A theory of residues for skew rational functions

Xavier Caruso

October 8, 2021

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.

Contents

In 1933, Ore introduced in [23] 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 [23], Jacobson [12, 13] and more recently by Ikehata [10, 11], who proved the Ore's polynomial rings are Azumaya algebras in certains cases, by Lam and Leroy [15, 17, 18] 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 [6] or Jacobson's book [14].

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 by extending the theory of residues to the so-called *skew polynomials*, which are a particular type of Ore polynomials.

Let K be a field equipped with an automorphism θ of finite order r. We consider the ring of skew polynomials $K[X;\theta]$ in which the multiplication is governed by the rule $Xa = \theta(a)X$ for $a \in K$. The first striking result of this article is the construction of Taylor-like expansions in this framework: we show that any skew polynomial $f \in K[X;\theta]$ admits expansions of the form:

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

for any given point z in a separable closure of K. Moreover, when 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). Residues at infinity can also be defined in a similar fashion.

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:

- (*cf* Theorems 3.2.1 and 3.2.2) a residue formula, relating all the residues (at all points) of a given skew rational function,
- (*cf* Theorems 3.3.2 and 3.3.4) a formula of change of variables, expliciting how residues behave under an endomomorphism of $\mathrm{Frac}(K[X;\theta])$.

Our theory of residues has interesting applications to coding theory as it allows for a nice description of duals of linearised Reed-Solomon codes (including Gabidulin codes) which have been recently defined by Martinez-Penas [21]. This application will be discussed in a forthcoming article [5].

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. In §2, we focus on Taylor-like expansions of skew polynomials and establish the formulas (1) and (2). Finally, the theory of residues (including the residue formula and the effect under change of variables) is presented in §3.

Convention. Throughout this article, all the modules over a (not necessarily commutative) ring $\mathfrak{A}$ will always be left modules, *i.e.* additive groups equipped with a linear action of $\mathfrak{A}$ on the left. Similarly, a $\mathfrak{A}$-algebra will be a (possible noncommutative) ring $\mathfrak{B}$ equipped with a ring homomorphism $\varphi : \mathfrak{A} \to \mathfrak{B}$. In this situation, $\mathfrak{B}$ becomes equipped with a structure of (left) $\mathfrak{A}$-module defined by $a \cdot b = \varphi(a)b$ for $a \in \mathfrak{A}$, $b \in \mathfrak{B}$.

1 Preliminaries

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 are Laurent polynomials over K in the variable X and the multiplication on them 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 first review the most important algebraic properties of $\mathcal{A}^+$ and $\mathcal{A}$, following the classical references [23, 15, 17, 18, 6, 14]. We then study endomorphisms and derivations of $\mathcal{A}^+$, $\mathcal{A}$ and some of their quotients as they will play an important role in this article.

1.1 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 right and left Euclidean divisions of aX by $X - c$ (for some $a, c \in \mathbb{C}$) read:

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

Remark 1.1.3. 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 1.1.4. *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 by:

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

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.

1.2 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 [22] (see also [16, §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:

$$\begin{tikzcd} \mathcal{A} \arrow[r, "\varphi"] \arrow[d] & \mathfrak{A} \\ \mathrm{Frac}(\mathcal{A}) \arrow[ur, "\psi"'] & \end{tikzcd} \tag{5}$$

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 1.2.1. *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 1.2.2. *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. $\square$

Proof of Theorem 1.2.1. 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 1.2.2, there exists $g \in \mathcal{A}$ 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. $\square$

The notion of degree extends without 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 $\deg g - \deg D = \deg g' - \deg D'$.

1.3 Endomorphisms of Ore polynomials rings

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

1.3.1 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 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 1.3.1. *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. $\mathrm{Frac}(\mathcal{A})$).

[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 $n \in \mathbb{Z}$.

Remark 1.3.2. 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 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 1.3.1. 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 1.3.2, it is enough to check that $\gamma(f) \neq 0$ when $f \neq 0$, which can be seen by comparing degrees. $\square$

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 1.3.1 ($X \mapsto CX$). 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-algebras of $\mathrm{Frac}(\mathcal{A})$ stabilizes the centre. This property holds similarly for endomorphism of $\mathcal{A}^+$ and endomorphisms of $\mathcal{A}$.

Proposition 1.3.3. *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). $\square$

For endomorphisms of $\mathcal{A}^+$ and $\mathcal{A}$, Proposition 1.3.3 can be made more precise.

