_q : x \mapsto x^q$.*
Let $z \in F$, $z \neq 0$ and $P \in \mathcal{A}^+$ be a divisor of $Y - z$. For $f \in \mathcal{A}^+$, we have:

$$\sum_{\substack{c \text{ s.t.} \\ \mathrm{ev}_c(P)=0}} \mathrm{ev}_c(f) \;=\; q_0^{-1} \cdot \sigma_0(fQ)_{|Y=z} \tag{14}$$

where $Q \in \mathcal{A}$ is defined by the relation $PQ = N$ and q_0 is the constant coefficient of Q.

An important ingredient of the proof is the next lemma.

Lemma 1.3.12. *We keep the notations and assumptions of Proposition 1.3.11. Let $c_0 \in K$ be such that $\mathrm{N}_{K/F}(c_0) = z$. Then, for all $u \in \operatorname{im} \varepsilon_{c_0}(Q)$, $u \neq 0$, we have:*

$$\frac{1}{u} = \sum_{v \in \varepsilon_{c_0}(Q)^{-1}(u)} \frac{q_0}{v}.$$

Proof. Write $Q = q_0 + q_1 X + \cdots + q_d X^d$ and define the (usual) polynomial:

$$S(x) = -u + q_0 x + q_1 x^q + \cdots + q_d x^{q^d} \in K[x].$$

Coming back to the definitions, we find that the elements of $\varepsilon_{c_0}(Q)^{-1}(u)$ are all roots of S. Moreover, the cardinality of $\varepsilon_{c_0}(Q)^{-1}(u)$ is equal to that of $\ker \varepsilon_{c_0}(Q)$ which is itself equal to q^d by Proposition 1.3.4. Since S has degree q^d, we deduce that the elements of $\varepsilon_{c_0}(Q)^{-1}(u)$ exhaust all the roots of S. The lemma now follows from the standard relations between coefficients and roots of a univariate classical polynomial. □

Proof of Proposition 1.3.11. After Proposition 1.3.10, we may assume safely that $\deg Q > 0$. Let s be the sum in the left hand side of (14). Since P is the divisor of N, any element c such that $\mathrm{ev}_c(P) = 0$ must satisfy $\mathrm{ev}_c(N) = 0$ as well. All such c then have norm z. By Hilbert's Theorem 90, they can all be written under the form $c = c_0 \cdot \frac{\theta(u)}{u}$ for exactly $(q-1)$ values of u. On the other hand $\mathrm{ev}_c(f) = \varepsilon_c(f)(1) = u^{-1} \cdot \varepsilon_{c_0}(f)(u)$ and similarly $\mathrm{ev}_c(P) = u^{-1} \cdot \varepsilon_{c_0}(P)(u)$. Therefore:

$$s = \frac{1}{q-1} \sum_{\substack{u \in \ker \varepsilon_{c_0}(P) \\ u \neq 0}} \frac{\varepsilon_{c_0}(f)(u)}{u} = - \sum_{\substack{u \in \ker \varepsilon_{c_0}(P) \\ u \neq 0}} \frac{\varepsilon_{c_0}(f)(u)}{u}$$

the second equality coming from the fact that $q = 0$ in K. Now observe that the relation $PQ = N$ implies that $\ker \varepsilon_{c_0}(P) \subset \operatorname{im} \varepsilon_{c_0}(Q)$. By Proposition 1.3.4 equality actually holds. Consequently:

$$s = - \sum_{\substack{u \in \operatorname{im} \varepsilon_{c_0}(Q) \\ u \neq 0}} \frac{\varepsilon_{c_0}(f)(u)}{u}.$$

Combining this relation with Lemma 1.3.12, we end up with:

$$s = -q_0^{-1} \sum_{\substack{v \in K \\ v \notin \ker \varepsilon_{c_0}(Q)}} \frac{\varepsilon_{c_0}(fQ)(v)}{v} = -q_0^{-1} \sum_{\substack{v \in K \\ v \neq 0}} \frac{\varepsilon_{c_0}(fQ)(v)}{v}.$$

Applying finally Proposition 1.3.10 with the skew polynomial fQ, we get $s = q_0^{-1} \cdot \sigma_0(fQ)(z)$ as wanted. □

Remark 1.3.13. The assumption on θ in Proposition 1.3.11 cannot be relaxed. As a counter-example, consider the case where K is the finite field with 5^3 elements and $\theta = \mathrm{Frob}_5^2$, *i.e.* $\theta(x) = x^{25}$ for all $x \in K$. Pick $\alpha \in K$ such that $\alpha^3 + 2\alpha + 4 = 0$. We consider the polynomial $N = Y - 1$ and the divisor:

$$P = X^2 + \big(\alpha^2 + 4\alpha + 3\big)X + \big(\alpha^2 + 2\big).$$

The quotient is $Q = X - \alpha$. The following table shows the elements $c \in K$ for which $\mathrm{ev}_c(P) = 0$ and the corresponding values of $\mathrm{ev}_c(X)$ and $\mathrm{ev}_c(X^2)$.

c	$\mathrm{ev}_c(X)$	$\mathrm{ev}_c(X^2)$
$\alpha^2 + 4\alpha + 3$	$\alpha^2 + 4\alpha + 3$	$4\alpha^2 + \alpha + 1$
$4\alpha^2 + 4\alpha + 4$	$4\alpha^2 + 4\alpha + 4$	$3\alpha + 1$
$\alpha^2 + 2$	$\alpha^2 + 2$	$\alpha^2 + 4\alpha + 3$
$\alpha^2 + 2\alpha + 1$	$\alpha^2 + 2\alpha + 1$	$4\alpha^2 + \alpha + 4$
$4\alpha + 4$	$4\alpha + 4$	$4\alpha^2 + 2$
$4\alpha^2 + \alpha + 4$	$4\alpha^2 + \alpha + 4$	$2\alpha^2 + \alpha + 4$

Summing up the entries of the right column of the table, we find that when $f = X$ (resp. $f = X^2$), the left hand side of (14) is equal to $\alpha^2 + 3$ (resp. to 0). On the other hand, the right hand side of (14) is equal to:

$$\begin{aligned} &\text{when } f = X: && -\alpha^{-1} \cdot \sigma_0\big(X^2 + (\alpha^2+3)X\big)_{|Y=1} \;=\; 0 \\ &\text{when } f = X^2: && -\alpha^{-1} \cdot \sigma_0\big(X^3 + (4\alpha^2+\alpha+2)X\big)_{|Y=1} \;=\; -\alpha^{-1} = 4\alpha^2 + 3 \end{aligned}$$

In both cases, the values do not agree.

1.3.3 The Azumaya property

Previously, we have seen that some quotients of $\mathcal{A}$ are isomorphic to $\mathrm{End}_F(K)$ or, equivalently, to some matrix algebras. This phenomenon is the reflection of a more general fact, stating that $\mathcal{A}$ is a Azumaya algebra.

Let us recall briefly that an algebra is said *Azumaya* if it becomes isomorphic to a matrix algebra after a suitable étale extension of its center. The fact that $\mathcal{A}$ is Azumaya was first observed by Ikehata in [9, 10] and then reproved by Caruso and Le Borgne in [3]. Below, we give another proof, giving in addition an explicit trivialization of $\mathcal{A}$.

Theorem 1.3.14. *We have an isomorphism of $\mathcal{C}$-algebras:*

$$\begin{array}{rccc} \alpha: & \mathcal{C} \otimes_{\mathcal{Z}} \mathcal{A} & \xrightarrow{\sim} & \mathrm{End}_{\mathcal{C}}(\mathcal{A}) \\ & C \otimes f & \mapsto & (x \mapsto Cxf). \end{array}$$

In particular, $\mathcal{A}$ is Azumaya over $\mathcal{Z}$.

Proof. It is routine to check that α preserves the structure of $\mathcal{C}$-algebra. Moreover, the domain and the codomain of α are both finite free $\mathcal{C}$-modules of rank r^2. It is then enough to check that α is surjective.

We endow $\mathcal{A}$ with its canonical $\mathcal{C}$-basis $(1, X, X^2, \dots, X^{r-1})$. This choice defines an isomorphism between $\mathrm{End}_{\mathcal{C}}(\mathcal{A})$ and the matrix algebra $M_r(\mathcal{C})$. Under this identification the pure tensor $C \otimes f \in \mathcal{C} \otimes_{\mathcal{Z}} \mathcal{Z}$ is mapped to the matrix M whose (i,j) entry is:

$$m_{i,j} = C \cdot \sigma_i(X^j f) = C \cdot \theta^j\big(\sigma_{i-j}(f)\big).$$

In particular, if C and C' lie in $\mathcal{C}$, α takes $C \otimes C'$ to the diagonal matrix whose successive entries are $C \cdot \theta^j(C')$, j varying from 0 to $r-1$. Since $\mathcal{C}/\mathcal{Z}$ is a cyclic Galois covering of degree r, we know that the mapping:

$$\mathcal{C} \otimes_{\mathcal{Z}} \mathcal{C} \to \mathcal{C}^r, \quad C \otimes C' \to C \cdot \big(\theta^j(C')\big)_{0 \le j < r}$$

is an isomorphism. Therefore the image of α contains all the diagonal matrices. Moreover a simple computation shows that $1 \otimes X$ is mapped to the following matrix:

$$\begin{pmatrix} & & & Y \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{pmatrix}.$$

The latter matrix, together with the subspace of diagonal matrices, generate $M_r(\mathcal{C})$. Hence α is surjective and the theorem is proved. □

The Azumaya property has several interesting consequences. First, it leads to the definition of three important maps:

- the *reduced trace* $\mathrm{T}_{\mathrm{rd}} : \mathcal{A} \to \mathcal{Z}$,
- the *reduced norm* $\mathrm{N}_{\mathrm{rd}} : \mathcal{A} \to \mathcal{Z}$, and
- the *adjoint* $\mathrm{adj} : \mathcal{A} \to \mathcal{A}$

which corresponds respectively to the usual trace, the determinant and the adjoint[2] at the level of matrices. The usual matrix relation $M \cdot \mathrm{adj}(M) = \mathrm{adj}(M) \cdot M = \det M$ immediately translates to:

$$f \cdot \mathrm{adj}(f) \;=\; \mathrm{adj}(f) \cdot f \;=\; \mathrm{N}_{\mathrm{rd}}(f)$$

for all $f \in \mathcal{A}$. This shows that $\mathrm{N}_{\mathrm{rd}}(f)$ is a left and a right multiple of f, reproving in particular Lemma 1.1.5. Similarly, the classical matrix formula $\mathrm{Tr}(MN) = \mathrm{Tr}(NM)$ translates to the relation $\mathrm{T}_{\mathrm{rd}}(fg) = \mathrm{T}_{\mathrm{rd}}(gf)$, which holds true for $f, g \in \mathcal{A}$.

Coming back to the definition, one checks that the reduced trace admits the following simple expression:

$$\mathrm{T}_{\mathrm{rd}}\Big(\sum_i a_i X^i\Big) = \sum_i \mathrm{Tr}_{K/F}(a_{ri})\, Y^i.$$

In short, $\mathrm{T}_{\mathrm{rd}} = \mathrm{Tr}_{\mathcal{C}/\mathcal{Z}} \circ \sigma_0$. In a similar fashion, one can show also that $\mathrm{T}_{\mathrm{rd}} = \mathrm{Tr}_{\mathcal{A}/\mathcal{C}}$. A similar formula exists for the reduced norm, namely $\mathrm{N}_{\mathrm{rd}} = \mathrm{N}_{\mathcal{A}/\mathcal{C}}$. However, there is no simple explicit expression for the reduced form, beyond the case of degree 1 skew polynomials for which we have:

$$\mathrm{N}_{\mathrm{rd}}(X - c) = (-1)^r \cdot \big(Y - \mathrm{N}_{K/F}(c)\big).$$

Finally, for a general f, we always have $\deg \mathrm{N}_{\mathrm{rd}}(f) = r \cdot \deg f$.

A second interesting corollary of the Azumaya property is the following statement: given an irreducible polynomial $N \in \mathcal{Z}^+$ with nonzero constant term, the quotient $\mathcal{A}/N\mathcal{A}$ is a simple central algebra over the field $\mathcal{Z}/N\mathcal{Z}$. By classical theorems of structure, one deduces that $\mathcal{A}/N\mathcal{A} \simeq M_s(E)$ where s is an integer and E is a skew field with center $\mathcal{Z}/N\mathcal{Z}$. Comparing dimension, we get the relation:

$$r^2 = s^2 \cdot [E : \mathcal{Z}/N\mathcal{Z}].$$

The integer s can be characterized by the factorisation of N in $\mathcal{A}$: if P is an irreducible factor of N in $\mathcal{A}^+$, then $s = \frac{\deg N}{\deg P}$. In this case, every irreducible factor of N has degree $\frac{\deg N}{s}$.

In the particular case where N has Y-degree 1, say $N = Y - z$, the above characterization indicates that $\mathcal{A}/N\mathcal{A}$ is isomorphic to $M_r(F)$ if and only if N has a factor P of degree 1. When this occurs, the central polynomials N and $\mathrm{N}_{\mathrm{rd}}(P)$ have a non trivial gcd (since they both admit P as a right divisor) and, therefore, have to coincide up to multiplication by a scalar. If $P = c_0 + c_1 X$, we derive that $z = \mathrm{N}_{K/F}(c)$ with $c = -\frac{c_0}{c_1}$. The abstract isomomorphism $\mathcal{A}/N\mathcal{A} \simeq M_r(F)$ is then concretely realized by evaluation morphism ε_c (after a choice of a F-basis of K). Another consequence of the above discussion is that $\mathcal{A}/N\mathcal{A}$ is isomorphic to $M_r(F)$ if and only if z is a norm in the extension K/F (compare with Proposition 1.2.7).

Proposition 1.3.15. *For $c \in K$, $c \neq 0$ and $f \in \mathcal{A}$, we have:*

$$\mathrm{Tr}\big(\varepsilon_c(f)\big) = \mathrm{T}_{\mathrm{rd}}(f)_{|Y = \mathrm{N}_{K/F}(c)}$$
$$\textit{and} \quad \det\big(\varepsilon_c(f)\big) = \mathrm{N}_{\mathrm{rd}}(f)_{|Y = \mathrm{N}_{K/F}(c)}.$$

Proof. Set $N = Y - \mathrm{N}_{K/F}(c)$. We know that the evaluation map ε_c induces an isomorphism of K-algebras $\varphi : \mathcal{A}/N\mathcal{A} \simeq \mathrm{End}_F(K)$. Besides, it follows from Noether–Skolem theorem that any isomorphism between simple central algebras automatically commutes with the reduced trace and the reduced norm. The proposition follows by applying this result to φ. □

1.4 Duality

One can define a duality on skew polynomials by the following explicit formula:

$$\Big(\sum_i a_i X^i\Big)^\star = \sum_i X^{-i} a_i = \sum_i \theta^{-i}(a_i) X^{-i} = \sum_i \theta^i(a_{-i}) X^i.$$

The mapping $f \mapsto f^\star$ is an involutive morphism of rings $\mathcal{A}^{\mathrm{op}} \to \mathcal{A}$ where $\mathcal{A}^{\mathrm{op}}$ stands for the opposite ring[3] of $\mathcal{A}$. We notice that the construction $f \mapsto f^\star$ commutes with the section operator σ_0 and, hence, with the reduced trace. More generally, for $j \in \mathbb{Z}$ and $f \in \mathcal{A}$, we have the relation $\sigma_j(f^\star) = \theta^j\big(\sigma_{-j}(f)^\star\big)$.

[2] We recall that the adjoint of a matrix is, by definition, the transpose of this comatrix.

[3] Given a ring $(\mathfrak{A}, +, \times)$, its oppositve ring is $(\mathfrak{A}, +, @)$ where the multiplication $@$ is defined by $x @ y = y \times x$ for $x, y \in \mathfrak{A}$.

Duality on general rings. In order to study further Ore's duality, it will be convenient to introduce a general framework for duality on rings. It is materialized by the following definition.

Definition 1.4.1. Let $\mathfrak{A}$ be a ring. A *$\star$-structure* on a ring $\mathfrak{A}$ is a ring homomorphism $\mathfrak{A}^{\mathrm{op}} \mapsto \mathfrak{A}$, $x \mapsto x^\star$ such that $x^{\star\star} = x$ for all $x \in \mathfrak{A}$.
A ring equipped with a $\star$-structure is called a *$\star$-algebra*.

Let $\mathfrak{A}$ be a $\star$-algebra with centre $\mathfrak{Z}$. One immediately checks that $z \in \mathfrak{Z}$ if and only if $z^\star \in \mathfrak{Z}$. In other words, the mapping $x \mapsto x^\star$ induces an involutive ring automorphism of $\mathfrak{Z}$, that is a $\star$-structure on $\mathfrak{Z}$. When $z \in \mathfrak{Z}$, we shall often write $\bar{z}$ for $z^\star$.

The case of matrix algebras is particularly interesting for us for two reasons: first, Theorem 1.3.14 shows that it is closely related to skew polynomial rings and, second, general theorems of structure allow for a complete classification on $\star$-structures on matrix algebras over a commutative field.

We fix a *commutative* ring $\mathfrak{Z}$ and set $\mathfrak{A} = M_n(\mathfrak{Z})$ for some fixed positive integer n. On $\mathfrak{A}$, we can define several $\star$-structures:

(i) *(symmetric case)* $M^\star = {}^{\mathrm{t}}M$,

(ii) *(symplectic case)* $M^\star = -{}^{\mathrm{t}}M$,

(iii) *(sesquilinear case)* $M^\star = {}^{\mathrm{t}}\bar{M}$ where $z \mapsto \bar{z}$ is an involutive ring automorphism of $\mathfrak{Z}$.

Theorem 1.4.2. *Let $\mathfrak{Z}$ be a commutative field and n be a positive integer. Let $M \mapsto M^\star$ be a $\star$-structure on $\mathfrak{A} = M_n(\mathfrak{Z})$. If the $\star$-structure induced on $\mathfrak{Z}$ (which is the centre of $\mathfrak{A}$) is the identity, then there exist $P \in \mathrm{GL}_n(\mathfrak{Z})$ such that ${}^{\mathrm{t}}P = \pm P$ and*

$$\forall M \in \mathfrak{A}, \quad M^\star = P \cdot {}^{\mathrm{t}}M \cdot P^{-1}$$

Otherwise, there exists $P \in \mathrm{GL}_n(\mathfrak{Z})$ such that ${}^{\mathrm{t}}P = \bar{P}$ and

$$\forall M \in \mathfrak{A}, \quad M^\star = P \cdot {}^{\mathrm{t}}\bar{M} \cdot P^{-1}.$$

Proof. Consider the ring homomorphism $\varphi : M_n(\mathfrak{Z}) \to M_n(\mathfrak{Z})$ taking M to ${}^{\mathrm{t}}\bar{M}^\star$. By Skolem–Noether Theorem, we know that φ is inner: there exists an invertible matrix $P \in \mathrm{GL}_n(Z)$ such that $\varphi(M) = PMP^{-1}$, *i.e.*

$$M^\star = P \cdot {}^{\mathrm{t}}\bar{M} \cdot P^{-1} \tag{15}$$

for all $M \in M_n(\mathfrak{Z})$. Writing down the condition $M^{\star\star} = M$, we find that ${}^{\mathrm{t}}\bar{P} \cdot P^{-1}$ must be a central element, *i.e.* must lie in $\mathfrak{Z}$. In other words, there exists a scalar $z \in \mathfrak{Z}$ such that ${}^{\mathrm{t}}P = z\bar{P}$. The latter equality implies moreover the norm equation $z\bar{z} = 1$.

If the $\star$-structure acts on $\mathfrak{Z}$ as the identity, the norm equation reduces to $z^2 = 1$, so that $z = \pm 1$ as claimed. Otherwise, by Hilbert's Theorem 90, the norm equation implies the existence of an element $u \in \mathfrak{Z}$ with the property that $z = \bar{u}/u$. Replacing P by uP, we then get ${}^{\mathrm{t}}P = \bar{P}$ without altering the validity of Eq. (15). □

Remark 1.4.3. Theorem 1.4.2 can be rephrased as follows: any $\star$-structure on $M_n(\mathfrak{Z})$ is the adjoint for a symmetric, symplectic or sesquilinear form on $\mathfrak{Z}^n$.

Duality and evaluation maps. We go back to the setting of skew polynomials. Under the isomorphism of Theorem 1.3.14, the Ore's $\star$-structure on $\mathcal{A}$ we defined above translates to the $\star$-structure on $M_r(\mathcal{C})$. Since $\mathcal{C}$ is not a field, we cannot directly apply Theorem 1.4.2. However, a direct computation shows that the $\star$-structure we get on $M_r(\mathcal{C})$ is simply $M \mapsto {}^{\mathrm{t}}\bar{M}$ where $\bar{M}$ is the matrix deduced from M by applying the transformation $Z(X) \mapsto Z(X^{-1})$ on each coefficient.

Beyond this observation, it is also interesting to analyze how Ore's $\star$-structure on $\mathcal{A}$ behaves under the isomorphisms ε_c's. Let c be a nonzero element of K. Set $z = \mathrm{N}_{K/F}(c)$ and $N = Y - z$, so that we have an identification:

$$\varepsilon_c : \mathcal{A}/N\mathcal{A} \xrightarrow{\sim} \mathrm{End}_F(K).$$

Similarly, observing that $\bar{N} = Y^{-1} - z = -zY^{-1} \cdot (Y - z^{-1})$ and $\mathrm{N}_{K/F}(c^{-1}) = z^{-1}$, we have a second identification

$$\varepsilon_{c^{-1}} : \mathcal{A}/\bar{N}\mathcal{A} \xrightarrow{\sim} \mathrm{End}_F(K).$$

The $\star$-structure on $\mathcal{A}$ then induces a $\star$-structure on $\mathrm{End}_F(K)$ *via*

$$\mathrm{End}_F(K) \xrightarrow{\varepsilon_c^{-1}} \mathcal{A}/N\mathcal{A} \xrightarrow{f \mapsto f^\star} \mathcal{A}/\bar{N}\mathcal{A} \xrightarrow{\varepsilon_{c^{-1}}} \mathrm{End}_F(K)\ .$$

Since this $\star$-structure acts as the identity on F, Theorem 1.4.2 shows that it must be the adjoint for a symmetric or symplectic F-bilinear form on K. In our setting, it is possible to make this explicit.

Proposition 1.4.4. *The $\star$-structure on $\mathrm{End}_K(F)$ defined above is the adjoint for the symmetric F-bilinear form on K:*

$$\langle x, y \rangle_K = \mathrm{Tr}_{K/F}(xy) \qquad (x, y \in K).$$

Proof. We have to show that:

$$\langle \varepsilon_c(f)(x), y \rangle_K = \langle x, \varepsilon_{c^{-1}}(f^\star)(y) \rangle_K \tag{16}$$

for all $f \in \mathcal{A}$ and $x, y \in K$. By linearity it is enough to check this formula when $f = aX^n$ with $a \in K$ and $n \in \mathbb{Z}$. A simple computation shows that the left hand side is equal to $\mathrm{Tr}_{K/F}(c)$ with $c = a \cdot c \cdot \theta(c) \cdots \theta^{n-1}(c) \cdot \theta^n(x) \cdot y$. On the other hand, we have $(aX^n)^\star = \theta^{-n}(a)X^{-n}$, so that:

$$\varepsilon_{c^{-1}}\big((aX^n)^\star\big) = \theta^{-n}(a)(c^{-1}\theta)^{-n} = \theta^{-n}(a) \cdot \theta^{-1}(c) \cdots \theta^{-n}(c) \cdot \theta^{-n}.$$

Consequently the right hand side of (16) is equal to:

$$\mathrm{Tr}_{K/F}\big(\theta^{-n}(a) \cdot \theta^{-1}(c) \cdots \theta^{-n}(c) \cdot x \cdot \theta^{-n}(y)\big) = \mathrm{Tr}_{K/F}(\theta^{-n}(c)) = \mathrm{Tr}_{K/F}(c)$$

and Eq. (16) is proved. □

2 Analysis with skew polynomials

The section constitutes a first attempt to do analysis with skew polynomials. After studying derivations (in §2.1) and Taylor expansions (in §2.2) of skew polynomials, we develop in §2.3 a theory of residues for skew rational functions, extending along the way several classical formulas (as the residue formula, or the substitution formula) to the noncommutative setting.

2.1 Derivations

Given a (possibly noncommutative) ring $\mathfrak{A}$ and a $\mathfrak{A}$-algebra $\mathfrak{B}$, we recall that a *derivation* $\partial : \mathfrak{A} \to \mathfrak{B}$ is an additive mapping satisfying the Leibitz rule:

$$\partial(xy) = \partial(x)y + x\partial(y) \quad (x, y \in \mathfrak{A}).$$

One checks that the subset $\mathfrak{C} \subset \mathfrak{A}$ consisting of elements x with $\partial(x) = 0$ is actually a subring de $\mathfrak{A}$. It is called the *ring of constants*. A derivation $\partial : \mathfrak{A} \to \mathfrak{B}$ with ring of constants $\mathfrak{C}$ is $\mathfrak{C}$-linear.

