Universidad de Concepción
Dirección de Postgrado
Facultad de Ciencias Físicas y Matemáticas - Programa Magister en Matemática

Algunos aspectos algebraicos y computacionales en anillos polinomiales torcidos multivariables

Some algebraic and computational aspects in multivariate skew polynomial rings

Tesis para optar al grado de Magíster en Matemática

JONATHAN ARMANDO BRIONES DONOSO
CONCEPCIÓN-CHILE
2022

Profesor Guía: Andrea Luigi Tironi
Departamento de Matemática, Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

Contents

Acknowledgments **3**

Introduction **4**

Introducción **7**

1 Background material **10**
1.1 Univariate skew polynomial rings 10
1.2 Multivariate skew polynomial rings 20

2 Derivatives for skew polynomials **24**
2.1 (σ, δ)-Partial derivatives 24
2.2 (σ, δ)-Univariate derivatives 29

3 Hermite-type interpolation for skew multivariate polynomial rings **34**
3.1 Skew Hermite-type interpolation 35

4 Resultants of skew polynomials over division rings **44**
4.1 Right (σ, δ)-Resultant 45
4.2 Left (σ, δ)-Resultant 67
4.3 Right and left multiple roots 75

Bibliography **76**

Acknowledgments

First, I thank God for giving me the strength and intelligence necessary to complete this stage as a master's student. I thank my parents for their constant support, without them nothing of this would be possible. Also, I am very grateful to my supervisor Dr. Andrea Tironi, who gave me all the tools to get ahead in this investigation. Finally, I want to thank one of the most important people for me, my girlfriend. Thank you Leslie for your infinite support, concern, patience and love that you give me every day.

Introduction

Skew polynomial rings $\mathbb{F}[x;\sigma,\delta]$ with coefficients over a division ring $\mathbb{F}$ (Definition 1.1.6), were introduced in [27] by Oystein Ore (1933), as a non-commutative generalization of the conventional polynomial rings. The first applications of skew polynomials appear with the work of [9, 10] and Jacobson [18] and recently, they have been used to construct algebraic codes (e.g. see [4, 6, 25]) and for applications in cryptography [5].

Although in general $\mathbb{F}[x;\sigma,\delta]$ behaves differently from the classical polynomial ring, it preserves the important property of having a Euclidean division algorithm. However, this algorithm holds for right division and not for left division, unless σ is an automorphism of $\mathbb{F}$, as stated in [27, Theorem 6]. This property, allowed Lam and Leroy in [21, p. 310] to define the evaluation of a polynomial $f(x) \in \mathbb{F}[x;\sigma,\delta]$ at any point $a \in \mathbb{F}$, as the unique remainder of the right-hand division of $f(x)$ by $x-a$ (Definition 1.1.11), forcing a remainder theorem as in the classical case. Having an evaluation map is key to begin the study of the zeros of a skew polynomial, but unlike the classical case, this study is more difficult, since in general a skew polynomial of degree $n \geq 2$ can have more than n zeros, possibly infinite (Example 1.1.15).

On the other hand, in literature there exist multivariate generalizations of $\mathbb{F}[x;\sigma,\delta]$, for instance the iterated polynomial rings $\mathbb{F}[x_1,\sigma_1,\delta_1][x_2,\sigma_2,\delta_2]\cdots[x_n,\sigma_n,\delta_n]$ (see [30], [9, p. 532]). However, to define an evaluation map that allows one to evaluate any polynomial $F \in \mathbb{F}[x_1,\sigma_1,\delta_1][x_2,\sigma_2,\delta_2]\cdots[x_n,\sigma_n,\delta_n]$ is not possible, because in general unique remainder algorithms do not hold for iterated skew polynomials (see [23] for more details). In 2019, the authors in [23] overcome this obstacle by considering an alternative construction and introduce the so-called free multivariate skew polynomial rings $\mathbb{F}[x_1,x_2,...,x_n;\sigma,\delta]$ (Definition 1.2.3), showing that in this case, it is possible to define the evaluation of any free skew polynomial F at any point $(a_1,a_2,...,a_n) \in \mathbb{F}^n$, as the unique remainder of the Euclidean division on the right of F by the polynomials $x_1-a_1, x_2-a_2, ..., x_n-a_n$ (Definition 1.2.5).

In this thesis, thanks to the uniqueness of the quotient and remainder that gives

us the right-hand division of $F \in \mathbb{F}[x_1, x_2, ..., x_n; \sigma, \delta]$ by the corresponding polynomials $x_1 - a_1, x_2 - a_2, ..., x_n - a_n$, we introduce for the first time the notion of right (σ, δ)-partial derivative of a polynomial $F \in \mathbb{F}[x_1, x_2, ..., x_n; \sigma, \delta]$ at any point $(a_1, ..., a_n) \in \mathbb{F}^n$ (Definition 2.1.1). Moreover, since in general left division does not work in the ring $\mathbb{F}[x_1, x_2, ..., x_n; \sigma, \delta]$, we show a necessary and sufficient condition that allows the left division of any polynomial $F \in \mathbb{F}[x_1, x_2, ..., x_n; \sigma, \delta]$ by the skew polynomials $x_1 - a_1, x_2 - a_2, ..., x_n - a_n$ (Lemma 2.1.2), thus defining the corresponding left (σ, δ)-evaluation (Definition 2.1.4) and the left (σ, δ)-partial derivatives (Definition 2.1.5).

By using the notion of (σ, δ)-partial derivative, we define generalized zero ideals (Definition 3.1.1), we introduce the notion of PD-independent (see Definition 3.1.4) which generalizes the P-independence given in [23, Definition 23] and we use these tools to prove one of the main results of this thesis which corresponds to a Hermite-type interpolation Theorem (Theorem 3.1.12) that generalizes the Lagrange interpolation Theorem given in [23, Theorem 4] and extends the cases $n = 1$ given in [14, Theorem 4.4] and [26, Corollary 41]. Moreover, unlike [23, Theorem 4], we provide a necessary and sufficient condition for Hermite and Lagrange interpolation problems to admit a solution (Theorem 3.1.12 and Corollary 3.1.13).

On the other hand, for the case $n = 1$, we introduce in the ring $\mathbb{F}[x; \sigma, \delta]$ the notion of right and left (σ, δ)-resultants ($R^{\sigma,\delta}_{\mathbb{F}}(f, g)$ and $R^{\sigma,\delta}_{\mathbb{F},L}(f, g)$, respectively) of two polynomials $f, g \in \mathbb{F}[x; \sigma, \delta]$ (Definitions 4.1.3 and 4.2.2), which in general are different in the non-commutative case, but coincide in the commutative case (i.e. when $\mathbb{F}$ is a field, $\sigma = Id$ and $\delta = 0$). Moreover, using these concepts and inspired by the classical situation, we give results that show equivalent conditions to $R^{\sigma,\delta}_{\mathbb{F}}(f, g) = 0$ ($R^{\sigma,\delta}_{\mathbb{F},L}(f, g) = 0$) (Theorems 4.1.6, 4.2.4, 4.1.23, 4.2.9 and Proposition 4.1.25). To conclude, we use $R^{\sigma,\delta}_{\mathbb{F}}(f, g)$ and $R^{\sigma,\delta}_{\mathbb{F},L}(f, g)$ to give equivalent conditions to the fact that a skew polynomial $f(x) \in \mathbb{F}[x; \sigma, \delta]$ admits a right or left root of positive multiplicity (Theorems 4.3.3 and 4.3.5). We would like to stress here that these latest results are a direct application of our notion of (σ, δ)-derivative given for the case $n = 1$ (Definition 2.2.1).

The thesis is organized as follows. In Chapter 1, we recall basic definitions and notations, the main properties of the rings $\mathbb{F}[x; \sigma, \delta]$ and $\mathbb{F}[x_1, x_2, ..., x_n; \sigma, \delta]$ and we give some preliminary results. In Chapter 2, we introduce the notion of right and left (σ, δ)-partial derivatives (Definitions 2.1.1 and 2.1.5), their corresponding higher-order partial derivatives (Definition 2.1.6) and prove some basic properties (Lemmas 2.1.8 and 2.1.9). Moreover, we show that every free multivariate skew polynomial can be written in terms of its (σ, δ)-partial derivatives, obtaining in this context a multivariate

Taylor-type expansion (Proposition 2.1.10). Finally, for the case $n = 1$, we define the notions of right and left (σ, δ)-derivatives of a polynomial $f(x) \in \mathbb{F}[x; \sigma, \delta]$ and we show some of their properties.

In Chapter 3, by using right (σ, δ)-partial derivatives, we introduce the left ideals $I^{\vec{m}}(\Omega)$ (Definition 3.1.1), we define the notion of DP-independence (Definition 3.1.4) and then we prove a Hermitian-type interpolation Theorem (Theorem 3.1.12). Moreover, we provide a tool for construct DP-independent sets by using conjugacy classes (Proposition 3.1.18) to apply in concrete situations Theorem 3.1.12.

Finally, in Chapter 4, after some technical lemmas, we first introduce the right (σ, δ)-resultant $R_{\mathbb{F}}^{\sigma,\delta}(f, g)$ of two skew polynomials $f, g \in \mathbb{F}[x; \sigma, \delta]$ (Definition 4.1.3) and, after some of its properties (Propositions 4.1.15 and 4.1.19), we prove three results about equivalent conditions to $R_{\mathbb{F}}^{\sigma,\delta}(f, g) = 0$ (Theorems 4.1.6, 4.1.23 and Proposition 4.1.25) and we give a characterization of the degree of the greatest common right divisor $gcrd(f, g)$ (Theorem 4.1.8) which can be also applied to check when $gcrd(f, g) \neq 1$. Moreover, we introduce the new notion of left (σ, δ)-resultant of two skew polynomials (Definition 4.2.2), rewriting in this context some of the main previous results and giving some equivalent conditions to the fact that a skew polynomial admits a right or left root of positive multiplicity (Theorems 4.3.3 and 4.3.5). Furthermore, through this chapter, we give some algorithms and their respective Magma programs [3] as computational applications of the main algebraic results which allowed us to construct all the examples in a very simple manner.

We hope that all the arguments presented here will be useful in the next future for both theoretical and computational topics involving univariate and free multivariate skew polynomials.

Introducción

Los anillos polinomiales torcidos $\mathbb{F}[x;\sigma,\delta]$ con coeficientes sobre un anillo de división $\mathbb{F}$ (Definición 1.1.6), fueron introducidos en [27] por Oystein Ore (1933) como una generalización no conmutativa de los anillos polinomiales convencionales. Las primeras aplicaciones de los polinomios torcidos aparecen con los trabajos de Cohn [9, 10] y Jacobson [18] y recientemente, han sido utilizados para construir códigos algebraicos (ver por ejemplo [4, 6, 25]) y para aplicaciones en Criptografía [5].

Aunque en general $\mathbb{F}[x;\sigma,\delta]$ se comporta de manera diferente al anillo polinomial clásico, conserva la importante propiedad de tener un algoritmo de división Euclidiano. Sin embargo, este algoritmo se cumple para la división por derecha y no para la división izquierda, a menos que σ sea un automorfismo de $\mathbb{F}$, como se indica en [27, Teorema 6]. Esta propiedad, permitió a Lam y Leroy en [21, p. 310] definir la evaluación de un polinomio $f(x) \in \mathbb{F}[x;\sigma,\delta]$ en cualquier punto $a \in \mathbb{F}$, como el único resto de la división a la derecha de $f(x)$ por $x - a$ (Definición 1.1.11), forzando un teorema del resto como en el caso clásico. Tener una función de evaluación es clave para iniciar el estudio de ceros de un polinomio torcido, pero a diferencia del caso clásico, este estudio es mas delicado, ya que en general un polinomio torcido de grado $n \geq 2$ puede tener mas de n raíces, posiblemente infinitas (Ejemplo 1.1.15).

Por otro lado, en literatura existen generalizaciones multivariables de $\mathbb{F}[x;\sigma,\delta]$, por ejemplo los anillos polinomiales iterados $\mathbb{F}[x_1,\sigma_1,\delta_1][x_2,\sigma_2,\delta_2]\cdots[x_n,\sigma_n,\delta_n]$ (ver [30], [9, p. 532]). Sin embargo, definir una función de evaluación que permita evaluar un cualquier polinomio $F \in \mathbb{F}[x_1,\sigma_1,\delta_1][x_2,\sigma_2,\delta_2]\cdots[x_n,\sigma_n,\delta_n]$ no es posible, ya que en general los algoritmos de división con resto único no se cumplen para polinomios torcidos iterados (ver [23] para mas detalles). El año 2019, en [23] los autores superan este obstáculo, considerando una construcción alternativa, e introducen los llamados anillos polinomiales torcidos multivariables libres $\mathbb{F}[x_1,x_2,...,x_n;\sigma,\delta]$ (Definición 1.2.3), mostrando que en este caso, es posible definir la evaluación de cualquier polinomio torcido libre F en cualquier punto $(a_1,a_2,...,a_n) \in \mathbb{F}^n$, como el único resto de la división Euclidiana a la

derecha de F por $x_1 - a_1, x_2 - a_2, ..., x_n - a_n$ (Definición 1.2.5).

En esta tesis, gracias a la unicidad del cociente y resto que nos otorga la división a la derecha de $F \in \mathbb{F}[x_1, x_2, ..., x_n; \sigma, \delta]$ por los correspondientes polinomios $x_1 - a_1, x_2 - a_2, ..., x_n - a_n$, introducimos por primera vez la noción de (σ, δ)-derivada parcial derecha de un polinomio $F \in \mathbb{F}[x_1, x_2, ..., x_n; \sigma, \delta]$ en cualquier punto $(a_1, ..., a_n) \in \mathbb{F}^n$ (Definición 2.1.1). Aún mas, dado que en general la división a la izquierda no funciona en el anillo $\mathbb{F}[x_1, x_2, ..., x_n; \sigma, \delta]$, mostramos una condición necesaria y suficiente que permite dividir a la izquierda cualquier polinomio $F \in \mathbb{F}[x_1, x_2, ..., x_n; \sigma, \delta]$ por los polinomios $x_1 - a_1, x_2 - a_2, ..., x_n - a_n$ (Lema 2.1.2), definiendo así la correspondiente (σ, δ)-evaluación izquierda (Definición 2.1.4) y las (σ, δ)-derivadas parciales izquierdas (Definición 2.1.5).

Usando la noción de (σ, δ)-derivada parcial, definimos ideales de cero generalizados (Definición 3.1.1), introducimos la noción de DP-independencia (Definición 3.1.4) que generaliza la P-independencia entregada en [23, Definición 23] y luego hacemos uso de estas herramientas para probar uno de los resultados principales de esta tesis, el cual corresponde a un Teorema de interpolación de tipo Hermitiano (Teorema 3.1.12) que generaliza el Teorema de interpolación de Lagrange dado en [23, Teorema 4] y extiende los casos $n = 1$ dados en [14, Teorema 4.4] y [26, Corolario 41]. Aún mas, a diferencia de [23, Teorema 4], entregamos una condición necesaria y suficiente para que los problemas de interpolación de Hermite y Lagrange admitan una solución (Teorema 3.1.12 y Corolario 3.1.13).

Por otro lado, para el caso $n = 1$, introducimos en el anillo $\mathbb{F}[x; \sigma, \delta]$ las nociones de (σ, δ)-resultantes derechos e izquierdos ($R^{\sigma,\delta}_{\mathbb{F}}(f, g)$ y $R^{\sigma,\delta}_{\mathbb{F},L}(f, g)$, respectivamente) de dos polinomios $f, g \in \mathbb{F}[x; \sigma, \delta]$ (Definiciones 4.1.3 y 4.2.2), que en general son diferentes en el caso no conmutativo, pero coinciden en el caso conmutativo, es decir, cuando $\mathbb{F}$ es un campo, $\sigma = Id$ y $\delta = 0$. Además, utilizando estos conceptos e inspirados por la situación clásica, entregamos resultados que muestran condiciones equivalentes a $R^{\sigma,\delta}_{\mathbb{F}}(f, g) = 0$ ($R^{\sigma,\delta}_{\mathbb{F},L}(f, g) = 0$) (Teoremas 4.1.6, 4.2.4, 4.1.23, 4.2.9 y Proposición 4.1.25). Para finalizar, utilizamos $R^{\sigma,\delta}_{\mathbb{F}}(f, g)$ y $R^{\sigma,\delta}_{\mathbb{F},L}(f, g)$ para dar condiciones equivalentes al hecho que un polinomio $f(x) \in \mathbb{F}[x; \sigma, \delta]$ admita una raíz derecha o izquierda de multiplicidad positiva (Teoremas 4.3.3 y 4.3.5). Nos gustaría destacar aquí que estos últimos resultados son una aplicación directa de nuestra noción de (σ, δ)-derivada dada para el caso $n = 1$ (Definición 2.2.1).

La tesis está organizada de la siguiente manera. En el Capítulo 1, recordamos definiciones básicas y notaciones, las principales propiedades de los anillos $\mathbb{F}[x; \sigma, \delta]$ y $\mathbb{F}[x_1, x_2, ..., x_n; \sigma, \delta]$ y damos algunos resultados preliminares. En el Capítulo 2, intro-

ducimos la noción de (σ, δ)-derivada parcial derecha e izquierda (Definiciones 2.1.1 y 2.1.5), sus correspondientes (σ, δ)-derivadas parciales de orden superior (Definición 2.1.6) y probamos algunas propiedades básicas (Lemas 2.1.8 y 2.1.9). Además, mostramos que todo polinomio torcido libre se puede escribir en función de sus (σ, δ)-derivadas parciales, obteniendo en este contexto una expansión tipo Taylor multivariable (Proposición 2.1.10). Finalmente, para el caso $n = 1$, definimos las nociones de (σ, δ)-derivadas derechas e izquierdas de un polinomio $f(x) \in \mathbb{F}[x; \sigma, \delta]$ y mostramos algunas de sus propiedades.

En el Capítulo 3, haciendo uso de las (σ, δ)-derivadas parciales, introducimos los ideales izquierdos $I^{\vec{m}}(\Omega)$ (Definición 3.1.1), definimos la noción de DP-independencia (Definición 3.1.4) y luego probamos un Teorema de interpolación de tipo Hermitiano (ver Teorema 3.1.12). Además, entregamos una herramienta para construir conjuntos DP-independientes usando clases de conjugación (Proposición 3.1.18) que permite aplicar en situaciones concretas el Teorema 3.1.12.

Finamente, en el Capítulo 4, luego de algunos lemas técnicos, introducimos el (σ, δ)-resultante derecho $R_{\mathbb{F}}^{\sigma,\delta}(f, g)$ de dos polinomios torcidos $f, g \in \mathbb{F}[x; \sigma, \delta]$ (Definición 4.1.3) y, después de algunas de sus propiedades (Proposiciones 4.1.15 y 4.1.19), probamos tres resultados que muestran condiciones equivalentes a $R_{\mathbb{F}}^{\sigma,\delta}(f, g) = 0$ (Teoremas 4.1.6, 4.1.23 y Proposición 4.1.25) y damos una caracterización del grado del máximo común divisor derecho $gcrd(f, g)$ (Teorema 4.1.8) que también puede ser aplicado para chequear cuando $gcrd(f, g) \neq 1$. Además, introducimos la nueva noción de (σ, δ)-resultante izquierdo de dos polinomios torcidos (Definición 4.2.2), reescribiendo en este contexto algunos de los principales resultados previos y dando algunas condiciones equivalentes al hecho que un polinomio torcido admita una raíz derecha o izquierda de multiplicidad positiva (Teoremas 4.3.3 y 4.3.5). Además, a través de este capítulo, damos algunos algoritmos y sus respectivos programas Magma [3] como aplicaciones computacionales de los principales resultados algebraicos que nos han permitido construir todos los ejemplos de forma muy sencilla.

Esperamos que todos los argumentos aquí presentados, sean útiles en un futuro próximo tanto para temas teóricos como computacionales, que involucren a los polinomios torcidos univariables y multivariables libres.

Chapter 1

Background material

We provide here some basic definitions and preliminary results concerning skew polynomials over division rings. The tools presented in this chapter will be useful for the later results of this thesis.

1.1 Univariate skew polynomial rings

Denote by $\mathbb{F}$ a division ring (or a skew field), that is, a unitary ring (not necessarily commutative) in which every non-zero element is invertible in $\mathbb{F}$. Evidently, every field is a division ring. The most familiar example of a division ring which is not a field is the ring $\mathbb{H}$ of Hamilton's quaternions. However, also there are interesting methods for constructing non-commutative division rings (e.g., if R is a ring and S is a simple module over R, then the endomorphisms ring of S is always a division ring [20, Lemma 3.6]). On the other hand, if we assume that $\mathbb{F}$ is a finite division ring, then it is known that $\mathbb{F}$ is a finite field (see [17, p. 250]).

To define univariate skew polynomial rings (Ore extensions), we begin by introducing the concept of σ-derivation.

Definition 1.1.1. Let $\sigma : \mathbb{F} \to \mathbb{F}$ be a non-zero ring endomorphism. An additive group homomorphism $\delta : \mathbb{F} \to \mathbb{F}$ is called a *σ-derivation* (over $\mathbb{F}$) if

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$$

for every $a, b \in \mathbb{F}$.

Example 1.1.2. Let $\sigma : \mathbb{F} \to \mathbb{F}$ be a ring homomorphism and let $\beta \in \mathbb{F}$. The map

$\delta_\beta : \mathbb{F} \to \mathbb{F}$ defined by

$$\delta_\beta(a) := \sigma(a)\beta - \beta a$$

for all $a \in \mathbb{F}$ is a σ-derivation. These kind of derivations are called in literature simply *inner derivations*.

Remark 1.1.3. From Definition 1.1.1, it follows that $\delta(1) = \delta(-1) = 0$. Furthermore, σ is always a monomorphism but, in general, it is not an automorphism. For instance, in $\mathbb{F}_p(t) := \left\{\frac{f}{g} : f, g \in \mathbb{F}_p[t], g \neq 0\right\}$ (field of rational functions in the variable t over the finite field $\mathbb{F}_p$ with p prime), the endomorphism $\phi : \mathbb{F}_p(t) \to \mathbb{F}_p(t), x \mapsto x^p$ is not surjective because $\phi(\mathbb{F}_p(t))$ does not contain t.

The role played by inner derivations when $\mathbb{F}$ is a field is shown by the following result, as indicated in [9, Section 8.3] (see also [24, Proposition 39]).

Proposition 1.1.4. *Let $\mathbb{F}$ be a field and consider an endomorphism $\sigma : \mathbb{F} \to \mathbb{F}$ and a σ-derivation $\delta : \mathbb{F} \to \mathbb{F}$. If $\sigma \neq Id$ (the identity automorphism), then δ is an inner derivation.*

Remark 1.1.5. From Proposition 1.1.4, it is natural to ask how are the Id-derivations over a field. With respect to this question, we can distinguish two cases. If $\mathbb{F}$ is a finite field then the unique Id-derivation is $\delta = 0$ (see [24, Proposition 44]). However, if $\mathbb{F}$ is infinite, then it is possible to define non-zero Id-derivations. For instance, the formal derivation with respect to the variable t, given by $\frac{d}{dt}$, is an Id-derivation over $\mathbb{F}_p(t)$.