Proposition 1.3.4. *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* $\gamma_C(f) = u^{-1} f u$ *for all* $f \in \mathrm{Frac}(\mathcal{A})$.

Proof. The proof is the same as that of Proposition 1.3.3, 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 1.3.5. *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 1.3.4. 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 1.3.3) and $\gamma_C \circ \gamma_{C^{-1}} = \gamma_{C^{-1}} \circ \gamma_C = \mathrm{id}$. □

1.3.2 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 $C \in \mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{C}$. Namely, 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 1.3.6. *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* $\gamma(f) = U^{-1} f U$ *for all* $f \in \mathcal{A}/N_1\mathcal{A}$.

Proof. The proof is entirely similar to that of Theorem 1.3.1 and Proposition 1.3.3. 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 1.3.6, 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 1.3.7. *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.*

1.3.3 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 1.3.8. *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 1.3.8 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, namely:

Lemma 1.3.9. *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. $\square$

Using Lemma 1.3.9, it is possible to construct some quantities that are invariant under all γ_C, that is, after Theorem 1.3.1 or 1.3.6, 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 1.3.10. *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 1.3.6). 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 1.3.1 or 1.3.6, it is enough to prove the Proposition when $\gamma = \gamma_C$ for some C. By Lemma 1.3.9, 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 1.3.4 or Theorem 1.3.6. $\square$

1.4 Derivations over Ore polynomials rings

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 Leibniz 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.

1.4.1 Classification

As we classified endomorphisms of K-algebras in §1.3, 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 1.4.1. *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:*

$$\partial\Big(\sum_i a_i X^i\Big) = \sum_i a_i \mathrm{Tr}_i(C) X^i. \tag{9}$$

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. (9) holds.

For the converse, we first check that Eq. (9) defines a derivation on $\mathcal{A}$. In the case of $\mathrm{Frac}(\mathcal{A})$, we need to justify in addition that ∂ (given by Eq. (9)) 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. $\square$

Let $\partial_C : \mathrm{Frac}(\mathcal{A}) \to \mathrm{Frac}(\mathcal{A})$ denote the derivation of Proposition 1.4.1. 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 these rings as the derivation $\mathrm{Tr}_{\mathrm{Frac}(\mathcal{C})/\mathrm{Frac}(\mathcal{Z})}(C)\cdot Y\cdot \frac{d}{dY}$.

Proposition 1.4.2. *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). $\square$

1.4.2 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 this condition is $C = r^{-1}Y^{-1}$.

Definition 1.4.3. When p does not divide r, we set $\partial_{Y,\mathrm{can}} = \partial_{r^{-1}Y^{-1}}$. Explicitely:

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

An 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 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 1.4.4. *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 $i \in \{1, 2, \dots, p\}$, we define $C_i = \partial_C^i(X)\, X^{-1}$. A direct computation shows that:

$$C_1 = C \quad ; \quad C_{i+1} = \frac{dC_i}{dY} + C_i\, C. \tag{10}$$

In particular, we deduce that $C_i \in \mathrm{Frac}(\mathcal{C})$ for all i. We claim that C has at most a simple pole at 0. Indeed, if we assume by contradiction that C has a pole of order $v \geq 2$ at 0, we would deduce that C_i has a pole of order vi at 0 for $i \in \{1, \dots, p\}$, contradicting the fact that C_p vanishes. We can then write $C = aY^{-1} + O(1)$ with $a \in K$. The recurrence relation (10) shows that, for $i \in \{1, \dots, p\}$, we have $C_i = a_i Y^{-i} + O(Y^{-i+1})$ where the coefficients a_i's satisfy:

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

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 1.4.5. 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 [24]) to get a closed formula for C_p, which reads:

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

1.4.3 Derivations over quotients of Ore rings

Following §1.3, 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 §1.3, 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 1.4.6. *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 1.4.1 and 1.4.2. ☐

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. Besides, when r is coprime to p, we will prove that the Taylor expansion is canonical and given by a Taylor-like series involving the successive divided powers of the derivation ∂_{can}.