As we classified endomorphisms of K-algebras in §1.2, it is possible to classify K-linear derivations over Ore rings. For $C \in \mathrm{Frac}(\mathcal{C})$, and $n \in \mathbb{Z}$, we define:

$$\begin{aligned} \mathrm{Tr}_n(C) &= C + \theta(C) + \cdots + \theta^{n-1}(C) && \text{if } n \geq 0 \\ &= -\theta^{-1}(C) - \theta^{-2}(C) - \cdots - \theta^n(C) && \text{if } n < 0 \end{aligned}$$

We observe that Tr_r is the trace from $\mathrm{Frac}(\mathcal{C})$ to $\mathrm{Frac}(\mathcal{Z})$. In particular, it takes its values in $\mathrm{Frac}(\mathcal{Z})$.

Proposition 2.1.1. *Let $\partial : \mathcal{A}^+ \to \mathcal{A}^+$ (resp. $\partial : \mathcal{A} \to \mathcal{A}$, resp. $\partial : \mathrm{Frac}(\mathcal{A}) \to \mathrm{Frac}(\mathcal{A})$) be a K-linear derivation,* i.e. *a derivation whose ring of constants contains K. Then, there exists a uniquely determined $C \in \mathcal{C}^+$ (resp. $C \in \mathcal{C}$, resp. $C \in \mathrm{Frac}(\mathcal{C})$) such that:*

$$\partial\Big(\sum_i a_i X^i\Big) = \sum_i a_i \mathrm{Tr}_i(C) X^i. \tag{17}$$

Conversely, any such C gives rise to a unique derivation of $\mathcal{A}^+$ (resp. $\mathcal{A}$, resp. $\mathrm{Frac}(\mathcal{A})$).

Proof. Unicity is clear since $C = \partial(X)X^{-1}$.

Let ∂ be a K-linear derivation as in the proposition. Applying ∂ to the equality $Xa = \theta(a)X$ ($a \in K$), we get $\partial(X)\cdot a = \theta(a)\cdot\partial(X)$. Writing $\partial(X) = \sum_i c_i X^i$, we deduce $c_i\theta^i(a) = c_i\theta(a)$ for all index i, showing that c_i has to vanish when $i \not\equiv 1 \pmod r$. Thus $\partial(X) = CX$ for some $C \in \mathcal{C}^+$ (resp. $C \in \mathcal{C}$). A direct computation then shows that:

$$\partial(X^2) = X\cdot\partial(X) + \partial(X)\cdot X = XCX + CX^2 = \big(C + \theta(C)\big)X^2 = \mathrm{Tr}_2(C)X^2$$

and, more generally, an easy induction leads to $\partial(X^i) = \mathrm{Tr}_i(C)X^i$ for all $i \geq 0$. In the cases of $\mathcal{A}$ and $\mathrm{Frac}(\mathcal{A})$, we can also compute $\partial(X^i)$ when i is negative. For this, we write:

$$0 = \partial(1) = \partial(X^{-1}X) = \partial(X^{-1})X + X^{-1}CX$$

from what we deduce that $\partial(X^{-1}) = -X^{-1}C = -\theta^{-1}(C)X^{-1} = \mathrm{Tr}_{-1}(C)X^{-1}$. As before, an easy induction on i then gives $\partial(X^i) = \mathrm{Tr}_i(C)\, X^i$ for all negative i. We deduce that Eq. (17) holds.

For the converse, we first check that Eq. (17) defines a derivation on $\mathcal{A}$. In the case of $\mathrm{Frac}(\mathcal{A})$, we need to justify in addition that ∂ (given by Eq. (17)) extends uniquely to $\mathrm{Frac}(\mathcal{A})$. This is a consequence of the following formula:

$$\partial\left(\frac{f}{D}\right) = \frac{\partial(f)\, D \,+\, f\, \partial(D)}{D^2} \qquad (f \in \mathcal{A},\, D \in \mathcal{Z})$$

which holds true because D is central. □

Let $\partial_C : \mathrm{Frac}(\mathcal{A}) \to \mathrm{Frac}(\mathcal{A})$ denote the derivation of Proposition 2.1.1. We have:

$$\partial_C(Y) = \mathrm{Tr}_r(C)\cdot Y = \mathrm{Tr}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C)\cdot Y \in \mathrm{Frac}(\mathcal{Z}).$$

We deduce that ∂_C stablizes $\mathrm{Frac}(\mathcal{C})$ and $\mathrm{Frac}(\mathcal{Z})$ and acts on there rings as the derivation $\mathrm{Tr}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C)\cdot Y\cdot\frac{d}{dY}$.

Proposition 2.1.2. *For $C \in \mathrm{Frac}(\mathcal{C})$, the following assertions are equivalent:*

(i) ∂_C is $\mathcal{C}$-linear,

(ii) $\mathrm{Tr}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C) = 0$,

(iii) there exists $U \in \mathrm{Frac}(\mathcal{C})$ such that $\partial_C(f) = fU - Uf$ for all $f \in \mathrm{Frac}(\mathcal{A})$.

Proof. The equivalence between (i) and (ii) is clear by what we have seen before. If (ii) holds, then the additive version of Hilbert's Theorem 90 ensures that C can be written as $\theta(U) - U$ with $U \in \mathrm{Frac}(\mathcal{C})$. Then $\partial_C(X^i) = \mathrm{Tr}_i(\theta(U) - U)X^i = \theta^i(U)X^i - UX^i = X^iU - UX^i$ for all integer i. By K-linearity, we deduce that $\partial_C(f) = fU - Uf$ for all $f \in \mathcal{A}$, implying (iii). Finally, if (iii) holds, ∂_C clearly vanishes on $\mathcal{C}$, implying (i). □

Extensions of the canonical derivation $\frac{d}{dY}$. An important case of interest occurs when $\mathrm{Tr}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C) = Y^{-1}$, as ∂_C then induces the standard derivation $\frac{d}{dY}$ on $\mathrm{Frac}(\mathcal{C})$. When p does not divide r, a distinguished element C satisfying the above condition is $C = r^{-1}Y^{-1}$.

Definition 2.1.3. When p does not divide r, we set $\partial_{Y,\mathrm{can}} = \partial_{r^{-1}Y^{-1}}$. Explicitely:

$$\partial_{Y,\mathrm{can}}\Big(\sum_i a_i X^i\Big) = r^{-1}\cdot\sum_i i a_i X^{i-r}.$$

Another interesting feature of the derivation $\partial_{Y,\mathrm{can}}$ is that its p-th power vanishes (as we can check easily by hand). This property will be very pleasant for us in §2.2 when we will define Taylor expansions of skew polynomials. Unfortunately, it seems that there is no simple analogue of $\partial_{Y,\mathrm{can}}$ when p divides r, as shown by the following proposition.

Proposition 2.1.4. *Let $C \in \mathrm{Frac}(\mathcal{C})$ with $\mathrm{Tr}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C) = Y^{-1}$ and $\partial_C^p = 0$. Then p does not divide r.*

Proof. Our assumptions ensure that ∂_C induces the derivation $\frac{d}{dY}$ on $\mathrm{Frac}(\mathcal{C})$. For $i \in \{1, 2, \ldots, p\}$, we define $C_i = \partial_C^i(X)\, X^{-1}$. A direct computation shows that:

$$C_1 = C \quad ; \quad C_{i+1} = \frac{dC_i}{dY} + C_i\, C. \tag{18}$$

In particular, we deduce that $C_i \in \mathrm{Frac}(\mathcal{C})$ for all i. Assume by contradiction that C has a pole of order $v \geq 2$ at 0. By induction, this would imply that C_i has a pole of order vi at 0 for $i \in \{1, \ldots, p\}$, contradicting the fact that C_p vanishes. Consequently, C has at most a simple pole at 0. Write $C = aY^{-1} + O(1)$ with $a \in K$. The recurrence relation (18) shows that, for $i \in \{1, \ldots, p\}$, we have $C_i = a_i Y^{-i} + O(Y^{-i+1})$ where the coefficients a_i's satisfy:

$$a_1 = a \quad ; \quad a_{i+1} = -ia_i + a_i a = a_i \cdot (a - i)$$

Hence $a_p = a \cdot (a-1) \cdots (a-(p-1)) = a^p - a$. In order to guarantee that a_p vanishes, we then need $a \in \mathbb{F}_p \subset F$. Taking the trace, we obtain $\mathrm{Tr}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C) = ra\, Y^{-1} + O(1)$. Thus $ra = 1$ in F and p cannot divide r. □

Remark 2.1.5. With the notation of the proof above, C_p is the function by which the p-curvature of the linear differential equation $y' = Cy$ acts. With this reinterpretation, one can use Jacobson identity (see Lemma 1.4.2 of [27]) to get a closed formula for C_p, which reads:

$$C_p = \frac{d^{p-1}C}{dY^{p-1}} + C^p.$$

Derivations over quotients of Ore rings. Following §1.2, we propose to classify K-linear derivations $\mathcal{A}/N_1\mathcal{A} \to \mathcal{A}/N_2\mathcal{A}$. However, we need to pay attention in this case that such derivations are only defined when $\mathcal{A}/N_2\mathcal{A}$ is an algebra over $\mathcal{A}/N_1\mathcal{A}$, that is when N_1 divides N_2.

As in §1.2, we consider in addition a commutative $\mathcal{Z}$-algebra $\mathcal{Z}'$. We extend readily the definition of ∂_C to an element $C \in \mathcal{Z}' \otimes_{\mathcal{Z}} \mathrm{Frac}(\mathcal{A})$.

Proposition 2.1.6. *Let $N_1, N_2 \in \mathcal{Z}^+$ be two nonconstant polynomials with nonzero constant terms. We assume that N_1 divides N_2. Let $\mathcal{Z}'$ be a commutative $\mathcal{Z}$-algebra.*

Let $\partial : \mathcal{A}/N_1\mathcal{A} \to \mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{A}/N_2\mathcal{A}$ be K-linear derivation. Then $\partial = \partial_C \mod N_2$ for some element $C \in \mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{C}$ with the property that N_2 divides $\partial_C(N_1)$. Such an element C is uniquely determined modulo N_2.

Moreover, the following assertions are equivalent:

(i) ∂ is a $\mathcal{C}$-linear

(ii) $\mathrm{Tr}_{\mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{C}/\mathcal{Z}'}(C) \equiv 0 \pmod{N_2}$.

(iii) there exists $U \in \mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{C}/N_2\mathcal{C}$ such that $\partial(f) = fU - Uf$ for all $f \in \mathcal{A}/N_1\mathcal{A}$.

Proof. It is entirely similar to the proofs of Propositions 2.1.1 and 2.1.2. □

2.2 Taylor expansions

The aim of this subsection is to show that skew polynomials admit Taylor expansion around any closed point of F and to study its properties. Especially, when r is coprime to p, we will prove that the Taylor expansion is canonical are given by a Taylor-like series involving the successive divided powers of the derivation ∂_{can}.

2.2.1 The commutative case: reminders

By definition, we recall that the *Taylor expansion* of a Laurent polynomial $f \in \mathcal{C}$ around a point $c \in K$, $c \neq 0$ is the series:

$$\sum_{n=0}^{\infty} f^{[n]}(c)\, T^n \tag{19}$$

where T is a formal variable playing the role of $Y+c$ and the notation $f^{[n]}$ stands for the n-th divided derivative of f defined by:

$$\Big(\sum_i a_i Y^i\Big)^{[n]} = \sum_i \binom{i}{n} \cdot a_i\, Y^{i-n} \qquad (a_i \in K).$$

The n-th divided derivative satisfies the following Leibniz-type relation:

$$(fg)^{[n]} = \sum_{m=0}^{n} f^{[m]} g^{[n-m]} \qquad (f, g \in \mathcal{C}^+)$$

for what we deduce that the mapping $\mathcal{C} \to K[[T]]$ taking a Laurent polynomial to its Taylor expansion is a homomorphism of K-algebras. Moreover, it induces an isomorphism:

$$\tau_c^{\mathcal{C}} : \varprojlim_{m>0} \mathcal{C}/(Y-c)^m\, \mathcal{C} \;\simeq\; K[[T]].$$

More generally, let $N \in \mathcal{C}$ be an irreducible separable polynomial. Let also $c \in \mathcal{C}/N\mathcal{C}$ be the image of X; by construction, it is a root of N. The Taylor expansion around c defines a homomorphism of K-algebras $\mathcal{C} \to (\mathcal{C}/N\mathcal{C})[[T]]$, inducing itself an isomorphism:

$$\tau_c^{\mathcal{C}} : \varprojlim_{m>0} \mathcal{C}/N^m\mathcal{C} \;\simeq\; (\mathcal{C}/N\mathcal{C})[[T]].$$

The image of N under this isomorphism is a series of valuation 1. As a consequence, twisting by an automorphism of $(\mathcal{C}/N\mathcal{C})[[T]]$, there exists an isomorphism of K-algebras:

$$\tau_N^{\mathcal{C}} : \varprojlim_{m>0} \mathcal{C}/N^m\mathcal{C} \;\simeq\; (\mathcal{C}/N\mathcal{C})[[T]]$$

mapping N to T and inducing the identity map $\mathcal{C}/N\mathcal{C} \to \mathcal{C}/N\mathcal{C}$ after reduction modulo N on the left and modulo T on the right. Moreover $\tau_N^{\mathcal{C}}$ is uniquely determined by these properties. In addition, we observe that when $N = Y-c$ is a polynomial of degree 1, the isomorphisms $\tau_{Y-c}^{\mathcal{C}}$ and $\tau_c^{\mathcal{C}}$ agree.

It turns out that the existence of the unicity of $\tau_N^{\mathcal{C}}$ continues to hold under the sole assumption that N is separable; this can be proved by noticing that N factors as a product of *distinct* irreducible factors $N_1 \cdots N_m$ and, then, by gluing the corresponding $\tau_{N_i}^{\mathcal{C}}$ using the Chinese Reminder Theorem. In this general setting, the inverse of $\tau_N^{\mathcal{C}}$ can be easily described: it maps T to N and $X \in \mathcal{C}/N\mathcal{C}$ to the unique root of N in $\varprojlim_{m>0} \mathcal{C}/N^m\mathcal{C}$ which is congruent to X modulo N. The existence and the unicity of this root follows from Hensel's Lemma thanks to our assumption that N is separable: it can be obtained as the limit of the Newton iterative sequence:

$$X_0 = X, \qquad X_{i+1} = X_i - \frac{N(X_i)}{N'(X_i)}.$$

Of course, the above discussion is still valid when $\mathcal{C}$ is replaced by $\mathcal{Z}$ (and K is replaced by F accordingly). For any separable polynomial $F \in \mathcal{Z}$, we then have constructed a well defined isomorphism:

$$\tau_N^{\mathcal{Z}} : \varprojlim_{m>0} \mathcal{Z}/N^m\mathcal{Z} \;\simeq\; (\mathcal{Z}/N\mathcal{Z})[[T]]$$

We note that N remains separable in $\mathcal{C}$, implying that $\tau_N^{\mathcal{C}}$ is also defined. The unicity property ensures moreover that the following diagram is commutative:

$$\begin{array}{ccc} \varprojlim_{m>0} \mathcal{C}/N^m\mathcal{C} & \xrightarrow{\tau_N^{\mathcal{C}}} & (\mathcal{C}/N\mathcal{C})[[T]] \\ \uparrow & & \uparrow \\ \varprojlim_{m>0} \mathcal{Z}/N^m\mathcal{Z} & \xrightarrow{\tau_N^{\mathcal{Z}}} & (\mathcal{Z}/N\mathcal{Z})[[T]] \end{array} \tag{20}$$

where the vertical arrows are the canonical inclusions.

2.2.2 A Taylor-like isomorphism for skew polynomials

We now aim at completing the diagram (20) by adding a top row at the level of Ore rings. For now on, we fix a separable polynomial $N \in \mathcal{Z}$. To simplify notations, we set:

$$\hat{\mathcal{A}}_N = \varprojlim_{m\geq 1} \mathcal{A}/N^m\mathcal{A} \quad ; \quad \hat{\mathcal{C}}_N = \varprojlim_{m\geq 1} \mathcal{C}/N^m\mathcal{C} \quad ; \quad \hat{\mathcal{Z}}_N = \varprojlim_{m\geq 1} \mathcal{Z}/N^m\mathcal{Z}.$$

Here is our first theorem.

Theorem 2.2.1. *(i) There exists an isomorphism of K-algebras $\tau_N : \hat{\mathcal{A}}_N \xrightarrow{\sim} (\mathcal{A}/N\mathcal{A})[[T]]$ mapping N to T and inducing the identity of $\mathcal{A}/N\mathcal{A}$ after quotienting out by N of the left and T and the right.*

(ii) Any isomomorphism τ_N satisfying the conditions of (i) sits in the following commutative diagram:

$$\begin{array}{ccc} \hat{\mathcal{A}}_N & \xrightarrow{\tau_N} & (\mathcal{A}/N\mathcal{A})[[T]] \\ \uparrow & & \uparrow \\ \hat{\mathcal{C}}_N & \xrightarrow{\tau_N^{\mathcal{C}}} & (\mathcal{C}/N\mathcal{C})[[T]] \end{array} \tag{21}$$

Remark 2.2.2. If N is an irreducible polynomial in $\mathcal{Z}$, the polynomials $aX^{nr}N$ (with $a \in F$ and $n \in \mathbb{Z}$) are also irreducible in $\mathcal{Z}$ and they all generate the same ideal. If τ_N satisfies the conditions of Theorem 2.2.1, then a suitable choice for $\tau_{aX^{nr}N}$ is $\iota \circ \tau_N$ where ι is the automorphism of $(\mathcal{A}/N\mathcal{A})[[T]]$ taking T to $aX^{nr}T$.

In what follows, we shall say that a Laurent polynomial $N \in \mathcal{Z}$ is *normalized* if $N \in \mathcal{Z}^+$, N is monic and N has a nonzero constant coefficient. With this definition, any ideal of $\mathcal{Z}$ has a unique normalized generator.

Proof of Theorem 2.2.1. The general strategy of the proof is inspired by the caracterization of the inverse of τ_N we gave earlier: we are going to construct the inverse of τ_N by finding a root of N is $\hat{\mathcal{A}}_N$. Without loss of generality, we may assume that N is normalized. Write $N = a_0 + a_1Y + \cdots + a_dY^d$ with $a_i \in F$. For $f \in \mathcal{A}$, we define:

$$N(f) = a_0 + a_1f^r + a_2f^{2r} + \cdots + a_df^{rd} \in \mathcal{A}.$$

We also set $N' = \frac{dN}{dY} = a_1 + 2a_2Y + \cdots + da_dY^{d-1}$. In addition, we choose and fix an element $a \in K$ with $\mathrm{Tr}_{K/F}(a) = 1$.

As in Hensel's Lemma, we proceed by successive approximations in order to find a root of N is $\hat{\mathcal{A}}_N$. Precisely, we shall construct by induction a sequence $(Z_m)_{m\geq 1}$ of polynomials in $\mathcal{Z}^+$ with $Z_1 = 0$, $Z_{m+1} \equiv Z_m \pmod{N^m}$ and $N(X + aZ_mX) \in N^m\mathcal{Z}^+$ for all $m > 1$. In what follows, we will often write C_m for $1 + aZ_m \in \mathcal{C}^+$. We assume that Z_m has been constructed for some $m \geq 1$. The second condition we need to fulfill implies that Z_{m+1} must take the form $Z_{m+1} = Z_m + aN^mZ$ for some $Z \in \mathcal{Z}^+$. The third condition then reads $N(C_{m+1}X) \in N^{m+1}\mathcal{Z}^+$.

Let us first prove that $N(C_{m+1}X)$ lies in $\mathcal{Z}^+$. For this, we observe that

$$(C_{m+1}X)^r = \big(1 + aZ_{m+1}\big) \cdot \big(1 + \theta(a)Z_{m+1}\big) \cdots \big(1 + \theta^{r-1}(a)Z_{m+1}\big) \cdot X^r.$$

The latter is obviously a polynomial in X^r with coefficients in K. Since it is moreover stable by the action of θ, its coefficients must lie in F and we have proved that $(C_{m+1}X)^r \in \mathcal{Z}^+$. The fact that $N(C_{m+1}X) \in \mathcal{Z}^+$ follows directly.

It remains now to ensure that $N(C_{m+1}X)$ is divisible by N^{m+1} for a suitable choice of Z. For any positive integer n, we have the following sequence of congruences modulo N^{m+1}:

$$\begin{aligned}
(C_{m+1}X)^{rn} &\equiv (C_mX)^{rn} + \sum_{i=0}^{rn-1} (C_mX)^i aN^m ZX (C_mX)^{rn-1-i} \\
&\equiv (C_mX)^{rn} + \sum_{i=0}^{rn-1} X^i aN^m ZX^{rn-i} && \text{since } C_m \equiv 1 \pmod N \\
&\equiv (C_mX)^{rn} + \sum_{i=0}^{rn-1} \theta^i(a) X^{rn} N^m Z \\
&\equiv (C_mX)^{rn} + X^{rn} N^m Z \pmod{N^{m+1}} && \text{since } \mathrm{Tr}_{K/F}(a) = 1.
\end{aligned}$$

Therefore $N(C_{m+1}X) \equiv N(C_mX) + X^r N' N^m Z \pmod{N^{m+1}}$. By the induction hypothesis, $N(C_mX) = N^m S$ with $S \in \mathcal{Z}^+$. We are then reduced to prove that there exists a polynomial $Z \in \mathcal{Z}^+$ such that $S + X^r N' Z \equiv 0 \pmod N$, which follows from the fact that $X^r N'$ is coprime with N.

The sequence $(Z_m)_{m\geq 1}$ we have just constructed defines an element $Z \in \hat{\mathcal{Z}}_N$. We set $C = 1 + aZ$; it is an element of $\hat{\mathcal{C}}_N$. Besides, by construction, CX is a root of N, in the sense that $N(CX) = 0$. This property together with the fact that C is invertible in $\hat{\mathcal{C}}_N$ ensure that the map $\iota : \mathcal{A}/N\mathcal{A} \to \hat{\mathcal{A}}_N$, $X \mapsto CX$ is a well defined morphism of K-algebras (see also §1.2). Moreover, since $C \equiv 1 \pmod N$, ι reduces to the identity modulo N. Mapping T to N, one extends ι to a second morphism of K-algebras:

$$\tau : (\mathcal{A}/N\mathcal{A})[[T]] \to \hat{\mathcal{A}}_N.$$

The latter induces the identity after reduction modulo T on the left and N on the right. Since the source and the target are both separated are complete (for the T-adic and the N-adic topology respectively), we conclude that τ has to be an isomorphism. We finally define $\tau_N = \tau^{-1}$ and observe that it satisfied all the requirements of the theorem.

It remains to prove (ii). By Theorem 1.2.6, given a positive integer m, any morphism of K-algebras $\mathcal{A}/N\mathcal{A} \to \mathcal{A}/N^m\mathcal{A}$ takes $\mathcal{C}/N\mathcal{C}$ to $\mathcal{C}/N^m\mathcal{C}$. Passing to the limit, we find that any morphism of K-algebras $\mathcal{A}/N\mathcal{A} \to \hat{\mathcal{A}}_N$ must send $\mathcal{C}/N\mathcal{C}$ to $\hat{\mathcal{C}}_N$. Therefore, any isomorphism τ_N satisfying the conditions of (i) induces a morphism of K-algebras $(\mathcal{C}/N\mathcal{C})[[T]] \to \hat{\mathcal{C}}_N$ which continues to map T to N and induces the identity modulo T. By the unicity result in the commutative case, we deduce that τ_N coincides with $\tau_N^{\mathcal{C}}$ on $(\mathcal{C}/N\mathcal{C})[[T]]$, hence (ii). □

About unicity. Unfortunately, unlike the commutative case, the isomorphism τ_N is not uniquely determined by the conditions of Theorem 2.2.1. We nevertheless have several results in this direction.