Following some Ore's ideas in [27], we recall the ring of univariate skew polynomials.

Definition 1.1.6. Given a ring endomorphism $\sigma : \mathbb{F} \to \mathbb{F}$ and a σ-derivation $\delta : \mathbb{F} \to \mathbb{F}$, we define the *univariate skew polynomial ring*, corresponding to σ and δ and denoted by

$$\mathcal{R} := \mathbb{F}[x; \sigma, \delta] \ ,$$

as the set of all polynomials $\sum_i a_i x^i$ ($a_i \in \mathbb{F}$) with the usual sum of polynomials and the product defined accordingly to the following rule

$$xa = \sigma(a)x + \delta(a) \tag{1.1}$$

for all $a \in \mathbb{F}$.

Example 1.1.7. Consider $\mathbb{F}_4[x;\sigma,\delta_\alpha]$ with $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, where $\alpha^2 + \alpha + 1 = 0$, $\sigma(a) = a^2$ and $\delta_\alpha(a) = \alpha(\sigma(a) + a)$ for all $a \in \mathbb{F}_4$. Then we have

$$\alpha x \cdot \alpha^2 x = \alpha(x\alpha^2)x = \alpha(\sigma(\alpha^2)x + \delta_\alpha(\alpha^2))x = \alpha^2 x^2 + \alpha^2 x \ ,$$

$$\alpha^2 x \cdot \alpha x = \alpha^2(x\alpha)x = \alpha^2(\sigma(\alpha)x + \delta_\alpha(\alpha))x = \alpha x^2 + x \ .$$

The previous example shows that in general the product of skew polynomials is not commutative and that the product of two monomials is not a monomial. Moreover, let us recall here some basic properties of $\mathcal{R}$:

1. Let $f(x) = \sum_{i=1}^{m} a_i x^i, g(x) = \sum_{j=1}^{n} b_j x^j \in \mathcal{R}$ of degrees m and n, respectively. By (1.4), we get $f(x)g(x) = ... + a_m\sigma^m(b_n)x^{m+n}$ with $a_m\sigma^m(b_n) \neq 0$ (because $a_m, b_n \neq 0$ and σ is a monomorphism). In particular, we have $\deg(fg) = \deg(f) + \deg(g)$ which implies that $\mathcal{R}$ has not zero divisors.

2. The Euclidean algorithm holds for *right division* (see [27, p. 483]). For any $f(x), g(x) \in \mathcal{R}$ with $g(x) \neq 0$, there are unique $q(x), r(x) \in \mathcal{R}$ such that

$$f(x) = q(x)g(x) + r(x)$$

   with either $\deg(r) < \deg(g)$, or $r(x) = 0$. For instance, in $\mathbb{F}_4[x;\sigma,\delta]$ with σ, δ defined as in Example 1.1.7, if we divide x^3 by αx, unlike the usual division algorithm, the action of δ in general makes the quotient is not a monomial, but a polynomial. In fact, we have $x^3 = (\alpha^2 x^2 + x + \alpha)(\alpha x)$.

3. An important consequence of the right division algorithm is that $\mathcal{R}$ is a left principal ideal domain (LPID), i.e. any left ideal $I \subset \mathcal{R}$ has the form $\mathcal{R}g$, where $g \in \mathcal{R}$ is a polynomial of minimal degree among non-zero elements of I. However, it is also widely known that if σ fails to be an automorphism of $\mathbb{F}$, i.e. $\sigma(\mathbb{F}) \neq \mathbb{F}$, then the left division does not work (see [27, Theorem 6]) showing that $\mathcal{R}$ is not in general a right principal ideal domain (RPID).

Consider now monomials $ax^i, bx^j, x^i\beta, x^j\alpha \in \mathcal{R}$. Motivated by Example 1.1.7, we will give formulas to calculate easily the products $ax^i \cdot bx^j$ and $x^i\beta \cdot x^j\alpha$.

Definition 1.1.8. Let $a \in \mathbb{F}$. We define $\mathcal{C}_{d,s}(a)$ as the sum of all possible compositions (as functions) of d copies of δ and s copies of σ evaluated in a when $(d, s) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} \setminus (0, 0)$, $\mathcal{C}_{0,0}(a) = a$ and $\mathcal{C}_{d,s}(a) = 0$ otherwise. Moreover, if σ is an automorphism, we define

$\mathcal{T}_{t,r}(a)$ as the sum of all possible compositions (as functions) of t copies of $\delta\sigma^{-1}$ and r copies of σ^{-1} evaluated in a when $(t,r) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} \setminus (0,0)$, $\mathcal{T}_{0,0}(a) = a$ and $\mathcal{T}_{t,r}(a) = 0$ otherwise.

Remark 1.1.9. From Definition 1.1.8, for all $a \in \mathbb{F}$ and $(d,s) \in \mathbb{Z} \times \mathbb{Z}$ we have

$$\mathcal{C}_{d,s}(a) = \delta(\mathcal{C}_{d-1,s}(a)) + \sigma(\mathcal{C}_{d,s-1}(a)) \ , \ \mathcal{T}_{d,s}(a) = \delta\sigma^{-1}(\mathcal{T}_{d-1,s}(a)) + \sigma^{-1}(\mathcal{T}_{d,s-1}(a)) \ .$$

Lemma 1.1.10. *Given a non-negative integer i and $a \in \mathbb{F}$, we have*

$$x^i a = \sum_{k=0}^{i} \mathcal{C}_{k,i-k}(a) x^{i-k} \ . \tag{1.2}$$

Moreover, if σ is an automorphism, we get

$$ax^i = \sum_{k=0}^{i} x^{i-k}(-1)^k \mathcal{T}_{k,i-k}(a). \tag{1.3}$$

Proof. We prove (1.2) by induction on i. If $i = 0, 1$, then it is true by the definition of $\mathcal{C}_{0,0}(a)$ and (1.1), respectively. So, assume that this formula is true for some $i - 1 \geq 0$, i.e. $x^{i-1}a = \sum_{k=0}^{i-1} \mathcal{C}_{k,i-1-k}(a)x^{i-1-k}$. Then, by Remark 1.1.9 we obtain that

$$\begin{aligned}
x^i a &= x(x^{i-1}a) \\
&= x \cdot \left(\sum_{k=0}^{i-1} \mathcal{C}_{k,i-1-k}(a) x^{i-1-k} \right) \\
&= x \cdot \mathcal{C}_{0,i-1}(a)x^{i-1} + x \cdot \mathcal{C}_{1,i-2}(a)x^{i-2} + x \cdot \mathcal{C}_{2,i-3}(a)x^{i-3} + ... + x \cdot \mathcal{C}_{i-1,0}(a) \\
&= \sigma(\mathcal{C}_{0,i-1}(a))x^i + [\delta(\mathcal{C}_{0,i-1}(a)) + \sigma(\mathcal{C}_{1,i-2}(a))]\, x^{i-1} + ... + \delta(\mathcal{C}_{i-1,0}(a)) \\
&= \mathcal{C}_{0,i}(a)x^i + \mathcal{C}_{1,i-1}(a)x^{i-1} + \mathcal{C}_{2,i-2}(a)x^{i-2} + ... + \mathcal{C}_{i,0}(a) \\
&= \sum_{k=0}^{i} \mathcal{C}_{k,i-k}(a) x^{i-k} \ .
\end{aligned}$$

By reasoning in a similar way, we obtain the expression for ax^i as in the statement.

□

From Lemma 1.1.10, it follows that

$$ax^i \cdot bx^j = \sum_{k=0}^{i} a \cdot \mathcal{C}_{k,i-k}(b) x^{i+j-k} \quad , \quad x^i\beta \cdot x^j\alpha = \sum_{k=0}^{j} x^{i+j-k}(-1)^k \mathcal{T}_{k,j-k}(\beta)\alpha \ .$$

Furthermore, given non-zero skew polynomials

$$f(x)=\sum_{i=0}^{m} a_i x^i \ , \ g(x)=\sum_{j=0}^{n} b_j x^j \ , \ F(x)=\sum_{i=0}^{m} x^i \beta_i \ , \ G(x)=\sum_{j=0}^{n} x^j \alpha_j$$

in $\mathcal{R}$, we have

$$f(x)g(x)=\sum_{i=0}^{m}\sum_{j=0}^{n}\left(\sum_{k=0}^{i} a_i \, \mathcal{C}_{k,i-k}(b_j)x^{i+j-k}\right) \ , \tag{1.4}$$

$$F(x)G(x)=\sum_{i=0}^{m}\sum_{j=0}^{n}\left(\sum_{k=0}^{j} x^{i+j-k}(-1)^k \mathcal{T}_{k,j-k}(\beta_i)\cdot\alpha_j\right) . \tag{1.5}$$

In particular, if $\delta=0$, then we get

$$\mathcal{C}_{d,s}(a)=\begin{cases} a & \text{if} \quad d=s=0 \\ \sigma^s(a) & \text{if} \quad d=0 \text{ and } s\neq 0 \\ 0 & \text{if} \quad d\neq 0 \end{cases} \tag{1.6}$$

$$\mathcal{T}_{d,s}(a)=\begin{cases} a & \text{if} \quad d=s=0 \\ \sigma^{-s}(a) & \text{if} \quad d=0 \text{ and } s\neq 0 \\ 0 & \text{if} \quad d\neq 0 \end{cases}$$

for all $a\in\mathbb{F}$ and $d,s\in\mathbb{Z}_{\geq 0}$. Thus, the products $f(x)g(x)$ and $F(x)G(x)$ become simply

$$f(x)g(x)=\left(\sum_{i=0}^{m} a_i x^i\right)\cdot\left(\sum_{j=0}^{n} b_j x^j\right)=\sum_{i=0}^{m}\sum_{j=0}^{n} a_i\sigma^i(b_j)x^{i+j} \ ,$$

$$F(x)G(x)=\left(\sum_{i=0}^{m} x^i\beta_i\right)\cdot\left(\sum_{j=0}^{n} x^j\alpha_j\right)=\sum_{i=0}^{m}\sum_{j=0}^{n} x^{i+j}\sigma^{-j}(\beta_i)\alpha_j \ .$$

The next Algorithms 1 and 2 show how to compute $\mathcal{C}_{d,s}(a)$ and $\mathcal{T}_{d,s}(a)$ (Definition 1.1.8).

Algorithm 1 Computation of $\mathcal{C}_{d,s}(a)$.

Input: $\mathcal{R}$, $d, s \in \mathbb{Z}_{\geq 0}$ and $a \in \mathbb{F}$
Output: $\mathcal{C}_{d,s}(a)$

Let $S_d \subset \mathbb{F}_2^{d+s}$ be the set of codewords with weight equal to d.
$\mathcal{C}_{d,s}(a) \leftarrow 0$
for all $(s_1, s_2, \ldots, s_{d+s}) \in S_d$ **do**
    $b \leftarrow a$
    for $i \leftarrow 1$ to $d+s$ **do**
        if $s_i = 0$ **then**
            $b \leftarrow \sigma(b)$
        else
            $b \leftarrow \delta(b)$
        end if
    end for
    $\mathcal{C}_{d,s}(a) \leftarrow \mathcal{C}_{d,s}(a) + b$
end for
return $\mathcal{C}_{d,s}(a)$

Algorithm 2 Computation of $\mathcal{T}_{d,s}(a)$.

Input: $\mathcal{R}$, σ^{-1}, $d, s \in \mathbb{Z}_{\geq 0}$ and $a \in \mathbb{F}$
Output: $\mathcal{T}_{d,s}(a)$

Let $S_d \subset \mathbb{F}_2^{d+s}$ be the set of codewords with weight equal to d.
$\mathcal{T}_{d,s}(a) \leftarrow 0$
for all $(s_1, s_2, \ldots, s_{d+s}) \in S_d$ **do**
    $b \leftarrow a$
    for $i \leftarrow 1$ to $d+s$ **do**
        if $s_i = 1$ **then**
            $b \leftarrow \delta(\sigma^{-1}(b))$
        else
            $b \leftarrow \sigma^{-1}(b)$
        end if
    end for
    $\mathcal{T}_{d,s}(a) \leftarrow \mathcal{T}_{d,s}(a) + b$
end for
return $\mathcal{T}_{d,s}(a)$

For instance, let $\mathbb{F}_4[x; \sigma, \delta]$ be the skew polynomial ring over the finite field $\mathbb{F}_4 = \{0, 1, w, w^2\}$, with $\sigma(a) = a^2$ and $\delta(a) = w(\sigma(a) + a)$ for all $a \in \mathbb{F}_4$. As an application of Algorithm 1, let us give here for this situation the following Magma program [3] (see Program 1).

We begin by typing the following instructions in Magma.

```
F<w>:=GF(4);
S:= map< F -> F | x :-> x^2 >;
D:= map< F -> F | x :-> w*(S(x)+x) >;
```

Then, by the following instructions, we define the function “PosCom".

Program 1.

```
PosCom:=function(d,s,a)
C:= [u: u in [VectorSpace(GF(2),d+s)!v : v in VectorSpace(GF(2),d+s)\
]| Weight(u) eq d];
A:=0;
 for k in [1..#C] do
  b:=a;
   for l in [1..d+s] do
    if C[k][l] eq 0 then
     b:=S(b);
     else
     b:=D(b);
    end if;
   end for;
  A:=A+b;
 end for;
return A;
end function;
```

Thus, to calculate the value of $\mathcal{C}_{1,2}(w) = \delta\sigma^2(w) + \sigma\delta\sigma(w) + \sigma^2\delta(w)$, we can simply write

```
PosCom(1,2,w);
```

which gives the answer w^2. Similarly, one can write a Magma program to calculate $\mathcal{T}_{d,s}(a)$ for any $d, s \in \mathbb{Z}_{\geq 0}$ and $a \in \mathbb{F}$.

Finally, using Algorithms 1 and 2, one can compute the products $f \cdot g$, $F \cdot G \in \mathcal{R}$ (see formulas (1.4) and (1.5)) by the next two algorithms (see Algorithms 3 and 4).

Algorithm 3 Computation of $f(x) \cdot g(x)$, where $f(x) = a_0 + a_1x + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$.

Input: $f, g \in \mathcal{R}$
Output: $M = f(x) \cdot g(x)$

$M \leftarrow 0$
for $i \leftarrow 1$ to Degree$(f) + 1$ **do**
  for $j \leftarrow 1$ to Degree$(g) + 1$ **do**
    for $k \leftarrow 0$ to $i - 1$ **do**
      $n \leftarrow (i - 1) + (j - 1) - k$
      $M \leftarrow M + a_{i-1} \cdot \mathcal{C}_{k,i-1-k}(b_{j-1}) \cdot x^n$
    end for
  end for
end for
return M

Algorithm 4 Computation of $F(x) \cdot G(x)$, where $F(x) = \beta_0 + x\beta_1 + \cdots + x^m\beta_m$ and $G(x) = \alpha_0 + x\alpha_1 + \cdots + x^n\alpha_n$.

Input: $F, G \in \mathcal{R}$
Output: $M = F(x) \cdot G(x)$

$M \leftarrow 0$
for $i \leftarrow 1$ to Degree$(F) + 1$ **do**
  for $j \leftarrow 1$ to Degree$(G) + 1$ **do**
    for $k \leftarrow 0$ to $j - 1$ **do**
      $n \leftarrow (i - 1) + (j - 1) - k$
      $M \leftarrow M + x^n \cdot (-1)^k \mathcal{T}_{k,j-1-k}(b_{i-1}) \cdot \alpha_{j-1}$
    end for
  end for
end for
return M

For instance, as an application of Algorithm 3, we give here a Magma program to compute the products fg and gf when $f = x^2 + 1$ and $g = x^2 + i$ are skew polynomials in $\mathbb{C}[x; \sigma, \delta]$ with $\sigma(z) = \bar{z}$ and $\delta(z) = z - \bar{z}$ for all $z \in \mathbb{C}$.

We begin by writing the following instructions:

```
F<i>:=ComplexField();
R<x>:=PolynomialRing(F);
S:= map< F -> F | x :-> ComplexConjugate(x) >;
D:= map< F -> F | x :-> x-ComplexConjugate(x) >;
```

then, using the function “PosCom" defined in Program 1, we can continue with the following instructions to define the new function “MultPol".

Program 2.

```
MultPol:=function(f,g)
M:=0;
 for i in [1..#f] do
  for j in [1..#g] do
   for k in [0..i-1] do
    n:=(i-1)+(j-1)-k;
    M:=M+f[i]*PosCom(k,i-k-1,g[j])*x^n;
   end for;
  end for;
 end for;
return M;
end function;
```

Thus, to calculate $(x^2+1)(x^2+i)$ and $(x^2+i)(x^2+1)$, we write in Magma

```
MultPol([1,0,1],[i,0,1]);
MultPol([i,0,1],[1,0,1]);
```

obtaining $x^4+(1+i)x^2-4ix+5i$ and $x^4+(1+i)x^2+i$, respectively.

Finally, let us recall here also the process of "evaluating" a skew polynomial $f(x) \in \mathcal{R}$ at an element $a \in \mathbb{F}$. To define an evaluation map for a skew polynomial ring, we need to consider the action of σ and δ. Indeed, the classical map that simply replaces the variable x with a value $a \in \mathbb{F}$ does not work in $\mathcal{R}$. So, Lam and Leroy in [21, p. 310] defined an appropriate evaluation using the fact that $\mathcal{R}$ is a right Euclidean domain.

Definition 1.1.11. For $a \in \mathbb{F}$ and $f \in \mathcal{R}$, where σ is an endomorphism (automorphism) of $\mathbb{F}$, we define the right (left) evaluation of f at a, denoted by $f(a)$ ($f_L(a)$), as the unique remainder upon right (left) division of f by $x-a$. In the special case when $f(a)=0$ ($f_L(a)=0$), we say that a is a *right (left) zero* of f.

We can also compute the right (left) evaluation of a polynomial in $\mathcal{R}$ at $a \in \mathbb{F}$ without using the right (left) division algorithm. To do this, we first need the following technical result.

Lemma 1.1.12. *Let σ be an automorphism of $\mathbb{F}$. Every skew polynomial $f=\sum_{i=0}^{m} a_i x^i \in \mathcal{R}$ can be represented as a polynomial with right-hand coefficients, that is, we can write*

$$f=\sum_{i=0}^{m} a_i x^i = \sum_{i=0}^{m} x^i \mathcal{A}_i \ ,$$

where

$$\mathcal{A}_i := \sum_{j=0}^{m-i} (-1)^j \mathcal{T}_{j,i}(a_{j+i}) \ , \quad \forall i = 0, ..., m \ . \tag{1.7}$$

Proof. By Lemma 1.1.10 we have

$$\sum_{i=0}^{m} a_i x^i = \sum_{i=0}^{m} \left(\sum_{k=0}^{i} x^{i-k} (-1)^k \mathcal{T}_{k,i-k}(a_i) \right) = \left(\sum_{h=0}^{m} x^0 (-1)^h \mathcal{T}_{h,0}(a_h) \right) +$$

$$+ \left(\sum_{h=1}^{m} x^1 (-1)^{h-1} \mathcal{T}_{h-1,1}(a_h) \right) + \cdots + \left(\sum_{h=m}^{m} x^m (-1)^{h-m} \mathcal{T}_{h-m,m}(a_h) \right) =$$

$$= x^0 \left(\sum_{j=0}^{m} (-1)^j \mathcal{T}_{j,0}(a_j) \right) + x^1 \left(\sum_{j=0}^{m-1} (-1)^j \mathcal{T}_{j,1}(a_{j+1}) \right) + \cdots + x^m \left(\sum_{j=0}^{m-m} (-1)^j \mathcal{T}_{j,m}(a_{j+m}) \right)$$

and this leads to the statement. □

Lemma 1.1.13. [21, Lemma 2.4] *For $f(x) = \sum_i a_i x^i \in \mathbb{F}[x; \sigma, \delta]$ and $a \in \mathbb{F}$, we have $f(a) = \sum_i a_i N_i^{\sigma,\delta}(a)$, where $N_0^{\sigma,\delta}(a) := 1$ and $N_i^{\sigma,\delta}(a) := \sigma(N_{i-1}^{\sigma,\delta}(a))a + \delta(N_{i-1}^{\sigma,\delta}(a))$.*

Lemma 1.1.14. [2, Theorem 3.1] *Let σ be an automorphism of $\mathbb{F}$. For $f(x) = \sum_i a_i x^i = \sum_i x^i \mathcal{A}_i \in \mathbb{F}[x; \sigma, \delta]$ and $a \in \mathbb{F}$, we have $f_L(a) = \sum_i M_i^{\sigma,\delta}(a)\mathcal{A}_i$, where $M_0^{\sigma,\delta}(a) := 1$ and $M_i^{\sigma,\delta}(a) := a\sigma^{-1}(M_{i-1}^{\sigma,\delta}(a)) - \delta\sigma^{-1}(M_{i-1}^{\sigma,\delta}(a))$.*

Example 1.1.15. In $\mathbb{F}_4[x; \sigma, 0]$ with $\sigma(a) = a^2$, the binomials $(x+1), (x+\alpha^2)$ and $(x+\alpha)$ are all right (left) factors of $f(x) := x^2 + 1$. Thus, $\mathcal{R}$ is not in general a unique factorization domain. Moreover, $\{1, \alpha, \alpha^2\}$ are right (left) zeros of $f(x)$, showing that in general a skew polynomial of degree $n \geq 2$ could have more than n roots, possibly infinite. For instance, consider $\mathbb{C}[x; \sigma, 0]$ with σ the complex conjugation (i.e. $\sigma(w) = \bar{w}$ for all $w \in \mathbb{C}$). Then, since $\sigma^{-1} = \sigma$, by applying Lemmas 1.1.13 and 1.1.14, we see that all the complex numbers z such that $|z| = 1$ are right (left) roots of the polynomial $x^2 - 1 \in \mathbb{C}[x; \sigma, 0]$.

For $f(x) = g(x)h(x) \in \mathcal{R}$ and $a \in \mathbb{F}$, we do not have $f(a) = g(a)h(a)$ in general. To properly define the right (left) evaluation of a product, we first need the notion of the right (left) (σ, δ)-conjugacy (see [21, p. 311–312] and [2, p. 24 for $\delta = 0$]).

Definition 1.1.16. Given $a \in \mathbb{F}$, $c \in \mathbb{F}^* := \mathbb{F} \setminus \{0\}$, we define the right (left) (σ, δ)-*conjugate* a^c (${}^c a$) of a with respect to c as

$$a^c := \sigma(c)ac^{-1} + \delta(c)c^{-1} \in \mathbb{F} \qquad (\ {}^c a := c^{-1}a\sigma^{-1}(c) - c^{-1}\delta(\sigma^{-1}(c)) \in \mathbb{F} \ ) \ .$$

Lemma 1.1.17. [21, p. 311 for the right case] *Given $a, b \in \mathbb{F}$ and $c, d \in \mathbb{F}^*$, we have $a^1 = a$ $({}^1a = a)$, $(a^c)^d = a^{dc}$ $({}^d({}^ca) = {}^{cd}a)$ and the relation $\sim$ $(\sim_L)$ defined on $\mathbb{F}$ as*

$$a \sim b \iff \exists\ e \in \mathbb{F}^* \text{ such that } b = a^e \quad (a \sim_L b \iff \exists\ e \in \mathbb{F}^* \text{ such that } b = {}^ea),$$

is an equivalence relation on $\mathbb{F}$.