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:

$$\sum_{n=0}^{\infty} f^{[n]}(c)\, T^n \tag{11}$$

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:

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

We recall also that the n-th divided derivative satisfies the following Leibniz-type relation:

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

from 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. Even better, it induces an isomorphism:

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

More generally, let us consider an irreducible separable polynomial $N \in \mathcal{C}$. Let also $c \in \mathcal{C}/N\mathcal{C}$ be the image of X, which is a root of N by construction. In this generality, the Taylor expansion around c is well-defined and induces 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 Remainder 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:

$$\begin{tikzcd} \varprojlim_{m>0} \mathcal{C}/N^m\mathcal{C} \arrow[r, "\tau_N^{\mathcal{C}}"] & (\mathcal{C}/N\mathcal{C})[[T]] \\ \varprojlim_{m>0} \mathcal{Z}/N^m\mathcal{Z} \arrow[r, "\tau_N^{\mathcal{Z}}"] \arrow[u, hook] & (\mathcal{Z}/N\mathcal{Z})[[T]] \arrow[u, hook] \end{tikzcd} \tag{12}$$

where the vertical arrows are the canonical inclusions.

2.2 A Taylor-like isomorphism for skew polynomials

We now aim at completing the diagram (12) 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:

$$\begin{tikzcd} \hat{\mathcal{A}}_N \arrow[r, "\tau_N"] & (\mathcal{A}/N\mathcal{A})[[T]] \\ \hat{\mathcal{C}}_N \arrow[u, hook] \arrow[r, "\tau_N^{\mathcal{C}}"] & (\mathcal{C}/N\mathcal{C})[[T]] \arrow[u, hook] \end{tikzcd} \tag{13}$$

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 in $\hat{\mathcal{A}}_N$. 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 in $\hat{\mathcal{A}}_N$. 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}:

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

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 §1.3). 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 satisfies all the requirements of the theorem.

It remains to prove (ii). By Theorem 1.3.6, 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). □

2.2.1 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 satisfying 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 1.3.6 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 $V = \tau_{N,2}(U)$. $\square$

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 $\sigma_{j_1,\ldots,j_m}(\tau_N(f))$ 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:

$$\tau_{N,1}(f) = V^{-1} \cdot \tau_{N,2}(f) \cdot V. \tag{14}$$

The items (i) and (ii) follows. Let $j \in \mathbb{Z}$. By Lemma 1.3.8, applying σ_j to (14), 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 1.3.10. $\square$

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 $\tau_{N,1} = \tau_{N,2}$. $\square$

2.3 Taylor expansions of skew rational functions

Recall that we have defined in §1.2 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 1.2.1).

2.3.1 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 $\sigma_{j_1,\ldots,j_m}(\mathrm{TS}_N(f))$ with $j_1+\cdots+j_m \equiv 0 \pmod r$.

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

- $\mathrm{ord}_N(f) = \min\big(\mathrm{ord}_{N,0}(f), \ldots, \mathrm{ord}_{N,r-1}(f)\big)$,

- $\mathrm{ord}_{N,j+r}(f) = \mathrm{ord}_{N,j}(f)$,
- $\mathcal{P}_N(f) = \sum_j \mathcal{P}_{N,j}(f) X^j$ where the sum runs over the indices $j \in \{0, 1, \ldots, r-1\}$ 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[2],
- $\mathcal{P}_N(fg) = \mathcal{P}_N(f) \cdot \mathcal{P}_N(g)$ 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 $\mathrm{ord}_N(f)$.

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

$$\begin{tikzcd}
\hat{\mathcal{A}}_N \arrow[r, "\varphi_z \circ \tau_N"] & (\mathcal{A}/N\mathcal{A})[[T]] \\
\hat{\mathcal{C}}_N \arrow[u, hook] \arrow[r, "\tau_z^{\mathcal{C}}"] & (\mathcal{C}/N\mathcal{C})[[T]] \arrow[u, hook]
\end{tikzcd} \tag{15}$$

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 2.3.1. *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

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

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 2.3.2. Given $z \in F^{\mathrm{s}}$, $z \neq 0$ as before, we say that a morphism $\tau : \hat{\mathcal{A}}_N \to (\mathcal{A}/N\mathcal{A})[[T]]$ is *z-admissible* if it satisfies the conditions of Proposition 2.3.1.

Remark 2.3.3. By Theorem 1.3.6, 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 2.3.1 shows that τ_z is z-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 z-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 2.3.4. *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. □

2.3.3 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.