Proposition 2.2.3. *Let $\tau_{N,1}, \tau_{N,2} : \hat{\mathcal{A}}_N \to (\mathcal{A}/N\mathcal{A})[[T]]$ be two isomorphisms of K-algebras satisyfing the conditions of Theorem 2.2.1. Then, there exists $V \in (\mathcal{C}/N\mathcal{C})[[T]]$ with $V \equiv 1 \pmod T$ such that $\tau_{N,1}(f) = V^{-1}\,\tau_{N,2}(f)\,V$ for all $f \in \hat{\mathcal{A}}_N$.*

Proof. Set $\gamma = \tau_{N,2}^{-1} \circ \tau_{N,1}$; it is an endomorphism of K-algebras of $\hat{\mathcal{A}}_N$. Besides, thanks to the unicity result in the commutative case, $\tau_{N,1}$ and $\tau_{N,2}$ have to coincide on $\hat{\mathcal{C}}_N$. This means that γ is in fact a morphism of $\hat{\mathcal{C}}_N$-algebras. Applying Theorem 1.2.6 and passing to the limit, this implies the existence of an invertible element $U \in \hat{\mathcal{C}}_N$, $U \equiv 1 \pmod N$ such that $\gamma(f) = U^{-1} f U$ for all $f \in \hat{\mathcal{A}}_N$. Applying $\tau_{N,2}$ to this equality, we find that the proposition holds with $V = \tau_{N,2}(U)$. □

Corollary 2.2.4. *Given $f \in \mathcal{A}$ and N as before, the following quantities are preserved when changing the isomorphism τ_N:*

(i) the T-adic valuation of $\tau_N(f)$,

(i') *more generally, for $j \in \mathbb{Z}$, the T-adic valuation of $\sigma_j(\tau_N(f))$,*

(ii) *the first nonzero coefficient of $\tau_N(f)$,*

(ii') *more generally, for $j \in \mathbb{Z}$, the first nonzero coefficient of $\sigma_j(\tau_N(f))$,*

(iii) *the 0-th section of $\tau_N(f)$, namely $\sigma_0(\tau_N(f))$,*

(iii') *more generally, any quantity of the form $\sigma_{j_1,\dots,j_m}(\tau_N(f))$ with $j_1 + \cdots + j_m \equiv 0 \pmod{r}$.*

Proof. By Proposition 2.2.3, if $\tau_{N,1}$ and $\tau_{N,2}$ are two suitable isomorphisms, there exists an invertible element $V \in (\mathcal{C}/N\mathcal{C})[[T]]$, $V \equiv 1 \pmod{T}$ such that:

$$\tau_{N,1}(f) = V^{-1} \cdot \tau_{N,2}(f) \cdot V. \tag{22}$$

The items (i) and (ii) follows. Let $j \in \mathbb{Z}$. By Lemma 1.2.8, applying σ_j to (22), we get:

$$\sigma_j \circ \tau_{N,1}(f) = V^{-1} \cdot \sigma_j \circ \tau_{N,2}(f) \cdot \theta^j(V)$$

which implies (i') and (ii'). Finally (iii) and (iii') follow from Proposition 1.2.10. □

When p does not divide r, the situation is even better because one can select a canonical representative for τ_N. Precisely, we have the following theorem.

Theorem 2.2.5. *We assume that p does not divide r.*

(i) *The homomorphism of K-algebras:*

$$\tau_{N,\mathrm{can}} : \hat{\mathcal{A}}_N \to (\mathcal{A}/N\mathcal{A})[[T]], \quad X \mapsto \left(\frac{\tau_N^{\mathcal{C}}(Y)}{Y}\right)^{1/r} \cdot X$$

satisfies the conditions of Theorem 2.2.1.

(ii) *The morphism $\tau_{N,\mathrm{can}}$ is the unique isomorphism $\tau_N : \hat{\mathcal{A}}_N \to (\mathcal{A}/N\mathcal{A})[[T]]$ which satisfies the conditions of Theorem 2.2.1 and the extra property $\tau_N(X) \in (\mathcal{Z}/N\mathcal{Z})[[T]] \cdot X$.*

Remark 2.2.6. Note that $\tau_N^{\mathcal{C}}(Y)$ is an element of $\mathcal{Z}$ which is congruent to Y modulo T. Therefore $\frac{\tau_N^{\mathcal{C}}(Y)}{Y}$ is congruent to 1 modulo T and raising it to the power $\frac{1}{r}$ makes sense in $(\mathcal{Z}/N\mathcal{Z})[[T]]$ thanks to the formula:

$$\big(1+xT\big)^{1/r} = \sum_{n=0}^{\infty} \underbrace{\frac{1}{n!} \cdot \frac{1}{r} \cdot \left(\frac{1}{r} - 1\right) \cdots \left(\frac{1}{r} - (n-1)\right)}_{c_n} \cdot x^n\, T^n.$$

Observe that all the coefficients c_n's lie in $\mathbb{Z}[\frac{1}{r}]$ and so can be safely reduced modulo p if p does not divide r.

Proof of Theorem 2.2.5. The first part of the theorem is easily checked. We now assume that we are given two isomorphisms of K-algebras $\tau_{N,1}$, $\tau_{N,2} : \hat{\mathcal{A}}_N \to (\mathcal{A}/N\mathcal{A})[[T]]$ satisfying the conditions of the theorem. For $i \in \{1,2\}$, we write $\tau_{N,i}(X) = Z_i X$ with $Z_i \in (\mathcal{Z}/N\mathcal{Z})[[T]]$. By Proposition 2.2.3, we know that these exists $V \in (\mathcal{C}/N\mathcal{C})[[T]]$ such that $V \equiv 1 \pmod{T}$ and

$$V \cdot \tau_{N,1}(f) = \tau_{N,2}(f) \cdot V$$

for all $f \in \hat{\mathcal{A}}_N$. In particular, for $f = X$, we get $VZ_1X = Z_2XV$, implying $VZ_1 = \theta(V)Z_2$ in $(\mathcal{C}/N\mathcal{C})[[T]]$. Taking the trace from K to F, we end up with $WZ_1 = WZ_2$ with $W = V + \theta(V) + \cdots + \theta^{r-1}(V)$. Observe that $W \equiv r \pmod{T}$; therefore, it is invertible in $(\mathcal{Z}/N\mathcal{Z})[[T]]$ and the equality $WZ_1 = WZ_2$ readily implies $Z_1 = Z_2$, that is $\tau_{N,1} = \tau_{N,2}$. □

2.2.3 Taylor expansions of skew rational functions

Recall that we have defined in §1.1 the fraction field $\mathrm{Frac}(\mathcal{A})$ of $\mathcal{A}$ and we have proved that $\mathrm{Frac}(\mathcal{A}) = \mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}} \mathcal{A}$ (see Theorem 1.1.4).

Taylor expansion at central separable polynomials. For a given separable polynomial $N \in \mathcal{Z}$, the isomorphism τ_N of Theorem 2.2.1 extends to an isomorphism $\mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}} \hat{\mathcal{A}}_N \to (\mathcal{A}/N\mathcal{A})(\!(T)\!)$ and we can consider the composite:

$$\mathrm{TS}_N : \mathrm{Frac}(\mathcal{A}) = \mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}} \mathcal{A} \longrightarrow \mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}} \hat{\mathcal{A}}_N \xrightarrow{\sim} (\mathcal{A}/N\mathcal{A})(\!(T)\!)$$

where the first map is induced by the natural inclusion $\mathcal{A} \to \hat{\mathcal{A}}_N$. By definition $\mathrm{TS}_N(f)$ is called the *Taylor expansion* of f around N. We notice that it does depend on a choice of the isomorphism τ_N. However, one can form several quantities that are independant of any choice and then are canonically attached to $f \in \mathrm{Frac}(\mathcal{A})$ and N as before. Many of them are actually given by Corollary 2.2.4; here are they:

(i) the *order of vanishing* of f at N, denoted by $\mathrm{ord}_N(f)$; it is defined as the T-adic valuation of $\mathrm{TS}_N(f)$,

(i') for $j \in \mathbb{Z}$, the *j-th partial order of vanishing* of f at N, denoted by $\mathrm{ord}_{N,j}(f)$; it is defined as the T-adic valuation of $\sigma_j(\mathrm{TS}_N(f))$,

(ii) the *principal part* of f at N, denoted by $\mathcal{P}_N(f)$; it is the element of $\mathcal{A}/N\mathcal{A}$ defined as the coefficient of $T^{\mathrm{ord}_N(f)}$ in the series $\mathrm{TS}_N(f)$,

(ii') for $j \in \mathbb{Z}$, the *j-th partial principal part* of f at N, denoted by $\mathcal{P}_{N,j}(f)$; it is the element of $\mathcal{C}/N\mathcal{C}$ defined as the coefficient of $T^{\mathrm{ord}_{N,j}(f)}$ in the series $\sigma_j(\mathrm{TS}_N(f))$,

(iii) the 0-th section of $\mathrm{TS}_N(f)$, namely $\sigma_0(\mathrm{TS}_N(f))$,

(iii') more generally, any quantity of the form $\sigma_{j_1,\dots,j_m}(\mathrm{TS}_N(f))$ with $j_1 + \cdots + j_m \equiv 0 \pmod{r}$.

The previous invariants are related by many relations, *e.g.*:

- $\mathrm{ord}_N(f) = \min\big(\mathrm{ord}_{N,0}(f), \dots, \mathrm{ord}_{N,r-1}(f)\big)$,
- $\mathrm{ord}_{N,j+r}(f) = \mathrm{ord}_{N,j}(f)$,
- $\mathcal{P}_N(f) = \sum_j \mathcal{P}_{N,j}(f)\, X^j$ where the sum is extended to the indices $j \in \{0, 1, \dots, r-1\}$ for which $\mathrm{ord}_{N,j}(f) = \mathrm{ord}_N(f)$,
- $\mathcal{P}_{N,j+r}(f) = X^r\, \mathcal{P}_{N,j}(f)$,
- $\mathrm{ord}_N(fg) \geq \mathrm{ord}_N(f) + \mathrm{ord}_N(g)$ and equality holds as soon as $\mathcal{A}/N\mathcal{A}$ is a division algebra[4],
- $\mathcal{P}_N(fg) = \mathcal{P}_N(f) \cdot \mathcal{P}_N(g)$ when $\mathrm{ord}_N(fg) = \mathrm{ord}_N(f) + \mathrm{ord}_N(g)$.

We say that f has *no pole* at N when $\mathrm{ord}_N(f) \geq 0$. It has a *simple pole* at N when $\mathrm{ord}_N(f) = -1$. Generally, we define the order of the pole of f at N as the opposite of $\mathrm{ord}_N(f)$.

Taylor expansion at nonzero closed points. In a similar fashion, one can define the Taylor expansion of a skew rational function at a nonzero closed point z of F. When z is rational, *i.e.* $z \in F$, $z \neq 0$, we simply set $\mathrm{TS}_z = \mathrm{TS}_{Y-z}$.

Otherwise, the construction is a bit more subtle. Let F^{s} be a fixed separable closure of F and let $z \in F^{\mathrm{s}}$, $z \neq 0$. Let also $N \in \mathcal{Z}^+$ be the minimal polynomial of N. We have recalled in §2.2.1 that the Taylor expansion around z defines an isomorphism:

$$\tau_z^{\mathcal{C}} : \hat{\mathcal{C}}_N \xrightarrow{\sim} (\mathcal{C}/N\mathcal{C})[[T]]$$

which is characterized by the fact that it sends Y to $z + T$. In general, $\tau_z^{\mathcal{C}}$ does not agree with $\tau_N^{\mathcal{C}}$ but there exists a series $S_z \in (\mathcal{C}/N\mathcal{C})[[T]]$ such that $\tau_z^{\mathcal{C}} = \varphi_z \circ \tau_N^{\mathcal{C}}$ where φ_z is the endomorphism of $(\mathcal{C}/N\mathcal{C})[[T]]$ taking T to S_z (and acting trivially on the coefficients). The latter extends to

[4]This is the case for instance if $K = \mathbb{C}$, θ is the complex conjugacy and $N = X^2 + z$ with $z \in \mathbb{R}_{>0}$.

an endomorphism of $(\mathcal{A}/N\mathcal{A})[[T]]$, that we continue to call φ_z. By construction, the following diagram is commutative:

$$\begin{array}{ccc} \hat{\mathcal{A}}_N & \xrightarrow{\varphi_z \circ \tau_N} & (\mathcal{A}/N\mathcal{A})[[T]] \\ \uparrow & & \uparrow \\ \hat{\mathcal{C}}_N & \xrightarrow{\tau_z^{\mathcal{C}}} & (\mathcal{C}/N\mathcal{C})[[T]] \end{array} \tag{23}$$

whenever $\tau_N : \hat{\mathcal{A}}_N \to (\mathcal{A}/N\mathcal{A})[[T]]$ is an isomorphism satisfying the conditions of Theorem 2.2.1.(i). It worths noticing that the morphisms of the form $\varphi_z \circ \tau_N$ can be characterized without any reference of τ_N.

Proposition 2.2.7. *Given $z \in F^{\mathrm{s}}$, $z \neq 0$, we have the following equivalence. A mapping $\tau_z : \hat{\mathcal{A}}_N \to (\mathcal{A}/N\mathcal{A})[[T]]$ is of the form $\varphi_z \circ \tau_N$ (where τ_N satisfies the condition of Theorem 2.2.1) if and only if τ_z is a morphism of K-algebras, $\tau_z(X) \equiv X \pmod T$ and $\tau_z(Y) = z + T$.*

Proof. If $\tau_z = \varphi_z \circ \tau_N$, it follows from the conditions of Theorem 2.2.1 that τ_z is morphism of K-algebras which induces the identity modulo T. Hence $\tau_z(X) \equiv X \pmod T$. Moreover, by the second part of Theorem 2.2.1, we know that τ_N coincides with $\tau_N^{\mathcal{C}}$ on $\hat{\mathcal{C}}_n$. Therefore τ_z has to agree with $\varphi_z \circ \tau_N^{\mathcal{C}} = \tau_z^{\mathcal{C}}$ on $\hat{\mathcal{C}}_N$, implying in particular that $\tau_z(Y) = z + T$.

Conversely, let us assume that τ_z satisfies the condition of the proposition. We have to check that $\tau_N = \varphi_z^{-1} \circ \tau_z$ satisfies the conditions of Theorem 2.2.1. The fact that τ_N is a morphism of K-algebras is obvious. The assumption $\tau_z(X) \equiv X \pmod T$ ensures that τ_N acts as the identity modulo T. Finally, the hypothesis $\tau_z(Y) = z + T$ implies that τ_z coincides with $\tau_z^{\mathcal{C}}$ on $\hat{\mathcal{C}}_N$. Hence:

$$\tau_N(N) = \varphi_z^{-1} \circ \tau_z(N) = \varphi_z^{-1} \circ \tau_z^{\mathcal{C}}(N) = \tau_N^{\mathcal{C}}(N) = T$$

and we are done. □

Definition 2.2.8. We say that a morphism $\tau : \hat{\mathcal{A}}_N \to (\mathcal{A}/N\mathcal{A})[[T]]$ is *admissible* if it satisfies the conditions of Proposition 2.2.7.

Remark 2.2.9. By Theorem 1.2.6, a homomorphism of K-algebras $\tau_z : \hat{\mathcal{A}}_N \to (\mathcal{A}/N\mathcal{A})[[T]]$ is entirely determined by the element $C = \tau_z(X)\, X^{-1} \in (\mathcal{C}/N\mathcal{C})[[T]]$. Proposition 2.2.7 shows that τ is admissible if and only if:

$$C \equiv 1 \pmod T \quad \text{and} \quad \mathrm{N}_{(\mathcal{C}/N\mathcal{C})[[T]]/(\mathcal{Z}/N\mathcal{Z})[[T]]}\big(C\big) = 1 + \frac{T}{z}.$$

Moreover any $C \in (\mathcal{C}/N\mathcal{C})[[T]]$ satisfying the above conditions gives rise to an admissible morphism τ_z.

From now on, we fix a choice of an admissible morphism τ_z. Accordingly, we define TS_z as the composite:

$$\mathrm{TS}_z : \mathrm{Frac}(\mathcal{A}) = \mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}} \mathcal{A} \longrightarrow \mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}} \hat{\mathcal{A}}_N \xrightarrow{\tau_z} (\mathcal{A}/N\mathcal{A})((T)).$$

Like TS_N, the morphism TS_z depends upon some choices but some quantities attached to it are canonical, as the order of vanishing at z, the principal part at z, *etc.* For $f \in \mathrm{Frac}(\mathcal{A})$ and $j \in \mathbb{Z}$, we use the transparent notations $\mathrm{ord}_z(f)$, $\mathrm{ord}_{z,j}(f)$, $\mathcal{P}_z(f)$ and $\mathcal{P}_{z,j}(f)$ to refer to them.

Proposition 2.2.10. *Let $z \in F^{\mathrm{s}}$, $z \neq 0$ and let $N \in \mathcal{Z}^+$ be its minimal polynomial. Then:*

(i) $\mathrm{ord}_z(f) = \mathrm{ord}_N(f)$,

(i') $\mathrm{ord}_{z,j}(f) = \mathrm{ord}_{N,j}(f)$ *for all* $j \in \mathbb{Z}$,

(ii) $\mathcal{P}_z(f) = \mathcal{P}_N(f)$,

(ii') $\mathcal{P}_{z,j}(f) = \mathcal{P}_{N,j}(f)$ *for all* $j \in \mathbb{Z}$.

Proof. Everything follows from the facts that φ_z preserves the valuation, the principal part and commutes with σ_j. □

Taylor expansion at 0. Until now, we have always paid attention to exclude the special point $z = 0$. Indeed, when $z = 0$, the situation is a bit different because, roughly speaking, the ideal (Y) ramifies in the extension $\mathcal{A}^+/\mathcal{C}^+$. However, it is also possible (and even simpler) to define Taylor expansions around 0. In order to do this, we first define:

$$\hat{\mathcal{A}}_0^+ = \varprojlim_{m>0} \mathcal{A}^+/Y^m\mathcal{A}^+ \qquad \text{and} \qquad \hat{\mathcal{A}}_0 = \hat{\mathcal{A}}_0^+[\tfrac{1}{Y}].$$

The elements of $\hat{\mathcal{A}}_0^+$ can be viewed as power series in the variable X, that is infinite sums of the form:

$$f = a_0 + a_1X + \cdots + a_nX^n + \cdots$$

where the coefficients a_i lie in K. The multiplication on $\hat{\mathcal{A}}_0$ is driven by Ore's rule $X \cdot c = \theta(c)X$ for $c \in K$. Similarly, the elements of $\hat{\mathcal{A}}_0$ are Laurent series of the form:

$$f = a_vX^v + a_{v+1}X^{v+1} + \cdots + a_0 + a_1X + \cdots + a_nX^n + \cdots$$

where v is a (possibly negative) integer and the a_i's are elements of K. For this reason, we will sometimes write $K(\!(X;\theta)\!)$ instead of $\hat{\mathcal{A}}_0$. Noticing that $\mathrm{Frac}(\mathcal{Z})$ canonically embeds into $F(\!(Y)\!) \subset K(\!(X;\theta)\!)$, we deduce that $\mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}^+} \hat{\mathcal{A}}_0^+ \simeq K(\!(X;\theta)\!)$. We are now ready the define the Taylor expansion at 0, following the construction of TS_N. We set:

$$\mathrm{TS}_0 : \mathrm{Frac}(\mathcal{A}) = \mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}^+} \mathcal{A}^+ \longrightarrow \mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}^+} \hat{\mathcal{A}}_0^+ \xrightarrow{\sim} K(\!(X;\theta)\!).$$

Unlike TS_z, the morphism TS_0 is entirely canonical and does not depend upon any choice.

Taylor expansion and derivations. In the commutative case, the coefficients of the Taylor expansion of a function f around one rational point z are given by the values at z of the successive divided derivatives of f (see Eq. (19)). Below, we will establish similar results in the noncommutative setting.

We consider an element $z \in F^{\mathrm{s}}$, $z \neq 0$. Let $N \in \mathcal{Z}^+$ be the minimal polynomial of z. Let $\tau_z : \hat{\mathcal{A}}_N \to (\mathcal{A}/N\mathcal{A})[[T]]$ be any admissible morphism (see Definition 2.2.8). We define $C = \tau_z(X)X^{-1} \in (\mathcal{C}/N\mathcal{C})[[T]]$. It is congruent to 1 modulo T; in particular, it is invertible in $(\mathcal{C}/N\mathcal{C})[[T]]$. The codomain of τ_z, namely $(\mathcal{A}/N\mathcal{A})[[T]]$, is canonically endowed with the derivation $\frac{d}{dT}$. A simple computation shows that it corresponds to the derivation $\partial_{\mathfrak{C}}$ on $\hat{\mathcal{A}}_N$ where $\mathfrak{C}$ is defined by:

$$\mathfrak{C} = \tau_z^{-1}\left(C^{-1}\,\frac{dC}{dT}\right) \in \hat{\mathcal{A}}_N.$$

The p-th power of $\partial_{\mathfrak{C}}$ vanishes since it corresponds to $\frac{d^p}{dT^p}$ through the isomorphism τ_z. Using τ_z, we can go further and define higher divided powers of $\partial_{\mathfrak{C}}$ by:

$$\partial_{\mathfrak{C}}^{[n]} = \tau_z^{-1} \circ \left(\frac{1}{n!}\,\frac{d^n}{dT^n}\right) \circ \tau_z \tag{24}$$

for all nonnegative integer n. With this definition, it is formal to check that:

$$\tau_z(f) = \sum_{n=0}^{\infty} \partial_{\mathfrak{C}}^{[n]}(f) \cdot T^n \;\in\; (\mathcal{A}/N\mathcal{A})[[T]]. \tag{25}$$

However, this result is not entirely satisfying because $\mathfrak{C}$ is hard to compute (and the $\partial_{\mathfrak{C}}^{[n]}$'s are even harder) and depends heavily on z. Typically, Proposition 2.1.4 shows that $\mathfrak{C}$ cannot be rational unless r is coprime with p. Nevertheless, when p does not divide r and τ_z is well chosen, we shall see that the computation of $\mathfrak{C}$ and $\partial_{\mathfrak{C}}^{[n]}$ can be carried out and yields eventually a simple interpretation of the Taylor coefficients.

Frow now on, we assume that p does not divide r. By Theorem 2.2.5, we know that there is a canonical choice for τ_z, called $\tau_{z,\mathrm{can}}$. The corresponding element C is:

$$C_{\mathrm{can}} = \left(\frac{\tau_z^{\mathcal{C}}(Y)}{Y}\right)^{1/r} = \left(1 + \frac{T}{z}\right)^{1/r}.$$

Therefore:

$$\mathfrak{C}_{\mathrm{can}} = \tau_z^{-1}\left(C_{\mathrm{can}}^{-1}\,\frac{dC_{\mathrm{can}}}{dT}\right) = \tau_z^{-1}\left(\frac{1}{r}\,\frac{1}{T+z}\right) = \frac{1}{rY}.$$

In particular, we observe that $\mathfrak{C}_{\mathrm{can}}$ is rational and, even better, $\partial_{\mathfrak{C}_{\mathrm{can}}}$ is equal to the canonical derivative ∂_{can} we introduced in Definition 2.1.3. Its divided powers (defined by Eq. (24)) also have a simple expression:

$$\partial_{\mathrm{can}}^{[n]}\Big(\sum_i a_i X^i\Big) = \sum_i \underbrace{\frac{1}{n!}\cdot\frac{i}{r}\cdot\left(\frac{i}{r}-1\right)\cdots\left(\frac{i}{r}-(n-1)\right)}_{c_{n,i}}\cdot a_i\, X^{i-rn}.$$

where the coefficients $c_{n,i}$'s all lie in $\mathbb{Z}[\frac{1}{r}]$ and, consequently, can be reduced modulo p without trouble. With these inputs, Eq. (25) reads:

$$\tau_{z,\mathrm{can}}(f) = \sum_{n=0}^{\infty} \partial_{\mathrm{can}}^{[n]}(f)\, T^n \;\in\; (\mathcal{A}/N\mathcal{A})[[T]] \tag{26}$$

which can be considered as a satisfying skew analogue of the classical Taylor expansion formula.

2.3 A theory of residues

The results of the previous subsection lays the foundations of a theory of residues for skew polynomials. The aim of the present subsection is to develop it: we will define a notion of residue at a closed point of F for skew rational functions and then study how residues behave under duality, change of variables, *etc.* Along the way, we will also prove an analogue in our setting of the classical residue formula.

Throughout this subsection, we fix a separable closure F^{s} of F, together with an embedding $K \hookrightarrow F^{\mathrm{s}}$. For $z \in F^{\mathrm{s}}$ and $C \in \mathrm{Frac}(\mathcal{C})$, we will write $\mathrm{res}_z(C{\cdot}dY)$ for the (classical) residue at z of the differential form $C{\cdot}dY$.

2.3.1 Definition and first properties

We recall that, for $z \in F^{\mathrm{s}}$, $z \neq 0$, we have defined in §2.2.3 a (non canonical) morphism of K-algebras:

$$\mathrm{TS}_z : \mathrm{Frac}(\mathcal{A}) \longrightarrow (\mathcal{A}/N\mathcal{A})(\!(T)\!)$$

where $N \in \mathcal{Z}^+$ is the minimal polynomial of z. On the other hand, there is a natural embedding $\mathcal{Z}/N\mathcal{Z} \hookrightarrow F^{\mathrm{s}}$ obtained by mapping Y to z. Extending scalars from F to K, it extends to a second embedding

$$\iota_z : \mathcal{C}/N\mathcal{C} \longrightarrow K \otimes_F F^{\mathrm{s}}.$$

Before going further, let us observe that the codomain of ι_z, namely $K \otimes_F F^{\mathrm{s}}$, is naturally isomorphic to a product of r copies of F^{s} *via* the mapping:

$$\beta : K \otimes_F F^{\mathrm{s}} \to (F^{\mathrm{s}})^r, \qquad c \otimes x \mapsto \big(cx, \theta(c)x, \dots, \theta^{r-1}(c)x\big).$$

We now arrive at the definition of residues of skew rational functions.