Using Definition 1.1.16, the following result provides formulas for right (left) evaluating a product (see [21, Theorem 2.7] and [2, Theorem 3.2 for $\delta = 0$]).

Theorem 1.1.18. *Let $f(x), g(x) \in \mathcal{R}$ and $a \in \mathbb{F}$. Then the following properties hold:*

1) *If $g(a) = 0$, then $(f \cdot g)(a) = 0$; if $g(a) \neq 0$ then $(f \cdot g)(a) = f\left(a^{g(a)}\right) g(a)$;*

2) *If $g_L(a) = 0$, then $(g \cdot f)_L(a) = 0$; if $g_L(a) \neq 0$ then $(g \cdot f)_L(a) = g_L(a) f_L\left({}^{g_L(a)}a\right)$.*

Proof. The statements 1) and 2) follows directly from Theorem 2.7 of [21] and a slight modification of its proof. □

1.2 Multivariate skew polynomial rings

As before, denote by $\mathbb{F}$ a division ring. Using similar notation as in [23] for positive integers m and n, $\mathbb{F}^{m\times n}$ will denote the set of $m \times n$ matrices over $\mathbb{F}$, and $\mathbb{F}^n$ will denote the set of column vectors of length n over $\mathbb{F}$, that is, $\mathbb{F}^n = \mathbb{F}^{n\times 1}$.

Following the main ideas given in [23], we begin by recalling the definition of the free multivariate skew polynomial ring, which corresponds to a multivariate generalization of the ring of univariate skew polynomials given in Definition 1.1.6. To do this, we need to introduce the concept of σ-vector derivation that extends Definition 1.1.1.

Definition 1.2.1. [23, Definition 1] Given a ring homomorphism

$$\sigma : \mathbb{F} \to \mathbb{F}^{n\times n},\ a \mapsto \begin{pmatrix} \sigma_{1,1}(a) & \sigma_{1,2}(a) & \cdots & \sigma_{1,n}(a) \\ \sigma_{2,1}(a) & \sigma_{2,2}(a) & \cdots & \sigma_{2,n}(a) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{n,1}(a) & \sigma_{n,2}(a) & \cdots & \sigma_{n,n}(a) \end{pmatrix},$$

we say that

$$\delta : \mathbb{F} \to \mathbb{F}^n\ ,\ a \mapsto \begin{pmatrix} \delta_1(a) \\ \delta_2(a) \\ \vdots \\ \delta_n(a) \end{pmatrix}$$

is a *σ-vector derivation* (over $\mathbb{F}$), if it is an additive group homomorphism and satisfies $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ for all $a, b \in \mathbb{F}$. The ring homomorphism $\sigma : \mathbb{F} \to \mathbb{F}^{n\times n}$ will be called a *matrix morphism*. The maps $\sigma_{i,j} : \mathbb{F} \to \mathbb{F}$, $\delta_i : \mathbb{F} \to \mathbb{F}$ are called *component functions* of σ and δ, respectively.

Example 1.2.2. [23, Example 4] Let $\sigma : \mathbb{F} \to \mathbb{F}^{n\times n}$ be a matrix morphism and let $\mathbf{v} \in \mathbb{F}^n$. The map $\delta : \mathbb{F} \to \mathbb{F}^n$ defined by $\delta(a)_{\mathbf{v}} = \sigma(a)\mathbf{v} - \mathbf{v}a$, for all $a \in \mathbb{F}$, is a σ-vector derivation. When $n = 1$, these vector derivations are called inner derivations.

By using Definition 1.2.1, we define the ring of free multivariate skew polynomials.

Definition 1.2.3. Let $x_1, x_2, ..., x_n$ be n pair-wise distinct letters, which we will call *variables*, and we denote by $\mathcal{M}$ the set of all finite strings using these characters, that is, the free (non-commutative) monoid with left basis $x_1, x_2, ..., x_n$. The empty string will be denoted by 1, a character x_i will be called a *variable*, an element $m \in \mathcal{M}$ formed by such variables will be called a *monomial*, and we will define its degree, denoted by $\deg(m)$, as its length as a string. We define the *Free multivariate skew polynomial ring* over $\mathbb{F}$ in the variables $x_1, x_2, ..., x_n$ with matrix morphism σ, σ-vector derivation δ and denoted by

$$\mathcal{A} := \mathbb{F}[\mathbf{x}; \sigma, \delta],$$

as the free left $\mathbb{F}$-module with left basis $\mathcal{M}$ and product given by appending monomials with the rule

$$\mathbf{x} \cdot a = \sigma(a)\mathbf{x} + \delta(a) \tag{1.8}$$

for all $a \in \mathbb{F}$. Each element $F(\mathbf{x}) \in \mathcal{A}$ is called a *free multivariate skew polynomial*, or simply skew polynomial, and can be expressed uniquely as a left linear combination

$$F(\mathbf{x}) = \sum_{m\in\mathcal{M}} F_m m,$$

where $F_m \in \mathbb{F}$ are all zero except for a finite number of monomials.

Remark 1.2.4. If we denote by $\mathbf{x} = (x_1, x_2, \cdots, x_n)^T \in \mathcal{M}^n$, then (1.8) is a short form of writing the equations:

$$x_i a = \sum_{j=1}^{n} \sigma_{i,j}(a)x_j + \delta_i(a), \tag{1.9}$$

for $i = 1, 2, ..., n$. On the other hand, if we denote by $Id : \mathbb{F} \to \mathbb{F}^{n\times n}$ the ring morphism given by $Id(a) = aI$, for $a \in \mathbb{F}$, where $I \in \mathbb{F}^{n\times n}$ is the $n \times n$ identity matrix, then

$\mathbb{F}[\mathbf{x}; Id, 0]$ is the free conventional polynomial ring in the variables $x_1, x_2, ..., x_n$ (see [9, Sec. 0.11]) which do not commute with each other, but commute with constants.

Thanks to the lack of relations among the variables, it was proven in [23, Lemma 5] that, for any $a_1, a_2, ..., a_n \in \mathbb{F}$ and any $F(\mathbf{x}) \in \mathcal{A}$, there exist unique $G_1(\mathbf{x})$, $G_2(\mathbf{x}), ...,$ $G_n(\mathbf{x}) \in \mathcal{A}$ and $b \in \mathbb{F}$ such that

$$F(\mathbf{x}) = \sum_{i=1}^{n} G_i(\mathbf{x})(x_i - a_i) + b \tag{1.10}$$

Hence, we may define the right (σ, δ)-evaluation of F at $\mathbf{a} \in \mathbb{F}^n$ as follows.

Definition 1.2.5. [23, Definition 9] For $\mathbf{a} = (a_1, a_2, \cdots, a_n) \in \mathbb{F}^n$ and any skew polynomial $F \in \mathcal{A}$, we define its right evaluation at $\mathbf{a}$, denoted by $F(\mathbf{a})$, as the unique constant $b \in \mathbb{F}$ of (1.10).

The following result allows to compute the right evaluation of any monomial $m \in \mathcal{M}$ at any point $\mathbf{a} \in \mathbb{F}^n$, using the so-called fundamentals functions $N_m^{\sigma,\delta} : \mathbb{F}^n \to \mathbb{F}$, for $m \in \mathcal{M}$. Note that these functions generalize the $N_i^{\sigma,\delta}$ functions of the case $n = 1$ given in Lemma 1.1.13.

Theorem 1.2.6. [23, Theorem 2] Given a monomial $m \in \mathcal{M}$ and a point $\mathbf{a} \in \mathbb{F}^n$, denote by $N_m(\mathbf{a}) \in \mathbb{F}$ the right evaluation of the skew monomial m at $\mathbf{a}$. It holds that

$$N_{\mathbf{x}m}(\mathbf{a}) = \begin{pmatrix} N_{x_1 m}(\mathbf{a}) \\ N_{x_2 m}(\mathbf{a}) \\ \vdots \\ N_{x_n m}(\mathbf{a}) \end{pmatrix} = \sigma(N_m(\mathbf{a}))\mathbf{a} + \delta(N_m(\mathbf{a})) \in \mathbb{F}^n$$

To properly define the right evaluation of a product, we first need the notion of the (σ, δ)-conjugacy.

Definition 1.2.7. [23, Definition 11] Given $\mathbf{a} \in \mathbb{F}^n$, $c \in \mathbb{F}^*$, we define the (σ, δ)-*conjugate of* $\mathbf{a}$ *with respect to* c as

$$\mathbf{a}^c := \sigma(c)\mathbf{a}c^{-1} + \delta(c)c^{-1} \in \mathbb{F}^n$$

Then, we have the following result which extends the right case $n = 1$ given in Lemma 1.1.17.

Lemma 1.2.8. [23, Lemma 12] Given $\mathbf{a}, \mathbf{b} \in \mathbb{F}^n$ and $c, d \in \mathbb{F}^*$, the following properties hold:

1) $\mathbf{a}^1 = \mathbf{a}$ and $(\mathbf{a}^c)^d = \mathbf{a}^{dc}$;

2) The relation $\sim$ defined on $\mathbb{F}^n$ as

$$\mathbf{a} \sim \mathbf{b} \iff \text{there exists } e \in \mathbb{F}^* \text{ such that } \mathbf{b} = \mathbf{a}^e,$$

is an equivalence relation on $\mathbb{F}^n$.

By Lemma 1.2.8, let us denote by $[\mathbf{a}] := \{\mathbf{a}^c : c \in \mathbb{F}^*\}$ the (σ, δ)-conjugacy class of $\mathbf{a} \in \mathbb{F}^n$. Using the notion of (σ, δ)-conjugation, we can give the following result that extends Theorem 1.1.18 1) and allows us to evaluate a product of two skew polynomials

Theorem 1.2.9. [23, Theorem 3] Consider two skew polynomials $F, G \in \mathcal{A}$ and $\mathbf{a} \in \mathbb{F}^n$. If $G(\mathbf{a}) = 0$, then $(FG)(\mathbf{a}) = 0$. If $G(\mathbf{a}) \neq 0$ then

$$(FG)(\mathbf{a}) = F(\mathbf{a}^{G(\mathbf{a})})G(\mathbf{a})$$

Finally, we show in the following example that in general the ring $\mathcal{A}$ is not Noetherian, unlike the case $n = 1$.

Example 1.2.10. Consider $\mathcal{A} := \mathbb{F}[x_1, x_2; \sigma, \delta]$ and the left (right) ideals

$$I_k := \mathcal{A}x_1x_2 + \mathcal{A}x_1x_2^2 + ... + \mathcal{A}x_1x_2^k \quad (I_{k,A} := x_1x_2\mathcal{A} + x_1x_2^2\mathcal{A} + ... + x_1x_2^k\mathcal{A})$$

with $k \geq 1$. We note that $I_1 \subsetneq I_2 \subsetneq ... \subsetneq I_k \subsetneq \mathcal{A}$ ($I_{1,A} \subsetneq I_{2,A} \subsetneq ... \subsetneq I_{k,A} \subsetneq \mathcal{A}$) because the variables x_1, x_2 do not commute and $x_1 \notin I_1$ ($I_{1,A}$). Then $\mathcal{A}$ does not satisfy the ascending chain condition on left and right ideals and therefore it is not Noetherian. In particular, when $\sigma = Id$ and $\delta = 0$, the free conventional polynomial ring $\mathbb{F}[\mathbf{x}; Id, 0]$ is not Noetherian.

Chapter 2

Derivatives for skew polynomials

Based on properties of the rings $\mathcal{A}$ and $\mathcal{R}$, we define here some notions of (σ, δ)-derivatives for multivariate and univariate skew polynomials. The tools presented in this chapter will be useful to solve a Hermite-type interpolation problem in $\mathcal{A}$ (see Theorem 3.1.12) and to provide equivalent conditions to the fact that a skew polynomial in $\mathcal{R}$ admits a right or left root of positive multiplicity (see Theorems 4.3.3 and 4.3.5).

2.1 (σ, δ)-Partial derivatives

We begin by introducing the concept of right (σ, δ)-partial derivative (for simplicity, partial derivative) for any skew polynomial in $\mathcal{A}$. Thanks to Lemma 5 of [23], we can give the following new definition.

Definition 2.1.1. Let $F \in \mathcal{A}$ and $\mathbf{a} = (a_1, ..., a_n) \in \mathbb{F}^n$. For every $i = 1, ..., n$, we define the *right (σ, δ)-first partial derivative of F at $\mathbf{a}$ with respect to the variable x_i* as the right evaluation of the unique skew polynomial $\Delta_{\mathbf{a}}^{x_i} F$ at the point $\mathbf{a}$, which is obtained by writing

$$F = \sum_{i=1}^{n} \Delta_{\mathbf{a}}^{x_i} F \cdot (x_i - a_i) + F(\mathbf{a}).$$

The skew polynomial $\Delta_{\mathbf{a}}^{x_i} F \in \mathcal{A}$ will be called *right (σ, δ)-partial derivative polynomial of F at $\mathbf{a}$ with respect to the variable x_i*. Moreover, we will denote $F(\mathbf{a})$ by $\Delta_{\mathbf{a}}^{0} F(\mathbf{a})$.

However, to define analogously left (σ, δ)-partial derivatives, we need a left-hand version of [23, Lemma 5] as follows.

Lemma 2.1.2. *For any $a_1, ..., a_n \in \mathbb{F}$ and any $F \in \mathcal{A}$, there exist unique $G_1, G_2, ..., G_n \in \mathcal{A}$ and $b \in \mathbb{F}$ such that*

$$F = \sum_{i=1}^{n}(x_i - a_i) \cdot G_i + b \tag{2.1}$$

if and only if the map $\varphi : \mathbb{F}^n \to \mathbb{F}^n$, defined by

$$\varphi\left((\gamma_1, \gamma_2, ..., \gamma_n)\right) := \left(\sum_{j=1}^{n}\sigma_{j,1}(\gamma_j), \sum_{j=1}^{n}\sigma_{j,2}(\gamma_j), ..., \sum_{j=1}^{n}\sigma_{j,n}(\gamma_j)\right) \tag{2.2}$$

is an isomorphism of additive groups, where $\sigma_{i,j} : \mathbb{F} \to \mathbb{F}$ are the component functions of $\sigma : \mathbb{F} \to \mathbb{F}^{n\times n}$.

Proof. First, evidently φ is an additive group homomorphism because the maps $\sigma_{i,j}$ are additive group homomorphisms. Since $F \in \mathcal{A}$ is a sum of monomials, it is sufficient to consider only monomials of the form $\alpha_k x_k$ ($\alpha_k \in \mathbb{F}$) for $k = 1, 2, .., n$.
Let $\alpha := (\alpha_1, \alpha_2, ..., \alpha_n) \in \mathbb{F}^n$ and write

$$\alpha_k x_k = \sum_{j=1}^{n}(x_j - a_j)G_{j,k} + b_k \quad (*)$$

with $G_{j,k}, b_k \in \mathbb{F}$. By (1.9), for every $k = 1, 2, ..., n$, we have

$$\alpha_k x_k = \sum_{j=1}^{n}\left(\sum_{i=1}^{n}\sigma_{i,j}(G_{i,k})\right)x_j + \sum_{j=1}^{n}(\delta_j(G_{j,k}) - a_j G_{j,k}) + b_k.$$

Then

$$\alpha_k = \sum_{i=1}^{n}\sigma_{i,k}(G_{i,k}),\ b_k = \sum_{j=1}^{n}(\delta_j(G_{j,k}) - a_j G_{j,k}) \text{ and } \sum_{i=1}^{n}\sigma_{i,j}(G_{i,k}) = 0 \text{ for all } j \neq k. \ (**)$$

Thus,

$$\begin{aligned}
\varphi((G_{1,1}, G_{2,1}, ..., G_{n,1})) &= (\alpha_1, 0, ..., 0)\\
\varphi((G_{1,2}, G_{2,2}, ..., G_{n,2})) &= (0, \alpha_2, ..., 0)\\
\vdots &= \vdots\\
\varphi((G_{1,n}, G_{2,n}, ..., G_{n,n})) &= (0, 0, ..., \alpha_n)
\end{aligned}$$

Therefore, $\alpha = \varphi((\beta_1, \beta_2, ..., \beta_n))$ for some $(\beta_1, \beta_2, ..., \beta_n) \in \mathbb{F}^n$ with $\beta_i = \sum_{j=1}^{n} G_{i,j}$ for $i = 1, 2, ..., n$. This proves that φ is a surjective homomorphism. On the other hand, by the uniqueness of the $G_{j,k}$ for all $k = 1, ..., n$, it follows that φ is injective and therefore and isomorphism of additive groups. Conversely, if φ is a group isomorphism, then given

$(\alpha_1, 0, ..., 0), (0, \alpha_2, ..., 0), ..., (0, ..., 0, \alpha_n) \in \mathbb{F}^n$, there exist unique $G_{1,k}, G_{2,k}, ..., G_{n,k}, b_k \in \mathbb{F}$ for all $k = 1, ..., n$ such that $(**)$ holds. Then, $\alpha_k x_k$ can be written as in $(*)$ and we are done. □

Remark 2.1.3. Note that for the case $n = 1$, the condition that φ is a group isomorphism is equivalent to ask that σ is an automorphism of $\mathbb{F}$. On the other hand, in the special case when $\sigma : \mathbb{F} \to \mathbb{F}^{n\times n}$ is a diagonal homomorphism, i.e. $\sigma_{i,j}(a) = 0$ for all $i \neq j$, it follows that any skew polynomial in $\mathcal{A}$ can be written as in (2.1) if and only if the component functions $\sigma_{i,i} : \mathbb{F} \to \mathbb{F}$ are ring automorphisms. Moreover, in this situation we can give explicit formulas to write ax_i as in (2.1). Indeed, for any $i = 1, ..., n$, we have

$$ax_i = (x_i - a_i)\sigma_{i,i}^{-1}(a) + a_i\sigma_{i,i}^{-1}(a) - \delta_i(\sigma_{i,i}^{-1}(a)).$$

From Lemma 2.1.2 and under the assumption that the map φ defined in (2.2) is a surjective additive group homomorphism, we can define the left (σ, δ)-evaluation of any skew polynomial $F \in \mathcal{A}$ at $\mathbf{a} \in \mathbb{F}^n$ and introduce the notion of left (σ, δ)-partial derivative as follows.

Definition 2.1.4. Let $\varphi : \mathbb{F}^n \to \mathbb{F}^n$ be a group isomorphism as in (2.2). For $\mathbf{a} = (a_1, a_2, \cdots, a_n) \in \mathbb{F}^n$ and any skew polynomial $F \in \mathcal{A}$, we define its left (σ, δ)-evaluation at $\mathbf{a}$, denoted by $F_L(\mathbf{a})$, to be the unique constant $b \in \mathbb{F}$ as in (2.1).

Definition 2.1.5. Let $\varphi : \mathbb{F}^n \to \mathbb{F}^n$ be a group isomorphism as in (2.2), $F \in \mathcal{A}$ and $\mathbf{a} := (a_1, ..., a_n) \in \mathbb{F}^n$. For all $i = 1, ..., n$, we define the *left (σ, δ)-first partial derivative of F at $\mathbf{a}$ with respect to the variable x_i* as the left (σ, δ)-evaluation of the skew polynomial $\Delta^{x_i}_{\mathbf{a},L}F$ at the point $\mathbf{a}$, obtained by writing as in (2.1)

$$F = \sum_{i=1}^{n}(x_i - a_i) \cdot \Delta^{x_i}_{\mathbf{a},L}F + F_L(\mathbf{a}).$$

The skew polynomial $\Delta^{x_i}_{\mathbf{a},L}F \in \mathcal{A}$ will be called *left (σ, δ)-partial derivative polynomial of F at $\mathbf{a}$ with respect to the variable x_i*. Moreover, we will denote $F_L(\mathbf{a})$ by $\Delta^0_{\mathbf{a},L}F(\mathbf{a})$.

Furthermore, we can define recursively right (left) (σ, δ)-partial derivatives of higher order of any multivariate skew polynomial in $\mathcal{A}$.

Definition 2.1.6. Let $F \in \mathcal{A}$ and let $\mathbf{a} \in \mathbb{F}^n$. For all $i = 1, ..., n$, we define the *right (left-with φ isomorphism) second (σ, δ)-partial derivative of F at $\mathbf{a}$ with respect to x_jx_i*, denoted by $\Delta^{x_jx_i}_{\mathbf{a}}F(\mathbf{a})$ ($\Delta^{x_jx_i}_{\mathbf{a},L}F(\mathbf{a})$), as the right (left) (σ, δ)-partial derivative at $\mathbf{a}$ with

respect to x_j of $\Delta_{\mathbf{a}}^{x_i}F$ ($\Delta_{\mathbf{a},L}^{x_i}F$), evaluated at the point $\mathbf{a}$, that is,

$$\Delta_{\mathbf{a}}^{x_jx_i}F(\mathbf{a}) := \Delta_{\mathbf{a}}^{x_j}(\Delta_{\mathbf{a}}^{x_i}F)(\mathbf{a}) \quad ((\Delta_{\mathbf{a},L}^{x_jx_i}F)_L(\mathbf{a}) := (\Delta_{\mathbf{a},L}^{x_j}(\Delta_{\mathbf{a},L}^{x_i}F))_L(\mathbf{a}))$$

More general, given any $m = x_{i_1}x_{i_2}...x_{i_s} \in \mathcal{M}$ with $i_l \in \{1,...,n\}$ for all $l = 1,...,n$, we define recursively the right (left-with φ isomorphism) (σ,δ)-*partial derivative of* F *at* $\mathbf{a}$ *with respect to* m as

$$\Delta_{\mathbf{a}}^{m}F(\mathbf{a}) := \Delta_{\mathbf{a}}^{x_{i_1}}(\Delta_{\mathbf{a}}^{x_{i_2}\cdots x_{i_s}}F)(\mathbf{a}) \quad ((\Delta_{\mathbf{a},L}^{m}F)_L(\mathbf{a}) := (\Delta_{\mathbf{a},L}^{x_{i_1}}(\Delta_{\mathbf{a},L}^{x_{i_2}\cdots x_{i_s}}F))_L(\mathbf{a}))$$

Remark 2.1.7. Let $\mathbb{F}$ be a division ring and let $\mathbf{a} = (a_1, a_2, ..., a_n) \in \mathbb{F}^n$. In the special case when $\sigma = Id$ and $\delta = 0$, we obtain a notion of partial derivative of classical type. For instance, given $F = x_1^2x_2 \in \mathbb{F}[x; Id, 0]$ and fixed the lexicographic order $<_{\text{lex}}$ over $\mathbb{F}[x; Id, 0]$, we have

$$F = (a_2x_1 + a_2a_1)(x_1 - a_1) + x_1^2(x_2 - a_2) + a_2a_1^2$$

Then, $\Delta_{\mathbf{a}}^{x_1}F(\mathbf{a}) = 2a_2a_1$ and $\Delta_{\mathbf{a}}^{x_2}F(\mathbf{a}) = a_1^2$. Note that if $\mathbb{F}$ is a commutative division ring, then we can write $\Delta_{\mathbf{a}}^{x_1}F(\mathbf{a}) = 2a_1a_2$. On the other hand, we have $\Delta_{\mathbf{a}}^{x_1x_2}F(\mathbf{a}) = 2a_1 \neq \Delta_{\mathbf{a}}^{x_2x_1}F(\mathbf{a}) = 0$. This shows that, unlike in the classical case, in general the mixed partial derivative of a multivariate skew polynomial are not equal.