2.3.4 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. (11)). 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 z-admissible morphism (see Definition 2.3.2). 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:

$$\partial_{\mathfrak{C}}^{[n]} = \tau_z^{-1} \circ \left(\frac{1}{n!}\,\frac{d^n}{dT^n}\right) \circ \tau_z \tag{16}$$

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

$$\tau_z(f) = \sum_{n=0}^{\infty} \partial_{\mathfrak{C}}^{[n]}(f) \cdot T^n \;\in\; (\mathcal{A}/N\mathcal{A})[[T]]. \tag{17}$$

However, this result does not give much information because $\mathfrak{C}$ is hard to compute (and the $\partial_{\mathfrak{C}}^{[n]}$'s are even harder) and depends heavily on z. Typically, Proposition 1.4.4 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 1.4.3. Its divided powers (defined by Eq. (16)) 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. (17) reads:

$$\tau_{z,\mathrm{can}}(f) = \sum_{n=0}^{\infty} \partial_{\mathrm{can}}^{[n]}(f)\,T^n \;\in\; (\mathcal{A}/N\mathcal{A})[[T]] \tag{18}$$

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

3 A theory of residues

The results of the previous section lay the foundations of a theory of residues for skew polynomials. The aim of the present section is to develop it: we define a notion of residue at a closed point of F for skew rational functions and then prove the residue formula and study how residues behave under change of variables.

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 $C{\cdot}dY$.

3.1 Definition and first properties

We recall that, for $z \in F^{\mathrm{s}}$, $z \neq 0$, we have defined in §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

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

We 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:

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

Definition 3.1.1. 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 $j \in \{0, \ldots, r-1\}$, 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 z-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 by $\mathrm{sres}_{z,\mathrm{can}}$ 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:

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

3.1.1 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 in §2.3.3 a *canonical* Taylor expansion map around 0:

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

Definition 3.1.2. 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 3.1.3. 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.

3.1.2 Commutative residues

The skew residues we just defined are closely related, in many cases, to classical residues of rational differential forms. In order to state precise results in this direction, we need extra notations. We observe that the map res_z defines by restriction an 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:

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

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

Proposition 3.1.4. *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 1.3.9 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 3.1.4 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 $\sigma_{j_1,\ldots,j_m}(\mathrm{sres}_z(f))$'s for $j_1, \ldots, j_m \in \mathbb{Z}$ 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, other partial skew residues are also related to residues of rational differential forms.

Proposition 3.1.5. *Let $z \in F^{\mathrm{s}} \sqcup \{\infty\}$, let $f \in \mathrm{Frac}(\mathcal{A})$ and let $j \in \{0, 1, \ldots, r{-}1\}$. 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 1.3.9, 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 3.1.4. □

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 3.2.1. *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 3.1.4 asserts that:

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

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 3.2.2. *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 $j \in \{0, 1, \ldots, r{-}1\}$.

Proof. Let $j \in \{0, \ldots, r{-}1\}$ and set $C_j = \sigma_j(f)$. By Proposition 3.1.5, we know that:

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

By the classical residue formula applied successively with $C_j, \theta(C_j), \ldots, \theta^{r-1}(C_j)$, 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 3.2.3. *We assume that p does not divide r.*
For $f \in \mathrm{Frac}(\mathcal{A})$, $j \in \{0, 1, \ldots, r{-}1\}$ 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 1.3.9, we know that:

$$\sigma_j \circ \tau_{z,\mathrm{can}} = \mathrm{N}_j(C_{\mathrm{can}}) \cdot (\tau_{z,\mathrm{can}} \circ \sigma_j). \tag{19}$$

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 (19), we obtain:

$$\sigma_j \circ \tau_{z,\mathrm{can}} = \left(1 + \frac{T}{z}\right)^{j/r} \cdot (\tau_{z,\mathrm{can}} \circ \sigma_j). \tag{20}$$

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. (20) 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. $\square$

Unfortunately, Proposition 3.2.3 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:

$$\sum_{\substack{\zeta \in F^{\mathrm{s}} \\ \zeta \neq 0}} \zeta^j \cdot \mathrm{sres}_{\zeta^r,j,\mathrm{can}}(f) \;=\; 0. \tag{21}$$

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 (21) holds equally true when $\mathrm{sres}_{\zeta^r,j,\mathrm{can}}(f)$ is replaced by any quantity depending only on ζ^r.