Definition 2.3.1. For $z \in F^{\mathrm{s}}$, $z \neq 0$, and $f \in \mathrm{Frac}(\mathcal{A})$, we define:

- the *skew residue* of f at z, denoted by $\mathrm{sres}_z(f)$, as the coefficient of T^{-1} in the series $\mathrm{TS}_z(f)$; it is an element of $\mathcal{A}/N\mathcal{A}$,
- for $j \in \{0, \dots, r{-}1\}$, the *$j$-th partial skew residue* of f at z, denoted by $\mathrm{sres}_{z,j}(f)$, as:

$$\iota_z \circ \sigma_j \circ \mathrm{sres}_z(f) \in \big(K \otimes_F F^{\mathrm{s}}\big).$$

Here are two important remarks concerning residues.

First, we insist on the fact that both $\mathrm{sres}_z(f)$ and $\mathrm{sres}_{z,j}(f)$ do depend on the choice of the admissible morphism τ_z (used in the definition of TS_z) in general. However, Corollary 2.2.4 shows that $\mathrm{sres}_z(f)$ and $\mathrm{sres}_{z,j}(f)$ are defined without ambiguity when f has (at most) a simple pole at z. Besides, when p does not divide r, there is a distinguished choice for TS_z (see Theorem 2.2.5), leading to distinguished choices for sres_z and $\mathrm{sres}_{z,j}$. In the sequel, we will denote them $\mathrm{sres}_{z,\mathrm{can}}$ and $\mathrm{sres}_{z,j,\mathrm{can}}$.

Second, we observe that, the collection of all the partial skew residues $\mathrm{sres}_{z,j}(f)$'s captures as much information as $\mathrm{sres}_z(f)$, given that $\mathrm{sres}_z(f)$ is determined by its sections $\sigma_j(\mathrm{sres}_z(f))$'s with $0 \leq j < r$ thanks to the formula:

$$\mathrm{sres}_z(f) = \sum_{j=0}^{p-1} \sigma_j \circ \mathrm{sres}_z(f).$$

Residues at special points. It will be convenient to define residues at 0 and ∞ as well. For residues at 0, we recall that we have defined a *canonical* Taylor expansion map around 0:

$$\mathrm{TS}_0 : \mathrm{Frac}(\mathcal{A}) \longrightarrow K(\!(X;\theta)\!)$$

Definition 2.3.2. For $f \in \mathrm{Frac}(\mathcal{A})$ and $j \in \{0, 1, \ldots, r-1\}$, we define the *$j$-th partial skew residue* of f at 0, denoted by $\mathrm{sres}_{0,j}(f)$, as the coefficient of X^{j-r} in the series $\mathrm{TS}_0(f)$.

Residues at infinity are defined in a similar fashion. Let $\tilde{X}$ be a new variable and form the skew algebra $\tilde{\mathcal{A}} = K[\tilde{X}^{\pm 1}; \theta^{-1}]$. Clearly $\tilde{\mathcal{A}}$ is isomorphic to $\mathcal{A}$ by letting $\tilde{X}$ correspond to X^{-1}. We then get a map:

$$\mathrm{TS}_\infty : \mathrm{Frac}(\mathcal{A}) \simeq \mathrm{Frac}(\tilde{\mathcal{A}}) \longrightarrow K(\!(\tilde{X};\theta^{-1})\!)$$

where the second map is the morphism TS_0 for $\tilde{\mathcal{A}}$.

Definition 2.3.3. For $f \in \mathrm{Frac}(\mathcal{A})$ and $j \in \{0, 1, \ldots, r-1\}$, we define the *$j$-th partial skew residue* of f at ∞, denoted by $\mathrm{sres}_{\infty,j}(f)$, as the opposite of the coefficient of $\tilde{X}^{r-j}$ in the series $\mathrm{TS}_\infty(f)$.

Unlike $\mathrm{sres}_{z,j}(f)$, the partial skew residues $\mathrm{sres}_{0,j}(f)$ and $\mathrm{sres}_{\infty,j}(f)$ do not depend on any choice and so are canonically attached to f.

Commutative residues. The residues we just defined are actually closely related, in many cases, to classical residues of usual rational functions. In order to state precise results in this direction, we need extra notations. We observe that the map res_z defines by restriction a F-linear mapping $\mathcal{Z}\,dY \to F^{\mathrm{s}}$. Tensoring it by K over F, we obtain a K-linear map $\rho_z : \mathcal{C}\,dY \longrightarrow K \otimes_F F^{\mathrm{s}}$. Letting $\mathrm{res} : (\mathcal{C}/N\mathcal{C})(\!(T)\!) \to \mathcal{C}/N\mathcal{C}$ be the map selecting the coefficient in T^{-1}, one checks the two following formulas:

$$\begin{aligned} \rho_z\big(C{\cdot}dY\big) &= \iota_z \circ \mathrm{res} \circ \mathrm{TS}_z\big(C\big) \\ \beta \circ \rho_z\big(C{\cdot}dY\big) &= \big(\mathrm{res}_z\big(C{\cdot}dY\big), \mathrm{res}_z\big(\theta(C){\cdot}dY\big), \ldots \mathrm{res}_z\big(\theta^{r-1}(C){\cdot}dY\big)\big) \end{aligned}$$

for all $C \in \mathrm{Frac}(\mathcal{C})$.

Proposition 2.3.4. *For $z \in F^{\mathrm{s}} \sqcup \{\infty\}$ and $f \in \mathrm{Frac}(\mathcal{A})$, we have* $\mathrm{sres}_{z,0}(f) = \rho_z\big(\sigma_0(f){\cdot}dY\big)$.

Proof. By definition, $\mathrm{sres}_{z,0}(f) = \iota_z \circ \sigma_0 \circ \mathrm{sres}_z(f)$. Applying Lemma 1.2.9 and passing to the limit, we find that the isomorphism τ_z commutes with σ_0. Hence $\sigma_0 \circ \mathrm{sres}_z$ is equal to the compositum:

$$\mathrm{Frac}(\mathcal{A}) \xrightarrow{\sigma_0} \mathrm{Frac}(\mathcal{C}) \xrightarrow{\mathrm{TS}_z} (\mathcal{C}/N\mathcal{C})(\!(T)\!) \xrightarrow{\mathrm{res}} \mathcal{C}/N\mathcal{C}.$$

Composing further by ι_z on the left, we get the proposition. □

Proposition 2.3.4 implies in particular that $\mathrm{sres}_{z,0}(f)$ does not depend on any choice and thus is canonically attached to f and z. According to Corollary 2.2.4, there are other invariants which are canonically attached to $\mathrm{sres}_z(f)$. A family of them consists of the $\sigma_{j_1,\dots,j_m}(\mathrm{sres}_z(f))$'s for $j_1,\dots,j_m \in \mathbb{Z}$ with $j_1+\cdots+j_m \equiv 0 \pmod r$. However, these invariants seem less interesting; for example, they do not define additive functions on $\mathrm{Frac}(\mathcal{A})$.

Under some additional assumptions, all the partial skew residues are related to residues of usual rational functions.

Proposition 2.3.5. *Let $z \in F^{\mathrm{s}} \sqcup \{\infty\}$, let $f \in \mathrm{Frac}(\mathcal{A})$ and let $j \in \{0,1,\dots,r-1\}$. If $z \in \{0,\infty\}$ or $\mathrm{ord}_{z,j}(f) \geq -1$, then:*

$$\mathrm{sres}_{z,j}(f) = \rho_z\big(\sigma_j(f)\cdot dY\big).$$

Proof. When $z \in \{0,\infty\}$, the proposition can be easily checked by hand. Let us now assume that $\mathrm{ord}_{z,j}(f) \geq -1$. By Lemma 1.2.9, we know that $\sigma_j \circ \tau_z = \mathrm{N}_j(C)\cdot(\tau_z \circ \sigma_j)$ with $C = \tau_z(X)X^{-1} \in (\mathcal{C}/N\mathcal{C})[[T]]$. Moreover, from the fact that τ_z induces the identity modulo N, we deduce that $C \equiv 1 \pmod T$. Consequently τ_z commutes with σ_j modulo T. The end of the proof is now similar to that of Proposition 2.3.4. □

2.3.2 The residue formula

In the classical commutative setting, the theory of residues is very powerful because we have at our disposal many formulas, allowing for a complete toolbox for manipulating them easily and efficiently. We now strive to establish analogues of these formulas in our noncommutative setting. We start by the "commutative" residue formula.

Theorem 2.3.6. *For $f \in \mathrm{Frac}(\mathcal{A})$, we have:*

$$\sum_{z \in F^{\mathrm{s}} \sqcup \{\infty\}} \mathrm{sres}_{z,0}(f) = 0.$$

Proof. Since β is an isomorphism, it is enough to prove that $\sum_{z\in F^{\mathrm{s}}\sqcup\{\infty\}} \beta\circ\mathrm{sres}_{z,0}(f) = 0$. Writing $C = \sigma_0(f) \in \mathcal{C}$, Proposition 2.3.4 asserts that:

$$\beta \circ \mathrm{sres}_{z,0}(f) = \beta \circ \rho_z\big(C\big) = \big(\mathrm{res}_z\big(C\cdot dY\big), \mathrm{res}_z\big(\theta(C)\cdot dY\big), \dots, \mathrm{res}_z\big(\theta^{r-1}(C)\cdot dY\big)\big)$$

in $(F^{\mathrm{s}})^r$. The theorem them follows from the classical residue formula applied to the $\theta^j(C)$'s for j varying between 0 and $r-1$. □

The reader might be a bit disappointed by the previous theorem as it only concerns 0-th partial skew residues and it reduces immediately to the classical setting. Unfortunately, in general, it seems difficult to obtain a vanishing result involving skew residues since the latter might be not canonically defined. There is however an important special case for which such a formula exists and can be proved.

Theorem 2.3.7. *Let $f \in \mathrm{Frac}(\mathcal{A})$. We assume that f has at most a simple pole at all points $z \in F^{\mathrm{s}}$, $z \neq 0$. Then:*

$$\sum_{z \in F^{\mathrm{s}} \sqcup \{\infty\}} \mathrm{sres}_{z,j}(f) = 0$$

for all $j \in \{0,1,\dots,r-1\}$.

Proof. Let $j \in \{0,\dots,r-1\}$ and set $C_j = \sigma_j(f)$. By Proposition 2.3.5, we know that:

$$\beta \circ \mathrm{sres}_{z,j}(f) = \beta \circ \rho_z(C_j) = \big(\mathrm{res}_z\big(C_j\cdot dY\big), \mathrm{res}_z\big(\theta(C_j\cdot dY)\big), \dots, \mathrm{res}_z\big(\theta^{r-1}(C_j)\cdot dY\big)\big)$$

By the classical residue formula applied successively with $C_j, \theta(C_j), \dots, \theta^{r-1}(C_j)$, we deduce that $\mathrm{sres}_{z,j}(f)$ has to vanish. □

The case of canonical residues also deserves some attention. As before, the main input is a formula relating the partial skew residues $\mathrm{sres}_{z,j,\mathrm{can}}(f)$ to classical residues. We consider a new variable y and form the *commutative* polynomial ring $K[y]$ and its field of fractions $K(y)$. We embed $\mathrm{Frac}(\mathcal{C})$ into $K(y)$ by taking Y into y^r. We insist on the fact that y is not X or, equivalently, $K(y)$ is not $\mathrm{Frac}(\mathcal{A})$: our new variable y commutes with the scalars. Since $K(y)$ is a genuine field of rational functions, it carries a well-defined notion of residue. For $f \in K(y)$ and $z \in F^{\mathrm{s}}$, we will denote by $\mathrm{res}_z(f{\cdot}dy)$ the residue at f of the differentiel form $f{\cdot}dy$. Similarly the map ρ_z extends to $K(y)\,dy$. Performing the change of variable $y \mapsto Y = y^r$, we obtain the relations:

$$\mathrm{res}_{z^r}\big(C \cdot dY\big) = r \cdot \mathrm{res}_z\big(y^{r-1}\, C \cdot dy\big)$$
$$\rho_{z^r}\big(C \cdot dY\big) = r \cdot \rho_z\big(y^{r-1}\, C \cdot dy\big)$$

which hold true for any $C \in \mathcal{C}$ and any $z \in F^{\mathrm{s}}$.

Proposition 2.3.8. *We assume that p does not divide r.*
For $f \in \mathrm{Frac}(\mathcal{A})$, $j \in \{0, 1, \dots, r-1\}$ and $z \in F^{\mathrm{s}}$, $z \neq 0$, we have:

$$\mathrm{sres}_{z,j,\mathrm{can}}(f) = r\,\zeta^{-j}\,\rho_\zeta\big(y^{j+r-1}\,\sigma_j(f)\cdot dy\big)$$

where ζ is any r-th root of z.

Proof. Set $C_{\mathrm{can}} = \tau_{z,\mathrm{can}}(X)\,X^{-1}$. From Lemma 1.2.9, we know that:

$$\sigma_j \circ \tau_{z,\mathrm{can}} = \mathrm{N}_j(C_{\mathrm{can}}) \cdot (\tau_{z,\mathrm{can}} \circ \sigma_j). \tag{27}$$

On the other hand, it follows from Theorem 2.2.5 that $C_{\mathrm{can}} \in (\mathcal{Z}/N\mathcal{Z})[[T]]$. Since moreover $C_{\mathrm{can}} \equiv 1 \pmod T$, writing $\tau_{z,\mathrm{can}}(Y) = z + T$, we find $C_{\mathrm{can}} = \big(1 + \frac{T}{z}\big)^{1/r}$. Plugging this in (27), we obtain:

$$\sigma_j \circ \tau_{z,\mathrm{can}} = \left(1 + \frac{T}{z}\right)^{j/r} \cdot (\tau_{z,\mathrm{can}} \circ \sigma_j). \tag{28}$$

The main observation is that the twisting function $\big(1 + \frac{T}{z}\big)^{j/r}$ which is *a priori* only defined on a formal neighborhood of $T = 0$ (or, equivalenty of $Y = z$) is closely related to a function of the variable y which is globally defined. Precisely, consider the local parameter $t = y - \zeta$ on a formal neighborhood of ζ. The relation $y^r = Y$ translates to $(\zeta + t)^r = z + T$. Dividing by z on both sides and raising to the power $\frac{j}{r}$, we obtain:

$$\zeta^{-j} y^j = \left(1 + \frac{t}{\zeta}\right)^j = \left(1 + \frac{T}{z}\right)^{j/r}$$

showing that our multiplier $\big(1 + \frac{T}{z}\big)^{j/r}$ is the Taylor expansion of the function $\zeta^{-j}y^j$. Eq. (28) then becomes $\sigma_j\big(\tau_{z,\mathrm{can}}(f)\big) = \tau_{z,\mathrm{can}}\big(\zeta^{-j}y^j\,\sigma_j(f)\big)$. Taking the coefficient in T^{-1}, we get:

$$\mathrm{sres}_{z,j,\mathrm{can}}(f) = \rho_z\big(\zeta^{-j}y^j \cdot \sigma_j(f)\cdot dY\big) = r \cdot \rho_\zeta\big(\zeta^{-j}y^{j+r-1}\,\sigma_j(f)\cdot dy\big)$$

which is exactly the formula in the statement of the proposition. □

Unfortunately, Proposition 2.3.8 does not give an interesting vanishing result for canonical partial skew residues. Indeed, if we apply the residue formula to the differential form $y^{j+r-1}\,\sigma_j(f){\cdot}dy$, we end up with:

$$\sum_{\substack{\zeta \in F^{\mathrm{s}} \\ \zeta \neq 0}} \zeta^j \cdot \mathrm{sres}_{\zeta^r,j,\mathrm{can}}(f) \;=\; 0. \tag{29}$$

Actually, this formula does not give any information because the sum on the left hand side can be refactored as follows:

$$\sum_{\substack{z \in F^{\mathrm{s}} \\ z \neq 0}} \left(\sum_{\zeta^r = z} \zeta^j \cdot \mathrm{sres}_{\zeta^r,j,\mathrm{can}}(f) \right)$$

and each internal sum vanishes simply because $\sum_{\zeta^r=z} \zeta^j = 0$. In other words, the formula (29) holds equally true when $\mathrm{sres}_{\zeta^r,j,\mathrm{can}}(f)$ is replaced by any quantity depending only on ζ^r.

However, Proposition 2.3.8 remains interesting for itself and can even be used to derive relations on partial skew residues of a skew rational function f. One way to achieve this goes as follows. Let $f \in \mathrm{Frac}(\mathcal{A})$ and $j \in \{1, \dots, r-1\}$. We assume that we know a finite set $\Pi = \{z_1, \dots, z_n\}$ containing the points $z \in F^{\mathrm{s}}$, $z \neq 0$ for which $\mathrm{ord}_{z,j}(f) < 0$. We assume further, for each index i, we are given an integer n_i with the guarantee that $\mathrm{ord}_{z,j}(f) \geq -n_i$. For each i, we choose a r-th root ζ_i of z_i. Let $P \in F^{\mathrm{s}}[y]$ be a polynomial such that, for all i, $P(\zeta_i) = \zeta_i^{-j}$ and the derivative $P'(y)$ has a zero of order at least $(n_i - 1)$ at ζ_i. This choice of P ensures that:

$$\rho_{\zeta_i}\big(P(y)\, y^{j+r-1}\, \sigma_j(f) \cdot dy\big) = \zeta_i^{-j}\, \rho_{\zeta_i}\big(y^{j+r-1}\, \sigma_j(f) \cdot dy\big)$$

for all index i. Thanks to Proposition 2.3.8, we obtain:

$$\mathrm{sres}_{z_i,j,\mathrm{can}}(f) = \rho_{\zeta_i}\big(P(y)\, y^{j+r-1}\, \sigma_j(f) \cdot dy\big).$$

Now applying the residue formula with the function $P(y)\, y^{j+r-1}\, \sigma_j(f)$, we end up with:

$$\sum_{\substack{z \in F^{\mathrm{s}} \\ z \neq 0}} \mathrm{sres}_{z,j,\mathrm{can}}(f) = -\rho_0\big(P(y)\, y^{j+r-1}\, \sigma_j(f) \cdot dy\big) - \rho_\infty\big(P(y)\, y^{j+r-1}\, \sigma_j(f) \cdot dy\big).$$

The right hand side of the last formula can be computed explicity on concrete examples (though determining a suitable polynomial $P(y)$ might be painful if the order of the poles are large). To begin with, note that, when $\mathrm{ord}_{z,j}(f) \geq 0$, the first summand $\rho_0\big(P(y)\, y^{j+r-1}\, \sigma_j(f) \cdot dy\big)$ vanishes.

2.3.3 Residue and duality

We recall that we have defined in §1.4 a duality $f \mapsto f^\star$ on $\mathrm{Frac}(\mathcal{A})$ and that this duality acts as the change of variables $Y \mapsto Y^{-1}$ on the subalgebra $\mathrm{Frac}(\mathcal{C})$. We aim at comparing the residues of f and $f^\star$ for $f \in \mathrm{Frac}(\mathcal{A})$. By what we have recalled above, when C lies in $\mathrm{Frac}(\mathcal{C})$, the formula we look for is nothing but the change of variables formula, which reads:

$$\mathrm{res}_z\big(C^\star \cdot dY\big) = \mathrm{res}_{z^{-1}}\big(C \cdot d(Y^{-1})\big) = \mathrm{res}_{z^{-1}}\big(-Y^{-2} C \cdot dY\big).$$

For a general $f \in \mathrm{Frac}(\mathcal{A})$, the result is more complicated to state because the skew residues themselves are not canonically defined.

Theorem 2.3.9. *Let $z \in F^{\mathrm{s}}$, $z \neq 0$ and let $f \in \mathrm{Frac}(\mathcal{A})$.*

(i) For any admissible choice of τ_z (see Definition 2.2.8), there is an admissible choice of $\tau_{z^{-1}}$ such that:

$$\mathrm{sres}_z(f^\star) = \big(\mathrm{sres}_{z^{-1}}\big(-Y^{-2} f\big)\big)^\star.$$

(ii) If p does not divide r, we have:

$$\mathrm{sres}_{z,\mathrm{can}}(f^\star) = \big(\mathrm{sres}_{z^{-1},\mathrm{can}}\big(-Y^{-2} f\big)\big)^\star.$$

Remark 2.3.10. By definition, the skew residue $\mathrm{sres}_z(f^\star)$ is an element of the quotient ring $\mathcal{A}/N\mathcal{A}$ where N is the minimal polynomial of z. On the other hand, the minimal polynomial of z^{-1} is $N^\star$ up to multiplication by a scalar. Therefore $\mathrm{sres}_{z^{-1}}(-Y^{-2} f)$ is naturally an element of $\mathcal{A}/N^\star\mathcal{A}$. Its image under duality then lies in $\mathcal{A}/N\mathcal{A}$, just like $\mathrm{sres}_z(f^\star)$. Hence, both formulas of Theorem 2.3.9 make sense.

Before entering into the proof of Theorem 2.3.9, we isolate a lemma that we will use several times. In what follows, if f is a series in the variable T, we use the notation $\mathrm{res}(f)$ to denote its coefficient in T^{-1}.

Lemma 2.3.11. *Let $N \in \mathcal{Z}$. Let $S \in (\mathcal{Z}/N\mathcal{Z})[[T]]$ be a series with constant term 0. Let:*

$$\begin{array}{rccc} \psi: & (\mathcal{A}/N\mathcal{A})(\!(T)\!) & \longrightarrow & (\mathcal{A}/N\mathcal{A})(\!(T)\!) \\ & \sum_i a_i T^i & \mapsto & \sum_i a_i S^i. \end{array}$$

For all $f \in (\mathcal{A}/N\mathcal{A})(\!(T)\!)$, we have the formula:

$$\operatorname{res}\left(\psi(f)\,\frac{dS}{dT}\right) = \operatorname{res}(f). \tag{30}$$

Proof. When $f \in (\mathcal{A}/N\mathcal{A})[[T]]$, both sides of Eq. (30) vanish and the conclusion of the lemma holds. Moreover, since ψ and res are both K-linear, it is enough to establish the lemma when $f = T^i$ with $i < 0$. Eq. (30) then reads $\operatorname{res}\big(S^i \frac{dS}{dT}\big) = \operatorname{res}\big(T^i\big)$ and is a direct consequence of the classical formula of change of variables for residues. □

Proof of Theorem 2.3.9. Let N be the minimal polynomial of z and let $\tau_z : \hat{\mathcal{A}}_N \to (\mathcal{A}/N\mathcal{A})[[T]]$ be an admissible morphism. Notice that $N^\star$ is the minimal polynomial of z^{-1} up to multiplication by an invertible element of $\mathcal{Z}$. Besides, observe that the duality $f \mapsto f^\star$ induces isomorphisms of rings $(\hat{\mathcal{A}}_N)^{\mathrm{op}} \xrightarrow{\sim} \hat{\mathcal{A}}_{N^\star}$ and $(\mathcal{A}/N\mathcal{A})^{\mathrm{op}} \xrightarrow{\sim} \mathcal{A}/N^\star\mathcal{A}$. The latter extends to an isomorphism $(\mathcal{A}/N\mathcal{A})[[T]]^{\mathrm{op}} \xrightarrow{\sim} (\mathcal{A}/N^\star\mathcal{A})[[T]]$ by letting T go to T. We can then consider the isomorphism

$$\tau : \hat{\mathcal{A}}_{N^\star} \to (\mathcal{A}/N^\star\mathcal{A})[[T]], \quad f \mapsto \big(\tau_z(f^\star)\big)^\star.$$

Setting $S = -\frac{z^2 T}{1+zT}$ and letting ψ be the corresponding morphism defined in Lemma 2.3.11, we have:

$$\psi \circ \tau(Y) = \psi\left(\frac{1}{z+T}\right) = \frac{1}{z+S} = z^{-1} + T.$$

We deduce from this computation that $\tau_{z^{-1}} = \psi \circ \tau$ is an admissible morphism for z^{-1}. For this particular choice of $\tau_{z^{-1}}$, the first assertion of the theorem follows from Lemma 2.3.11 after noticing that:

$$\frac{dS}{dT} = -\frac{z^2}{(1+zT)^2} = \tau_{z^{-1}}\left(-Y^{-2}\right).$$

For the second part of the theorem, we assume that the morphism τ_z we started with is $\tau_{z,\mathrm{can}}$. By Theorem 2.2.5, $Z = \tau_z(X)\,X^{-1}$ lies in $(\mathcal{Z}/N\mathcal{Z})[[T]]$. Let us compute:

$$\tau_{z^{-1}}(X) = \psi \circ \tau(X) = \psi\big(\tau_z(X^{-1})^\star\big) = \psi\big((X^{-1}Z^{-1})^\star\big) = \psi\big((Z^{-1})^\star X\big) = \psi\big((Z^{-1})^\star\big) \cdot X.$$

In particular we find that $\tau_{z^{-1}}(X)\,X^{-1} \in (\mathcal{Z}/N\mathcal{Z})[[T]]$. By Theorem 2.2.5 again, $\tau_{z^{-1}} = \tau_{z^{-1},\mathrm{can}}$ and we finally conclude by applying (i). □

The formula for partial skew residues. Theorem 2.3.9 concerns skew residues but, of course, it has direct consequences on partial skew residues. In what follows, in a slight abuse of notations, we will write θ instead of $\theta \otimes \mathrm{id}$ for its action on $K \otimes_F F^{\mathrm{s}}$.