The linearity of the right (left-with φ isomorphism) (σ,δ)-partial derivatives is shown below.

Lemma 2.1.8. *Let* $F, G \in \mathcal{A}$, $\mathbf{a} \in \mathbb{F}^n$, $\lambda \in \mathbb{F}$ *and* $m \in \mathcal{M}$. *The following properties hold:*

1) $\Delta_{\mathbf{a}}^{m}\lambda = 0$ $(\Delta_{\mathbf{a},L}^{m}\lambda = 0)$;

2) $\Delta_{\mathbf{a}}^{m}(\lambda F + G) = \lambda(\Delta_{\mathbf{a}}^{m}F) + \Delta_{\mathbf{a}}^{m}G \quad (\Delta_{\mathbf{a},L}^{m}(F\lambda + G) = (\Delta_{\mathbf{a},L}^{m}F)\lambda + \Delta_{\mathbf{a},L}^{m}G)$.

Proof. We will only show that the statements are valid for right (σ,δ)-partial derivatives, because for the left case the proof are analogous, provided that φ is a group isomorphism.

1) Since $\lambda = \sum_{k=1}^{n} 0 \cdot (x_i - a_i) + \lambda$ it follows that $\Delta_{\mathbf{a}}^{x_i}\lambda = 0$ for all $i = 1,...,n$. Therefore, for any $m \in \mathcal{M}$, we have $\Delta_{\mathbf{a}}^{m}\lambda = 0$.

2) It is sufficient to show that it is valid for any variable x_i with $i = 1,..,n$. In fact, we can write $\lambda F = \sum_{i=1}^{n} \lambda\Delta_{\mathbf{a}}^{x_i}F \cdot (x_i - a_i) + \lambda F(\mathbf{a})$, $G = \sum_{i=1}^{n} \Delta_{\mathbf{a}}^{x_i}G \cdot (x_i - a_i) + G(\mathbf{a})$. Then,

$$\lambda F + G = \sum_{i=1}^{n} (\lambda\Delta_{\mathbf{a}}^{x_i}F + \Delta_{\mathbf{a}}^{x_i}G) \cdot (x_i - a_i) + \lambda F(\mathbf{a}) + G(\mathbf{a})$$

Thus, for each variable x_i, we have $\Delta_{\mathbf{a}}^{x_i}(\lambda F+G)=\lambda(\Delta_{\mathbf{a}}^{x_i}F)+\Delta_{\mathbf{a}}^{x_i}G$. Finally, by a recursive argument, it follows that for any $m\in\mathcal{M}$, $\Delta_a^m(\lambda F+G)=\lambda(\Delta_a^m F)+\Delta_a^m G$. □

By using Lemma 2.1.8, we can obtain a useful formula to compute the right (left) (σ,δ)-partial derivatives of a product of two multivariate skew polynomials in $\mathcal{A}$.

Lemma 2.1.9. *Given $F,G\in\mathcal{A}$, $\mathbf{a}\in\mathbb{F}^n$, $\lambda\in\mathbb{F}$ and $m:=x_{i_1}\cdots x_{i_s}\in\mathcal{M}$ with $i_l\in\{1,\ldots,n\}$ for all $l=1,\ldots,n$, we have*

$$\Delta_{\mathbf{a}}^m(F\cdot G)=F\cdot\Delta_{\mathbf{a}}^m G+\sum_{k=1}^{s}\Delta_{\mathbf{a}}^{x_{i_1}\cdots x_{i_k}}\left(F\cdot\Delta_{\mathbf{a}}^{x_{i_{k+1}}\cdots x_{i_s}}G(\mathbf{a})\right),\tag{2.3}$$

$$\Delta_{\mathbf{a},L}^m(F\cdot G)=\Delta_{\mathbf{a},L}^m F\cdot G+\sum_{k=1}^{s}\Delta_{\mathbf{a},L}^{x_{i_1}\cdots x_{i_k}}\left(F_L(\mathbf{a})\cdot\Delta_{\mathbf{a},L}^{x_{i_{k+1}}\cdots x_{i_s}}G\right).\tag{2.4}$$

Proof. We begin by showing that (2.3) holds for any variable x_i for $i=1,\ldots,n$. Indeed, we have

$$\begin{aligned}F\cdot G&=\sum_{i=1}^{n}F\cdot\Delta_{\mathbf{a}}^{x_i}G\cdot(x_i-a_i)+F\cdot G(\mathbf{a})\\&=\sum_{i=1}^{n}F\cdot\Delta_{\mathbf{a}}^{x_i}G\cdot(x_i-a_i)+\sum_{i=1}^{n}\Delta_{\mathbf{a}}^{x_i}(F\cdot G(\mathbf{a}))(x_i-a_i)+(F\cdot G(\mathbf{a}))(\mathbf{a})\\&=\sum_{i=1}^{n}\left(F\cdot\Delta_{\mathbf{a}}^{x_i}G+\Delta_{\mathbf{a}}^{x_i}(F\cdot G(\mathbf{a}))\right)(x_i-a_i)+(F\cdot G(\mathbf{a}))(\mathbf{a})\end{aligned}$$

Thus, $\Delta_{\mathbf{a}}^{x_i}(F\cdot G)=F\cdot\Delta_{\mathbf{a}}^{x_i}G+\Delta_{\mathbf{a}}^{x_i}(F\cdot G(\mathbf{a}))$. Suppose (2.3) holds for any monomial $m'\in\mathcal{M}$ such that $\deg(m')=s-1$. Then, we have

$$\begin{aligned}\Delta_{\mathbf{a}}^m(F\cdot G)&=\Delta_{\mathbf{a}}^{x_{i_1}}\left(\Delta_{\mathbf{a}}^{x_{i_2}\cdots x_{i_s}}(F\cdot G)\right)\\&=\Delta_{\mathbf{a}}^{x_{i_1}}\left(F\cdot\Delta_{\mathbf{a}}^{x_{i_2}\cdots x_{i_s}}G+\sum_{k=2}^{s}\Delta_{\mathbf{a}}^{x_{i_2}\cdots x_{i_k}}\left(F\cdot\Delta_{\mathbf{a}}^{x_{i_{k+1}}\cdots x_{i_s}}G(\mathbf{a})\right)\right)\\&=\Delta_{\mathbf{a}}^{x_{i_1}}\left(F\cdot\Delta_{\mathbf{a}}^{x_{i_2}\cdots x_{i_s}}G\right)+\Delta_{\mathbf{a}}^{x_{i_1}}\left(\sum_{k=2}^{s}\Delta_{\mathbf{a}}^{x_{i_2}\cdots x_{i_k}}\left(F\cdot\Delta_{\mathbf{a}}^{x_{i_{k+1}}\cdots x_{i_s}}G(\mathbf{a})\right)\right)\\&=F\cdot\Delta_{\mathbf{a}}^m G+\sum_{k=1}^{s}\Delta_{\mathbf{a}}^{x_{i_1}\cdots x_{i_k}}\left(F\cdot\Delta_{\mathbf{a}}^{x_{i_{k+1}}\cdots x_{i_s}}G(\mathbf{a})\right),\end{aligned}$$

where the third equality is due to the linearity of the right (σ,δ)-partial derivatives and the last equality is due to what was shown in the previous case. Finally, by similar arguments, one can prove that formula (2.4) holds. □

Finally, let us show here that every skew polynomial $F \in \mathcal{A}$ can be written in terms of its right and left (σ,δ)-partial derivatives and keeping in mind that the left (σ,δ)-partial derivatives exist under the assumption that φ defined in (2.2) is a group isomorphism. This allows us to obtain a right and left multivariate Taylor-type expansion of F centered at a point $\mathbf{a} = (a_1, ..., a_n) \in \mathbb{F}^n$.

Proposition 2.1.10 (**Skew Taylor-type expansion**). *Let $F(\mathbf{x}) \in \mathcal{A}$ and let $\mathbf{a} \in \mathbb{F}^n$. The following properties hold:*

$$F(\mathbf{x}) = \sum_{k=1}^{\deg F} \left(\sum_{i_1,i_2,...,i_k=1}^{n} \Delta_{\mathbf{a}}^{x_{i_1}x_{i_2}\cdots x_{i_k}} F(\mathbf{a})(x_{i_k} - a_{i_k}) \cdots (x_{i_2} - a_{i_2})(x_{i_1} - a_{i_1}) \right) + F(\mathbf{a}) \tag{2.5}$$

$$F(\mathbf{x}) = \sum_{k=1}^{\deg F} \left(\sum_{i_1,i_2,...,i_k=1}^{n} (x_{i_1} - a_{i_1})(x_{i_2} - a_{i_2}) \cdots (x_{i_k} - a_{i_k})(\Delta_{\mathbf{a},L}^{x_{i_1}x_{i_2}\cdots x_{i_k}} F)_L(\mathbf{a}) \right) + F_L(\mathbf{a}) \tag{2.6}$$

Proof. By Definition 2.1.1, for any variables x_i, x_j with $i, j \in \{1, 2, ..., n\}$, we have

$$F(\mathbf{x}) = \sum_{i=1}^{n} \Delta_{\mathbf{a}}^{x_i} F(x) \cdot (x_i - a_i) + F(\mathbf{a}), \quad \Delta_{\mathbf{a}}^{x_i} F(x) = \sum_{j=1}^{n} \Delta_{\mathbf{a}}^{x_j x_i} F \cdot (x_j - a_j) + \Delta_{\mathbf{a}}^{x_i} F(\mathbf{a}).$$

Then, by substituting $\Delta_{\mathbf{a}}^{x_i} F(x)$ in $F(\mathbf{x})$, it follows that

$$\begin{aligned} F(\mathbf{x}) &= \sum_{i=1}^{n} \left(\sum_{j=1}^{n} \Delta_{\mathbf{a}}^{x_j x_i} F(\mathbf{x})(x_j - a_j)(x_i - a_i) \right) + \sum_{i=1}^{n} \Delta_{\mathbf{a}}^{x_i} F(\mathbf{a})(x_i - a_i) + F(\mathbf{a}) \\ &= \sum_{i_1,i_2=1}^{n} \left(\Delta_{\mathbf{a}}^{x_{i_2}x_{i_1}} F(\mathbf{x})(x_{i_2} - a_{i_1})(x_{i_1} - a_{i_1}) \right) + \sum_{i_1=1}^{n} \Delta_{\mathbf{a}}^{x_{i_1}} F(\mathbf{a})(x_{i_1} - a_{i_1}) + F(\mathbf{a}) \, . \end{aligned}$$

Finally, by a recursive argument we can obtain (2.5). The proof of (2.6) is analogous. □

2.2 (σ,δ)-Univariate derivatives

In this section, we will give only some further remarks for the (σ,δ)-derivatives of skew polynomials in $\mathcal{R}$. First, note that specializing Definitions 2.1.1 (2.1.5) to the case $n = 1$, we obtain the following definitions of right (left) (σ,δ)-derivatives in $\mathcal{R}$.

Definition 2.2.1. Let $f \in \mathcal{R}$ with σ an endomorphism (automorphism) of $\mathbb{F}$ and $a \in \mathbb{F}$. We define the *first right (left)* (σ,δ)*-derivative* of f at a as the right (left) (σ,δ)-evaluation of $\Delta_a^1 f(x) \in \mathcal{R}$ ($\Delta_{a,L}^1 f(x) \in \mathcal{R}$) at the point a, where $\Delta_a^1 f(x)$ ($\Delta_{a,L}^1 f(x)$) is obtained

by writing $f(x)=\Delta_a^1 f(x)\cdot(x-a)+f(a)$ $(f(x)=(x-a)\cdot\Delta_{a,L}^1 f(x)+f_L(a))$. The skew polynomial $\Delta_a^1 f(x)$ $(\Delta_{a,L}^1 f(x))$ will be called the *first right (left)* (σ,δ)*-derivative polynomial of* f *by* a.

By a recursive argument, from Definition 2.2.1 one can construct the right (left) (σ,δ)-derivative polynomials of higher order for any polynomial in $\mathcal{R}$.

Definition 2.2.2. Let σ be an endomorphism (automorphism) of $\mathbb{F}$. Given $f\in\mathcal{R}$, $r\in\mathbb{Z}_{>0}$ and a sequence $\mathbf{a}=(a_1,a_2,...,a_r)\in\mathbb{F}^r$, we define the *right (left)* (σ,δ)*-derivative polynomial of* f *of order* r *via* $\mathbf{a}$, denoted by $\Delta_{\mathbf{a}}f(x)$ $(\Delta_{\mathbf{a},L}f(x))$ as the quotient upon right (left) division of f by $P_{\mathbf{a}}:=(x-a_r)\cdots(x-a_2)(x-a_1)$ $(P_{\mathbf{a},L}:=(x-a_1)(x-a_2)\cdots(x-a_r))$. In particular, when $a=a_1=\cdots=a_r$, we will simply write $\Delta_a^r f(x)$ $(\Delta_{a,L}^r f(x))$.

Remark 2.2.3. Let σ be an endomorphism (automorphism) of $\mathbb{F}$ and consider $\mathbf{a}=(a_1,\ldots,a_r)\in\mathbb{F}^r$. As in [26], one can define *the right (left) Hasse derivative* $D_{\mathbf{a}}(f)\in\mathbb{F}$ $(D_{\mathbf{a},L}(f)\in\mathbb{F})$ *of order* r as the coefficient of the monomial of degree $r-1$ of the remainder in the right (left) division of f by $P_{\mathbf{a}}$ $(P_{\mathbf{a},L})$ (see [26, Definition 31 and Lemma 52]). In this case, we have $D_{\mathbf{a}}(f)=\Delta_{\mathbf{a}'}f(a_r)$ $(D_{\mathbf{a},L}(f)=(\Delta_{\mathbf{a}',L}f)_L(a_r))$, where $\mathbf{a}'=(a_1,\ldots,a_{r-1})$.

Let $f(x)=\sum_{i=0}^m\alpha_i x^i$ and $\Delta_a^1 f(x)=\sum_{j=0}^{m-1}\beta_j x^j$ be skew polynomials in $\mathcal{R}$ as in Definition 2.2.1 for some $a\in\mathbb{F}$. By Lemma 1.1.10, we have

$$f(x)-f(a)=\Delta_a^1 f(x)\cdot(x-a)\iff\sum_{i=0}^m\alpha_i x^i-f(a)=\sum_{i=0}^{m-1}\left(\beta_i x^{i+1}-\sum_{k=0}^{i}\beta_i\,\mathcal{C}_{k,i-k}(a)x^{i-k}\right).$$

Then, comparing the coefficients of the positive powers x^t in the latest equality, we get the following recursive formula:

$$\beta_{m-1}=\alpha_m\ ,\quad \beta_k=\alpha_{k+1}+\sum_{i=0}^{m-k-2}\beta_{k+1+i}\,\mathcal{C}_{i,k+1}(a)\qquad\forall k=m-2,m-3,...,0. \tag{2.7}$$

Using (2.7), the next Algorithm 5 shows how to compute $\Delta_{\mathbf{a}}f(x)$, $\mathbf{a}=(a_1,\ldots,a_n)\in\mathbb{F}^n$.

Algorithm 5 Computation of $\Delta_{\mathbf{a}}f(x)\in\mathcal{R}$.

Input: $f(x)=\sum_{i=0}^m\alpha_i x^i\in\mathcal{R}$, $\mathbf{a}=(a_1,\ldots,a_n)\in\mathbb{F}^n$, $n\in\mathbb{Z}_{\geq 1}$ and $n\leq m$
Output: $\Delta_{\mathbf{a}}f(x)$
1: **for** $i\leftarrow 1$ to n **do**
2: $\quad m\leftarrow\deg f(x)$
3: $\quad\beta_{m-1}\leftarrow\alpha_m$

4: **for** $h \leftarrow 0$ to $m-2$ **do**
5: $s \leftarrow 0$
6: **for** $j \leftarrow 0$ to h **do**
7: $s_1 \leftarrow \beta_{m-1-h+j} \cdot \mathcal{C}_{j,m-1-h}(a_i)$
8: $s \leftarrow s + s_1$
9: **end for**
10: $\beta_{m-2-h} \leftarrow \alpha_{m-1-h} + s$
11: **end for**
12: $q(x) \leftarrow \sum_{t=0}^{m-1} \beta_t x^t$
13: $f(x) \leftarrow q(x)$
14: **end for**
15: **return** $q(x)$

Note that, when σ is an automorphism, similar accounts as above can be made with $f(x) - f_L(a) = (x-a) \cdot \Delta^1_{a,L} f(x)$. Moreover, as an application of Algorithm 5, we apply the next Magma program to compute $\Delta_{(a,a)} f$ when $f = x^4 - jx^2 + (2i-k) \in \mathbb{H}[x; \sigma, 0]$, $a = 1 + j$ and $\sigma(h) := ihi^{-1}$ for all $h \in \mathbb{H}$. To do this, begin by writing in Magma the following instructions:

```
F<i,j,k> := QuaternionAlgebra< RealField() | -1, -1 >;
R<x>:=PolynomialRing(F);
S:= map< F -> F | x :-> i*x*(1/i) >;
D:= map< F -> F | x :-> 0 >;
```

then, using the function “PosCom" defined in Program 1, we can continue with the following instructions to define a new function “DerNA".

Program 3.

```
DerNA:=function(f,A)
 t:=#f;
 if #A ge t then
  f:=F!0;
 end if;
 if #A le t-1 then
  if t eq 2 then
   f:=F!f[t];
  end if;
  if t ge 3 then
   for i in [1..#A] do
```

```
    t:=#f;
    b:=[ f[t] ];
    for h in [0..t-3] do
     s:=F!0;
     for j in [0..h] do
      s1:=b[h+1-j]*PosCom(j,t-2-h,A[i]);
      s:= s + s1;
     end for;
     b:= b cat [ f[t-1-h] + s ];
    end for;
    g:=[];
    for k in [1..#b] do
     g:=g cat [ b[#b+1-k] ];
    end for;
    f:=g;
   end for;
  end if;
 end if;
 return R!f;
end function;
```

Thus, typing in Magma

```
DerNA([2*i-k,0,-j,0,1],[1+j,1+j]);
```

we get $\Delta_{(1+j,1+j)}(x^4 - jx^2 + 2i - k) = x^2 + 2x + 4 - 3j$.

Remark 2.2.4. Consider $f, g \in \mathcal{R}$, $a \in \mathbb{F}$ and suppose that σ is an endomorphism (automorphism) of $\mathbb{F}$. Then the linearity of $\Delta_{\mathbf{a}}$ and the fact that for any $a \in \mathbb{F}$

$$\Delta_a^1(f \cdot g) = f \cdot \Delta_a^1 g + \Delta_a^1(f \cdot g(a)) \quad (\Delta_{a,L}^1(f \cdot g) = \Delta_{a,L}^1 f \cdot g + \Delta_{a,L}^1(f_L(a) \cdot g))$$

allow one to obtain recursive formulas for right (left) (σ, δ)-derivative polynomials of order $r \in \mathbb{Z}_{\geq 1}$ via $\mathbf{a} = (a_1, \ldots, a_r) \in \mathbb{F}^r$. For instance, given any $n \in \mathbb{Z}_{\geq 1}$, we get $\Delta_a^1 x^n = x^{n-1} + \sum_{k=0}^{n-1} C_{k,n-1-k}(a) \cdot \Delta_a^1 x^{n-1-k}$ $\left(\Delta_{a,L}^1 x^n = x^{n-1} + \Delta_{a,L}^1 \left(\sum_{k=0}^{n-1} x^{n-1-k}(-1)^k \mathcal{T}_{k,n-1-k}(a)\right)\right)$. In particular, if $\sigma = Id$ and $\delta = 0$, then $\Delta_a^1 x^n = x^{n-1} + ax^{n-2} + a^2 x^{n-3} + ... + a^{n-1}$ and therefore $\Delta_a^1 x^n(a) = na^{n-1}$. This shows that the right evaluation of $\Delta_a^1 x^n$ in $a \in \mathbb{F}$ coincides with the classical notion of derivative of a monomial.

In [14] the author define a notion of right derivative in scalars for skew polynomials in $\mathbb{F}[x;\sigma,0]$. In Proposition 2.2.6, we will show a relationship between $\Delta_a^n f(a)$ (see Definition 2.2.2) and [14, Definition 2]. However, to prove this result, we need first to give a version of Proposition 2.1.10 for $n = 1$.

Proposition 2.2.5. *Let $f(x) \in \mathcal{R}$ with σ an endomorphism (automorphism) of $\mathbb{F}$ and $\mathbf{a} = (a_1, a_2, ..., a_{\deg f})$. Then,*

$$f(x) = \sum_{i=0}^{\deg f} \Delta_{\mathbf{a_i}} F(a_{i+1}) \cdot P_{\mathbf{a_i}} \quad \left(f(x) = \sum_{i=0}^{\deg f} P_{\mathbf{a_i},L} \cdot (\Delta_{\mathbf{a_i},L} F)_L(a_{i+1}) \right)$$

where $\mathbf{a_i} = (a_1, a_2, ..., a_i) \in \mathbb{F}^i$, $P_{\mathbf{a_i}}$ $(P_{\mathbf{a_i},L}) \in \mathcal{R}$ is as in Definition 2.2.2, *$\Delta_{\mathbf{a_0}} F = F$ $(\Delta_{\mathbf{a_0},L} F = F)$ and $P_{\mathbf{a_0}} = 1$ $(P_{\mathbf{a_0},L} = 1)$ for all $i = 1, ..., \deg f$. In particular, if $\mathbf{a} = (a, a, ..., a)$, then*

$$f(x) = \sum_{i=0}^{\deg f} \Delta_a^i f(a)(x-a)^i \quad \left(f(x) = \sum_{i=0}^{\deg f} (x-a)^i \Delta_{a,L}^i f(a) \right),$$

where $\Delta_a^0 f(a) = f(a)$ $((\Delta_{a,L}^0 f)_L(a) = f_L(a))$.

By using Proposition 2.2.5, we have the following result.

Proposition 2.2.6. *Let $f \in \mathbb{F}[x;\sigma,0]$ and let $a \in \mathbb{F}$. Then, for every $n \in \mathbb{Z}_{\geq 0}$ the following property hold*

$$n! \cdot \Delta_a^n f(a) = f^{(n)}(a),$$

where $f^{(n)}(a)$ denotes the n-th right derivative of f at a (see [14, Definition 2]) *and $\Delta_a^0 f(a) = f^{(0)}(a) = f(a)$. In particular, the two definitions coincide when $n = 1$.*

Proof. By Proposition 2.2.5, we have

$$f(x) = f(a) + \Delta_a^1 f(a)(x-a) + \Delta_a^2 f(a)(x-a)^2 + ... + \Delta_a^{\deg(f)} f(a)(x-a)^{\deg(f)}.$$

On the other hand, by [14, Theorem 3.14] we know that

$$f(x) = f(a) + \frac{f^{(1)}(a)}{1!}(x-a) + \frac{f^{(2)}(a)}{2!}(x-a)^2 + ... + \frac{f^{\deg(f)}(a)}{\deg(f)!}(x-a)^{\deg(f)}.$$

Then, by the equality property of skew polynomials, we obtain the statement.