However, Proposition 3.2.3 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 $j \in \{1, \ldots, r{-}1\}$. We assume that we know a finite set $\Pi = \{z_1, \ldots, z_n\}$ 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 $\operatorname{ord}_{z,j}(f) \geq -n_i$. 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 3.2.3, we obtain:

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

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

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

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). For example, when $\operatorname{ord}_{z,j}(f) \geq 0$, the first summand $\rho_0\big(P(y)\, y^{j+r-1}\, \sigma_j(f) \cdot dy\big)$ vanishes.

3.3 Change of variables

In this final subsection, we analyse the effect of an endomorphism γ of $\operatorname{Frac}(\mathcal{A})$ on the residues. According to Theorem 1.3.1, $\gamma(X) = CX$ for some $C \in \operatorname{Frac}(\mathcal{C})$ 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:

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

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

Definition 3.3.1. 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 $f \in \operatorname{Frac}(\mathcal{C})$ and $z \in F^{\mathrm{s}}$, we have the formula

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

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

3.3.1 A general formula

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 3.3.2. *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 2.3.2) there exists an admissible choice of τ_z such that:

$$\gamma \circ \mathrm{sres}_{\gamma_\star z}(f) = \mathrm{sres}_z \left(\gamma(f)\, \frac{d\gamma(Y)}{dY} \right) \tag{22}$$

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 this occurs, Eq. (22) holds for any admissible choices of $\tau_{\gamma_\star z}$ and τ_z.

The following lemma will be used in the proof of Theorem 3.3.2.

Lemma 3.3.3. *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:

$$\mathrm{res}\left(\psi(f)\, \frac{dS}{dT} \right) = \mathrm{res}(f). \tag{23}$$

Proof. When $f \in (\mathcal{A}/N\mathcal{A})[[T]]$, both sides of Eq. (23) 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. (23) then reads $\mathrm{res}\big(S^i \frac{dS}{dT}\big) = \mathrm{res}\big(T^i\big)$ and is a direct consequence of the classical formula of change of variables for residues. $\square$

Proof of Theorem 3.3.2. 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

$$\begin{tikzcd} \hat{\mathcal{C}}_{N_1} \arrow[r, "\tau_1^{\mathcal{C}}", "\sim"'] \arrow[d, "\gamma"'] & K \otimes_F E_1[[T]] \arrow[d, "\varphi^{\mathcal{C}}"] \\ \hat{\mathcal{C}}_{N_2} \arrow[r, "\tau_2^{\mathcal{C}}", "\sim"'] & K \otimes_F E_2[[T]] \end{tikzcd}$$

is commutative, *i.e.* $\varphi^{\mathcal{C}} \circ \tau_1^{\mathcal{C}} = \tau_2^{\mathcal{C}} \circ \gamma$. Let us now consider a z_1-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 1.3.6, 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 2.3.3). Applying $\varphi^{\mathcal{C}}$ to this relation, we find:

$$\mathrm{N}_{K\otimes_F E_2[[T]]/E_2[[T]]}\big(\varphi^{\mathcal{C}}(C_1)\big) = 1 + \frac{S}{z_1} = \frac{\tau_2^{\mathcal{Z}}(Z)}{z_1}. \tag{24}$$

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:

$$\mathrm{N}_{K\otimes_F E_2[[T]]/E_2[[T]]}\big(\bar{C}\big) = \mathrm{N}_{K\otimes_F E_2/E_2}\big(\bar{C}\big) = \frac{z_1}{z_2} \tag{25}$$

and:

$$\mathrm{N}_{K\otimes_F E_2[[T]]/E_2[[T]]}\big(\tau_2^{\mathcal{C}}(C)\big) = \tau_2^{\mathcal{C}}\big(Z\,Y^{-1}\big) = \frac{\tau_2^{\mathcal{Z}}(Z)}{z_2 + T}. \tag{26}$$

Combining Eqs. (24), (25) and (26), 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 a z-admissible choice for τ_z. Moreover, it sits in the following commutative diagram:

$$\begin{tikzcd} \hat{\mathcal{A}}_{N_1} \arrow[r, "\tau_1", "\sim"'] \arrow[d, "\gamma"'] & (\mathcal{A}/N_1\mathcal{A})[[T]] \arrow[d, "\varphi"] \\ \hat{\mathcal{A}}_{N_2} \arrow[r, "\tau_2", "\sim"'] & (\mathcal{A}/N_2\mathcal{A})[[T]] \end{tikzcd}$$

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 3.3.3 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. (22) holds for any $\gamma_s tar z$-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. $\square$