Corollary 2.3.12. *Let $z \in F^{\mathrm{s}}$, $z \neq 0$ and let $f \in \mathrm{Frac}(\mathcal{A})$.*

(i) We have:

$$\operatorname{sres}_{z,0}(f^\star) = \operatorname{sres}_{z^{-1},0}\big(-Y^{-2} f\big).$$

Moreover, for any admissible choice of τ_z, there is an admissible choice of $\tau_{z^{-1}}$ such that, for all $j \in \{1, \dots, r-1\}$, we have:

$$\operatorname{sres}_{z,j}(f^\star) = z \cdot \theta^j\big(\operatorname{sres}_{z^{-1},r-j}\big(-Y^{-2} f\big)\big).$$

(ii) If p does not divide r, for all $j \in \{1, \dots, r-1\}$, we have:

$$\operatorname{sres}_{z,j,\mathrm{can}}(f^\star) = z \cdot \theta^j\big(\operatorname{sres}_{z^{-1},r-j,\mathrm{can}}\big(-Y^{-2} f\big)\big).$$

Proof of Corollary 2.3.12. Given an admissible choice of τ_z, we know by Theorem 2.3.9 that there exists an admissible choice of $\tau_{z^{-1}}$ for which

$$\mathrm{sres}_z(f^\star) = \big(\mathrm{sres}_{z^{-1}}\big(-Y^{-2}f\big)\big)^\star. \tag{31}$$

For simplicity, let us write $g = \mathrm{sres}_{z^{-1}}(-Y^2 f)$. Let $j \in \{0, \dots, r-1\}$. applying $\iota_z \circ \sigma_j$ to (31), we find that the $\mathrm{sres}_{z,j}(f^\star) = \iota_z \circ \sigma_j(g^\star)$, When $j = 0$, it is equal to

$$\iota_z\big(\sigma_0(g)^\star\big) = \iota_{z^{-1}}\big(\sigma_0(g)\big) = \iota_{z^{-1}} \circ \sigma_0 \circ \mathrm{sres}_{z^{-1}}\big(-Y^2 f\big)$$

the first equality following from the fact that the duality acts on $\mathcal{C}$ through the change of variables $Y \mapsto Y^{-1}$. This gives the first statement of (i). When $j > 0$, we write:

$$\sigma_j(g^\star) = \theta^j\big(\sigma_{-j}(g)\big)^\star = \theta^j\big(Y^{-1}\,\sigma_{r-j}(g)\big)^\star = \theta^j\big(\sigma_{r-j}(g)\big)^\star \cdot \big(Y^{-1}\big)^\star = Y \cdot \theta^j\big(\sigma_{r-j}(g)\big)^\star.$$

Applying now ι_z, we get:

$$\iota_z \circ \sigma_j(g^\star) = z \cdot \iota_z\big(\theta^j\big(\sigma_{r-j}(g)\big)^\star\big) = z \cdot \iota_{z^{-1}}\big(\theta^j\big(\sigma_{r-j}(g)\big)\big) = z \cdot \theta^j\big(\iota_{z^{-1}}\big(\sigma_{r-j}(g)\big)\big).$$

Replacing g by its value, we find:

$$\mathrm{sres}_{z,j}(f^\star) = z \cdot \theta^j\big(\iota_{z^{-1}} \circ \sigma_{r-j} \circ \mathrm{sres}_{z^{-1}}\big(-Y^{-2}f\big)\big).$$

The first part of the corollary is then proved. The second part follows as in the proof of Theorem 2.3.9. □

Corollary 2.3.12 admits an analogue with residues at 0 and ∞.

Theorem 2.3.13. *For $f \in \mathrm{Frac}(\mathcal{A})$ and $j \in \{1, \dots, r-1\}$, we have:*

$$\begin{aligned}
\mathrm{sres}_{\infty,0}(f^\star) &= \mathrm{sres}_{0,0}\big(-Y^{-2}f\big),\\
\mathrm{sres}_{\infty,j}(f^\star) &= \theta^j\big(\mathrm{sres}_{0,r-j}(-Y^{-1}f)\big)
\end{aligned}$$

and similarly:

$$\begin{aligned}
\mathrm{sres}_{0,0}(f^\star) &= \mathrm{sres}_{\infty,0}\big(-Y^{-2}f\big),\\
\mathrm{sres}_{0,j}(f^\star) &= \theta^j\big(\mathrm{sres}_{\infty,r-j}(-Y^{-1}f)\big).
\end{aligned}$$

Proof. We consider the rings $K(\!(X;\theta)\!)$ and $K(\!(\tilde{X};\theta^{-1})\!)$. The duality induces a well-defined ring isomorphism $K(\!(X;\theta)\!)^{\mathrm{op}} \to K(\!(\tilde{X};\theta^{-1})\!)$ defined by:

$$\Big(\sum_i a_i X^i\Big)^\star = \sum_i \tilde{X}^i a_i = \sum_i \theta^{-i}(a_i)\tilde{X}^i.$$

Moreover this duality is compatible with Taylor expansions, in the sense that it sits in the following commutative diagram:

$$\begin{array}{ccc}
\mathrm{Frac}(\mathcal{A}) & \xrightarrow{f \mapsto f^\star} & \mathrm{Frac}(\mathcal{A}) \\
\Big\downarrow{\scriptstyle \mathrm{TS}_0} & & \Big\downarrow{\scriptstyle \mathrm{TS}_\infty} \\
K(\!(X;\theta)\!) & \xrightarrow{f \mapsto f^\star} & K(\!(\tilde{X};\theta^{-1})\!)
\end{array}$$

We now consider $f \in \mathrm{Frac}(\mathcal{A})$. We write $\mathrm{TS}_0(f) = \sum_i a_i X^i$ with $a_i \in K$ and deduce $\mathrm{TS}_\infty(f^\star) = \sum_i \theta^{-i}(a_i)\tilde{X}^i$. Thus, for all index j, we have $\mathrm{sres}_{\infty,j} = -\theta^j(a_{r-j})$. On the other hand, a simple computation gives $\mathrm{sres}_{0,j}(-Y^{-1}f) = -a_j$ and $\mathrm{sres}_{0,j}(-Y^{-2}f) = -a_{r+j}$. The two first formulas follow easily. The two other formulas are proved similarly. □

2.3.4 Change of variables

We now analyse the effect of an endomorphism γ of $\mathrm{Frac}(\mathcal{A})$ on the residues. According to Theorem 1.2.1, $\gamma(X) = CX$ for some $C \in \mathrm{Frac}(\mathcal{C})$ and we have:

$$\gamma\Big(\sum_i a_i X^i\Big) = \sum_i a_i \mathrm{N}_i(C) X^i$$

where, by definition, $\mathrm{N}_i(C) = C \cdot \theta(C) \cdots \theta^{i-1}(C)$. Define $Z = \gamma(Y)$. We have:

$$Z \;=\; \mathrm{N}_r(C) \cdot Y \;=\; \mathrm{N}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C) \cdot Y \;\in\; \mathrm{Frac}(\mathcal{Z})$$

and γ acts on $\mathrm{Frac}(\mathcal{C})$ through the change of variables $Y \mapsto Z$.

Definition 2.3.14. Let γ as above and let $z \in F^{\mathrm{s}}$
We say that z is *γ-regular* if Z has no zero and no pole at $Y = z$.
When z is γ-regular, we define $\gamma_\star z$ as the value taken by Z at the point $Y = z$.

For $f \in \mathrm{Frac}(\mathcal{C})$ and $z \in F^{\mathrm{s}}$, we have the formula

$$\mathrm{res}_{\gamma_\star z}\big(f \cdot dY\big) = \mathrm{res}_z\big(\gamma(f) \cdot dZ\big) = \mathrm{res}_z\left(\gamma(f)\,\frac{dZ}{dY} \cdot dY\right).$$

The aim of this subsection is to extend this relation to any $f \in \mathrm{Frac}(\mathcal{A})$, replacing classical commutative residues by skew residues.

Comparing skew residues at $\gamma_\star z$ and z is not straightforward because they do not live in the same space: the former lies in $\mathcal{A}/N_1\mathcal{A}$ where N_1 is the minimal polynomial of $\gamma_\star z$ while the latter sits in $\mathcal{A}/N_2\mathcal{A}$ where N_2 is the minimal polynomial of z. We then first need to relate $\mathcal{A}/N_1\mathcal{A}$ and $\mathcal{A}/N_2\mathcal{A}$. For this, we remark that, as γ acts through the change of variables $Y \mapsto Z$ on $\mathcal{Z}$, it maps N_1 to a multiple of N_2. Therefore it induces a morphism of K-algebras $\mathcal{A}/N_1\mathcal{A} \to \mathcal{A}/N_2\mathcal{A}$.

Theorem 2.3.15. *Let $\gamma : \mathrm{Frac}(\mathcal{A}) \to \mathrm{Frac}(\mathcal{A})$ be an endomorphism of K-algebras. Let $z \in F^{\mathrm{s}}$, $z \neq 0$ be a γ-regular point.*

(i) For any admissible choice of $\tau_{\gamma_\star z}$ (see Definition 2.2.8) there exists an admissible choice of τ_z such that:

$$\gamma \circ \mathrm{sres}_{\gamma_\star z}(f) = \mathrm{sres}_z\left(\gamma(f)\,\frac{d\gamma(Y)}{dY}\right) \tag{32}$$

for all $f \in \mathrm{Frac}(\mathcal{A})$.

(ii) A skew rational function $f \in \mathrm{Frac}(\mathcal{A})$ has a single pole at $\gamma_\star z$ if and only if $\gamma(f)$ has a single pole at f. When its occurs, Eq. (32) holds for any admissible choices of $\tau_{\gamma_\star z}$ and τ_z.

Proof. We begin by some preliminaries. As before, we define $C = \gamma(X)\,X^{-1}$ and $Z = \gamma(Y) = \mathrm{N}_{\mathcal{C}/\mathcal{Z}}(C) \cdot Y$. We put $z_1 = \gamma_\star z$ and $z_2 = z$. For $i \in \{1, 2\}$, we define N_i as the minimal polynomial of z_i. The quotient ring $\mathcal{Z}/N_i\mathcal{Z}$ is an algebraic separable extension of F; we will denote it by E_i in the rest of the proof. By construction, E_i admits a natural embedding into F^{s} (obtained by mapping Y to z_i). The fact that γ acts on $\mathcal{Z}$ by right composition by Z shows that γ_C induces a field inclusion $E_1 \hookrightarrow E_2$, which is compatible with the embeddings in F^{s}. In what follows, we shall always view E_1 and E_2 as subfields of F^{s} with $E_1 \subset E_2$.

For $i \in \{1, 2\}$, we recall that the Taylor expansion around z_i provides us with a canonical isomorphism $\tau_i^{\mathcal{Z}} : \hat{\mathcal{Z}}_{N_i} \xrightarrow{\sim} E_i[[T]]$. The latter extends by K-linearity to an isomorphism $\tau_i^{\mathcal{C}} : \hat{\mathcal{C}}_{N_i} \xrightarrow{\sim} K \otimes_F E_i[[T]]$. We recall that $\tau_i^{\mathcal{Z}}(Y) = \tau_i^{\mathcal{C}}(Y) = z_i + T$. We set $S = \tau_2^{\mathcal{Z}}(Z) - z_1$ and consider the mapping:

$$\begin{array}{rccc} \varphi^{\mathcal{Z}} : & E_1[[T]] & \longrightarrow & E_2[[T]] \\ & \sum_i a_i T^i & \mapsto & \sum_i a_i S^i. \end{array}$$

We extend it by K-linearity to a map $\varphi^{\mathcal{C}} : K \otimes_F E_1[[T]] \to K \otimes_F E_2[[T]]$. We have:

$$\varphi^{\mathcal{C}} \circ \tau_1^{\mathcal{C}}(Y) = \varphi^{\mathcal{C}}(z_1 + T) = z_1 + S = \tau_2^{\mathcal{C}}(Z) = \tau_2^{\mathcal{C}} \circ \gamma(Y).$$

We deduce from this equality that the diagram

$$\begin{array}{ccc} \hat{\mathcal{C}}_{N_1} & \xrightarrow[\sim]{\tau_1^{\mathcal{C}}} & K \otimes_F E_1[[T]] \\ \Big\downarrow{\scriptstyle \gamma} & & \Big\downarrow{\scriptstyle \varphi^{\mathcal{C}}} \\ \hat{\mathcal{C}}_{N_2} & \xrightarrow[\sim]{\tau_2^{\mathcal{C}}} & K \otimes_F E_2[[T]] \end{array}$$

is commutative, *i.e.* $\varphi^{\mathcal{C}} \circ \tau_1^{\mathcal{C}} = \tau_2^{\mathcal{C}} \circ \gamma$. Let us now consider an admissible choice of τ_{z_1} and call it τ_1 for simplicity. It is a prolongation of $\tau_1^{\mathcal{C}}$. Besides, by Theorem 1.2.6, there exists $C_1 \in (\mathcal{C}/N_1\mathcal{C})[[T]] \simeq K \otimes_F E_1[[T]]$ such that $\tau_1(X) = C_1 X$. The properties of τ_1 ensure in addition that $C_1 \equiv 1 \pmod{T}$ and that:

$$\mathrm{N}_{K\otimes_F E_1[[T]]/E_1[[T]]}\big(C_1\big) = \frac{\tau_1(Y)}{Y} = 1 + \frac{T}{z_1}$$

(see also Remark 2.2.9). Applying $\varphi^{\mathcal{C}}$ to this relation, we find:

$$\mathrm{N}_{K\otimes_F E_2[[T]]/E_2[[T]]}\big(\varphi^{\mathcal{C}}(C_1)\big) = 1 + \frac{S}{z_1} = \frac{\tau_2^{\mathcal{Z}}(Z)}{z_1}. \tag{33}$$

Let $\bar{C} \in \mathcal{C}/N_2\mathcal{C} \simeq K \otimes_F E_2$ be the reduction of C modulo N_2. We shall often view $\bar{C}$ as a constant series in $(\mathcal{A}/N_2\mathcal{A})[[T]]$. Since the norm of C in the extension $\mathcal{C}/\mathcal{Z}$ is by definition $Z\,Y^{-1}$, we find:

$$\mathrm{N}_{K\otimes_F E_2[[T]]/E_2[[T]]}\big(\bar{C}\big) = \mathrm{N}_{K\otimes_F E_2/E_2}\big(\bar{C}\big) = \frac{z_1}{z_2} \tag{34}$$

and:

$$\mathrm{N}_{K\otimes_F E_2[[T]]/E_2[[T]]}\big(\tau_2^{\mathcal{C}}(C)\big) = \tau_2^{\mathcal{C}}\big(Z\,Y^{-1}\big) = \frac{\tau_2^{\mathcal{Z}}(Z)}{z_2 + T}. \tag{35}$$

Combining Eqs. (33), (34) and (35), we obtain:

$$\mathrm{N}_{K\otimes_F E_2[[T]]/E_2[[T]]}\left(\frac{\bar{C}\cdot\varphi^{\mathcal{C}}(C_1)}{\tau_2(C)}\right) = 1 + \frac{T}{z_2}.$$

Set $C_2 = \frac{\bar{C}\cdot\varphi^{\mathcal{C}}(C_1)}{\tau_2(C)}$ and let $\tau_2 : \hat{\mathcal{A}}_{N_2} \to (\mathcal{A}/N_2\mathcal{A})[[T]]$ be the morphism mapping X to C_2X. The above computations show that τ_2 is well defined and coincide with $\tau_2^{\mathcal{C}}$ on $\hat{\mathcal{C}}_{N_2}$. On the other hand, one checks immediately that $C_2 \equiv 1 \pmod{N_2}$, proving then that τ_2 induces the identity modulo N_2. As a consequence, τ_2 is an isomorphism and it is an admissible choice for τ_z. Moreover, it sits in the following commutative diagram:

$$\begin{array}{ccc} \hat{\mathcal{A}}_{N_1} & \xrightarrow[\sim]{\tau_1} & (\mathcal{A}/N_1\mathcal{A})[[T]] \\ \Big\downarrow{\scriptstyle \gamma} & & \Big\downarrow{\scriptstyle \varphi} \\ \hat{\mathcal{A}}_{N_2} & \xrightarrow[\sim]{\tau_2} & (\mathcal{A}/N_2\mathcal{A})[[T]] \end{array}$$

where φ is the extension of $\varphi^{\mathcal{C}}$ defined by $\varphi\big(\sum_i a_i T^i\big) = \sum_i \gamma(a_i) S^i$. The first assertion now follows from Lemma 2.3.11 together with the fact that $\frac{dS}{dT} = \tau_2^{\mathcal{Z}}\big(\frac{dZ}{dY}\big)$.

The equivalence in assertion (ii) follows from what we have done before after noticing that S has T-valuation 1 by the regularity assumption on z. The fact that Eq. (32) holds for any admissible choices of $\tau_{\gamma\star z}$ and τ_z in this case is a direct consequence of the fact that skew residues do not depend on the choice of the Taylor isomorphisms when poles are simple. □

Canonical residues. We recall that, when p does not divide r, there is a distinguished choice for τ_z leading to a notion of canonical skew residues, denoted by $\mathrm{sres}_{z,\mathrm{can}}$. In what follows, we examine how canonical residues behave under change of variables. After Theorem 2.3.15, one could hope that Eq. (32) always holds with canonical residues, as the latter are canonical. Unfortunately, it is not that simple in general. However, there is an important case where our first naive hope is correct.

Theorem 2.3.16. *We assume that p does not divide r.*
Let $\gamma : \mathrm{Frac}(\mathcal{A}) \to \mathrm{Frac}(\mathcal{A})$ be an endomorphism of K-algebras. Let $z \in F^{\mathrm{s}}$, $z \neq 0$ be a γ-regular point. If $\gamma(X)\, X^{-1} \in \mathrm{Frac}(\mathcal{Z})$, *we have:*

$$\gamma \circ \mathrm{sres}_{\gamma_\star z,\mathrm{can}}(f) = \mathrm{sres}_{z,\mathrm{can}}\left(\gamma(f)\,\frac{d\gamma(Y)}{dY}\right)$$

for all $f \in \mathrm{Frac}(\mathcal{A})$.

Proof. After Theorem 2.3.15, it is enough to check that the admissible choice $\tau_{\gamma_\star z,\mathrm{can}}$ leads to the admissible choice $\tau_{z,\mathrm{can}}$. By Theorem 2.2.5, this reduces further to check that C_2 lies in $(\mathcal{Z}/N_2\mathcal{Z})[[T]]$ as soon as C_1 is in $(\mathcal{Z}/N_1\mathcal{Z})[[T]]$ (with the notations of the proof of Theorem 2.3.15). This is obvious from the definition of C_2. □

We now consider the general case. Proposition 2.2.3 tells us that different choices of τ_z are conjugated. As a consequence, $\mathrm{sres}_{\gamma_\star z}(f)$ and $\mathrm{sres}_{z,\mathrm{can}}\big(\gamma(f)\frac{d\gamma(Y)}{dY}\big)$ should be eventually related up to some conjugacy. In the present situation, it turns out that the conjugating function can be explicited. From now on, we assume that p does not divide r. As before, we consider an endomorphism of K-algebras $\gamma : \mathrm{Frac}(\mathcal{A}) \to \mathrm{Frac}(\mathcal{A})$ and we define $C = \gamma(X)\, X^{-1} \in \mathrm{Frac}(\mathcal{C})$. We introduce the extension $\mathcal{Z}'$ of $\mathrm{Frac}(\mathcal{Z})$ obtained by adding a r-th root of $\mathrm{N}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C)$ and form the tensor products $\mathcal{C}' = \mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{C}$ and $\mathcal{A}' = \mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{C}$. We emphasize that $\mathcal{C}'$ is not a field in general but a product of fields. However, the extension $\mathcal{C}'/\mathcal{Z}'$ is always a cyclic Galois covering of degree r whose Galois group is generated by the automorphism $\mathrm{id} \otimes \theta$. Similarly, $\mathcal{A}'$ could be not isomorphic to an algebra of skew rational functions. Nevertheless, we have the following lemma.

Lemma 2.3.17. *Given a γ-regular point $z \in F^{\mathrm{s}}$ and its minimal polynomial $N \in \mathcal{Z}^+$, any admissible isomorphism $\tau_z : \hat{\mathcal{A}}_N \xrightarrow{\sim} (\mathcal{A}/N\mathcal{A})[[T]]$ extends uniquely to an isomorphism:*

$$\tau_z^{\mathcal{A}'} : \mathcal{Z}' \otimes_{\mathcal{Z}} \hat{\mathcal{A}}_N \xrightarrow{\sim} (\mathcal{A}'/N\mathcal{A}')(\!(T)\!)$$

inducing the identity after reduction modulo N on the left and modulo T on the right.

Proof. Let us first prove an analogous statement for that $\tau_z^{\mathcal{Z}} : \hat{\mathcal{Z}}_N \to (\mathcal{Z}/N\mathcal{Z})[[T]]$. For simplicity, set $Z_0 = \mathrm{N}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C) \in \mathcal{Z}$ and let $\bar{Z}_0$ be the reduction of Z_0 modulo N. By the regularity assumption, $\bar{Z}_0 \neq 0$. Hence $\tau_z^{\mathcal{Z}}(Z_0)$ has a unique r-th root in $(\mathcal{Z}'/N\mathcal{Z}')[[T]]$ whose constant term is the image of $\sqrt[r]{Z_0}$ in $\mathcal{Z}'/N\mathcal{Z}'$. This basically proves the existence and the unicity of a prolongation $\tau_z^{\mathcal{Z}'}$ of $\tau_z^{\mathcal{Z}}$.

Now, a prolongation of τ_z is given by $\tau_z^{\mathcal{A}'} = \tau_z^{\mathcal{Z}'} \otimes \tau_z$, which proves the existence. For unicity, we remark that, by unicity of $\tau_z^{\mathcal{Z}'}$, any isomorphism $\tau_z^{\mathcal{A}'}$ satisfying the conditions of the lemma has to coincide with $\tau_z^{\mathcal{Z}'}$ on $\mathcal{Z}' \otimes_{\mathcal{Z}} \hat{\mathcal{Z}}_N$. Since $\tau_z^{\mathcal{A}'}$ is a ring homomorphism, we deduce that it must necessarily agree with $\tau_z^{\mathcal{Z}'} \otimes \tau_z$ on its domain of definition. Unicity follows. □

Lemma 2.3.17 shows that the function $\mathrm{sres}_{z,\mathrm{can}} : \mathrm{Frac}(\mathcal{A}) \to \mathcal{A}/N\mathcal{A}$ admits a canonical extension to $\mathcal{C}'$. We will continue to call it $\mathrm{sres}_{z,\mathrm{can}}$ in the sequel. We now consider the element:

$$C' = \frac{C}{\sqrt[r]{\mathrm{N}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C)}} \in \mathcal{C}'.$$

By construction, it has norm 1 in the extension $\mathcal{C}'/\mathcal{Z}'$. Hilbert's Theorem 90 then guarantees the existence of an invertible element $U \in \mathcal{C}'$ (uniquely determined up to multiplication by an element of $\mathcal{Z}'$) such that:

$$C' = \frac{(\mathrm{id} \otimes \theta)(U)}{U}. \tag{36}$$

Remark 2.3.18. Raising Eq. (36) to the r-th power, we get:

$$\frac{(\mathrm{id} \otimes \theta)(U^r)}{U^r} = (C')^r = \frac{(\mathrm{id} \otimes \theta)(V)}{V} \quad \text{with} \quad V = \prod_{i=0}^{r-1} \theta^i\big(C\big)^{i+1-r}.$$

Therefore $U^r \in V\mathcal{Z}'$. This observation gives an alternative option for finding U: we look for an element $Z' \in \mathcal{Z}'$ for which VZ' is the r-th power in $\mathcal{C}'$ and we extract its r-th root.

Theorem 2.3.19. *With the above notations, we have:*

$$\gamma \circ \mathrm{sres}_{\gamma_\star z,\mathrm{can}}(f) = U^{-1} \cdot \mathrm{sres}_{z,\mathrm{can}}\left(U\,\gamma(f)\,U^{-1}\,\frac{d\gamma(Y)}{dY}\right) \cdot U$$

for all γ-regular point $z \in F^{\mathrm{s}}$, $z \neq 0$ and all $f \in \mathrm{Frac}(\mathcal{A})$.

Remarks 2.3.20. (1) When $C \in \mathrm{Frac}(\mathcal{Z})$, the norm of C is equal to 1, so that we have $\mathcal{C}' = \mathrm{Frac}(\mathcal{C})$ and $C' = 1$. In this case, one can take $U = 1$ and the statement of Theorem 2.3.19 reduces to that of Theorem 2.3.16.