□

Chapter 3

Hermite-type interpolation for skew multivariate polynomial rings

Let K be a field. Given a finite set of points $\Omega = \{a_1, a_2, ..., a_k\} \subseteq K$ and $S = \{(r, s_r) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} : 1 \leq r \leq k,\ 0 \leq s_r \leq n_r\}$ where $n_1, n_2, ..., n_k \in \mathbb{Z}_{\geq 0}$ and $b_{r,s_r} \in K$, the classical Hermite interpolation problem consists of finding a polynomial $f \in K[x]$ of degree $\leq N-1$ such that $f^{(s_r)}(a_r) = b_{r,s_r}$ for all pairs $(r, s_r) \in S$, where $N = \sum_{r=1}^{k}(n_r+1)$ and $f^{(s_r)}$ denotes the derivatives of f of order s_r. In the special case when derivatives are replaced by only the evaluations of $f(x)$ at the points a_i, the problem is referred in literature as Lagrange interpolation problem, and it can be stated in the following form: given a finite number of points $\Omega = \{a_1, a_2, ..., a_k\} \subseteq K$ and any values $b_1, b_2, ..., b_k \in K$ one wants to find a polynomial $f \in K[x]$ of degree $\leq k$, such that $f(a_i) = b_i$ for all $i = 1, 2, ..., k$.

It is well known that if the elements of Ω are different, then there exist unique polynomials satisfying the above conditions of the Hermite and Lagrange problem. However, the condition $a_i \neq a_j$ for all i, j is not sufficient for existence of such a polynomial in the non-commutative cases.

Inspired by [14] and [23], the main purpose of this chapter is to solve a Hermite-type interpolation problem in $\mathcal{A}$ that generalizes the Lagrange interpolation Theorem given in [23, Theorem 4] and extends the cases $n = 1$ given in [14, Theorem 4.4] and [26, Corollary 41].

3.1 Skew Hermite-type interpolation

Let us start by defining the following generalized zero ideals associated to a finite set of points in $\mathbb{F}^n$.

Definition 3.1.1. Let $\Omega = \{\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_k}\} \subseteq \mathbb{F}^n$ be a finite set and consider the monomials $m_j = x_{j_{s(j)}} \cdots x_{j_2} x_{j_1} \in \mathcal{M}$ such that either $j_l \in \{1, 2, ..., n\}$ and $l \geq 1$, or $m_j = 0$ (zero monomial). Given $\vec{m} = (m_1, m_2, ..., m_k)$, we denote by $I^{\vec{m}}(\Omega)$ the following set:

$$\{F \in \mathcal{A} : F(\mathbf{a_j}) = \Delta_{\mathbf{a_j}}^{x_{j_1}} F(\mathbf{a_j}) = \Delta_{\mathbf{a_j}}^{x_{j_2} x_{j_1}} F(\mathbf{a_j}) = ... = \Delta_{\mathbf{a_j}}^{m_j} F(\mathbf{a_j}) = 0,\ \forall j = 1, \ldots, k\} .$$

Proposition 3.1.2. *For any finite set $\Omega = \{\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_k}\} \subseteq \mathbb{F}^n$ and $\vec{m} = (m_1, m_2, ..., m_k)$, the set $I^{\vec{m}}(\Omega) \subseteq \mathcal{A}$ is a left ideal.*

Proof. Given $F, G \in I^{\vec{m}}(\Omega)$, by Lemma 2.1.8 we have $F + G \in I^{\vec{m}}(\Omega)$. Finally, for any $F \in \mathcal{A}$ and $G \in I^{\vec{m}}(\Omega)$, by Lemma 2.1.9 and the product rule (Theorem 1.2.9) we obtain that $FG \in I^{\vec{m}}(\Omega)$. Thus, $I^{\vec{m}}(\Omega)$ is a left ideal. □

Remark 3.1.3. In the special case when $\vec{m} = \vec{0} := (0, \ldots, 0)$, denoting by $\Delta_{\mathbf{a_j}}^0 F(\mathbf{a_j}) := F(\mathbf{a_j})$ for every $j \geq 1$, we have

$$I^{\vec{0}}(\Omega) = I(\Omega) := \{F \in \mathcal{A} : F(\mathbf{a}) = 0,\ \forall \mathbf{a} \in \Omega\} ,$$

obtaining the left ideal given in [23, Definition 13].

By using the left ideals $I^{\vec{m}}(\Omega)$, we can define the notion of Derivative Polynomial (DP) independence of type $(m_1, \ldots, m_k) \in \mathcal{M}^k$ as follows.

Definition 3.1.4. For $k \in \mathbb{Z}_{\geq 1}$, let $\Omega = \{\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_k}\} \subseteq \mathbb{F}^n$ be a finite set and let $\vec{m} = (m_1, \ldots, m_k) \in \mathcal{M}^k$ with either $m_j = x_{j_{s(j)}} \cdots x_{j_2} x_{j_1}$, or $m_j = 0$, for all $j = 1, ..., k$. We say that $\mathbf{a} \in \mathbb{F}^n \setminus \Omega$ is *DP-independent of type $\vec{m}$ from Ω* if

$$I^{\vec{m}}(\Omega) \supsetneq I^{\vec{m},0}(\Omega \cup \{\mathbf{a}\}) := \{F \in I^{\vec{m}}(\Omega) : F(\mathbf{a}) = 0\} .$$

Moreover, letting $\Omega_{(j)} := \Omega \setminus \{\mathbf{a_j}\}$ and $\vec{m}_j := (m_1, \ldots, m_{j-1}, m_{j+1}, \ldots, m_k) \in \mathcal{M}^{k-1}$ for each $j \in \{1, \ldots, k\}$, we say that Ω is *DP-independent of type $\vec{m} = (m_1, \ldots, m_k)$* if

$$I^{\vec{m}_j}\left(\Omega_{(j)}\right) \supsetneq I^{\vec{m}_j,0}(\Omega_{(j)} \cup \{\mathbf{a_j}\})$$

for all $j = 1, \ldots, k$.

Remark 3.1.5. The definition of $\Omega := \{\mathbf{a_1}, \ldots, \mathbf{a_k}\} \subset \mathbb{F}^n$ as a P-independent set given in [23, Definition 23] is equivalent to require that $I(\Omega \setminus \{\mathbf{a_j}\}) \supsetneq I(\Omega)$ for all $j = 1, \ldots, k$.

The next result shows that in the special case when Ω is DP-independent of type $(0, \ldots, 0)$, we obtain the notion of P-independence given in [23, Definition 23].

Lemma 3.1.6. *A finite set $\Omega = \{\mathbf{a_1}, \ldots, \mathbf{a_k}\} \subseteq \mathbb{F}^n$ is DP-independent of type $(0, \ldots, 0)$ if and only if it is P-independent.*

Proof. From Definition 3.1.4 and Remark 3.1.3, it follows that $\Omega \subseteq \mathbb{F}^n$ is DP-independent of type $(0, \ldots, 0)$ if and only if $I(\Omega \setminus \{\mathbf{a_j}\}) \supsetneq I(\Omega)$ for all $j = 1, 2, ..., k$, that is, Ω is P-independent by Remark 3.1.5. □

From Definition 3.1.4 and Lemma 3.1.6, we can deduce also the following result.

Proposition 3.1.7. *If $\Omega = \{\mathbf{a_1}, \ldots, \mathbf{a_k}\} \subseteq \mathbb{F}^n$ is DP-independent of type $(m_1, \ldots, m_k)$, then any $W = \{\mathbf{a_{j_1}}, \ldots, \mathbf{a_{j_s}}\} \subseteq \Omega$ is DP-independent of type $(m_{j_1}, ..., m_{j_s})$, where $j_i \in \{1, 2, .., k\}$. In particular, every subset of a P-independent set is P-independent.*

Proof. Let $\mathbf{t} \in \{\mathbf{j_1}, \ldots, \mathbf{j_s}\}$, $\vec{m} := (m_1, \ldots, m_k)$ and $\vec{m}' := (m_{j_1}, ..., m_{j_s})$. Since we have

$$I^{\vec{m}_\mathbf{t}}\left(\Omega_{(\mathbf{t})}\right) \supsetneq I^{\vec{m}_t,0}(\Omega_{(\mathbf{t})} \cup \{\mathbf{a_t}\}) \ ,$$

it follows that there exists $F \in I^{\vec{m}_\mathbf{t}}\left(\Omega_{(\mathbf{t})}\right) \subseteq I^{\vec{m}'_\mathbf{t}}\left(W_{(\mathbf{t})}\right)$ such that $F(\mathbf{a_t}) \neq 0$. Hence $I^{\vec{m}'_\mathbf{t}}\left(W_{(\mathbf{t})}\right) \supsetneq I^{\vec{m}'_t,0}(W_{(\mathbf{t})} \cup \{\mathbf{a_t}\})$ for any $\mathbf{t} \in \{\mathbf{j_1}, \ldots, \mathbf{j_s}\}$, i.e. $W = \{\mathbf{a_{j_1}}, \ldots, \mathbf{a_{j_s}}\} \subseteq \Omega$ is DP-independent of type $\vec{m}' = (m_{j_1}, ..., m_{j_s})$. Finally, the last part of the statement follows from Lemma 3.1.6. □

The following result will be crucial to perform the skew Hermite-type interpolation recursively in $\mathcal{A}$ and it extends the equivalence between 1 and 3 of [23, Proposition 25].

Proposition 3.1.8. *Let $\Omega = \{\mathbf{a_1}, \ldots, \mathbf{a_k}\} \subseteq \mathbb{F}^n$ be a finite set and let $m_1, \ldots, m_k \in \mathcal{M}$. Then the following conditions are equivalent:*

1) *Ω is DP-independent of type $(m_1, \ldots, m_k)$;*

2) *for any ordering $\mathbf{b_1}, \ldots, \mathbf{b_k}$ of the elements in Ω and for any $i = 1, \ldots, k-1$, it holds that $\mathbf{b_{i+1}}$ is DP-independent of type $(m'_1, \ldots, m'_i)$ from $\Omega_i := \{\mathbf{b_1}, \ldots, \mathbf{b_i}\}$, where $m'_j = m_{k(j)}$ with $\mathbf{b_j} = \mathbf{a_{k(j)}}$ for $j = 1, \ldots, i$.*

Proof. 1) $\Rightarrow$ 2) Suppose that $\mathbf{b_{i+1}}$ is not DP-independent of type $(m'_1,\dots,m'_i)$ from Ω_i for some i and a given ordering $\mathbf{b_1},\dots,\mathbf{b_k}$ of Ω. Then from Definition 3.1.4 it follows that $F(\mathbf{b_{i+1}})=0$ for all $F\in I^{(m'_1,\dots,m'_i)}(\Omega_i)$, but this contradicts Proposition 3.1.7 by considering $W=\{\mathbf{b_1},\dots,\mathbf{b_i},\mathbf{b_{i+1}}\}\subseteq\Omega$.

2) $\Rightarrow$ 1) Assume that Ω is not DP-independent of type $\vec{m}:=(m_1,m_2,...,m_k)$. Thus there exists $\mathbf{a_i}\in\Omega$ such that $F(\mathbf{a_i})=0$ for every $F\in I^{\vec{m}_i}(\Omega\setminus\{\mathbf{a_i}\})$. By ordering the k elements in Ω in such a way that $\mathbf{b_k}=\mathbf{a_i}$, it follows that $\mathbf{b_k}$ is not DP-independent of type $(m'_1,\dots,m'_{k-1})$ from Ω_{k-1}, but this contradicts 2). □

The following technical results will be the key tools for the skew Hermite-type interpolation problem.

Lemma 3.1.9. *Let $\Omega=\{\mathbf{a_1},\dots,\mathbf{a_k}\}\subseteq\mathbb{F}^n$ be a finite set and let $\vec{m}=(m_1,\dots,m_k)\in\mathcal{M}^k$ with either $m_j=0$, or $m_j=x_{j_{s(j)}}\cdots x_{j_2}x_{j_1}$ for all $j=1,...,k$ and $j_l\in\{1,\dots,n\}$. Then for any $m\in\mathcal{M}$ with $\deg m=N:=\sum_{i=1}^k[\deg(m_i)+1]$ there exists $F\in I^{\vec{m}}(\Omega)$ such that $\deg F=N$ and $LM(F)=m$.*

Proof. Write $m=x_{k_N}\cdot\ldots\cdot x_{k_2}\cdot x_{k_1}\in\mathcal{M}$. Defining $F_1(\mathbf{x}):=x_{k_1}-(\mathbf{a_1})_{k_1}$, we have $F_1(\mathbf{a_1})=0$ with $\deg F_1(\mathbf{x})=1$ and $\Delta_{\mathbf{a_1}}^{x_{1_1}}F_1(\mathbf{x})=0$ or 1. Then, define $F_2(\mathbf{x}):=(x_{k_2}-(\mathbf{a_1})_{k_2})\,F_1(\mathbf{x})$. By Lemma 2.1.9, we have

$$\Delta_{\mathbf{a_1}}^{x_{1_1}}F_2(\mathbf{x})=(x_{k_2}-(\mathbf{a_1})_{k_2})\,\Delta_{\mathbf{a_1}}^{x_{1_1}}F_1(\mathbf{x})\ .$$

In any case, we get $F_2(\mathbf{a_1})=\Delta_{\mathbf{a_1}}^{x_{1_1}}F_2(\mathbf{a_1})=0$ with $\deg F_2(\mathbf{x})=2$ and $\Delta_{\mathbf{a_1}}^{x_{1_2}x_{1_1}}F_2(\mathbf{x})=0$ or 1. By a recursive argument, we can construct $F_m(\mathbf{x}):=\Pi_{i=1}^m(x_{k_i}-(\mathbf{a_1})_{k_i})$ with $m=\deg(m_1)+1$ and such that $F_m(\mathbf{x})\in I^{m_1}(\{\mathbf{a_1}\})$. Thus, define now $G_1(\mathbf{x}):=(x_{k_{m+1}}-\alpha_1)F_m(\mathbf{x})$ for some $\alpha_1\in\mathbb{F}$. If $F_m(\mathbf{a_2})=0$ then $G_1(\mathbf{x})\in I^{m_1,0}(\{\mathbf{a_1}\}\cup\{\mathbf{a_2}\})$. Otherwise, by taking $\alpha_1:=\left(\mathbf{a_2}^{F_m(\mathbf{a_2})}\right)_{k_{m+1}}$ we get again $G_1(\mathbf{x})\in I^{m_1,0}(\{\mathbf{a_1}\}\cup\{\mathbf{a_2}\})$ with $\deg G_1(\mathbf{x})=m+1$. Therefore, defining $G_2(\mathbf{x})=\left(x_{k_{m+2}}-\alpha_2\right)G_1(\mathbf{x})$, we have $G_2(\mathbf{x})\in I^{m_1,0}(\{\mathbf{a_1}\}\cup\{\mathbf{a_2}\})$ and by Lemma 2.1.9 it follows that

$$\Delta_{\mathbf{a_2}}^{x_{2_1}}G_2(\mathbf{x})=\left(x_{k_{m+2}}-\alpha_2\right)\cdot\Delta_{\mathbf{a_2}}^{x_{2_1}}G_1(\mathbf{x})\ .$$

If $\Delta_{\mathbf{a_2}}^{x_{2_1}}G_1(\mathbf{a_2})=0$, then $\Delta_{\mathbf{a_2}}^{x_{2_1}}G_2(\mathbf{a_2})=0$. If $\Delta_{\mathbf{a_2}}^{x_{2_1}}G_1(\mathbf{a_2})\neq0$, then by choosing $\alpha_2:=\left(\mathbf{a_2}^{\Delta_{\mathbf{a_2}}^{x_{2_1}}G_1(\mathbf{a_2})}\right)_{k_{m+2}}$ we obtain $\Delta_{\mathbf{a_2}}^{x_{2_1}}G_2(\mathbf{a_2})=0$ again. Hence there exists $G_2(\mathbf{x})\in I^{m_1,x_{2_1}}(\{\mathbf{a_1}\}\cup\{\mathbf{a_2}\})$ with $\deg G_2(\mathbf{x})=m+2$. By recursive arguments, we can find a skew polynomial $F(\mathbf{x})\in I^{\vec{m}}(\Omega)$ such that $\deg F(\mathbf{x})=N$ and $LM(F(\mathbf{x}))=m$ by construction. □

Lemma 3.1.10. *Let $\Omega = \{\mathbf{a_1}, \ldots, \mathbf{a_k}\} \subseteq \mathbb{F}^n$ be a finite DP-independent set of type $\vec{m} := (m_1, \ldots, m_k)$ and let $\mathbf{a} \in \mathbb{F}^n \setminus \Omega$ such that $I^{\vec{m}}(\Omega) \supsetneq I^{\vec{m},0}(\Omega \cup \{\mathbf{a}\})$. Then there exists a skew polynomial $F \in I^{\vec{m}}(\Omega) \setminus I^{\vec{m},0}(\Omega \cup \{\mathbf{a}\})$ such that*

$$\deg(F) \leq \sum_{i=1}^{k} (\deg(m_i) + 1) \ .$$

Proof. Since $I^{\vec{m}}(\Omega) \supsetneq I^{\vec{m}}(\Omega \cup \{\mathbf{a}\})$, take $F \in I^{\vec{m}}(\Omega) \setminus I^{\vec{m},0}(\Omega \cup \{\mathbf{a}\})$ such that $LM(F)$ is minimum possible with respect to $\prec$, where $\prec$ denotes any monomial order of $\mathcal{M}$ preserving degrees. If we suppose that $\deg(F) \geq N + 1$, where $N := \sum_{i=1}^{k} (\deg(m_i) + 1)$, then $\deg(LM(F)) \geq N + 1$ by the choice of $\prec$. Then, applying Lemma 3.1.9 we can construct a skew polynomial $G \in I^{\vec{m}}(\Omega)$ such that $LM(F) = m \cdot LM(G)$ for some $m \in \mathcal{M}$ with $\deg m > 0$. If $G(\mathbf{a}) \neq 0$, then we get $G \in I^{\vec{m}}(\Omega) \setminus I^{\vec{m},0}(\Omega \cup \{\mathbf{a}\})$, a contradiction because $\deg F > \deg G$. Suppose now that $G(\mathbf{a}) = 0$. Then there exists $\alpha \in \mathbb{F}$ such that $H := F - \alpha m \cdot G$ satisfies $LM(H) \prec LM(F)$. Now, by the definition of G, it holds that $H \in I^{\vec{m}}(\Omega) \setminus I^{\vec{m},0}(\Omega \cup \{\mathbf{a}\})$, which is absurd by the minimality of $LM(F)$. Therefore we have $\deg(F) \leq N$ and this gives the statement. □

Lemma 3.1.11. *Let $\Omega \subseteq \mathbb{F}^n$ be a finite set and consider $\mathbf{a} \notin \Omega$. If there exists $F \in I^{\vec{m}}(\Omega) \setminus I^{\vec{m},0}(\Omega \cup \{\mathbf{a}\})$, then for any $x_j, m' \in \mathcal{M}$ there exists $G \in I^{\vec{m},m'}(\Omega \cup \{\mathbf{a}\}) \setminus I^{\vec{m},x_j m'}(\Omega \cup \{\mathbf{a}\})$ such that $\Delta_{\mathbf{a}}^{x_j m'} G(\mathbf{a}) = 1$ and $\deg G = \deg F + \deg(m') + 1$.*

Proof. Without loss of generality, we can assume that $F(\mathbf{a}) = 1$. Define

$$G(\mathbf{x}) := [x_t - (\mathbf{a})_t] \cdot F(\mathbf{x}) \ .$$

Therefore we see that $G(\mathbf{a}) = 0$, $\deg G = \deg F + 1$ and

$$\Delta_{\mathbf{a}}^{x_j} G(\mathbf{x}) = [x_t - (\mathbf{a})_t] \cdot \Delta_{\mathbf{a}}^{x_j} F(\mathbf{x}) + \Delta_{\mathbf{a}}^{x_j} [x_t - (\mathbf{a})_t] \ .$$

Let $H(\mathbf{x}) := [x_t - (\mathbf{a})_t] \cdot \Delta_{\mathbf{a}}^{x_j} F(\mathbf{x})$. If $H(\mathbf{a}) = 0$, then we choose $t = j$. If $H(\mathbf{a}) \neq 0$, then we take any $t \neq j$. In both cases, we obtain that $\Delta_{\mathbf{a}}^{x_j} G(\mathbf{a}) \neq 0$. Hence, up to multiplying $G(\mathbf{x})$ by a non zero scalar, we have $G(\mathbf{x}) \in I^{\vec{m},0}(\Omega \cup \{\mathbf{a}\}) \setminus I^{\vec{m},x_j}(\Omega \cup \{\mathbf{a}\})$ with $\Delta_{\mathbf{a}}^{x_j} G(\mathbf{a}) = 1$ and $\deg G(\mathbf{x}) = \deg F(\mathbf{x}) + \deg(0) + 1$.

By induction, assume that there exists $G(\mathbf{x}) \in I^{\vec{m},\hat{m}}(\Omega \cup \{\mathbf{a}\}) \setminus I^{\vec{m},x_j\hat{m}}(\Omega \cup \{\mathbf{a}\})$ with $\Delta_{\mathbf{a}}^{x_j\hat{m}} G(\mathbf{a}) = 1$ and $\deg G(\mathbf{x}) = \deg F(\mathbf{x}) + \deg(\hat{m}) + 1$, where either $\deg \hat{m} > 0$, or $\hat{m} = 0$ and $x_j\hat{m} = x_j$. Therefore, define

$$L(\mathbf{x}) := [x_t - (\mathbf{a})_t] \cdot G(\mathbf{x}) \ .$$

Then we have

$$\Delta_{\mathbf{a}}^{x_j\hat{m}}L(\mathbf{x}) = [x_t - (\mathbf{a})_t] \cdot \Delta_{\mathbf{a}}^{x_j\hat{m}}G(\mathbf{x}) \ ,$$

$$\Delta_{\mathbf{a}}^{x_ix_j\hat{m}}L(\mathbf{x}) = [x_t - (\mathbf{a})_t] \cdot \Delta_{\mathbf{a}}^{x_ix_j\hat{m}}G(\mathbf{x}) + \Delta_{\mathbf{a}}^{x_i}[x_t - (\mathbf{a})_t] \ .$$

Note that $\Delta_{\mathbf{a}}^{x_j\hat{m}}L(\mathbf{a}) = 0$ and write $M(\mathbf{x}) := [x_t - (\mathbf{a})_t] \cdot \Delta_{\mathbf{a}}^{x_ix_j\hat{m}}G(\mathbf{x})$. If $M(\mathbf{a}) = 0$, then we choose $t = j$. If $M(\mathbf{a}) \neq 0$, then we take any $t \neq j$. In both cases, we get that $\Delta_{\mathbf{a}}^{x_ix_j\hat{m}}L(\mathbf{a}) \neq 0$. Hence, up to multiplying $L(\mathbf{x})$ by a non zero scalar, we obtain that $L(\mathbf{x}) \in I^{\vec{m},x_j\hat{m}}(\Omega \cup \{\mathbf{a}\}) \setminus I^{\vec{m},x_ix_j\hat{m}}(\Omega \cup \{\mathbf{a}\})$ with $\Delta_{\mathbf{a}}^{x_ix_j\hat{m}}L(\mathbf{a}) = 1$ and $\deg L(\mathbf{x}) = \deg G(\mathbf{x}) + 1 = \deg F(\mathbf{x}) + \deg(\hat{m}) + 1 + 1 = \deg F(\mathbf{x}) + \deg(x_j\hat{m}) + 1$. □

The main result here is a Hermite-type interpolation theorem in $\mathcal{A}$ that generalizes the skew Lagrange interpolation given in [23, Theorem 4] and it extends the cases $n = 1$ given in [26, Theorem 3, Corollary 41].