3.3.2 The case of 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 $\mathrm{sres}_{z,\mathrm{can}}$. After Theorem 3.3.2, one could hope that Eq. (22) 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 3.3.4. *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 3.3.2, 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 3.3.2). 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 $\mathcal{A}' = \mathcal{Z}' \otimes_{\mathcal{Z}} \mathcal{A}$. We emphasize that $\mathcal{C}'$ is not a field in general but a product of fields. However, the extension $\mathcal{C}'/\mathcal{Z}'$ is 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 3.3.5. *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 $\tau_z^{\mathcal{Z}} : \hat{\mathcal{Z}}_N \to (\mathcal{Z}/N\mathcal{Z})[[T]]$. 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 necessarily agrees with $\tau_z^{\mathcal{Z}'} \otimes \tau_z$ on its domain of definition. Unicity follows. □

Lemma 3.3.5 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:

$$C' = \frac{(\mathrm{id} \otimes \theta)(U)}{U}. \tag{27}$$

Remark 3.3.6. Raising Eq. (27) to the r-th power, we get:

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

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 3.3.7. *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 3.3.8. (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 3.3.7 reduces to that of Theorem 3.3.4.

(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 3.3.7 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 3.3.7. We keep the notations of the proof of Theorem 3.3.4 and assume in addition that the isomorphism $\tau_{\gamma_\star z}$ we started with is $\tau_{\gamma_\star z,\mathrm{can}}$, *i.e.*:

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

By the proof of Theorem 3.3.2, Eq. (22) 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:

$$\tau(f) = \bar{U}^{-1} \cdot \tau^{\mathcal{A}'}_{z,\mathrm{can}}\big(Ug\, U^{-1}\big) \cdot \bar{U} \tag{28}$$

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

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

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

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

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

$$Q^r = \frac{z_1}{z_2} \cdot \left(\frac{\bar{C}'}{\tau^{\mathcal{C}}_z(C)}\right)^r \cdot \left(1 + \frac{S}{z_1}\right). \tag{29}$$

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. (29), we finally find:

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

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. (28)), we obtain:

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

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

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] X. Caruso, *Duals of linearized Reed-Solomon codes*

[6] P. M. Cohn, *Free Rings and Their Relations*, London Math. Soc. Monographs, Academic Press (1971)

[7] J.-M. Couveignes, R. Lercier, *Elliptic Periods for Finite Fields*, Finite Fields Appl., **15** (2009), 1–22

[8] P. Delsarte, *Bilinear Forms over a Finite Field with Applications to Coding Theory*, J. Combin. Theory **25** (1978), 226–241

[9] E. Gabidulin, *Theory of codes with maximum rank distance*, Problemy Peredachi Informatsii **21** (1985), no. 1, 3–16

[10] S. Ikehata, *Azumaya algebras and skew polynomial rings*, Math. J. Okayama Univ. **23** (1981), no. 1, 19–32

[11] S. Ikehata, *Azumaya algebras and skew polynomial rings. II*, Math. J. Okayama Univ. **26** (1984), 49–57

[12] N. Jacobson, *Non commutative polynomials and cyclic algebras*, Ann. of Math. **35** (1934), 197–208

[13] N. Jacobson, *Pseudo-linear transformations*, Ann. of Math. **38** (1937), 484–507

[14] N. Jacobson, *Finite-Dimensional Division Algebras Over Fields*, Grundlehren der Mathematischen Wissenschaften Series (1996), Springer

[15] T. Y. Lam, *A general theory of Vandermonde matrices*, Expos. Math. **4** (1986), 193–215

[16] T. Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Math. **189**, Springer (1999), New York

[17] T. Y. Lam, A. Leroy, *Vandermonde and Wronskian matrices over division rings*, J. Algebra **119** (1988), 308–336

[18] T. Y. Lam, A. Leroy, *Principal one-sided ideals in Ore polynomial rings*, Algebra and Its Applications, Comtemp. Math. **259** (2000), 333–352

[19] 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

[20] 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`

[21] 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

[22] Ø. Ore, *Linear equations in non-commutative fields*, Ann. of Math. **32** (1931), 463–477

[23] Ø. Ore, *Theory of non-commutative polynomials*, Ann. of Math. **34** (1933), 480–508

[24] M. Van der Put, *Differential equations in characteristic p*, Compositio Math. **97** (1995), 227–251