(2) When $f \in \mathrm{Frac}(\mathcal{C})$, $\gamma(f)$ also lies in $\mathrm{Frac}(\mathcal{C})$ and thus commutes with f. Hence, the product $U\,\gamma(f)\,U^{-1}$ reduces to $\gamma(f)$. Similarly the skew residue $\mathrm{sres}_{z,\mathrm{can}}\big(\gamma(f)\,\frac{d\gamma(Y)}{dY}\big)$ is an element of $\mathcal{C}/N_2\mathcal{C}$ and thus also commutes with U. Finally, Theorem 2.3.19 reads in this case:

$$\gamma \circ \mathrm{sres}_{\gamma_\star z,\mathrm{can}}(f) = \mathrm{sres}_{z,\mathrm{can}}\left(\gamma(f)\,\frac{d\gamma(Y)}{dY}\right)$$

which is the usual formula for commutative residues.

Proof of Theorem 2.3.19. We keep the notations of the proof of Theorem 2.3.16 and assume in addition that the isomorphism $\tau_{\gamma_\star z}$ we started with is $\tau_{\gamma_\star z,\mathrm{can}}$, *i.e.* $C_1 \in (\mathcal{Z}/N_1\mathcal{Z})[[T]]$. Actually, we know more precisely that:

$$C_1 = \left(1 + \frac{T}{z_1}\right)^{1/r}.$$

By the proof of Theorem 2.3.15, Eq. (32) holds when τ_z is defined by $\tau_z(X) = C_2 X$ with:

$$C_2 = \frac{\bar{C}}{\tau_z^{\mathcal{C}}(C)} \cdot \left(1 + \frac{S}{z_2}\right)^{1/r}.$$

Here we recall that $\bar{C}$ is the image of C in $\mathcal{C}/N_2\mathcal{C}$ and $S = \tau_2(Z) - z_2$ where Z was defined by $Z = \mathrm{N}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C) \cdot Y$. On the other hand, the isomorphism $\tau_{z,\mathrm{can}}$ is defined by:

$$\tau_{z,\mathrm{can}}(X) = \left(1 + \frac{T}{z_2}\right)^{1/r} X.$$

Let $\bar{C}'$ and $\bar{U}$ be the image of C' and U in $\mathcal{C}'/N_2\mathcal{C}'$ respectively. We consider the ring homomorphism $\tau : \mathcal{Z}' \otimes_{\mathcal{Z}} \hat{\mathcal{A}}'_N \to (\mathcal{A}'/N\mathcal{A}')[[T]]$ defined by:

$$\tau(f) = \bar{U}^{-1} \cdot \tau_{z,\mathrm{can}}^{\mathcal{A}'}\big(U g\, U^{-1}\big) \cdot \bar{U} \tag{37}$$

for $g \in \hat{\mathcal{A}}_N$. A simple computation shows that $\tau(X) = QX$ with:

$$\begin{aligned} Q &= \frac{\mathrm{id} \otimes \theta(\bar{U})}{\bar{U}} \cdot \tau_{z,\mathrm{can}}^{\mathcal{A}'}\left(\frac{U}{\mathrm{id} \otimes \theta(U)}\right) \cdot \left(1 + \frac{T}{z_2}\right)^{1/r} \\ &= \bar{C}' \cdot \tau_{z,\mathrm{can}}^{\mathcal{A}'}\left(\frac{\sqrt[r]{\mathrm{N}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C)}}{C}\right) \cdot \left(1 + \frac{T}{z_2}\right)^{1/r}. \end{aligned}$$

Raising this equality to the r-th power, we get:

$$\begin{aligned} Q^r &= (\bar{C}')^r \cdot \tau_z^{\mathcal{C}}\left(\frac{\mathrm{N}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C)}{C^r}\right) \cdot \left(1 + \frac{T}{z_2}\right) \\ &= (\bar{C}')^r \cdot \tau_z^{\mathcal{C}}\left(\frac{Z}{Y}\,\frac{1}{C^r}\right) \cdot \left(1 + \frac{T}{z_2}\right). \end{aligned}$$

Noticing that $\tau_z^{\mathcal{C}}(Y) = z_2 + T$ and $\tau_z^{\mathcal{C}}(Z) = z_1 + S$, we obtain:

$$Q^r = \frac{z_1}{z_2} \cdot \left(\frac{\bar{C}'}{\tau_z^{\mathcal{C}}(C)}\right)^r \cdot \left(1 + \frac{S}{z_1}\right). \tag{38}$$

Now, observe that the identity $(C')^r = C^r \frac{Y}{Z}$ gives $(\bar{C}')^r = \bar{C}^r \frac{z_2}{z_1}$ after reduction modulo N_2. Putting this input in Eq. (38), we finally find:

$$Q^r = \left(\frac{\bar{C}}{\tau_z^{\mathcal{C}}(C)}\right)^r \cdot \left(1 + \frac{S}{z_1}\right) = C_2^r$$

Besides, a direct computation shows that both series Q and C_2 have a constant coefficient equal to 1. Therefore, the equality $Q^r = C_2^r$ we have just proved implies $Q = C_2$. In other words $\tau(X) = \tau_z(X)$. Since moreover τ and τ_z agree on $\sqrt[r]{\mathrm{N}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C)}$, they coincide everywhere. Coming back to the defintion of τ (see Eq. (37)), we obtain:

$$\mathrm{sres}_z\big(g\big) = \bar{U}^{-1} \cdot \mathrm{sres}_{z,\mathrm{can}}\big(U g\, U^{-1}\big) \cdot \bar{U} = U^{-1} \cdot \mathrm{sres}_{z,\mathrm{can}}\big(U g\, U^{-1}\big) \cdot U$$

for all $g \in \mathrm{Frac}(\mathcal{A})$. Specializing this equality to $g = \gamma(f)\,\frac{d\gamma(Y)}{dY}$, we get the theorem. □

3 Application to coding theory

In this section, we aim at defining a linearized version of geometric Goppa codes (over the projective line), making use of the theory of residues we have developed earlier. The codes we are going to construct will appear as a generalization of Wang's linearized Goppa codes [29] in the same way that linearized Reed–Solomon codes, introduced recently by Martínez-Peñas [20], are an extension of Gabidulin codes. We will also prove that our linearized Goppa codes are dual of Martínez-Peñas' linearized Reed–Solomon codes, as classical Goppa codes are duals of classical Reed–Solomon codes. This section also contains efficient decoding algorithms, with subquadratic complexity, for linearized Reed–Solomon codes and linearized Goppa codes.

3.1 From Gabidulin codes to linearized Reed–Solomon codes

In this subsection, we briefly review the very first construction of Gabidulin codes, due independently to Delsarte [7], Gabidulin [8] and Roth [26]. This initial construction is based on the notion of linearized polynomials over a finite field. Let us start by fixing a finite field K. We denote by p the characteristic of K and by q its cardinality. We then have $q = p^r$ for some positive integer r. By definition, a linearized polynomial over K is a polynomial of the form:

$$L(x) = a_0 + a_1 x^p + a_2 x^{p^2} + \cdots + a_n x^{p^n}$$

where n is an integer and the coefficients $a_0, a_1, \ldots, a_n$ are in K. The largest integer d for which $a_d \neq 0$ is called the *height* of L. The adjective "linearized" comes from the fact that the associated function $\mathbb{F}_q \to \mathbb{F}_q$, $u \mapsto L(u)$ is $\mathbb{F}_p$-linear. Let $K[x]_{\mathrm{lin}}$ be the set of linearized polynomials over K and $K[x]_{\mathrm{lin},<d}$ be its subset consisting of polynomials of height less than d. Obviously $K[x]_{\mathrm{lin}}$ and $K[x]_{\mathrm{lin},<d}$ are vector spaces over K. Moreover, one checks that $K[x]_{\mathrm{lin}}$ is stable under composition and that $\big(K[x]_{\mathrm{lin}}, +, \circ\big)$ is a ring (which is noncommutative, except when $r = 1$).

Definition 3.1.1. Let $\underline{c} = (c_1, \ldots, c_n) \in K^n$ be a $\mathbb{F}_p$-linearly independent family of elements of K. Let also k be a positive integer with $k \leq n$. The Gabidulin code associated to these parameters is:

$$\mathrm{Gab}\big(k, \underline{c}\big) = \Big\{ \big(f(c_1), \ldots, f(c_n)\big) \text{ with } f \in K[x]_{\mathrm{lin},<k} \Big\} \subset K^n.$$

In the framework of Gabidulin codes, the Hamming distance is not the most relevant one. Instead, it is more interesting to use the rank distance defined as follows.

Definition 3.1.2. The *rank weight* of a tuple $\underline{c} = (c_1, \ldots, c_n) \in K^n$ is:

$$w_{\mathrm{rk}}(\underline{c}) = \dim_{\mathbb{F}_p} \langle c_1, \ldots, c_n \rangle_{\mathbb{F}_p}$$

where the notation $\langle c_1, \ldots, c_n \rangle_{\mathbb{F}_p}$ denotes the $\mathbb{F}_p$-span of the c_i's.

The *rank distance* over K^n is the distance d_{rk} defined by $d_{\mathrm{rk}}(\underline{c}, \underline{c}') = w_{\mathrm{rk}}(\underline{c} - \underline{c}')$.

The parameters of the code $\mathrm{Gab}(k, \underline{c})$ are given by Theorem 3.1.3 below. We underline in particular that $\mathrm{Gab}(k, \underline{c})$ meets the Singleton bound; we say that it is *Maximal Rank Distance* (MRD).

Theorem 3.1.3. *Given a $\mathbb{F}_p$-linearly independent family $\underline{c} = (c_1, \dots, c_n) \in K^n$ and $k \in \{1, \dots, n\}$:*

- *the length of* $\mathrm{Gab}(k, \underline{c})$ *is* n,
- *the dimension of* $\mathrm{Gab}(k, \underline{c})$ *is* k,
- *the minimal rank distance of* $\mathrm{Gab}(k, \underline{c})$ *is* $d = n - k + 1$.

Reformulation with skew polynomials. The presentation of Gabidulin codes we have followed above is the one that was proposed initially by Delsarte, Roth and Gabidulin. However, nowadays, following Boucher and Ulmer [2], we prefer using skew polynomials in place of linearized polynomials. Indeed, this new point of view positions Gabidulin codes in a more general framework for which powerful tools have been designed for many years and are available in the literature. Eventually, this has been the key for establishing new properties of Gabidulin codes and designing interesting generalizations.

The starting point is the observation that the ring $(K[x]_{\mathrm{lin}}, +, \circ)$ is canonically isomorphic to $K[X; \theta]$ where $\theta : K \to K$, $x \mapsto x^p$ is the Frobenius endomorphism. Precisely, the correspondance is given explicitely by:

$$\begin{array}{ccc} K[X;\theta] & \longrightarrow & \big(K[x]_{\mathrm{lin}}, +, \circ\big) \\ \sum_i a_i X^i & \mapsto & \sum_i a_i x^{p^i}. \end{array}$$

Under this identification, the degree of a skew polynomial corresponds to the height of the corresponding linearized polynomial. Moreover, if $F \in K[X; \theta]$ corresponds to $f \in K[x]_{\mathrm{lin}}$, we have $f(c) = \varepsilon_1(F)(c)$ for any $c \in K$, where we recall from §1.3.1 (see more precisely Eq. (10)) that ε_1 is the ring homomorphism:

$$\begin{array}{rccc} \varepsilon_1 : & K[X;\theta] & \longrightarrow & \mathrm{End}_{\mathbb{F}_p}(K) \\ & \sum_i a_i X^i & \mapsto & \sum_i a_i \theta^i. \end{array}$$

Therefore, letting $K[X; \theta]_{<k}$ be the subspace of $K[X; \theta]$ consisting of skew polynomials of degree less than k, Gabidulin codes can be alternatively defined as follows:

$$\mathrm{Gab}\big(k, \underline{c}\big) = \Big\{ \big(\varepsilon_1(f)(c_1), \dots, \varepsilon_1(f)(c_n)\big) \text{ with } f \in K[X;\theta]_{<k} \Big\}$$

with $\underline{c} = (c_1, \dots, c_n) \in K^n$ and $k \leq n$. Interestingly, we notice that this new definition makes sense for any field K equipped with an endomorphism θ of finite order[5]. In this more general setting, the prime subfield $\mathbb{F}_p$ needs to be replaced by $F = K^{\theta=1}$ (defined as the subfield of K consisting of elements fixed by θ); in particular, the rank weight now needs to be defined by:

$$w_{\mathrm{rk}}\big((c_1, \dots, c_n)\big) = \dim_F \langle c_1, \dots, c_n \rangle_F$$

and the definition of the rank distance should be updated accordingly. Apart from this, everything works similarly and we have the next theorem, which is the straight generalization of Theorem 3.1.3.

Theorem 3.1.4. *Let K be a field equipped with an automorphism θ of finite order. Set $F = K^{\theta=1}$. Given a F-linearly independent family $\underline{c} = (c_1, \dots, c_n) \in K^n$ and $k \in \{1, \dots, n\}$:*

- *the length of* $\mathrm{Gab}(k, \underline{c})$ *is* n,
- *the dimension of* $\mathrm{Gab}(k, \underline{c})$ *is* k,
- *the minimal rank distance of* $\mathrm{Gab}(k, \underline{c})$ *is* $d = n - k + 1$.

[5] Actually, the assumption that θ has finite order is not necessary for defining and studying Gabidulin codes. However, this hypothesis allows for a simplified exposition of the theory that fits better in the spirit of this article. Moreover, it will be definitely needed in §3.2 when we will introduce linearized Goppa codes. For these reasons, we prefer assuming that θ has finite order from now on.

Proof. The assertion on the length is obvious. The two other assertions follow from Proposition 1.3.4. □

It worths noticing that the definition of Gabidulin codes can be made shorter and more intrinsic. Indeed, we see on the definition, that the codewords of $\mathrm{Gab}(k, \underline{c})$ are given by the evaluation of the *same* linear function, namely $\varepsilon_1(f)$, at the points $c_1, \ldots, c_n$. This datum is obviously equivalent to that of the restriction of $\varepsilon_1(f)$ to the F-span of the c_i's. Hence, instead of viewing a codeword as a tuple in K^n, we could alternatively consider it as a linear mapping defined on $V = \langle c_1, \ldots, c_n \rangle_F$. Moreover the rank weight has also a natural interpretation: it simply corresponds to the rank of the corresponding linear mapping. These observations motivate the following definition.

Definition 3.1.5. Given a F-linear subspace V of K and a positive integer $k \leq \dim_F V$, we set:

$$\mathrm{Gab}\big(k, V\big) = \Big\{ \varepsilon_1(f)_{|V} \text{ with } f \in K[X;\theta]_{<k} \Big\} \subset \mathrm{Hom}_F(V, K).$$

Moreover, we endow $\mathrm{Hom}_F(V, K)$ with the *rank weight* w_{rk} defined by $w_{\mathrm{rk}}(\varphi) = \mathrm{rank}(\varphi)$.

Under this second reformulation, the code $\mathrm{Gab}\big(k, \underline{c}\big)$ corresponds to $\mathrm{Gab}\big(k, \langle c_1, \ldots, c_n \rangle_F\big)$, as discussed earlier. We complete the picture by defining further the notions of length of dimension for codes sitting in $\mathrm{Hom}_F(V, K)$: if V is a F-linear subspace of K and C is a K-linear subspace of $\mathrm{Hom}_F(V, K)$, we set:

$$\begin{aligned} \mathrm{length}(C) &= \dim_K \big(\mathrm{Hom}_F(V, K)\big) = \dim_F V, \\ \dim(C) &= \dim_K C. \end{aligned}$$

Theorem 3.1.4 then asserts that the Gabidulin code $\mathrm{Gab}(k, V)$ has length $n = \dim_F V$, dimension k and minimal rank distance $d = n - k + 1$ (assuming $k \leq n$).

Linearized Reed–Solomon codes. We now present Martínez-Peñas' extension of Gabidulin codes developed in [20]. Before proceeding, we underline that the framework considered by Martínez-Peñas is much more general than that of this article: Martínez-Peñas does not assume that θ has finite order, he works with general Ore polynomials and even does not assume that K is a field but just a skew field. However, in what follows, we restrict ourselves to the general assumptions of this article, since these assumptions will be needed later on. For this reason, our exposition slightly differs from that of [20].

The latest presents Gabidulin codes we have encoutered (see Definition 3.1.5) shows that they are obtained by evaluating skew polynomials at the special semi-linear endomorphism θ. However, we have seen in Proposition 1.3.3 that K carries more semi-linear endomorphisms, which are the $(c\,\theta)$'s for c varying in K. It is tempting to use them to define more general Gabidulin codes. It is actually the purpose of linearized Reed–Solomon codes.

Definition 3.1.6. Let k and m be positive integers. Let $\underline{c} = (c_1, \ldots, c_m)$ be a tuple of nonzero elements of K and let $\underline{V} = (V_1, \ldots, V_m)$ be a tuple of F-linear subspaces of K. We define:

$$\begin{aligned} \mathrm{LRS}\big(k, \underline{c}, \underline{V}\big) = \Big\{ \big(\varepsilon_{c_1}(f)_{|V_1}, \ldots, \varepsilon_{c_m}(f)_{|V_m}\big) \text{ with } f \in K[X;\theta]_{<k} \Big\} \\ \subset \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K). \end{aligned}$$

The relevant notion of distance in this context is the so-called *sum-rank* distance, which is a mixture between the rank distance and the classical Hamming distance. It is defined as follows.

Definition 3.1.7. Let $V_1, \ldots, V_m$ be F-vector spaces. The *sum-rank* weight of a tuple $\underline{\varphi} = (\varphi_1, \ldots, \varphi_m) \in \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K)$ is:

$$w_{\text{s-rk}}\big(\underline{\varphi}\big) = \mathrm{rank}(\varphi_1) + \mathrm{rank}(\varphi_2) + \cdots + \mathrm{rank}(\varphi_m).$$

The *sum-rank* distance $d_{\text{s-rk}}$ on $\mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K)$ is defined by $d_{\text{s-rk}}\big(\underline{\varphi}, \underline{\varphi}'\big) = w_{\text{s-rk}}\big(\underline{\varphi} - \underline{\varphi}'\big)$.

Furthermore, codes C sitting inside $\mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K)$ are naturally endowed with a notion of length and a notion of dimension:

$$\begin{aligned}\mathrm{length}(C) &= \dim_K \big(\mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K)\big) = \dim_F V_1 + \cdots + \dim_F V_m,\\ \dim(C) &= \dim_K C.\end{aligned}$$

In the sequel, we will use the shorter notation $\dim \underline{V}$ to denote the sum $\dim_F V_1 + \cdots + \dim_F V_m$.

Theorem 3.1.8. *Let k and m be positive integers. Let $\underline{c} = (c_1, \ldots, c_m)$ be a tuple of nonzero elements of K and let $\underline{V} = (V_1, \ldots, V_m)$ be a tuple of F-linear subspaces of K. We set $n = \dim \underline{V}$ and assume $k \leq n$. We assume further that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct. Then:*

- *the length of $\mathrm{LRS}(k, \underline{c}, \underline{V})$ is n,*
- *the dimension of $\mathrm{LRS}(k, \underline{c}, \underline{V})$ is k,*
- *the minimal sum-rank distance of $\mathrm{LRS}(k, \underline{c}, \underline{V})$ is $d = n - k + 1$.*

Proof. The assertion on the length is obvious. The two other assertions follow from Proposition 1.3.7. □

3.2 Linearized Goppa codes

As before, we consider a field K equipped with an automorphism $\theta : K \to K$ of finite order. We denote by r the order of θ. We set $F = K^{\theta=1}$. As in §1, we put $Y = X^r$ and define $\mathcal{A}^+ = K[X; \theta]$, $\mathcal{C}^+ = K[Y]$, $\mathcal{Z}^+ = F[Y]$ and $\mathcal{A} = K[X^{\pm 1}; \theta]$, $\mathcal{C} = K[Y^{\pm 1}]$, $\mathcal{Z} = F[Y^{\pm 1}]$. We recall that $\mathcal{Z}^+$ (resp. $\mathcal{Z}$) is the centre of $\mathcal{A}^+$ (resp. $\mathcal{A}$). We shall also work with the field of fractions of $\mathcal{A}$, denoted by $\mathrm{Frac}(\mathcal{A})$. We recall that $\mathrm{Frac}(\mathcal{A}) = \mathrm{Frac}(\mathcal{Z}) \otimes_{\mathcal{Z}} \mathcal{A}$ by Theorem 1.1.4.

3.2.1 Definition

We fix a positive integer m. Let $\underline{c} = (c_1, \ldots, c_m)$ be a tuple of nonzero elements of K and let $\underline{V} = (V_1, \ldots, V_m)$ be a tuple of F-linear subspaces of K. For each i, we set $z_i = \mathrm{N}_{K/F}(c_i)$. From now on, *we assume that the z_i's are pairwise distinct.* We define $N_i = Y - z_i \in \mathcal{Z}^+$ and $N = N_1 N_2 \cdots N_m$. We also set:

$$n \;=\; \mathrm{codim}_F V_1 + \cdots + \mathrm{codim}_F V_m \;=\; mr - \dim \underline{V}.$$

Lemma 3.2.1. *With the previous notations, there exists a unique monic skew polynomial $D \in \mathcal{A}^+$ of degree n such that $\mathrm{im}\, \varepsilon_{c_i}(D) = V_i$ for all $i \in \{1, \ldots, m\}$. Moreover D divides N.*

Proof. It is similar to that of Proposition 1.3.4, except that we have to consider right ideals instead of left ideals. We consider the morphism of K-algebras:

$$\begin{array}{rccc}\varepsilon : & \mathcal{A} & \longrightarrow & \mathrm{End}_F(K)^m\\ & f & \mapsto & \big(\varepsilon_{c_i}(f), \ldots, \varepsilon_{c_m}(f)\big).\end{array}$$

The fact that the z_i's are pairwise distinct implies that ε is surjective (see the proof of Proposition 1.3.4). Let I be the right ideal of $\mathrm{End}_F(K)^m$ consisting of elements $\underline{\varphi} = (\varphi_1, \ldots, \varphi_m)$ for which $\mathrm{im}\, \varphi_i \subset V_i$ for all i. The inverse image of I by ε is a right ideal of $\mathcal{A}$ and thus is of the form $D\mathcal{A}$ for some monic skew polynomial $D \in \mathcal{A}^+$. Moreover:

$$\begin{aligned}r \cdot \deg D &= \dim_F \big(\mathcal{A}/D\mathcal{A}\big) = \dim_F \big(\mathcal{A}/\varepsilon^{-1}(I)\big)\\ &= \dim_F \big(\mathrm{End}_F(K)^m / I\big) = r \cdot n.\end{aligned}$$

Thus D has degree n. From $D \in \varepsilon^{-1}(I)$, we immediately deduce that $\mathrm{im}\, \varepsilon_{c_i}(D) \subset V_i$ for all index i. If one of these inclusions were strict, we would deduce that:

$$\sum_{i=1}^{m} \dim_F \ker \varepsilon_{c_i}(D) > mr - \sum_{i=1}^{m} \dim V_i = n = \deg D$$

contradicting Proposition 1.3.4. We conclude that $\mathrm{im}\, \varepsilon_{c_i}(D) = V_i$ for all i. Finally, the fact that D divides N follows from the observation that N lies in $\varepsilon^{-1}(I)$. □

In what follows, the letter D will always refer to the skew polynomial of Lemma 3.2.1. The linearized Goppa codes we are going to construct will be defined by taking skew residues of rational functions in $\mathcal{A}\,D^{-1} \subset \mathrm{Frac}(\mathcal{A})$ at the z_i's (see Definition 2.3.1). We recall that the skew residue of f at z_i is an element of $\mathcal{A}/N_i\mathcal{A}$ which is denoted by $\mathrm{sres}_{z_i}(f)$. Since the evaluation map ε_{c_i} factors through the quotient $\mathcal{A}/N_i\mathcal{A}$, it makes sense to consider $\varepsilon_{c_i}\big(\mathrm{sres}_{z_i}(f)\big)$ which is, by definition, a F-linear endomorphism of K.

Lemma 3.2.2. *Let $f \in \mathcal{A}\,D^{-1}$. For all index $i \in \{1, \dots, m\}$, f has at most a simple pole at z_i and $\varepsilon_{c_i}\big(\mathrm{sres}_{z_i}(f)\big)$ vanishes on V_i.*

Remark 3.2.3. The fact that f has at most a simple pole at z_i ensures that the skew residue $\mathrm{sres}_{z_i}(f)$ is defined without ambiguity and is simply equal to the image of $N_i f$ in the quotient ring $\mathcal{A}/N_i\mathcal{A}$.