Theorem 3.1.12 (**A skew Hermite-type interpolation**). *Let $\Omega = \{\mathbf{a_1}, \ldots, \mathbf{a_k}\} \subseteq \mathbb{F}^n$ be a finite set and let $m_1, \ldots, m_k \in \mathcal{M}$. The following conditions are equivalent:*

1) *Ω is DP-independent of type $(m_1, ..., m_k)$.*

2) *The map $\psi : \mathcal{A}_N \to \mathbb{F}^N$ defined by*

$$F \mapsto (F(\mathbf{a_1}), \ldots, \Delta_{\mathbf{a_1}}^{m_1}F(\mathbf{a_1}), \ldots, F(\mathbf{a_j}), \ldots, \Delta_{\mathbf{a_j}}^{m_j}F(\mathbf{a_j}), \ldots, F(\mathbf{a_k}), \ldots, \Delta_{\mathbf{a_k}}^{m_k}F(\mathbf{a_k}))$$

is a surjective left $\mathbb{F}$-module homomorphism, where $N := \sum_{j=1}^{k}(\deg(m_j) + 1)$ and $\mathcal{A}_N := \{F \in \mathcal{A} : \deg F < N\}$.

3) *Given any finite set of N values in $\mathbb{F}$*

$$\{b_{j,0}, b_{j,x_{j_1}}, b_{j,x_{j_2}x_{j_1}}, \ldots, b_{j,m_j} : j = 1, 2, \ldots, k\} \ ,$$

where $N := \sum_{i=1}^{k}(\deg(m_i) + 1)$, there exists a skew polynomial $F \in \mathcal{A}$ with $\deg(F) < N$ such that

$$F(\mathbf{a_j}) = b_{j,0}, \Delta_{\mathbf{a_j}}^{x_{j_1}}F(\mathbf{a_j}) = b_{j,x_{j_1}}, \Delta_{\mathbf{a_j}}^{x_{j_2}x_{j_1}}F(\mathbf{a_j}) = b_{j,x_{j_2}x_{j_1}}, ..., \Delta_{\mathbf{a_j}}^{m_j}F(\mathbf{a_j}) = b_{j,m_j}$$

for all $j = 1, \ldots, k$.

Proof. First, note that the equivalence between 2) and 3) is immediate.

1) ⇒ 2) From Lemma 2.1.8, it is evident that ψ is a left $\mathbb{F}$-module homomorphism. Let $\mathbf{a_1} := (a_{1_1}, a_{1_2}, ..., a_{1_n}) \in \mathbb{F}^n$. We start by defining the skew polynomial $G_{1,0} := 1$.

Then we see that $G_{1,0}(\mathbf{a_1}) = 1$, $\deg(G_{1,0}) = 0 < 1$ and $\Delta_{\mathbf{a_1}}^{x_{1_j}\cdots x_{1_2}x_{1_1}} G_{1,0}(\mathbf{a_1}) = 0$ for all $j = 1, \ldots, \deg(m_1)$. On the other hand, note that the skew polynomials

$$G_{1,j} := (x_{1_j} - a_{1_j}) \cdots (x_{1_2} - a_{1_2})(x_{1_1} - a_{1_1}) \in \mathcal{A}$$

are such that $G_{1,j} \in I^{x_{1_{j-1}}\cdots x_{1_2}x_{1_1}}(\{\mathbf{a_1}\}) \setminus I^{x_{1_j}\cdots x_{1_2}x_{1_1}}(\{\mathbf{a_1}\})$, $\deg(G_{1,j}) < j + 1$ and $\Delta_{a_1}^{x_{1_j}\cdots x_{1_2}x_{1_1}} G_{1,j}(\mathbf{a_1}) = 1$ for all $j = 1, \ldots, \deg(m_1)$, where $I^{x_{1_0}}(\{\mathbf{a_1}\}) := I(\{\mathbf{a_1}\})$.

Let $\mathbf{a_2} := (a_{2_1}, a_{2_2}, ..., a_{2_n}) \in \mathbb{F}^n$. Since Ω is DP-independent of type $(m_1, ..., m_k)$, then by Proposition 3.1.8 and Lemma 3.1.10 there exists $F_{2,0} \in I^{m_1}(\{\mathbf{a_1}\}) \setminus I^{m_1,0}(\{\mathbf{a_1}, \mathbf{a_2}\})$ such that $\deg(F_{2,0}) \leq \deg(m_1) + 1$. Then the skew polynomial $G_{2,0} := F_{2,0}(\mathbf{a_2})^{-1} F_{2,0}$ is such that $G_{2,0} \in I^{m_1}(\{\mathbf{a_1}\}) \setminus I^{m_1,0}(\{\mathbf{a_1}, \mathbf{a_2}\})$, $G_{2,0}(\mathbf{a_2}) = 1$ and $\deg(G_{2,0}) \leq \deg(m_1) + 1$. By Lemma 3.1.11, we can construct polynomials $G_{2,i} \in \mathcal{A}$ for $i = 1, \ldots, \deg(m_2)$ such that $G_{2,i} \in I^{m_1,x_{2_{i-1}}\cdots x_{2_2}x_{2_1}}(\{\mathbf{a_1}, \mathbf{a_2}\}) \setminus I^{m_1,x_{2_i}\cdots x_{2_2}x_{2_1}}(\{\mathbf{a_1}, \mathbf{a_2}\})$, $\Delta_{\mathbf{a_2}}^{x_{2_i}\cdots x_{2_2}x_{2_1}} G_{2,i}(\mathbf{a_2}) = 1$ and $\deg G_{2,i} \leq \deg(m_1) + 1 + i$, for all $i = 2, \ldots, \deg(m_2)$. Then, arguing as above, by Lemmas 3.1.10 and 3.1.11 we can construct for all $\mathbf{a_j} \in \Omega$ with $j = 1, \ldots, k$ skew polynomials $G_{j,0}, G_{j,1}, \ldots, G_{j,\deg(m_j)} \in \mathcal{A}$ such that

$$\begin{aligned}
\psi(G_{j,0}) &= (0, ..., 0, ..., 1, *, *, ..., *, *, ..., *, ..., *) \\
\psi(G_{j,1}) &= (0, ..., 0, ..., 0, 1, *, ..., *, *, ..., *, ..., *) \\
\vdots &= \vdots \\
\psi(G_{j,\deg(m_j)}) &= (0, ..., 0, ..., 0, 0, 0, ..., 1, *, ..., *, ..., *)
\end{aligned}$$

Thus, making left linear operations on all the skew polynomials $G_{j,0}, G_{j,1}, \ldots, G_{j,\deg(m_j)}$ for $j = 1, \ldots, k$, we can obtain polynomials $\tilde{G}_{j,0}, \tilde{G}_{j,1}, \ldots, \tilde{G}_{j,\deg(m_j)} \in \mathcal{A}$ such that

$$\begin{aligned}
\psi(\tilde{G}_{j,0}) &= \vec{e}_{j,0} &:= (0, ..., 0, ..., 1, 0, 0, ..., 0, ..., 0, ..., 0) \\
\psi(\tilde{G}_{j,1}) &= \vec{e}_{j,1} &:= (0, ..., 0, ..., 0, 1, 0, ..., 0, ..., 0, ..., 0) \\
\vdots &= \vdots &:= \vdots \\
\psi(\tilde{G}_{j,\deg(m_j)}) &= \vec{e}_{j,\deg(m_j)} &:= (0, ..., 0, ..., 0, 0, 0, ..., 1, ..., 0, ..., 0)
\end{aligned}$$

for all $j = 1, ..., k$. Therefore, given any

$$\mathbf{b} = (b_{1,0}, b_{1,1}, ..., b_{1,\deg(m_1)}, ..., b_{j,0}, b_{j,1}, ..., b_{j,\deg(m_j)}, ..., b_{k,0}, b_{k,1}, ..., b_{k,\deg(m_k)}) \in \mathbb{F}^N$$

it follows that

$$\begin{aligned}\mathbf{b} &= \sum_{i=0}^{\deg(m_1)} b_{1,i}\vec{e}_{1,i} + \ldots + \sum_{i=0}^{\deg(m_j)} b_{j,i}\vec{e}_{j,i} + \ldots + \sum_{i=0}^{\deg(m_k)} b_{k,i}\vec{e}_{k,i} \\ &= \sum_{i=0}^{\deg(m_1)} b_{1,i}\psi(\tilde{G}_{1,i}) + \ldots + \sum_{i=0}^{\deg(m_j)} b_{j,i}\psi(\tilde{G}_{j,i}) + \ldots + \sum_{i=0}^{\deg(m_k)} b_{k,i}\psi(\tilde{G}_{k,i}) \\ &= \psi\left(\sum_{t=1}^{k}\left(\sum_{i=0}^{\deg(m_t)} b_{t,i}\tilde{G}_{t,i}\right)\right)\end{aligned}$$

with $\deg\left(\sum_{t=1}^{k}\left(\sum_{i=0}^{\deg(m_t)} b_{t,i}\tilde{G}_{t,i}\right)\right) \leq N-1 < N$ and we are done.

2) $\Rightarrow$ 1) Since ψ is a surjective left $\mathbb{F}$-module homomorphism, then for each $\vec{e}_{j,0} \in \mathbb{F}^N$ with $j = 1, 2, ..., k$ as before, there exists a skew polynomial

$$F_{j,0} \in I^{\vec{m}_j}\left(\Omega_{(j)}\right) \supsetneq I^{\vec{m}_j,0}(\Omega_{(j)} \cup \{\mathbf{a_j}\})$$

for all $j = 1, ..., k$, where $\vec{m} = (m_1, \ldots, m_k)$. Hence, from Definition 3.1.4 we deduce that Ω is DP-independent of type $(m_1, ..., m_k)$. □

In the special case when Ω is DP-independent of type $(0, ..., 0)$, that is, Ω is P-independent (see Lemma 3.1.6), we give a necessary and sufficient condition to solve the skew Lagrange interpolation problem as follows.

Corollary 3.1.13 (**Skew Lagrange interpolation**). *Let $\Omega = \{\mathbf{a_1}, \ldots, \mathbf{a_k}\} \subseteq \mathbb{F}^n$ be a finite set. The following conditions are equivalent:*

1) *Ω is P-independent.*

2) *The map $\phi : \mathcal{A}_k \to \mathbb{F}^k$, defined by $F \mapsto (F(\mathbf{a_1}), F(\mathbf{a_2}), ..., F(\mathbf{a_k}))$ is a surjective left $\mathbb{F}$-module homomorphism.*

3) *For every $b_1, b_2, ..., b_k \in \mathbb{F}$, there exists a skew polynomial $F \in \mathcal{A}$ with $\deg(F) < k$ such that $F(\mathbf{a_j}) = b_j$ for all $j = 1, ..., k$.*

By using Theorem 3.1.12, we give also the following result which allows us to construct DP-independent sets of type $(m_1, \ldots, m_k)$ for some $m_i \in \mathcal{M}$.

Corollary 3.1.14. *Let $\Omega = \{\mathbf{a_1}, \ldots, \mathbf{a_k}\} \subseteq \mathbb{F}^n$ be a DP-independent finite set of type $\vec{m} := (m_1, \ldots, m_k)$. If $\mathbf{a_{k+1}} \in \mathbb{F}^n \setminus \Omega$ is such that $I^{\vec{m}}(\Omega) \supsetneq I^{\vec{m},0}(\Omega \cup \{\mathbf{a_{k+1}}\})$, then $\Omega \cup \{\mathbf{a_{k+1}}\}$ is DP-independent of type $(m_1, \ldots, m_k, m_{k+1})$ for any $m_{k+1} \in \mathcal{M}$.*

Proof. Since Ω is DP-independent of type $\vec{m}$ and $\mathbf{a_{k+1}} \in \mathbb{F}^n \setminus \Omega$ is such that $I^{\vec{m}}(\Omega) \supsetneq I^{\vec{m},0}(\Omega \cup \{\mathbf{a_{k+1}}\})$, then by Lemma 3.1.10 we deduce that there exists $F \in I^{\vec{m}}(\Omega) \supsetneq I^{\vec{m},0}(\Omega \cup \{\mathbf{a_{k+1}}\})$ such that $\deg F \leq \sum_{i=1}^{k} (\deg(m_i) + 1)$. Thus by Lemma 3.1.11 it follows that $\psi : \mathcal{A}_N \to \mathbb{F}^N$ defined by $F \mapsto (F(\mathbf{a_1}), ..., \Delta_{\mathbf{a_1}}^{m_1} F(\mathbf{a_1}), ..., F(\mathbf{a_{k+1}}), ..., \Delta_{\mathbf{a_{k+1}}}^{m_{k+1}} F(\mathbf{a_{k+1}}))$ is a surjective left linear map for any $m_{k+1} \in \mathcal{M}$ with $N := \sum_{j=1}^{k+1} (\deg(m_j) + 1)$. Thus, by Theorem 3.1.12 it follows that $\Omega \cup \{\mathbf{a}\}$ is DP-independent of type $(m_1, ..., m_{k+1})$. □

Remark 3.1.15. In the special case when Ω is DP-independent of type $(0, ..., 0)$, i.e. Ω is P-independent, and $\mathbf{a} \in \mathbb{F}^n \setminus \Omega$ is such that $I(\Omega \setminus \{\mathbf{a}\}) \supsetneq I(\Omega)$, it follows that $\Omega \cup \{\mathbf{a}\}$ is P-independent, obtaining [23, Lemma 36].

Note that Proposition 3.1.14 gives us a method to construct DP-independent sets of a certain type. Another way to construct DP-independent sets will be given in Proposition 3.1.18, but before to prove it we need the following two technical results.

Lemma 3.1.16. *Let $\Omega_h = \{\mathbf{a_1}, \ldots, \mathbf{a_h}\}$ be a subset of $\mathbb{F}^n$ and consider $\mathbf{a} \in \mathbb{F}^n$ such that $\mathbf{a} \notin \{[\mathbf{a_1}], \ldots, [\mathbf{a_h}]\}$, where $[\mathbf{a_j}]$ denotes the (σ, δ)-conjugacy class of $\mathbf{a_j}$ for all $j = 1, \ldots, h$. If there exists*

$$F \in I^{m_1,\ldots,m_{h-1},m}(\Omega_h) \setminus I^{m_1,\ldots,m_{h-1},m,0}(\Omega_h \cup \{\mathbf{a}\}) \ ,$$

then for any $x_j \in \mathcal{M}$ there exists

$$G \in I^{m_1,\ldots,m_{h-1},x_j m}(\Omega_h) \setminus I^{m_1,\ldots,m_{h-1},x_j m,0}(\Omega_h \cup \{\mathbf{a}\})$$

such that $\deg G = \deg F + 1$.

Proof. Define $G(\mathbf{x}) := (x_t - \alpha)F(\mathbf{x})$. Let $\delta := \Delta_{\mathbf{a_h}}^{x_j m} F(\mathbf{a_h})$. Moreover, by Lemma 2.1.9 we have $\Delta_{\mathbf{a_h}}^{x_j m} G(\mathbf{a_h}) = \left((\mathbf{a_h}^{\delta})_t - \alpha\right) \cdot \delta$. If $\delta = 0$, then we take any $\alpha \in \mathbb{F}$ such that $\alpha \neq \left(\mathbf{a}^{F(\mathbf{a})}\right)_t$. If $\delta \neq 0$, then there exists $t \in \{1, \ldots, n\}$ such that $\left(\mathbf{a_h}^{\delta}\right)_t \neq \left(\mathbf{a}^{F(\mathbf{a})}\right)_t$, because $\mathbf{a} \notin [\mathbf{a_h}]$. In this situation, take $\alpha := \left(\mathbf{a_h}^{\delta}\right)_t$. Therefore, in both cases we have $G \in I^{m_1,\ldots,m_{h-1},x_j m}(\Omega_h) \setminus I^{m_1,\ldots,m_{h-1},x_j m,0}(\Omega_h \cup \{\mathbf{a}\})$ with $\deg G = \deg F + 1$. □

Lemma 3.1.17. *Let $\Omega_h = \{\mathbf{a_1}, \ldots, \mathbf{a_h}\}$ be a subset of $\mathbb{F}^n$ and consider $\mathbf{a} \in \mathbb{F}^n$ such that $\mathbf{a} \notin \{[\mathbf{a_1}], \ldots, [\mathbf{a_h}]\}$, where $[\mathbf{a_j}]$ denotes the (σ, δ)-conjugacy class of $\mathbf{a_j}$ for all $j = 1, \ldots, h$. Define $\Omega_s := \{\mathbf{a_1}, \ldots, \mathbf{a_s}\}$ for $s = 1, \ldots, h$. If for some $t = 1, \ldots, h-1$ there exists*

$$F \in I^{m_1,\ldots,m_t}(\Omega_t) \setminus I^{m_1,\ldots,m_t,0}(\Omega_t \cup \{\mathbf{a}\}) \ ,$$

then there exists

$$G \in I^{m_1,\dots,m_t,0}(\Omega_{t+1}) \setminus I^{m_1,\dots,m_t,0,0}(\Omega_{t+1} \cup \{\mathbf{a}\})$$

such that $\deg G = \deg F + 1$.

Proof. Define $G(\mathbf{x}) := (x_s - \beta)F(\mathbf{x})$. Let $\gamma := F(\mathbf{a_{t+1}})$. If $\gamma = 0$, then take any $\beta \in \mathbb{F}$ such that $\beta \neq \left(\mathbf{a}^{F(\mathbf{a})}\right)_s$. If $\gamma \neq 0$, then there exists $s \in \{1,\dots,n\}$ such that $(\mathbf{a_{t+1}}^{\gamma})_s \neq \left(\mathbf{a}^{F(\mathbf{a})}\right)_s$, because $\mathbf{a} \notin [\mathbf{a_{t+1}}]$. In this situation, take $\beta := (\mathbf{a_{t+1}}^{\gamma})_s$. Thus, in both cases, we get that $G \in I^{m_1,\dots,m_t,0}(\Omega_{t+1}) \setminus I^{m_1,\dots,m_t,0,0}(\Omega_{t+1} \cup \{\mathbf{a}\})$ with $\deg G = \deg F + 1$. □

Finally, the next result gives another method to construct a DP-independent set in $\mathbb{F}^n$.

Proposition 3.1.18. *If* $\Omega = \{\mathbf{a_1},\dots,\mathbf{a_k}\} \subseteq \mathbb{F}^n$ *is a DP-independent finite set of type* $(m_1,\dots,m_k)$ *and* $\mathbf{a} \in \mathbb{F}^{\mathbf{n}}$ *is such that* $\mathbf{a} \notin \{[\mathbf{a_1}],\dots,[\mathbf{a_k}]\}$, *where* $[\mathbf{a_j}]$ *denotes the* (σ,δ)*-conjugacy class of* $\mathbf{a_j}$ *for all* $j = 1,\dots,k$, *then* $\Omega \cup \{\mathbf{a}\}$ *is DP-independent of type* $(m_1,\dots,m_k,m_{k+1})$ *for any* $m_{k+1} \in \mathcal{M}$.

Proof. Since $\mathbf{a} \notin [\mathbf{a_1}]$, we deduce that $(\mathbf{a})_s \neq (\mathbf{a_1})_s$ for some $s \in \{1,\dots,n\}$. Thus, start with the skew polynomial $F(\mathbf{x}) := x_s - (\mathbf{a_1})_s$. Then $\deg F = 1$ and $F \in I^0(\Omega_1) \setminus I^{0,0}(\Omega_1 \cup \{\mathbf{a}\})$. Therefore, by iterating the Lemmas 3.1.16 and 3.1.17, we obtain that there exists $F \in I^{m_1,\dots,m_h}(\Omega_h) \setminus I^{m_1,\dots,m_h,0}(\Omega_h \cup \{\mathbf{a}\})$ with $\deg F = \sum_{i=1}^{h}(\deg(m_i)+1)$. Thus, one can conclude by using Lemma 3.1.11. □

Chapter 4

Resultants of skew polynomials over division rings

In commutative algebra, the notion of resultant (or eliminant) of two univariate polynomials defined over a field is well-known and classical and many results about it can be found in literature (e.g, see [29], [16] or [22]). The classical resultant of two polynomials is in fact a polynomial expression of their coefficients, which is equal to zero if and only if the polynomials have a common root, possibly in a field extension, or equivalently, a common factor over their field of coefficients. The resultant is widely used in number theory, algebraic geometry, symbolic integration, computer algebra, and it is a built-in function of most computer algebra systems. The resultant of two univariate polynomials over a field, or a commutative ring, is commonly defined as the determinant of their Sylvester matrix. More precisely, let $p(x) = p_r x^r + \cdots + p_1 x + p_0$ and $q(x) = q_s x^s + \cdots + q_1 x + q_0$ be two non-zero polynomials with $p_r \neq 0, q_s \neq 0$. The map $\varphi : \mathcal{P}_s \times \mathcal{P}_r \to \mathcal{P}_{r+s}$ given by $\varphi(a, b) = ap + bq$ is a linear map between two vector spaces of the same dimension, where $\mathcal{P}_i$ is the vector space of dimension i whose elements are the polynomials of degree less than i. Over the basis of the powers of the variable x, the above map φ is represented by a square matrix of dimension $r + s$, which is called the Sylvester matrix of p and q.

Inspired by [15], the main purpose of this chapter is to extend in $\mathbb{F}[x; \sigma, \delta]$ all the above results and well-known criteria equivalent to the condition that the resultant of two univariate skew polynomials is equal to zero. Finally, through this chapter, we give some algorithms and their respective Magma programs [3] as computational applications of the main algebraic results which allowed us to construct all the examples in a very simple manner.

4.1 Right (σ, δ)-Resultant

Let $\mathbb{F}$ be a division ring. We begin by proving two technical results which are useful to define the so called right (σ, δ)-resultant of two skew polynomials in $\mathcal{R}$ (see Definition 4.1.3).