Proof of Lemma 3.2.2. Let us write $f = gD^{-1}$ with $g \in \mathcal{A}$. On the other hand, by Lemma 3.2.1, we know that we can write $N = D'D$ for some $D' \in \mathcal{A}^+$. Thus $D^{-1} = D'N^{-1}$ and so $f = gD'N^{-1}$. The fact that f has a at most a simple pole at z_i follows from the latter equality since N itself has a simple pole at z_i. Furthermore, if $\hat{N}_i$ denotes the inverse of $N/N_i = N_1 \cdots N_{i-1}N_{i+1} \cdots N_m$ in $\mathcal{Z}/N_i\mathcal{Z} \subset \mathcal{A}/N_i\mathcal{A}$, we find that $\mathrm{sres}_{z_i}(f)$ is the image of $g\hat{N}_i D'$ in $\mathcal{A}/N_i\mathcal{A}$. Applying ε_{c_i}, we obtain:

$$\varepsilon_{c_i}\big(\mathrm{sres}_{z_i}(f)\big) = \varepsilon_{c_i}(g\hat{N}_i) \circ \varepsilon_{c_i}(D').$$

It is then enough to justify that $\varepsilon_{c_i}(D')$ vanishes on V_i. For this, we simply observe that the equality $D'D = N$ implies $\varepsilon_{c_i}(D') \circ \varepsilon_{c_i}(D) = 0$ and then $\ker \varepsilon_{c_i}(D') \supset \mathrm{im}\, \varepsilon_{c_i}(D) = V_i$. □

Lemma 3.2.2 shows that the mapping:

$$\begin{array}{rccl} \gamma_{\underline{c},\underline{V}}: & \mathcal{A}\,D^{-1} & \longrightarrow & \mathrm{Hom}_F(K/V_1, K) \times \cdots \mathrm{Hom}_F(K/V_m, K) \\ & f & \mapsto & \big(\varepsilon_{c_1}(\mathrm{sres}_{z_1}(f)),\ \dots,\ \varepsilon_{c_m}(\mathrm{sres}_{z_m}(f))\big). \end{array}$$

is well-defined. It is K-linear as the functions sres_{z_i} and ε_{c_i} are for all i. Moreover, the notion of sum-rank distance makes sense on the codomain of $\gamma_{\underline{c},\underline{V}}$; according to Definition 3.1.7, if we are given F-linear functions $\varphi_i : K/V_i \to K$, the sum-rank weight of the tuple $\underline{\varphi} = (\varphi_1, \dots, \varphi_m)$ is defined by:

$$w_{\text{s-rk}}\big((\varphi_1, \dots, \varphi_m)\big) = \mathrm{rank}(\varphi_1) + \cdots + \mathrm{rank}(\varphi_m).$$

Similarly, there is no problem for extending the notions of length and dimension for codes sitting in $\mathrm{Hom}_F(K/V_1, K) \times \cdots \mathrm{Hom}_F(K/V_m, K)$. If C is such a code, its length is n by definition and its dimension is $\dim_K C$. We are now ready to define our version of linearized Goppa and describe its parameters.

Definition 3.2.4. Keeping the above notations, we set:

$$\begin{aligned} \mathrm{LG}(k, \underline{c}, \underline{V}) &= \gamma_{\underline{c},\underline{V}}\big(\mathcal{A}_{[n-k,n)}\, Y^{-m-1}D^{-1}\big) \\ &= \Big\{ \big(\varepsilon_{c_1}(\mathrm{sres}_{z_1}(f)),\ \dots,\ \varepsilon_{c_m}(\mathrm{sres}_{z_m}(f))\big) \text{ with } f \in \mathcal{A}_{[n-k,n)}\, Y^{-m-1}D^{-1} \Big\} \\ &\subset \mathrm{Hom}_F(K/V_1, K) \times \cdots \times \mathrm{Hom}_F(K/V_m, K) \end{aligned}$$

where $\mathcal{A}_{[n-k,n)}$ is the set of skew polynomials of the form $\sum_{i=n-k}^{n-1} a_i X^i$.

Remark 3.2.5. In [29], Wang already proposed a definition for linearized Goppa codes in the framework of Gabidulin codes, that is with linearized polynomials over finite fields. Her construction does not make use of residues but follows the very first definition of Goppa codes. After rewriting it with the notations of this paper, it reads:

$$\mathrm{LG}_{\mathrm{Wang}}(\underline{c}, L) = \left\{ (a_1, \dots, a_n) \in k^n \quad \text{s.t.} \quad \sum_{i=1}^{n} (X - c_i)^{-1}\, a_i \equiv 0 \pmod{L} \right\}$$

where k is an intermediate extension between F and K, $\underline{c} = (c_1, \dots, c_n)$ is a tuple of elements of K of norm 1 (satisfying some additional conditions) and L is a skew polynomial which is coprime with each $X - c_i$. Wang's linearized Goppa codes are not directly related to ours. However, up to some normalization factors, both constructions should appear as special cases of the notion of "linearized geometric alternant Goppa codes", which still needs to be defined.

3.2.2 Comparison with linearized Goppa codes and consequences

As before, we set $N_i = Y - z_i$ and $N = \prod_{i=1}^m N_i \in \mathcal{Z}^+$. As in the proof of Lemma 3.2.2, we consider the skew polynomial D' defined by $D'D = N$ and, for each index i, the polynomial $\hat{N}_i$ defined as the multiplicative inverse of N/N_i in $\mathcal{Z}/N_i\mathcal{Z} \subset \mathcal{A}/N_i\mathcal{A}$. Noticing that $\mathcal{Z}/N_i\mathcal{Z}$ is canonically isomorphic to F, we easily find that:

$$\hat{N}_i = \prod_{j \neq i} (z_i - z_j)^{-1} \in F.$$

We now consider the morphism:

$$\begin{aligned}\hat{\tau}_i &= \varepsilon_{c_i}\big(X^{n-k}Y^{-m-1}D^{-1}\big) = \varepsilon_{c_i}\big(X^{n-k}Y^{-m-1}D'\hat{N}_i\big) \\ &= z_i^{-m-1} \cdot \prod_{j \neq i} (z_i - z_j)^{-1} \cdot \varepsilon_{c_i}\big(X^{n-k}D'\big).\end{aligned}$$

From the relation $D'D = N$, we deduce that $\varepsilon_{c_i}(D')$ vanishes on V_i. Therefore $\hat{\tau}_i$ vanishes on V_i as well and it then induces a F-linear mapping $\tau_i : K/V_i \to W_i$ where $W_i = \operatorname{im} \hat{\tau}_i$.

Lemma 3.2.6. *For all $i \in \{1, \dots, m\}$, the morphism τ_i is an isomorphism.*

Proof. We have to show that $\ker \hat{\tau}_i = V_i$. Since X^{n-k} is invertible in $\mathcal{A}/N_i\mathcal{A}$, it is enough to prove that $\ker \varepsilon_{c_i}(D') = V_i$. The inclusion $V_i \subset \ker \varepsilon_{c_i}(D')$ has been already noticed. On the other hand, we have the following dimension inequality:

$$\sum_{i=1}^m \dim_F \ker \varepsilon_{c_i}(D') \leq \deg D' = \deg N - \deg D = mr - n = \sum_{i=1}^m \dim_F V_i.$$

Putting these inputs together, we obtain the lemma. □

We now define:

$$\begin{array}{rcl}\Psi : \operatorname{Hom}_F(W_1, K) \times \cdots \times \operatorname{Hom}_F(W_m, K) & \longrightarrow & \operatorname{Hom}_F(K/V_1, K) \times \cdots \times \operatorname{Hom}_F(K/V_m, K) \\ (\varphi_1, \dots, \varphi_m) & \mapsto & (\varphi_1 \circ \tau_1, \dots, \varphi_m \circ \tau_m)\end{array}$$

Given that the τ_i's are all isomorphisms, we deduce that Ψ itself is an isomorphism, its inverse being given by the explicit formula $\Psi^{-1}(\psi_1, \dots, \psi_m) = (\psi_1 \circ \tau_1^{-1}, \dots, \psi_m \circ \tau_m^{-1})$. Moreover, since composing by an isomorphism obviously preserves the rank, Ψ preserves the sum-rank weight and the sum-rank distance: for all $\underline{\varphi} \in \operatorname{Hom}_F(W_1, K) \times \cdots \times \operatorname{Hom}_F(W_m, K)$, we have $w_{\text{s-rk}}\big(\Psi(\underline{\varphi})\big) = w_{\text{s-rk}}\big(\underline{\varphi}\big)$.

Proposition 3.2.7. *With the above notations and letting $\underline{W} = (W_1, \dots, W_m)$, the mapping Ψ induces an isomorphism of codes* $\mathrm{LRS}(k, \underline{c}, \underline{W}) \simeq \mathrm{LG}(k, \underline{c}, \underline{V})$.

Proof. This follows from the relation (already observed in the proof of Lemma 3.2.2):

$$\varepsilon_{c_i}\big(\operatorname{sres}_{z_i}(f)\big) = \varepsilon_{c_i}(g) \circ \varepsilon_{c_i}\big(X^{n-k}Y^{-m-1}D^{-1}\big) = \varepsilon_{c_i}(g) \circ \hat{\tau}_i$$

when $f = gX^{n-k}Y^{-m-1}D^{-1}$. □

Theorem 3.2.8. *Let k and m be positive integers. Let $\underline{c} = (c_1, \dots, c_m)$ be a tuple of nonzero elements of K and let $\underline{V} = (V_1, \dots, V_m)$ be a tuple of F-linear subspaces of K. We set $n = mr - \dim \underline{V}$ and assume $k \leq n$. We assume further that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct. Then:*

- *the length of* $\mathrm{LG}(k, \underline{c}, \underline{V})$ *is n,*
- *the dimension of* $\mathrm{LG}(k, \underline{c}, \underline{V})$ *is k,*
- *the minimal sum-rank distance of* $\mathrm{LG}(k, \underline{c}, \underline{V})$ *is $d = n - k + 1$.*

Proof. It is a direct consequence of Proposition 3.2.7 and Theorem 3.1.8. □

3.2.3 A theorem of duality

We aim at proving that linearized Reed–Solomon codes are duals of linearized Goppa codes and *vice versa*. In order to do so, we first need to define a pairing between the spaces in which these codes live. For this, we begin by equipping K with its canonical pairing:

$$\langle x, y\rangle_K = \mathrm{Tr}_{K/F}(xy) \qquad (x, y \in K).$$

If V is a F-linear subspace of K, we denote by $V^\perp$ its orthogonal; we recall that it consists of all vectors $x \in K$ for which $\langle x, y\rangle_K = 0$ for all $y \in V$. If $\varphi : K \to K$ is a F-linear mapping, we denote by $\varphi^\star$ its adjoint; we recall that it is defined by the identity $\langle \varphi^\star(x), y\rangle_K = \langle x, \varphi(y)\rangle_K$ for $x, y \in K$. It is well-known that $\ker \varphi^\star = (\mathrm{im}\,\varphi)^\perp$ and, similarly, $\mathrm{im}\,\varphi^\star = (\ker\varphi)^\perp$. It follows from these equalities that φ vanishes on some F-linear subspace V of K if and only if $\varphi^\star$ takes its values in $V^\perp$. In other words, the adjoint construction $\varphi \mapsto \varphi^\star$ induces a F-linear bijection $\mathrm{Hom}_F(K/V, K) \xrightarrow{\sim} \mathrm{Hom}(K, V^\perp)$.

Lemma 3.2.9. *Let V be a F-linear subspace of K. The bilinear mapping:*

$$\begin{array}{rcl} \mathrm{Hom}_F(K/V, K) \times \mathrm{Hom}_F(V^\perp, K) & \longrightarrow & F \\ (\varphi, \psi) & \mapsto & \mathrm{Tr}(\varphi^\star\psi) \end{array}$$

is a perfect pairing.

Proof. Since $\mathrm{Hom}_F(K/V, K)$ and $\mathrm{Hom}_F(V^\perp, K)$ have the same dimension over F, it is enough to check the following property: if $\psi \in \mathrm{Hom}_F(V^\perp, K)$ verifies $\mathrm{Tr}(\varphi^\star\psi)$ for all $\varphi \in \mathrm{Hom}_F(K/V, K)$, then $\psi = 0$. Since the adjoint realizes a bijection between $\mathrm{Hom}_F(K/V, K)$ and $\mathrm{Hom}(K, V^\perp)$, it is enough to prove that $\psi = 0$ assuming that $\mathrm{Tr}(\varphi\psi) = 0$ for all $\varphi \in \mathrm{Hom}_F(K, V^\perp)$. Considering F-basis of $V^\perp$ and K, we are reduced to check that a matrix $M \in F^{r\times d}$ (with $d = \dim V^\perp$) necessarily vanishes if it satisfies $\mathrm{Tr}(NM) = 0$ for all $N \in F^{d\times r}$. This follows from the observation that $\mathrm{Tr}(NM)$ is the (i, j) entry of M when N is the matrix with all entries set to 0, except the one in position (j, i) which is set to 1. □

It follows from Lemma 3.2.9 that the spaces

$$\begin{array}{rl} & \mathrm{Hom}_F(K/V_1, K) \times \mathrm{Hom}_F(K/V_2, K) \times \cdots \times \mathrm{Hom}_F(K/V_m, K) \\ \text{and} & \mathrm{Hom}_F(V_1^\perp, K) \times \mathrm{Hom}_F(V_2^\perp, K) \times \cdots \times \mathrm{Hom}_F(V_m^\perp, K) \end{array}$$

are dual to each other, a pairing between them being given by $\langle \underline{\varphi}, \underline{\psi}\rangle = \sum_{i=1}^m \mathrm{Tr}(\varphi_i^\star\psi_i)$ with $\underline{\varphi} = (\varphi_1, \ldots, \varphi_m)$ and $\underline{\psi} = (\psi_1, \ldots, \psi_m)$. If C is a subspace of one these spaces, we denote by $C^\perp$ its orthogonal in the dual space.

Theorem 3.2.10. *Let k and m be positive integers. Let $\underline{c} = (c_1, \ldots, c_m)$ be a tuple of nonzero elements of K and let $\underline{V} = (V_1, \ldots, V_m)$ be a tuple of F-linear subspaces of K. We set $n = \dim \underline{V}$ and assume $k \le n$. We assume further that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct. Then:*

$$\mathrm{LRS}\big(k, (c_1, \ldots, c_m), (V_1, \ldots, V_m)\big)^\perp = \mathrm{LG}\big(n{-}k, (c_1^{-1}, \ldots, c_m^{-1}), (V_1^\perp, \ldots, V_m^\perp)\big).$$

Proof. To simplify notations, we write $\underline{c} = (c_1, \ldots, c_m)$, $\underline{V} = (V_1, \ldots, V_m)$, $\underline{c}^{-1} = (c_1^{-1}, \ldots, c_m^{-1})$ and $\underline{V}^\perp = (V_1^\perp, \ldots, V_m^\perp)$. We also define $z_i = \mathrm{N}_{K/F}(c_i)$. Since the dimensions of $\mathrm{LRS}(k, \underline{c}, \underline{V})$ and $\mathrm{LG}(n{-}k, \underline{c}^{-1}, \underline{V}^\perp)$ sum up to the dimension of the ambiant space, that is n, it is enough to prove that $\langle \underline{\varphi}, \underline{\psi}\rangle = 0$ for all $\underline{\varphi} \in \mathrm{LRS}(k, \underline{c}, \underline{V})$ and all $\underline{\psi} \in \mathrm{LG}(n{-}k, \underline{c}^{-1}, \underline{V}^\perp)$. Set $\gamma = \gamma_{\underline{c}^{-1}, \underline{V}^\perp}$ and similarly define:

$$\begin{array}{rcccl} \rho : & \mathcal{A} & \longrightarrow & \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ & g & \mapsto & \big(\varepsilon_{c_1}(g), \ldots, \varepsilon_{c_m}(g)\big). \end{array}$$

We have to prove that $\langle \gamma(f), \rho(g)\rangle$ vanishes whenever $f \in \mathcal{A}_{[n-k,n)}Y^{-m-1}D^{-1}$ and $g \in \mathcal{A}_{[0,k)}$ where D is the skew polynomial associated to $\underline{c}^{-1}$ and $\underline{V}^\perp$ by Lemma 3.2.1. We consider f and g

as above and compute:

$$\begin{aligned}\langle \gamma(f), \rho(g)\rangle &= \sum_{i=1}^{m} \mathrm{Tr}\big(\gamma(f)^\star \circ \rho(g)\big) \\ &= \sum_{i=1}^{m} \mathrm{Tr}\big(\varepsilon_{c_i^{-1}}(\mathrm{sres}_{z_i^{-1}}(f))^\star \circ \varepsilon_{c_i}(g)\big). \end{aligned} \tag{39}$$

By Proposition 1.4.4, the adjoint of $\varepsilon_{c_i^{-1}}(\mathrm{sres}_{z_i^{-1}}(f))$ is $\varepsilon_{c_i}(\mathrm{sres}_{z_i^{-1}}(f)^\star)$, which is itself equal to $\varepsilon_{c_i}(\mathrm{sres}_{z_i}(-Y^{-2}f^\star))$ by Theorem 2.3.9 (applied with $-Y^2 f$). Plugging this input in (39), we obtain:

$$\begin{aligned}\langle \gamma(f), \rho(g)\rangle &= -\sum_{i=1}^{m} \mathrm{Tr}\big(\varepsilon_{c_i}(\mathrm{sres}_{z_i}(Y^{-2}f^\star)) \circ \varepsilon_{c_i}(g)\big) \\ &= -\sum_{i=1}^{m} \mathrm{Tr}\big(\varepsilon_{c_i}(\mathrm{sres}_{z_i}(Y^{-2}f^\star)\cdot g)\big) \\ &= -\sum_{i=1}^{m} \mathrm{Tr}\big(\varepsilon_{c_i}(\mathrm{sres}_{z_i}(Y^{-2}f^\star g))\big) \end{aligned}$$

the last equality being true because f has at most a simple pole at z_i and g has no pole at z_i. By Proposition 1.3.15, the above expression reduces to:

$$\langle \gamma(f), \rho(g)\rangle = -\sum_{i=1}^{m} \mathrm{T}_{\mathrm{rd}}\big(\mathrm{sres}_{z_i}(Y^{-2}f^\star g)\big).$$

Noticing that $\mathrm{T}_{\mathrm{rd}} \circ \mathrm{sres}_{z_i} = \mathrm{Tr}_{K/F} \circ \sigma_0 \circ \mathrm{sres}_{z_i} = \mathrm{Tr}_{K/F} \circ \mathrm{sres}_{z_i,0}$ (see Definition 2.3.1), we end up with:

$$\langle \gamma(f), \rho(g)\rangle = -\mathrm{Tr}_{K/F}\left(\sum_{i=1}^{m} \mathrm{sres}_{z_i,0}(Y^{-2}f^\star g)\right). \tag{40}$$

Let us now write $f = f_0 Y^{-m-1} D^{-1}$ with $f_0 \in \mathcal{A}_{[n-k,n)}$ and consider $D' \in \mathcal{A}^+$ such that $D'D = N$ with $N = \prod_{i=1}^{m}\big(Y - z_i^{-1}\big)$. We have $\deg D' = mr - \deg D = mr - n$ and $D^{-1} = D'N^{-1}$. Hence:

$$Y^{-2}f^\star g = \frac{(D')^\star \cdot Y^{m-1} \cdot X^{-k} \cdot f_0^\star \cdot g}{N^\star}$$

and a simple computation shows that the numerator only has terms in X^i for i in the range $(-r, (m-1)r)$. We deduce that $\mathrm{sres}_{0,0}(Y^{-2}f^\star g) = \mathrm{sres}_{\infty,0}(Y^{-2}f^\star g) = 0$ (see Definition 2.3.2 for the definition of skew residues at 0 and ∞). By the residue formula (see Theorem 2.3.6), it follows that:

$$\sum_{i=1}^{m} \mathrm{sres}_{z_i,0}(Y^{-2}f^\star g) = 0.$$

Plugging this in Eq. (40), we finally obtain $\langle \gamma(f), \rho(g)\rangle = 0$ as wanted. □

Remark 3.2.11. In [21, Theorem 4], Martínez-Peñas and Kschischang proved that the duals of certain linearized Reed–Solomon codes remains linearized Reed–Solomon. Our theorem, combined with Proposition 3.2.7 extends this result to all linearized Reed–Solomon codes considered in this article.

3.3 Encoding and decoding algorithms

The aim of this subsection is to design fast algorithms for encoding and decoding linearized Reed–Solomon codes and linearized Goppa codes. Throughout this subsection, we will estimate the efficiency of our algorithms by evaluating their *algebraic complexity*, that is the number of operations in F they perform. In what follows, we will often use the soft-O notation $\tilde{O}(\cdot)$. We recall that, by definition, $\tilde{O}(u_n)$ refers to any sequence who absolute value is bounded by $C\cdot|u_n|\cdot\log^k(1+|u_n|)$ for some constants C and k. Throughout this subsection, we make the following assumption.

Hypothesis 3.3.1. All algebraic operations (addition, subtraction, multiplication, division) in K and all applications of θ cost $\tilde{O}(r)$ operations in F.

By the results of [6], Hypothesis 3.3.1 is fulfilled when K is a finite field. Exhibiting an explicit normal basis, one shows that it is also fulfilled when K/F is cyclotomic or a Kummer extension.

We also consider also a feasible exponent ω for matrix multiplication, that is a real number ω for which there exists an algorithm that performs multiplications of square $n \times n$ matrices over F within $O(n^\omega)$ operations in F. It is well known that Strassen's algorithm leads to $\omega = \log_2 7 \approx 2.807$ (this is better than 3, which is the exponent given by the naive multiplication algorithm). Nowadays, the best known value is due to Le Gall [18] and is about 2.373.

3.3.1 Algorithms for skew polynomials

The algorithms we are going to describe will mostly rely on the algorithms for manipulating skew polynomials designed in [4]. Below, we briefly review the results of *loc. cit.* we will need and complete some of them. The first important tool for us is an algorithm for computing the evaluation morphisms ε_c. Remember that the codomain of ε_c is $\mathrm{End}_F(K)$. In practice, we shall represent this space as the matrix algebra $F^{r\times r}$ after the choice of a F-basis of K.

Theorem 3.3.2. *We assume Hypothesis 3.3.1. There exists an algorithm* `MatrixEvaluation` *which takes as input a scalar $c \in K$, $c \neq 0$ and a skew polynomial $f \in \mathcal{A}^+$ of degree at most r and outputs $\varepsilon_c(f)$ for a cost of $\tilde{O}(r^\omega)$ operations in F.*

Proof. See the proof of Corollary 2.2 of [4]. □

For the applications we have in mind, we shall need a refinement of Theorem 3.3.2 allowing for multiple evaluation points.

Theorem 3.3.3. *We assume Hypothesis 3.3.1. There exists an algorithm* `MatrixMultiEvaluation` *which takes as input a tuple $\underline{c} = (c_1, \ldots, c_m)$ of nonzero elements of K, together with a skew polynomial $f \in \mathcal{A}^+$ of degree at most d and outputs $\varepsilon_c(f)$ for a cost of $\tilde{O}(dr + mr^\omega)$ operations in F.*

Proof. Of course, the rough idea is to call repeatedly *MatrixEvaluation*. However, in order to reach the announced complexity, we need some preparation. Set $z_i = \mathrm{N}_{K/F}(c_i)$ and $N_i = Y - z_i \in \mathcal{Z}^+$. We first aim at computing the reduction of f modulo the N_i's. For this, we recall from Lemma 1.2.8 that f decomposes as a sum:

$$f = \sigma_0(f) + \sigma_1(f)X + \cdots + \sigma_{r-1}(f)X^{r-1} \tag{41}$$

where $\sigma_j : \mathcal{A} \to \mathcal{C}$ denotes the j-th section operator. Reducing Eq. (41) modulo N_i, we get:

$$f \equiv \sigma_0(f)_{|Y=z_i} + \sigma_1(f)_{|Y=z_i}X + \cdots + \sigma_{r-1}(f)_{|Y=z_i}X^{r-1} \pmod{N_i}.$$

Computing the reduction of f modulo the N_i's then reduces to evaluating the *commutative* polynomials $\sigma_j(f)$ at z_i. By the algorithms of [22, §10.1], for a fixed index j, all the $\sigma_0(f)_{|Y=z_i}$'s (for i varying in $i \in \{1, \ldots, m\}$) can be computed within $\tilde{O}(m + \deg_Y \sigma_0(f))$ operations in K. This complexity corresponds to $\tilde{O}(mr + d)$ operations in F, noticing that $r \cdot \deg_Y \sigma_j(f) \leq \deg f \leq d$. Letting now j vary between 0 and $r-1$, we find that we can compute the reduction of f modulo all the N_i's for a cost of $\tilde{O}(mr^2 + dr)$ operations in F.

For each $i \in \{1, \ldots, m\}$, we now call the algorithm `MatrixEvaluation` with input c_i and the reduction of f modulo N_i we just computed. By Theorem 3.3.2, each call costs $\tilde{O}(r^\omega)$ operations in F. The total cost of this step is then $\tilde{O}(mr^\omega)$. All in all, we find that the total cost of our algorithm is within $\tilde{O}(dr + mr^\omega)$. □

Remark 3.3.4. The complexity of `MatrixEvaluation` and `MatrixMultiEvaluation` can be reduced to $\tilde{O}(r^2)$ and $\tilde{O}(dr + mr^2)$ respectively when K is equipped with a normal basis.