Lemma 4.1.1. *Let $f, g \in \mathcal{R}$ be non-constant skew polynomials. The following hold:*

1) *$\mathcal{R}/\mathcal{R}f$ is a left $\mathbb{F}$-module and $\dim \mathcal{R}/\mathcal{R}f = \deg(f)$.*

2) *If $\mathcal{R}g \subseteq \mathcal{R}f$, then $\mathcal{R}f/\mathcal{R}g$ is a left $\mathbb{F}$-module and $\dim \mathcal{R}f/\mathcal{R}g = \deg(g) - \deg(f)$.*

3) *If $k, h \in \mathcal{R}$ are such that $\mathcal{R}f \cap \mathcal{R}g = \mathcal{R}h$ and $\mathcal{R}f + \mathcal{R}g = \mathcal{R}k$, then*

$$\deg(f) + \deg(g) = \deg(h) + \deg(k)$$

Proof. 1) Defining in $\mathcal{R}/\mathcal{R}f := \{p + \mathcal{R}f : p \in \mathcal{R}\}$ the usual operations of addition and scalar multiplication (on the left) given by $(p_1 + \mathcal{R}f) + (p_2 + \mathcal{R}f) := (p_1 + p_2) + \mathcal{R}f$ and $\alpha(p_1 + \mathcal{R}f) := \alpha p_1 + \mathcal{R}f$, for all $p_1, p_2 \in \mathcal{R}$ and $\alpha \in \mathbb{F}$, one can see easily that $\mathcal{R}/\mathcal{R}f$ is a left $\mathbb{F}$-module. Since every coset in $\mathcal{R}/\mathcal{R}f$ contains a unique representative of degree less than $\deg(f)$, it follows that $B := \{1 + \mathcal{R}f, x + \mathcal{R}f, x^2 + \mathcal{R}f, ..., x^{\deg(f)-1} + \mathcal{R}f\}$ is a left basis for $\mathcal{R}/\mathcal{R}f$. Therefore, $\dim \mathcal{R}/\mathcal{R}f = \deg(f)$.

2) Since $g \in \mathcal{R}g \subseteq \mathcal{R}f$, we have $g = hf$ for some $h \in \mathcal{R}$. Thus, we can write $Rf/Rg = \{rf + Rhf : r \in R\}$. On the other hand, since $\psi : \mathcal{R} \to \mathcal{R}f/\mathcal{R}hf$, $p \mapsto pf + \mathcal{R}hf$ is a surjective left $\mathbb{F}$-module homomorphism with $\ker \psi = \mathcal{R}h$, we have $\mathcal{R}/\mathcal{R}h \cong \mathcal{R}f/\mathcal{R}hf = \mathcal{R}f/\mathcal{R}g$. Finally, by 1) it follows that $\dim \mathcal{R}f/\mathcal{R}g = \dim \mathcal{R}/\mathcal{R}h = \deg(h) = \deg(g) - \deg(f)$

3) Since $\mathcal{R}$ is a LPID, we can write $\mathcal{R}f \cap \mathcal{R}g = \mathcal{R}h$ and $\mathcal{R}f + \mathcal{R}g = \mathcal{R}k$ for some $h, k \in \mathcal{R}$. Since Rf, Rg, Rh and Rk are left $\mathbb{F}$-submodules of $\mathcal{R}$, we deduce that $(Rf + Rg)/Rf \cong Rg/(Rf \cap Rg)$, i.e. $Rk/Rf \cong Rg/Rh$. Hence $\dim Rk/Rf = \dim Rg/Rh$ and by 2) we have $\deg(f) + \deg(g) = \deg(h) + \deg(k)$. □

The previous lemma is an extension of some results showed in [15, p. 4]. Moreover, by Lemma 4.1.1 it is possible to prove also the following technical result, but we omit its proof because it is analogous to the one presented in [15, Theorem 2.4] for the case $\delta = 0$.

Lemma 4.1.2. *Two non-constant skew polynomials $f, g \in \mathcal{R}$ of respective degrees m and n, have a common (non-unit) right factor in $\mathcal{R}$, if and only if there exist skew polynomials $c, d \in \mathcal{R}$ such that $cf + dg = 0$, $\deg(c) < n$ and $\deg(d) < m$.*

By Lemma 4.1.2 we can define the right (σ, δ)-resultant of two skew polynomials in $\mathcal{R}$ as shown below. Let

$$f = a_m x^m + ... + a_1 x + a_0, a_m \neq 0 \ , \quad g = b_n x^n + ... + b_1 x + b_0, b_n \neq 0 \ ,$$
$$c = c_{n-1} x^{n-1} + ... + c_1 x + c_0 \ , \quad d = d_{m-1} x^{m-1} + ... + d_1 x + d_0$$

be skew polynomials as in Lemma 4.1.2. By (1.4), we have

$$cf = \sum_{i=0}^{n-1} \sum_{j=0}^{m} \left(\sum_{k=0}^{i} c_i \cdot \mathcal{C}_{k,i-k}(a_j) x^{i+j-k} \right), \ dg = \sum_{i=0}^{m-1} \sum_{j=0}^{n} \left(\sum_{k=0}^{i} d_i \cdot \mathcal{C}_{k,i-k}(b_j) x^{i+j-k} \right)$$

Keeping in mind that two skew polynomials are equal if and only if they have the same degree and their respective coefficients are equal, the equation $cf + dg = 0$ of Lemma 4.1.2 gives a system of $m+n$ linear equations with $m+n$ unknowns $c_0, ..., c_{n-1}, d_0, ..., d_{m-1}$, that is

$$(c_0, ..., c_{n-1}, d_0, ..., d_{m-1}) \cdot A = (0, ..., 0) \ , \tag{4.1}$$

where A is the following $(m+n) \times (m+n)$ matrix:

$$A = \begin{pmatrix}
a_0 & a_1 & a_2 & \cdots & a_m & 0 & 0 & 0 & \cdots & 0 \\
\mathcal{C}_{1,0}(a_0) & \sum_{i=0}^{1} \mathcal{C}_{1-i,i}(a_{1-i}) & \sum_{i=0}^{1} \mathcal{C}_{1-i,i}(a_{2-i}) & \cdots & \sum_{i=0}^{1} \mathcal{C}_{1-i,i}(a_{m-i}) & \mathcal{C}_{0,1}(a_m) & 0 & 0 & \cdots & 0 \\
\mathcal{C}_{2,0}(a_0) & \sum_{i=0}^{1} \mathcal{C}_{2-i,i}(a_{1-i}) & \sum_{i=0}^{2} \mathcal{C}_{2-i,i}(a_{2-i}) & \cdots & \sum_{i=0}^{2} \mathcal{C}_{2-i,i}(a_{m-i}) & \sum_{i=1}^{2} \mathcal{C}_{2-i,i}(a_{m+1-i}) & \mathcal{C}_{0,2}(a_m) & 0 & \cdots & 0 \\
\mathcal{C}_{3,0}(a_0) & \sum_{i=0}^{1} \mathcal{C}_{3-i,i}(a_{1-i}) & \sum_{i=0}^{2} \mathcal{C}_{3-i,i}(a_{2-i}) & \cdots & \sum_{i=0}^{3} \mathcal{C}_{3-i,i}(a_{m-i}) & \sum_{i=1}^{3} \mathcal{C}_{3-i,i}(a_{m+1-i}) & \sum_{i=2}^{3} \mathcal{C}_{3-i,i}(a_{m+2-i}) & \mathcal{C}_{0,3}(a_m) & \cdots & 0 \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\
\mathcal{C}_{n-1,0}(a_0) & \sum_{i=0}^{1} \mathcal{C}_{n-1-i,i}(a_{1-i}) & \sum_{i=0}^{2} \mathcal{C}_{n-1-i,i}(a_{2-i}) & \cdots & \sum_{i=0}^{m} \mathcal{C}_{n-1-i,i}(a_{m-i}) & \sum_{i=1}^{n-1} \mathcal{C}_{n-1-i,i}(a_{m+1-i}) & \sum_{i=2}^{n-1} \mathcal{C}_{n-1-i,i}(a_{m+2-i}) & \sum_{i=3}^{n-1} \mathcal{C}_{n-1-i,i}(a_{m+3-i}) & \cdots & \mathcal{C}_{0,n-1}(a_m) \\
b_0 & b_1 & b_2 & \cdots & b_n & 0 & 0 & 0 & \cdots & 0 \\
\mathcal{C}_{1,0}(b_0) & \sum_{i=0}^{1} \mathcal{C}_{1-i,i}(b_{1-i}) & \sum_{i=0}^{1} \mathcal{C}_{1-i,i}(b_{2-i}) & \cdots & \sum_{i=0}^{1} \mathcal{C}_{1-i,i}(b_{n-i}) & \mathcal{C}_{0,1}(b_n) & 0 & 0 & \cdots & 0 \\
\mathcal{C}_{2,0}(b_0) & \sum_{i=0}^{1} \mathcal{C}_{2-i,i}(b_{1-i}) & \sum_{i=0}^{2} \mathcal{C}_{2-i,i}(b_{2-i}) & \cdots & \sum_{i=0}^{2} \mathcal{C}_{2-i,i}(b_{n-i}) & \sum_{i=1}^{2} \mathcal{C}_{2-i,i}(b_{n+1-i}) & \mathcal{C}_{0,2}(b_n) & 0 & \cdots & 0 \\
\mathcal{C}_{3,0}(b_0) & \sum_{i=0}^{1} \mathcal{C}_{3-i,i}(b_{1-i}) & \sum_{i=0}^{2} \mathcal{C}_{3-i,i}(b_{2-i}) & \cdots & \sum_{i=0}^{3} \mathcal{C}_{3-i,i}(b_{n-i}) & \sum_{i=1}^{3} \mathcal{C}_{3-i,i}(b_{n+1-i}) & \sum_{i=2}^{3} \mathcal{C}_{3-i,i}(b_{n+2-i}) & \mathcal{C}_{0,3}(b_n) & \cdots & 0 \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\
\mathcal{C}_{m-1,0}(b_0) & \sum_{i=0}^{1} \mathcal{C}_{m-1-i,i}(b_{1-i}) & \sum_{i=0}^{2} \mathcal{C}_{m-1-i,i}(b_{2-i}) & \cdots & \sum_{i=0}^{n} \mathcal{C}_{m-1-i,i}(b_{n-i}) & \sum_{i=1}^{m-1} \mathcal{C}_{m-1-i,i}(b_{n+1-i}) & \sum_{i=2}^{m-1} \mathcal{C}_{m-1-i,i}(b_{n+2-i}) & \sum_{i=3}^{m-1} \mathcal{C}_{m-1-i,i}(b_{n+3-i}) & \cdots & \mathcal{C}_{0,m-1}(b_n)
\end{pmatrix}$$

Note that the first n rows involve the a_i's and the last m rows involve the b_j's.

By the previous $(m+n) \times (m+n)$ matrix A, we can define the right (σ, δ)-resultant of two skew polynomials in $\mathcal{R}$ as follows.

Definition 4.1.3. Let $f, g \in \mathcal{R}$ be skew polynomials of non-negative degrees m and n, respectively. The above matrix A will be called the *right* (σ, δ)-*Sylvester matrix* of f and g, which we denote by $\mathrm{Sylv}_{\mathbb{F}}^{\sigma,\delta}(f, g)$. We define the *right* (σ, δ)-*resultant* of f and g (over $\mathbb{F}$), denoted by $R_{\mathbb{F}}^{\sigma,\delta}(f, g)$, as the Dieudonné determinant of $\mathrm{Sylv}_{\mathbb{F}}^{\sigma,\delta}(f, g)$.

Let us recall that the Dieudonné determinant, denoted here by Ddet, is a non-commutative generalization of the classical determinant of a matrix with entries in a field, to matrices over division rings. This determinant takes values in $\{0\} \cup \mathbb{F}^*/[\mathbb{F}^*, \mathbb{F}^*]$, where $[\mathbb{F}^*, \mathbb{F}^*]$ is the commutator of the multiplicative group $\mathbb{F}^* := \mathbb{F} \setminus \{0\}$. If $\mathbb{F}$ is a field, then Ddet coincides with the classical definition of determinant and in this case, we will write simply det instead of Ddet. For more details on the properties of the Dieudonné determinant, see e.g [11], [1, p. 151] and [12, p. 133].

Remark 4.1.4. In the special case when $\delta = 0$, $R_{\mathbb{F}}^{\sigma,\delta}(f, g)$ coincides with the resultant $R(f, g)$ defined in [15, p. 6]. In fact, by (1.6) we have

$$R_{\mathbb{F}}^{\sigma,0}(f, g) = \mathrm{Ddet}\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_m & 0 & \cdots & 0 \\ 0 & \sigma(a_0) & \sigma(a_1) & \cdots & \sigma(a_{m-1}) & \sigma(a_m) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \sigma^{n-1}(a_0) & \sigma^{n-1}(a_1) & \cdots & \sigma^{n-1}(a_m) \\ b_0 & b_1 & b_2 & \cdots & b_n & 0 & \cdots & 0 \\ 0 & \sigma(b_0) & \sigma(b_1) & \cdots & \sigma(b_{n-1}) & \sigma(b_n) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \sigma^{m-1}(b_0) & \sigma^{m-1}(b_1) & \cdots & \sigma^{m-1}(b_n) \end{pmatrix}$$

Furthermore, if $\sigma = Id$ then we obtain the classical notion of resultant.

Applying Algorithm 1, the next algorithm shows how to find the right (σ, δ)-Silvester matrix of f and g (see Definition 4.1.3).

Algorithm 6 Computation of the right (σ, δ)-Sylvester matrix of $f(x) = a_0 + a_1x + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$.

Input: $f, g \in \mathcal{R}$.
Output: (σ, δ)-Sylvester matrix M of f and g.

1: $M_1 \leftarrow \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n+m} \end{pmatrix}$
2: $M_2 \leftarrow \begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_{n+m} \end{pmatrix}$
3: **for** $p \leftarrow 1$ to $n - 1$ **do**
4: $\quad M_3 \leftarrow \begin{pmatrix} \mathcal{C}_{p,0}(a_0) \end{pmatrix}$

for $q \leftarrow 1$ to $n+m-1$ **do**
  $Z_1 \leftarrow 0$
  for $l \leftarrow 0$ to p **do**
    if $0 \leq q-l \leq m$ **then**
      $Z_1 \leftarrow Z_1 + \mathcal{C}_{p-l,l}(a_{q-l})$
    end if
  end for
  $M_3 \leftarrow \left(\begin{array}{c|c} M_3 & Z_1 \end{array} \right)$
end for
$M_1 \leftarrow \left(\dfrac{M_1}{M_3} \right)$
end for
for $p \leftarrow 1$ to $m-1$ **do**
  $M_4 \leftarrow \left(\mathcal{C}_{p,0}(b_0) \right)$
  for $q \leftarrow 1$ to $n+m-1$ **do**
    $Z_2 \leftarrow 0$
    for $l \leftarrow 0$ to p **do**
      if $0 \leq q-l \leq n$ **then**
        $Z_2 \leftarrow Z_2 + \mathcal{C}_{p-l,l}(b_{q-l})$
      end if
    end for
    $M_4 \leftarrow \left(\begin{array}{c|c} M_4 & Z_2 \end{array} \right)$
  end for
  $M_2 \leftarrow \left(\dfrac{M_2}{M_4} \right)$
end for
return $M \leftarrow \left(\dfrac{M_1}{M_2} \right)$

As an application of Algorithm 6, let us give here the following Magma program to compute $\mathrm{Sylv}_{\mathbb{H}}^{\sigma,\delta}(f,g)$ when $f = x^4 + kx^3 - jx^2 - i$ and $g = x^3 + j$ are skew polynomials in $\mathbb{H}[x;\sigma,0]$ with $\sigma(h) := ihi^{-1}$ for all $h \in \mathbb{H}$.

```
F<i,j,k> := QuaternionAlgebra< RealField() | -1, -1 >;
S:= map< F -> F | x :-> i*x*(1/i) >;
D:= map< F -> F | x :-> 0 >;
```

Then, using the function “PosCom" defined in Program 1, we can define the new function “SylvesterMatrix" (see Program 4) with previously the function “SumPosCom" as follows.

Program 4.

```
SumPosCom:=function(f,i,j)
AA:=0;
n:=#f-1;
 for I in [0..i-1] do
  if j-1-I ge 0 and j-1-I le n then
   if i-1 ne 0 then
    AA:=AA+PosCom(i-1-I,I,f[j-I]);
    else
    AA:=f[j-I];
   end if;
  end if;
 end for;
return AA;
end function;

SylvesterMatrix:=function(f,g)
n:=#f-1;
m:=#g-1;
if m ne 0 then
 M1:= Matrix(F,1,n+m,[SumPosCom(f,s,t): s in {1}, t in {1..n+m}]);
  for p in [2..m] do
   X:=Matrix(F,1,n+m,[SumPosCom(f,s,t): s in {p}, t in {1..n+m}]);
   M1:=VerticalJoin(M1,X);
  end for;
else
 M1:=RemoveRow(ZeroMatrix(F,1,n+m),1);
end if;
if n ne 0 then
 M2:= Matrix(F,1,n+m,[SumPosCom(g,s,t): s in {1}, t in {1..n+m}]);
  for p in [2..n] do
   X:=Matrix(F,1,n+m,[SumPosCom(g,s,t): s in {p}, t in {1..n+m}]);
   M2:=VerticalJoin(M2,X);
  end for;
else
 M2:=RemoveRow(ZeroMatrix(F,1,n+m),1);
```

```
end if;
M:=VerticalJoin(M1,M2);
return M;
end function;
```

Then, by typing in Magma

```
SylvesterMatrix([-i,-j,0,k,1],[j,0,0,1]);
```

we obtain the right (σ, δ)-Sylvester matrix of $f(x) = x^4 + kx^3 - jx - i$ and $g(x) = x^3 + j$:

$$\begin{pmatrix} -i & -j & 0 & k & 1 & 0 & 0 \\ 0 & -i & j & 0 & -k & 1 & 0 \\ 0 & 0 & -i & -j & 0 & k & 1 \\ j & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -j & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & j & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -j & 0 & 0 & 1 \end{pmatrix} . \tag{4.2}$$

Remark 4.1.5. When $\mathbb{F}$ is a field, we can write $\mathrm{R}_{\mathbb{F}}^{\sigma,\delta}(f, g) := \det(\mathrm{Sylv}_{\mathbb{F}}^{\sigma,\delta}(f, g))$, where det is the classical determinant. Therefore, in this case, we can easily compute $\mathrm{R}_{\mathbb{F}}^{\sigma,\delta}(f, g)$ in Magma by using the command "Determinant( )". However, this command in Magma generates difficulties in some situations. For example, when $\mathbb{F}$ is the field of the complex numbers, this field can only be dealt with a certain level of precision, and therefore Magma cannot give the exact value of the determinant. For this reason, we provide below a Magma program (Program 5) based on the definition of the determinant $\det A$ of an $n \times n$ matrix A with entries $a_{ij} \in \mathbb{F}$ using the Leibniz's formula, i.e.

$$\det A := \sum_{\Sigma \in S_n} \left(\mathrm{sgn}(\Sigma) a_{1,\Sigma_1} \dots a_{n,\Sigma_n}\right) ,$$

where S_n is the symmetric group of n elements, $\mathrm{sgn}(\Sigma)$ is the sign of the permutation $\Sigma \in S_n$ and Σ_i is the value in the i-th position after the reordering Σ. The advantage of this Magma program is that it avoids the Gaussian elimination and consequently the computation of quotients, because it only works with sums and products.

Program 5.

```
Det:=function(M)
n:=NumberOfColumns(M);
P:=[ p : p in Permutations({a : a in [1..n]})];
S2:=0;
 for k in [1..#P] do
  S1:=1;
  for j in [1..n] do
   S1:=S1*M[j,P[k][j]];
  end for;
  g:=Sym(n)!P[k];
  if IsEven(g) then
   S2:=S2+S1;
   else
   S2:=S2-S1;
  end if;
 end for;
return S2;
end function;
```

Now, let us give here the main results of this section for polynomials in $\mathcal{R}$.

Theorem 4.1.6. *Let $f, g \in \mathcal{R}$ be non-constant skew polynomials of degrees m and n, respectively. The following conditions are equivalent:*

1) $R_{\mathbb{F}}^{\sigma,\delta}(f, g) = 0$;

2) *f and g have a common (non-unit) right factor in $\mathcal{R}$;*

3) *$gcrd(f, g) \neq 1$ (where "gcrd" means greatest common right divisor);*

4) *there are no polynomials $p, q \in \mathcal{R}$ such that $pf + qg = 1$;*

5) $\mathcal{R}f + \mathcal{R}g \subsetneq \mathcal{R}$.

Proof. 1) $\Leftrightarrow$ 2) : $R_{\mathbb{F}}^{\sigma,\delta}(f, g) := \mathrm{Ddet}(A) = 0$ if and only if the homogeneous linear system (4.1) has a non-trivial solution. The above, is equivalent to say that there exist skew polynomials $c, d \in \mathcal{R}$ such that $cf + dg = 0$, $\deg(c) < n$ and $\deg(d) < m$. However, by

Lemma 4.1.2, the latter is true if and only if f and g have a common (non-unit) right factor in $\mathcal{R}$.

2) $\Leftrightarrow$ 3) : obvious.

3) $\Rightarrow$ 4) : Let $r \in \mathcal{R}$ be the common (non-unit) right factor of f and g (it exists because $\operatorname{gcrd}(f, g) \neq 1$). Then, $f = q_1 r$ y $g = q_2 r$, for some $q_1, q_2 \in \mathcal{R}$. Since for all $p, q \in \mathcal{R}$, $pf + qg = (pq_1 + qq_2)r$, it follows that $pf + qg \neq 1$.

4) $\Rightarrow$ 3) : Assume that for all $p, q \in \mathcal{R}$, $pf + qg \neq 1$. Since $\mathcal{R}$ is a LPID, we can write $\mathcal{R}f + \mathcal{R}g = \mathcal{R}h \subsetneq \mathcal{R}$, for some $h \in \mathcal{R}$ of positive degree. Thus h is a common (non-unit) right factor of f and g.

4) $\Leftrightarrow$ 5) : It follows from the fact that $\mathcal{R}f + \mathcal{R}g = \mathcal{R}$ if and only if $1 \in \mathcal{R}f + \mathcal{R}g$. $\square$

Remark 4.1.7. When $\delta = 0$, the equivalence between 1) and 2) in Theorem 4.1.6 gives Theorem 2.5 in [15]. Moreover, if $\mathbb{F} = \mathbb{H}$ (Hamilton's quaternions), $\sigma = Id$ and $\delta = 0$, then the equivalence between 1) and 3) in Theorem 4.1.6 gives also an analogous result to [32, Theorem 4.3], but with a different notion of determinant.

In what follows, the objective is to determine if the Dieudonné determinant of any matrix is zero or not in line with 1) of Theorem 4.1.6. To do this, we first need Algorithm 7 to obtain (via elementary row operations on the left) the corresponding upper triangular matrix D of any matrix M with entries in $\mathbb{F}$. Note that this operation does not change the nullity of M.