The main result of [4] is a fast algorithm for multiplying skew polynomials. In order to state the associated complexity result, we introduce the bivariate function SM defined by:

$$\begin{aligned} \mathrm{SM}(d, r) &= d^{(\omega+1)/2}r && \text{for } d \leq r^{(5-\omega)/2} \\ &= d^{\omega-2}r^2 && \text{for } r^{(5-\omega)/2} \leq d \leq r \\ &= dr^{\omega-1} && \text{for } d \geq r. \end{aligned}$$

Theorem 3.3.5. *We assume Hypothesis 3.3.1. There exists an algorithm* `SkewMultiplication` *which takes as input two skew polynomials $f, g \in \mathcal{A}^+$ of degree at most d and outputs the product fg for a cost of $\tilde{O}(\mathrm{SM}(d,r))$ operations in F.*

Adapting standard techniques coming from the classical commutative case, one derives efficient algorithms for performing many operations on skew polynomials, such as Euclidean divisions, gcd and lcm computations, *etc.* In order to state the complexity results, we introduce yet another function, namely $\mathrm{SM}^{\geq 1}$, which is defined as follows:

$$\begin{aligned} \mathrm{SM}^{\geq 1}(d,r) &= d^{(\omega+1)/2} r \quad \text{for } d \leq r^{(5-\omega)/2} \\ &= d r^{4/(5-\omega)} \quad \text{for } d \geq r^{(5-\omega)/2}. \end{aligned}$$

The first result we will use frequently is the following.

Theorem 3.3.6. *We assume Hypothesis 3.3.1. There exists an algorithm* `SkewLLCM` *which takes as input a family $(f_1, \ldots, f_n)$ of skew polynomials of degree 1 and outputs $\mathrm{LLCM}(f_1, \ldots, f_n)$ for a cost of $\tilde{O}(\mathrm{SM}(n,r))$ operations in F.*

Proof. See the discussion in §3 of [4]. □

Another tool we will need is multi-evaluation and Lagrange interpolation of skew polynomials. Let $\underline{c} = (c_1, \ldots, c_n)$ be a tuple of nonzero elements of K such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct. Let also $\underline{V} = (V_1, \ldots, V_m)$ be a tuple of F-linear subspaces of K. We recall from Proposition 1.3.7 that there exists a skew polynomial P of degree $\dim \underline{V}$ for which the K-linear mapping:

$$\begin{array}{rccl} \varepsilon_{\underline{c},\underline{V}} : & \mathcal{A}^+/\mathcal{A}^+P & \xrightarrow{\sim} & \mathrm{Hom}_F(V_1,K) \times \mathrm{Hom}_F(V_2,K) \times \cdots \times \mathrm{Hom}_F(V_m,K) \\ & f & \mapsto & \big(\varepsilon_{c_1}(f)_{|V_1},\, \varepsilon_{c_2}(f)_{|V_2},\, \ldots,\, \varepsilon_{c_m}(f)_{|V_m}\big). \end{array}$$

is an isomorphism. The purpose of multi-evaluation (resp. Lagrange interpolation) is to compute efficiently $\varepsilon_{\underline{c},\underline{V}}$ (resp. its inverse).

Theorem 3.3.7. *We assume Hypothesis 3.3.1.*

(i) There exists an algorithm `SkewMultiEvaluation` *which takes as input two tuples $\underline{c}$ and $\underline{V}$ as above and a skew polynomial $f \in \mathcal{A}^+$ of degree at most d and outputs $\varepsilon_{\underline{c},\underline{V}}(f)$ for a cost of $\tilde{O}\big(\mathrm{SM}^{\geq 1}(\max(d, \dim \underline{V}),\, r)\big)$ operations in F.*

(ii) There exists an algorithm `SkewInterpolation` *which takes as input two tuples $\underline{c}$ and $\underline{V}$ as above and an element $\underline{\varphi} \in \mathrm{Hom}_F(V_1,K) \times \mathrm{Hom}_F(V_2,K) \times \cdots \times \mathrm{Hom}_F(V_m,K)$ and outputs $\varepsilon^{-1}_{\underline{c},\underline{V}}(\underline{\varphi})$ for a cost of $\tilde{O}\big(\mathrm{SM}^{\geq 1}(\dim \underline{V}, r)\big)$ operations in F.*

Proof. For each index $i \in \{1, \ldots, m\}$, we set $d_i = \dim_F V_i$ and we choose a basis $u_{i,1}, \ldots, u_{i,d_i}$ of V_i. Given two nonzero elements $c, u \in K$ and $f \in \mathcal{A}^+$, we have seen in §1.3 that $u^{-1}\mathrm{ev}_c(f)(u)$ is equal to the remainder in the Euclidean division of f by $X - \frac{c\theta(u)}{u}$. This observation shows that $\varepsilon_{\underline{c},\underline{V}}(f) = (\varphi_1, \ldots, \varphi_m)$ if and only if:

$$f \equiv u_{i,j}\, \varphi_i(u_{i,j}) \pmod{L_{i,j}} \quad \text{with} \quad L_{i,j} = X - \frac{c_i\, \theta(u_{i,j})}{u_{i,j}} \tag{42}$$

for (i,j) varying in $\mathcal{I} = \{(i,j) \text{ s.t. } 1 \leq i \leq m \text{ and } 1 \leq j \leq d_i\}$. If I is a subset of $\mathcal{I}$, let L_I denote the LLCM of the $L_{i,j}$'s for (i,j) varying in I. Clearly $\deg L_I \leq \mathrm{Card}\, I$. Besides, the injectivity of $\varepsilon_{\underline{c},\underline{V}}$ implies $P = L_{\mathcal{I}}$, and so $\deg L_{\mathcal{I}} = \dim \underline{V} = \mathrm{Card}\, \mathcal{I}$. We deduce that $\deg L_I = \mathrm{Card}\, I$ for all $I \subset \mathcal{I}$ and that $\mathrm{RGCD}(L_I, L_J) = 1$ as soon as I and J are disjoint.

By Theorem 3.3.6, one can compute $L_{\mathcal{I}}$ within $\tilde{O}\big(\mathrm{SM}^{\geq 1}(\mathrm{Card}\, \mathcal{I}, r)\big) = \mathrm{SM}^{\geq 1}(\dim \underline{V}, r)$ operations in F. Now, following [4, §3], given a skew polynomial $f \in \mathcal{A}^+$ of degree d, one can use the techniques of [22, §10.1] to compute the reduction of f modulo all the $L_{i,j}$'s for an additional cost of $\mathrm{SM}^{\geq 1}(\max(d, \dim \underline{V}), r)$ operations in F. After this computation, one can derive the value of $\varepsilon_{\underline{c},\underline{V}}(f)$ using Eq. (42) for a additional cost of $\dim \underline{V}$ divisions in K, corresponding

to $\tilde{O}(r \cdot \dim \underline{V})$ operations in F. Summing up all the contributions, we end up with an algorithm `SkewMultiEvaluation` that computes $\varepsilon_{\underline{c},\underline{V}}(f)$ for a total cost of $\tilde{O}\big(\mathrm{SM}^{\geq 1}(\max(d, \dim \underline{V}), r)\big)$ operations in F.

Conversely, we consider the equations (42) as a system of congruences with unknown f. As discussed in [4, §3], one can again adapt the methods of [22, §10.1] to solve it for a cost of $\tilde{O}\big(\mathrm{SM}^{\geq 1}(\dim \underline{V}, r)\big)$ operations in F. This gives the algorithm `SkewInterpolation`. □

3.3.2 Linearized Reed–Solomon codes

As before, we fix two positive integers m and k together with a tuple $\underline{c} = (c_1, \dots, c_m)$ of nonzero elements of K and a tuple $\underline{V} = (V_1, \dots, V_m)$ of F-linear subspaces of K. We let $n = \dim \underline{V} = \dim_F V_1 + \cdots + \dim_F V_m$ and assume that $k \leq n$. Under these hypothesis, we recall that the linearized Reed–Solomon code associated to these parameters, denoted by $\mathrm{LRS}(k, \underline{c}, \underline{V})$ is the image of the K-linear mapping:

$$\begin{array}{rccc} \rho_{k,\underline{c},\underline{V}} : & \mathcal{A}_{[0,k)} & \longrightarrow & \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ & f & \mapsto & \big(\varepsilon_{c_1}(f), \dots, \varepsilon_{c_m}(f)\big) \end{array}$$

(see Definition 3.1.6). By Theorem 3.1.8, we know that the minimal sum-rank distance of this code is $d = n - k + 1$. The encoding and decoding problems can be formulated as follows:

- The encoding problem: given $f \in \mathcal{A}_{[0,k)}$, compute $\rho_{k,\underline{c},\underline{V}}(f)$
- The decoding problem: given $\underline{\varphi} \in \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K)$, find, if it exists, the unique $f \in \mathcal{A}_{[0,k)}$ such that $d_{\text{s-rk}}\big(\underline{\varphi}, \rho_{k,\underline{c},\underline{V}}(f)\big) < \frac{d}{2}$.

These questions were actually already addressed in the literature. In a slightly different setting, Boucher designed in [1] an algorithm that solves the decoding problem. It has cubic complexity, meaning that it runs in $O(n^3)$ operations in K, which is roughly equivalent to $\tilde{O}(n^3 r)$ operations in F. Another important contribution is due to Martínez-Peñas himself, who designed in [21] a decoding algorithm for linearized Reed–Solomon codes running in quadratic complexity, that is for a cost of $\tilde{O}(n^2 r)$ operations in F. In the case of Gabidulin codes, Puchinger and Wachter-Zeh obtained in [25] the first algorithm with subquadratic complexity; it runs in $\tilde{O}(n^{(\omega+1)/2} r)$ operations in F. The algorithms we are going to design below will improve on these bounds.

Encoding algorithms. A first solution to encode a message is to rely on the algorithm `SkewMultiEvaluation` of Theorem 3.3.7. This provides directly an encoding algorithm with complexity:

$$\tilde{O}\big(\mathrm{SM}^{\geq 1}(n, r)\big) \subset \tilde{O}\big(n \cdot r^{4/(5-\omega)}\big). \tag{43}$$

Another option is to use the algorithm `MatrixMultiEvaluation` of Theorem 3.3.3. This leads to a cost of $\tilde{O}(mr^\omega)$ operations in F. Comparing with Eq. (43), we find that this second approach runs faster than the first one when the ratio $\frac{n}{m}$ (which represents the average dimension of the V_i's) exceeds $r^{\omega - \frac{4}{5-\omega}}$. In particular, if we are choosing $V_i = K$ for all i, we have $n = mr$ and our second algorithm is always at least as good as the first one.

Decoding algorithms. Linearized Reed–Solomon codes can be decoded by a noncommutative extension of Berlekamp–Welch algorithm. This fact was actually already observed in the works of Wachter-Zeh and al. [28] in the special case of usual Gabidulin codes. After what we have recalled in §3.3.1, the extension to linearized Reed–Solomon codes is not difficult.

We suppose that we are given parameters k, m, $\underline{c}$ and $\underline{V}$ as above. We set $n = \dim \underline{V}$. The minimal distance of the code $\mathrm{LRS}(k, \underline{c}, \underline{V})$ is $d = n - k + 1$ by Theorem 3.1.8. We set $w = \lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{n-k}{2} \rfloor$; it is the maximal number of errors one can correct without ambiguity. We also consider $\underline{\varphi} \in \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K)$ and assume that:

$$\underline{\varphi} = \gamma_{k,\underline{c},\underline{V}}(f) + \underline{e}$$

with $f \in \mathcal{A}_{[0,k)}$ and $w_{\text{s-rk}}(\underline{e}) \leq w$. Our objective is to recover f and $\underline{e}$ for the datum of $\underline{\varphi}$. For this, as in §3.3.1, we consider the isomorphism

$$\begin{array}{rccl} \varepsilon_{\underline{c},\underline{V}}: & \mathcal{A}^+/\mathcal{A}^+P & \xrightarrow{\sim} & \mathrm{Hom}_F(V_1,K) \times \mathrm{Hom}_F(V_2,K) \times \cdots \times \mathrm{Hom}_F(V_m,K) \\ & f & \mapsto & \big(\varepsilon_{c_1}(f)_{|V_1},\, \varepsilon_{c_2}(f)_{|V_2},\, \ldots,\, \varepsilon_{c_m}(f)_{|V_m}\big) \end{array}$$

given by Proposition 1.3.7. Moreover, after Theorem 3.3.7, we have at our disposal fast algorithms for computing $\varepsilon_{\underline{c},\underline{V}}$ and its inverse. The proof of this theorem provides in addition an explicit formula for the skew polynomial P, that is:

$$P = \operatorname{LLCM}\left(X - \frac{c_i\,\theta(u_{i,j})}{u_{i,j}}\right)_{\substack{1\leq i\leq m \\ 1\leq j\leq d_i}} \tag{44}$$

where $d_i = \dim_F V_i$ and the family $(u_{i,1}, \ldots, u_{i,d_i})$ is a F-basis of V_i.

Our algorithm proceeds in several steps.

Step 0: Annihilator. We compute the skew polynomial P defined by Eq. (44). We observe that this step is independent of $\underline{\varphi}$; it can the be precomputed once for all when the code is designed.

Step 1: Interpolation. We compute (the representant in $\mathcal{A}^+$ of mimimal degree of) $\varepsilon^{-1}_{\underline{c},\underline{V}}(\underline{\varphi})$ and call it g.

Step 2: Partial RGCD. We compute a relation of the form $Ug + VP = R$ for skew polynomials U, V and R with $\deg U \leq w$ and $\deg R < w + k$. This relation can be computed by applying the extended Euclidean algorithm with the input (g, P) and stopping it the first time the remainder R has degree less than $w + k$.

Step 3: Left Euclidean division. We compute and output the quotient in the *left* Euclidean division of R by U.

Theorem 3.3.8. *The algorithm described above is correct and, under Hypothesis 3.3.1, it performs at most $\tilde{O}\big(\mathrm{SM}^{\geq 1}(n,r)\big)$ operations in F.*

Proof. Let us first prove correctness. It is enough to establish that $R = Uf$. We set $h = R - Uf$ and assume by contradiction that $h \neq 0$. Set $\underline{\psi} = \varepsilon_{\underline{c},\underline{V}}(h)$. We write $\underline{\psi} = (\psi_1, \ldots, \psi_m)$ and similarly $\underline{e} = (e_1, \ldots, e_m)$. Both ψ_i and e_i are then F-linear mapping $V_i \to K$. We observe that, by definition of g, the mapping $\varepsilon_{c_i}(g - f)$ coincides with e_i on V_i. Therefore, it follows from the equality $h = U \cdot (g - f) + VP$ that $\psi_i = \varepsilon_{c_i}(U) \circ e_i$ for all $i \in \{1, \ldots, m\}$. Consequently:

$$\sum_{i=1}^{m} \mathrm{rank}(\psi_i) \leq \sum_{i=1}^{m} \mathrm{rank}(e_i) = w_{\text{s-rk}}(\underline{e}) \leq w. \tag{45}$$

On the other hand, by construction, we know that $\deg R < w + k$ and $\deg(Uf) < w + k$. Hence $\deg h < w + k$ as well. From Proposition 1.3.7, we deduce that:

$$\sum_{i=1}^{m} \dim_F \ker \psi_i = \sum_{i=1}^{m} \dim_F \ker \varepsilon_{c_i}(h) \leq \deg h < w + k. \tag{46}$$

Putting together the inequalities (45) and (46), we get:

$$2w + k > \sum_{i=1}^{m} \mathrm{rank}(\psi_i) + \dim_F \ker \psi_i = \sum_{i=1}^{m} \dim_F V_i = n.$$

This is a contradiction since $w \leq \frac{n-k}{2}$ by definition.

We now move to the complexity statement. By Theorem 3.3.6, step 0 requires at most $\tilde{O}\big(\mathrm{SM}^{\geq 1}(n,r)\big)$ operations in F. By Theorem 3.3.7, step 1 can be done for a cost of $\tilde{O}\big(\mathrm{SM}^{\geq 1}(n,r)\big)$ operations in F as well. By Proposition 3.2 of [4], step 2 can be completed again with the same complexity. Finally, this is again the same for step 3 by the results of [4, §3]. Summing up all these contributions, we obtain the announced complexity. □

3.3.3 Linearized Goppa codes

We now move to linearized Goppa codes. As in §3.2, we consider a tuple $\underline{c} = (c_1, \dots, c_m)$ of nonzero elements of K, together with a tuple $\underline{V} = (V_1, \dots, V_m)$ of F-linear subspaces of K. We set:

$$n = \operatorname{codim}_F V_1 + \cdots + \operatorname{codim}_F V_m = mr - \dim \underline{V}$$

and pick an integer k in the range $[0, n]$. For each index i, we also define $z_i = \mathrm{N}_{K/F}(c_i)$ and we assume that the z_i's are pairwise distinct. We let D be the skew polynomial given by Lemma 3.2.1. By definition, the linearized Goppa code associated to these data is the image of the following mapping:

$$\begin{array}{rccl} \gamma_{k,\underline{c},\underline{V}} : & \mathcal{A}_{[n-k,n)} Y^{-m-1} D^{-1} & \longrightarrow & \operatorname{Hom}_F(K/V_1, K) \times \cdots \operatorname{Hom}_F(K/V_m, K) \\ & f & \mapsto & \big(\varepsilon_{c_1}(\operatorname{sres}_{z_1}(f)),\ \dots,\ \varepsilon_{c_m}(\operatorname{sres}_{z_m}(f))\big) \end{array}$$

(see Definition 3.2.4). As for linearized Reed–Solomon codes, the encoding and decoding problems are formulated as follows:

- The encoding problem: given $f \in \mathcal{A}_{[n-k,n)} Y^{-m-1} D^{-1}$, compute $\gamma_{k,\underline{c},\underline{V}}(f)$
- The decoding problem: given $\underline{\varphi} \in \operatorname{Hom}_F(K/V_1, K) \times \cdots \times \operatorname{Hom}_F(K/V_m, K)$, find, if it exists, the unique $f \in \mathcal{A}_{[n-k,n)} Y^{-m-1} D^{-1}$ such that $d_{\text{s-rk}}\big(\underline{\varphi}, \gamma_{k,\underline{c},\underline{V}}(f)\big) < \frac{d}{2}$.

In what follows, we will reduce the case of linearized Goppa codes to that of linearized Reed–Solomon codes using Proposition 3.2.7. In order to do so, the main point is to justify that the isomorphism Ψ that appears in this proposition is efficiently computable. Concretely, we have the following lemma.

Lemma 3.3.9. *The mappings τ_i and τ_i^{-1} defined in §3.2.2 can all be computed (for all i) for a total cost of $\tilde{O}\big(\mathrm{SM}^{\geq 1}(\dim \underline{V}, r) + mr^\omega\big)$ operations in F.*

Proof. We set $z_i = \mathrm{N}_{K/F}(c_i)$. We recall that:

$$\tau_i = z_i^{-m-1} \cdot \prod_{j \neq i} (z_i - z_j)^{-1} \cdot \varepsilon_{c_i}(X^{n-k} D')$$

where D' is defined by the identity $D'D = \prod_{i=1}^m (Y - z_i)$. Using a divide-and-conquer algorithm, computing all the prefactors (for i varying between 1 and m) can be acheived for a cost of $\tilde{O}(m)$ operations in F. Besides, we know by Lemma 3.2.6 that the kernel of $\varepsilon_{c_i}(D')$ is V_i. Since moreover $\deg D' = mr - n = \dim \underline{V}$, we find that:

$$D' = \operatorname{LLCM}\left(X - \frac{c_i\, \theta(u_{i,j})}{u_{i,j}} \right)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq d_i}}$$

where, for each i, the family $(u_{i,1}, \dots, u_{i,d_i})$ is a F-basis of V_i. By Theorem 3.3.6, D' can be computed for a cost of $\tilde{O}\big(\mathrm{SM}^{\geq 1}(\dim \underline{V}, r)\big)$ operations in F. Calling finally the algorithm `MatrixMultiEvaluation` (see Theorem 3.3.3) with the skew polynomial $X^{n-k} D'$ (which has degree at most mr) and doing standard linear algebra, we get the lemma. □

Putting all the inputs together, we end up with an encoding algorithm and a decoding algorithm that both cost at most:

$$\tilde{O}\big(\mathrm{SM}^{\geq 1}(\dim \underline{V}, r) + \mathrm{SM}^{\geq 1}(n, r)\big) \subset \tilde{O}\big(\mathrm{SM}^{\geq 1}(mr, r)\big)$$

operations in F. Moreover, we underline that the term $\mathrm{SM}^{\geq 1}(\dim \underline{V}, r)$ in the complexity corresponds to the computation of the τ_i's and their inverses, which is actually a precomputation that needs to be done only once when the code is designed. After that, each encoding and each decoding costs only $\tilde{O}\big(\mathrm{SM}^{\geq 1}(n, r)\big)$ operations in F.

References

[1] D. Boucher, *An algorithm for decoding skew Reed-Solomon codes with respect to the skew metric*, proceedings WCC 2019

[2] D. Boucher, F. Ulmer, *Coding with skew polynomial rings*, J. Symbolic Comput. **44** (2009), 1644–1656

[3] X. Caruso, J. Le Borgne, *A new faster algorithm for factoring skew polynomials over finite fields*, J. Symbolic Comput. **79** (2017), 411–443

[4] X. Caruso, J. Le Borgne, *Fast multiplication for skew polynomials*, proceedings ISSAC 2017

[5] P. M. Cohn, *Free Rings and Their Relations*, London Math. Soc. Monographs, Academic Press (1971)

[6] J.-M. Couveignes, R. Lercier, *Elliptic Periods for Finite Fields*, Finite Fields Appl., **15** (2009), 1–22

[7] P. Delsarte, *Bilinear Forms over a Finite Field with Applications to Coding Theory*, J. Combin. Theory **25** (1978), 226–241

[8] E. Gabidulin, *Theory of codes with maximum rank distance*, Problemy Peredachi Informatsii **21** (1985), no. 1, 3–16

[9] S. Ikehata, *Azumaya algebras and skew polynomial rings*, Math. J. Okayama Univ. **23** (1981), no. 1, 19–32

[10] S. Ikehata, *Azumaya algebras and skew polynomial rings. II*, Math. J. Okayama Univ. **26** (1984), 49–57

[11] N. Jacobson, *Non commutative polynomials and cyclic algebras*, Ann. of Math. **35** (1934), 197–208

[12] N. Jacobson, *Pseudo-linear transformations*, Ann. of Math. **38** (1937), 484–507

[13] N. Jacobson, *Finite-Dimensional Division Algebras Over Fields*, Grundlehren der Mathematischen Wissenschaften Series (1996), Springer

[14] T. Y. Lam, *A general theory of Vandermonde matrices*, Expos. Math. **4** (1986), 193–215

[15] T. Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Math. **189**, Springer (1999), New York

[16] T. Y. Lam, A. Leroy, *Vandermonde and Wronskian matrices over division rings*, J. Algebra **119** (1988), 308–336

[17] T. Y. Lam, A. Leroy, *Principal one-sided ideals in Ore polynomial rings*, Algebra and Its Applications, Comtemp. Math. **259** (2000), 333–352

[18] F. Le Gall, *Powers of tensors and fast matrix multiplication*, ISSAC 2014—Proceedings of the 2014 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2014, pp. 296–303

[19] S. Liu, *Generalized Skew Reed-Solomon Codes and Other Applications of Skew Polynomial Evaluation*, PhD thesis (2016), available at `https://tspace.library.utoronto.ca/bitstream/1807/73073/1/Liu_Siyu_201606_PhD_thesis.pdf`

[20] U. Martínez-Peñas, *Skew and linearized Reed–Solomon codes and maximum sum rank distance codes over any division ring*, J. Algebra **504** (2018), 587–612

[21] U. Martínez-Peñas, F. Kschischang, *Reliable and Secure Multishot Network Coding using Linearized Reed-Solomon Codes*, available at `https://arxiv.org/abs/1805.03789`

[22] J. von zur Gathen, J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, Cambridge (2003)

[23] Ø. Ore, *Linear equations in non-commutative fields*, Ann. of Math. **32** (1931), 463–477

[24] Ø. Ore, *Theory of non-commutative polynomials*, Ann. of Math. **34** (1933), 480–508

[25] S. Puchinger, A. Wachter-Zeh, *Sub-quadratic decoding of Gabidulin codes*, IEEE Int. Symp. Inf. Theory (ISIT) (2016)

[26] R. Roth, *Maximum-Rank Array Codes and their Application to Crisscross Error Correction*, IEEE Trans. Inform. Theory (1991)

[27] M. Van der Put, *Differential equations in characteristic p*, Compositio Math. **97** (1995), 227–251

[28] A. Wachter-Zeh, *Decoding of Block and Convolutional Codes in Rank Metric*, PhD Dissertation, Ulm University (2013)

[29] L.-P. Wang, *Linearized Goppa Codes*, proceedings ISIT 2018, 2496–2500