Algorithm 7 Computation of the upper triangular matrix D of M

Input: Square matrix $M = (a_{ij})$ of order n, with entries in $\mathbb{F}$
Output: Upper triangular matrix D

$j \leftarrow 0$
repeat
  $j \leftarrow j + 1$
  $i \leftarrow 0$, $k \leftarrow 0$
  repeat
    $i \leftarrow i + 1$
    if $a_{ij} \neq 0$ **then**
      $B_i = (b_{ij}) \leftarrow \begin{pmatrix} a_{1j} & a_{2j} & \cdots & a_{nj} \end{pmatrix}$
      for $i_1 \leftarrow 1$ to n and $i_1 \neq i$ **do**
        $C_{i_1} \leftarrow \begin{pmatrix} (a_{i_1 1} - a_{i_1 j} \cdot a_{ij}^{-1} \cdot b_{11}) & (a_{i_1 2} - a_{i_1 j} \cdot a_{ij}^{-1} \cdot b_{1j}) \cdots \\ \cdots & (a_{i_1 n} - a_{i_1 j} \cdot a_{ij}^{-1} \cdot b_{1n}) \end{pmatrix}$
      end for
      $D \leftarrow \left(\frac{D}{B_i} \right)$

$M = (a_{ij}) \leftarrow \begin{pmatrix} C_1 \\ \hline \vdots \\ \hline C_n \end{pmatrix}$
Let m be the number of rows of M.
else
$k \leftarrow k + 1$
end if
if $k = m$ and $k \neq 0$ **then**
$B_i \leftarrow \begin{pmatrix} 0 & 0 & \cdots & 0 \end{pmatrix}$
$D \leftarrow \begin{pmatrix} D \\ \hline B_i \end{pmatrix}$
end if
until $i \geq m$
until $j = n$
return D

Moreover, as an application of Algorithm 7, we give here a Magma program to compute the upper triangular matrix of (4.2) with entries in the real quaternion division ring $\mathbb{H}$.

Defining before the division ring $\mathbb{H}$,

```
F<i,j,k> := QuaternionAlgebra< RealField() | -1, -1 >;
```

we have the following Magma program:

Program 6.

```
MT:=function(M)
n:=NumberOfRows(M); m:=NumberOfRows(M);
MM:=RemoveRow(SubmatrixRange(M,1,1,1,n),1);
j:=0;
repeat
j:=j+1; i:=0; k:=0;
 repeat
 i:=i+1;
  if M[i,j] ne 0 then
   a:=M[i,j]; M1:=SubmatrixRange(M,i,1,i,n); M4:=M1; M2:=RemoveRow(M,i);
   n1:=NumberOfRows(M2);
    for i1 in [1..n1] do
     M3:=Matrix(F,1,n,[ M2[i1,j1]-M2[i1,j]*(1/a)*M1[1,j1] : j1 in [1..n]]);
```

```
     M4:=VerticalJoin(M4,M3);
    end for;
   MM:=VerticalJoin(MM,M1); M:=RemoveRow(M4,1); m:=NumberOfRows(M);
   else
   k:=k+1;
  end if;
 if k eq m and k ne 0 then
  MM:=VerticalJoin(MM,ZeroMatrix(F,1,n));
 end if;
 if k eq n then
  j:=n;
 end if;
until i ge m;
until j eq n;
return MM;
end function;
```

So, by typing in Magma

```
MT(Matrix(F,7,7,[-i,-j,0,k,1,0,0,0,-i,j,0,-k,1,0,0,0,-i,-j,0,k,1,j,0,0,
1,0,0,0,0,-j,0,0,1,0,0,0,0,j,0,0,1,0,0,0,0,-j,0,0,1]));
```

we obtain the upper triangular matrix E of (4.2),

$$E = \begin{pmatrix} -i & -j & 0 & k & 1 & 0 & 0 \\ 0 & -i & j & 0 & -k & 1 & 0 \\ 0 & 0 & -i & -j & 0 & k & 1 \\ 0 & 0 & 0 & i & 0 & 0 & k \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{4.3}$$

Now, let us recall that the Dieudonné determinant of an upper (or lower) triangular matrix D with entries in a division ring $\mathbb{F}$ is the coset $a[\mathbb{F}^*, \mathbb{F}^*]$, where a is the product of the elements of the main diagonal of D (see [13, p. 104]). Having in mind this, the above Algorithm 7 together with the next Algorithm 8 allow us to calculate up to a sign the Dieudonné determinant of any square matrix with entries in $\mathbb{F}$.

Algorithm 8 Computation of Dieudonné determinant of an upper triangular matrix.

Input: Upper triangular matrix M.
Output: Dieudonné determinant of M

Let $M = (a_{ij})$ be the upper triangular matrix
$A \leftarrow 1$
for $n \leftarrow 1$ to n **do**
    $A \leftarrow A \cdot a_{nn}$
end for
if $A = 0$ **then**
return Dieudonné determinant is 0
else
    if $A \in [\mathbb{F}^*, \mathbb{F}^*]$ **then**
return Dieudonné determinant is 0
    else
return Dieudonné determinant is A (mod $[\mathbb{F}^*, \mathbb{F}^*]$)
    end if
end if

Finally, using the function "MT" of Program 6 and having in mind that $[\mathbb{H}^*, \mathbb{H}^*] = \{q \in \mathbb{H} : |q| = 1\}$ (see [31, Lemma 8, p. 151]), the following Magma test allows us to check if the Dieudonné determinant of a matrix with entries in $\mathbb{H}$ is zero or not.

Program 7.

```
DD:=function(M)
MM:=MT(M);
A:=1;
n:=NumberOfRows(M);
 for N in [1..n] do
  A:=A*MM[N,N];
 end for;
 if A*Conjugate(A) eq F!1 or A*Conjugate(A) eq F!0 then
  print"Ddet is";
  return 0;
 end if;
print"Ddet is NOT";
return 0;
end function;
```

Let us give here a characterization of the degree of the $gcrd(f, g)$ which can be useful also to check condition 3) in Theorem 4.1.6.

Theorem 4.1.8. *Let $\mathcal{P}_k(\mathbb{F})$ be the set of the polynomials in $\mathcal{R}$ of degree less than or equal to k with coefficients in $\mathbb{F}$. Let $f, g \in \mathcal{R}$ be two polynomials of positive degree m, n respectively. Consider the left $\mathbb{F}$-linear map*

$$\varphi : \mathcal{P}_{n-1}(\mathbb{F}) \oplus \mathcal{P}_{m-1}(\mathbb{F}) \to \mathcal{P}_{n+m-1}(\mathbb{F})$$

defined by $\varphi((a, b)) := af + bg$. Then

$$\deg gcrd(f, g) = \dim \ker \varphi = \dim \ker \phi = n + m - lr.rk(A) = n + m - rc.rk(A) \ ,$$

where $\phi : \mathbb{F}^{n+m} \to \mathbb{F}^{n+m}$ is the left $\mathbb{F}$-linear map given by $\phi(\vec{x}) := \vec{x}A$ with $A := Sylv_{\mathbb{F}}^{\sigma,\delta}(f, g)$ the matrix defined in (4.1) and $lr.rk(A)$ ($rc.rk(A)$) is the left row (right column) rank of A which means the dimension of the $\mathbb{F}$-subspace spanned by the rows (columns) of A viewed as elements of the $n + m$-dimensional left (right) vector space $\mathcal{P}_{n+m-1}(\mathbb{F})$ over $\mathbb{F}$.

Proof. The equality $\dim \ker \varphi = \dim \ker \phi$ can be obtained using the identification $\mathcal{P}_k(\mathbb{F}) \cong \mathbb{F}^{k+1}$ given by the left $\mathbb{F}$-linear map $p_k x^k + \cdots + p_1 x + p_0 \ \mapsto \ (p_k, \ldots, p_1, p_0)$. Since $\mathcal{R}$ is a LPID, then we have

$$\mathcal{R}f + \mathcal{R}g = \mathcal{R}M \ , \ \mathcal{R}f \cap \mathcal{R}g = \mathcal{R}m \ ,$$

where $M := gcrd(f, g)$ and $m := lcrm(f, g)$ (least common right multiple). Then there are unique polynomials $\alpha, \beta \in \mathcal{R}$ such that $m = \alpha f = \beta g$. Moreover, by Lemma 4.1.1 3) we get also

$$\deg \alpha = \deg(m) - \deg f = (n + m - \deg M) - m = n - \deg M \ ,$$

$$\deg \beta = \deg(m) - \deg g = (n + m - \deg M) - n = m - \deg M \ .$$

Now, let $(a, b) \in \ker \varphi$. Hence $af = (-b)g \in \mathcal{R}m$. Thus there exists $t \in \mathcal{R}$ such that $af = (-b)g = tm$. This gives $af = t\alpha f$ and $(-b)g = t(-\beta)g$, i.e $a = t\alpha$ and $b = t\beta$. Therefore, by Lemma 4.1.1 3) we obtain that $(a, b) = (t\alpha, t\beta)$ with

$$\deg t + (n - \deg M) = \deg(t\alpha) = \deg a \leq n - 1 \ ,$$

$$\deg t + (m - \deg M) = \deg(t\beta) = \deg b \leq m - 1 \ ,$$

that is, $\deg t \leq \deg M - 1$ for both cases. This shows that

$$\ker \varphi \subseteq \{(t\alpha, t\beta) \ : \ t \in \mathcal{R} \ , \ \deg t \leq \deg M - 1\} \ .$$

Finally, let $(t\alpha, t\beta)$ for some $t \in \mathcal{R}$ with $\deg t \leq \deg M - 1$. Then $(t\alpha, t\beta) \in \mathcal{P}_{n-1}(\mathbb{F}) \oplus \mathcal{P}_{m-1}(\mathbb{F})$ and $\varphi((t\alpha, t\beta)) = t\alpha f + t\beta g = t(\alpha f + \beta g) = 0$. Hence $(t\alpha, t\beta) \in \ker \varphi$ for some $t \in \mathcal{R}$ with $\deg t \leq \deg M - 1$. This gives

$$\ker \varphi = \{(t\alpha, t\beta) \ : \ t \in \mathcal{R} \ , \ \deg t \leq \deg M - 1\} \ .$$

Observe that the set

$$(\alpha, \beta), (x\alpha, x\beta), (x^2\alpha, x^2\beta), \ldots, (x^{\deg M - 1}\alpha, x^{\deg M - 1}\beta)$$

is a left basis for $\ker \varphi$. Thus it follows that $\dim \ker \varphi = \deg M = \deg gcrd(f, g)$. Finally, since $\dim \mathrm{Im}(\phi) = lr.rk(A) = rc.rk(A)$, by the rank-nullity theorem we obtain also that $\dim \ker \phi = n + m - \dim \mathrm{Im}(\phi) = n + m - lr.rk(A) = n + m - rc.rk(A)$. □

Remark 4.1.9. Given a matrix A over a division ring $\mathbb{F}$, it is known that the rank of A, denoted by $rk(A) := lr.rk(A) = rc.rk(A)$, is equal to the number of all non-zero rows of the reduced-row echelon matrix of A (see [8, Theorem 1.3]). Thus, by Algorithm 7 we can easily compute $rk(\mathrm{Sylv}_{\mathbb{F}}^{\sigma,\delta}(f, g))$ (see Example 4.1.13).

Here are some examples concerning Theorem 4.1.6.

Example 4.1.10. Consider $\mathbb{F}_4[x; \sigma, \delta_t]$ with $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, where $\alpha^2 + \alpha + 1 = 0$, $\sigma(a) = a^2$ and $\delta_t(a) = t(\sigma(a) + a)$ for all $a \in \mathbb{F}_4$ and $t \in \{0, 1, \alpha, \alpha^2\}$. Given $f_1 := x^2 + \alpha^2 x + \alpha$ and $g_1 := x^2 + \alpha x + \alpha^2$, we have

$$R_{\mathbb{F}_4}^{\sigma,\delta_t}(f_1, g_1) = \det \begin{pmatrix} \alpha & \alpha^2 & 1 & 0 \\ t & \alpha^2 + t & \alpha & 1 \\ \alpha^2 & \alpha & 1 & 0 \\ t & \alpha + t & \alpha^2 & 1 \end{pmatrix} = 0$$

This shows that f_1 and g_1 have a common (non-unit) right factor, independent of $t \in \mathbb{F}_4$. In fact, the common right factor is $(x + 1)$, because $f_1 = (x + \alpha)(x + 1)$ and $g_1 = (x + \alpha^2)(x + 1)$. On the other hand, consider $\delta_\alpha(a) = \alpha(\sigma(a) + a)$ and the skew polynomials

$$f_2 := (x+1)(x+\alpha) = x^2 + \alpha x \ \ , \ \ g_2 := (x+1)(x+\alpha^2) = x^2 + \alpha^2 x + 1.$$

Note that $(x+1)$ is a common (non-unit) left factor of f_2 and g_2, but this does not guarantee that $R^{\sigma,\delta_\alpha}_{\mathbb{F}_4}(f_2, g_2)$ is zero as in the commutative case. Indeed, we have

$$R^{\sigma,\delta_\alpha}_{\mathbb{F}_4}(f_2, g_2) = \det \begin{pmatrix} 0 & \alpha & 1 & 0 \\ 0 & \alpha & \alpha^2 & 1 \\ 1 & \alpha^2 & 1 & 0 \\ 0 & \alpha^2 & \alpha & 1 \end{pmatrix} = \alpha^2 \neq 0.$$

Example 4.1.11. Let $\mathbb{F}_5(t)$ be the field of rational functions over $\mathbb{F}_5$ and consider $\mathbb{F}_5(t)[x; \sigma, \delta]$, where $\sigma : \mathbb{F}_5(t) \to \mathbb{F}_5(t), t \mapsto t^5$ (σ is not an automorphism by Remark 1.1.3) and δ is the classical derivation with respect to the variable t, i.e. $\delta := \frac{d}{dt}$. Given $f_1 := \frac{1}{t}x(x+1) = \frac{1}{t}x^2 + \frac{1}{t}x$ and $g_1 := (x+t^2)(x+1) = x^2 + (t^2+1)x + t^2$, we have

$$R^{\sigma,\delta}_{\mathbb{F}_5(t)}(f_1, g_1) = \det \begin{pmatrix} 0 & \frac{1}{t} & \frac{1}{t} & 0 \\ 0 & \frac{4}{t^2} & \frac{1+4t^3}{t^5} & \frac{1}{t^5} \\ t^2 & t^2+1 & 1 & 0 \\ 2t & t^{10}+2t & t^{10}+1 & 1 \end{pmatrix} = 0.$$

Thus, f_1 and g_1 have a common right factor in $\mathbb{F}_5(t)[x; \sigma, \delta]$. On the other hand, if we consider $f_2 := (x+1)\frac{1}{t}x = \frac{1}{t^5}x^2 + \left(\frac{t+4}{t^2}\right)x$ and $g_2 := (x+1)(x+t^2) = x^2 + (t^{10}+1)x + (t^2+2t)$, having $(x+1)$ as a common left factor, we have

$$R^{\sigma,\delta}_{\mathbb{F}_5(t)}(f_2, g_2) = \det \begin{pmatrix} 0 & \frac{t+4}{t^2} & \frac{1}{t^5} & 0 \\ 0 & \frac{2+4t}{t^3} & \frac{t^5+4}{t^{10}} & \frac{1}{t^{25}} \\ t^2+2t & t^{10}+1 & 1 & 0 \\ 2t+2 & t^{10}+2t^5 & t^{50}+1 & 1 \end{pmatrix} = k \neq 0$$

where $k = \frac{1}{t^{30}}(4t^{56} + 4t^{55} + 2t^{54} + t^{26} + 2t^{25} + 3t^{24} + t^{23} + 4t^{21} + 4t^{20} + 2t^{19} + t^{12} + 3t^{10} + 2t^7 + 3t^6 + t^5 + 2t^4 + 3t^3 + 3t + 3)$.

Example 4.1.12. Consider $\mathbb{C}[x; \sigma, \delta]$, with $\sigma(z) = \bar{z}$ (the complex conjugation) and $\delta(z) = z - \bar{z}$, for all $z \in \mathbb{C}$. Given $f = x^4 + (1+i)x^2 - 4ix + 5i$ and $g = x^3 - ix + 2i$,

we have

$$R_{\mathbb{C}}^{\sigma,\delta}(f,g)=\det\begin{pmatrix}5i & -4i & 1+i & 0 & 1 & 0 & 0\\ 10i & -13i & 6i & 1-i & 0 & 1 & 0\\ 20i & -36i & 25i & -8i & 1+i & 0 & 1\\ 2i & -i & 0 & 1 & 0 & 0 & 0\\ 4i & -4i & i & 0 & 1 & 0 & 0\\ 8i & -12i & 6i & -i & 0 & 1 & 0\\ 16i & -32i & 24i & -8i & i & 0 & 1\end{pmatrix}=0.$$

Then, by Theorem 4.1.6 we have $\operatorname{gcrd}(f,g)\neq 1$. By using the right division algorithm, we can find $\operatorname{gcrd}(f,g)$ (as in the classical case):

$$\begin{aligned}x^4+(1+i)x^2-4ix+5i &= x(x^3-ix+2i)+x^2+i\\ x^3-ix+2i &= x(x^2+i)+0\end{aligned}$$

Hence $\operatorname{gcrd}(f,g)=x^2+i$.

Example 4.1.13. Consider $\mathbb{H}[x;\sigma,0]$, where $\sigma(h):=ihi^{-1}$ (inner automorphism) for all $h\in\mathbb{H}$. Given $p=x^2+(i-j)x+k$ and $q=x+i$ in $\mathbb{H}[x;\sigma,0]$, we have

$$R_{\mathbb{H}}^{\sigma,0}(p,q)=\operatorname{Ddet}\begin{pmatrix}k & i-j & 1\\ i & 1 & 0\\ 0 & i & 1\end{pmatrix}=0$$

Therefore p and q have a common (non-unit) right factor in $\mathbb{H}[x;\sigma,0]$, which must be $q=(x+i)$. In fact, $p=x^2+(i-j)x+k=(x-j)(x+i)$. Given now $f=x^4+kx^3-jx-i$ and $g=x^3+j$, the right (σ,δ)-Sylvester matrix of $f(x)$ and $g(x)$ and its upper triangular matrix are (4.2) and (4.3), respectively. Hence we have $R_{\mathbb{H}}^{\sigma,0}(f,g)=0$. Therefore f and g have a common (non-unit) right factor in $\mathbb{H}[x;\sigma,0]$, which must be $g=(x^3+j)$. In fact, $f=x^4+kx^3-jx-i=(x+k)(x^3+j)$. Moreover, note that the echelon form of $\operatorname{Sylv}_{\mathbb{H}}^{\sigma,0}(f,g)$ is the matrix (4.3). Therefore $rk(\operatorname{Sylv}_{\mathbb{H}}^{\sigma,0}(f,g))=4$ and by Theorem 4.1.8 we have $\deg(gcrd(f,g))=3$. In fact, $gcrd(f,g)=x^3+j$.

Remark 4.1.14. In the commutative case, it is known that the last non-zero row of the Sylvester's matrix, when we put it in echelon form by using only row transformations, gives the coefficients of the greatest common divisor (see [19, Theorem 3]). However, this is not true for the noncommutative case. In fact, given $f,g\in\mathbb{H}[x;\sigma,0]$ as in Example 4.1.13, the echelon form of $\operatorname{Sylv}_{\mathbb{H}}^{\sigma,0}(f,g)$ is the matrix (4.3) and the entries of the last non-zero row of (4.3) are different from the coefficients of $\operatorname{gcrd}(f,g)=x^3+j$.

Here are some basic properties of the right (σ, δ)-resultant.

Proposition 4.1.15. *Let $f, g \in \mathcal{R}$ be two skew polynomials of non-negative degrees m and n, respectively. The following properties hold:*

1) $R_{\mathbb{F}}^{\sigma,\delta}(g, f) = (-1)^{mn} R_{\mathbb{F}}^{\sigma,\delta}(f, g)$;

2) $R_{\mathbb{F}}^{\sigma,\delta}(-f, g) = (-1)^{n} R_{\mathbb{F}}^{\sigma,\delta}(f, g)$ *and* $R_{\mathbb{F}}^{\sigma,\delta}(f, -g) = (-1)^{m} R_{\mathbb{F}}^{\sigma,\delta}(f, g)$;

3) *if* $g = x - a$, *then* $R_{\mathbb{F}}^{\sigma,\delta}(f, g) = 0$ *if and only if* $f(a) = 0$. *In particular, for* $a = 0$ *we have* $R_{\mathbb{F}}^{\sigma,\delta}(f, g) = f(0)$ $(mod\ [\mathbb{F}^*, \mathbb{F}^*])$;

4) *if* $g = b_0$, *then* $R_{\mathbb{F}}^{\sigma,\delta}(f, g) = b_0 \sigma(b_0) \sigma^2(b_0) \cdots \sigma^{m-1}(b_0)$ $(mod\ [\mathbb{F}^*, \mathbb{F}^*])$;

5) *if* $\delta = 0$ *and* $c \in \mathbb{F}^*$, *then* $R_{\mathbb{F}}^{\sigma,0}(cf, g) = N_n^{\sigma,0}(c) (mod\ [\mathbb{F}^*, \mathbb{F}^*])\ R_{\mathbb{F}}^{\sigma,0}(f, g)$.

Proof. 1) The (σ, δ)-resultant $R_{\mathbb{F}}^{\sigma,\delta}(g, f)$ is obtained by permuting the rows of the Sylvester matrix $\mathrm{Sylv}_{\mathbb{F}}^{\sigma,\delta}(f, g)$. The number of permutations is mn and, since the exchange of two any rows of a matrix changes the sign of the Dieudonné determinant, it follows that $R_{\mathbb{F}}^{\sigma,\delta}(g, f) = (-1)^{mn} R_{\mathbb{F}}^{\sigma,\delta}(f, g)$.

2) By the properties of the Dieudonné determinant, if a row of a matrix is left multiplied by $a \in \mathbb{F}^*$, then Ddet is left multiplied by a (mod $[\mathbb{F}^*, \mathbb{F}^*]$). Thus, since the first n rows of $\mathrm{Sylv}_{\mathbb{F}}^{\sigma,\delta}(f, g)$ contain the coefficients of f, $\sigma(-a) = -\sigma(a)$ and $\delta(-a) = -\delta(a)$, it follows that $R_{\mathbb{F}}^{\sigma,\delta}(-f, g) = (-1)^{n} R_{\mathbb{F}}^{\sigma,\delta}(f, g)$. Similarly, we get $R_{\mathbb{F}}^{\sigma,\delta}(f, -g) = (-1)^{m} R_{\mathbb{F}}^{\sigma,\delta}(f, g)$.

3) It follows easily from the equivalence between 1) and 2) of Theorem 4.1.6.

4) If $g = b_0$, then $\mathrm{Sylv}_{\mathbb{F}}^{\sigma,\delta}(f, g)$ is a lower triangular matrix whose elements on the main diagonal are $b_0, \sigma(b_0), \sigma^2(b_0), ..., \sigma^{m-1}(b_0)$. Then, the statement holds because Ddet of a lower (or upper) triangular matrix is the coset $a[\mathbb{F}^*, \mathbb{F}^*]$, where a is the (ordered) product of the elements on the main diagonal (see [13, p. 104]).

5) Since $\delta = 0$ and σ is an endomorphism of $\mathbb{F}$, we have

$$\mathrm{Sylv}_{\mathbb{F}}^{\sigma,0}(cf, g) = \begin{pmatrix} ca_0 & ca_1 & ca_2 & \cdots & ca_m & 0 & \cdots & 0 \\ 0 & \sigma(c)\sigma(a_0) & \sigma(c)\sigma(a_1) & \cdots & \sigma(c)\sigma(a_{m-1}) & \sigma(c)\sigma(a_m) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \sigma^{n-1}(c)\sigma^{n-1}(a_0) & \sigma^{n-1}(c)\sigma^{n-1}(a_1) & \cdots & \sigma^{n-1}(c)\sigma^{n-1}(a_m) \\ b_0 & b_1 & b_2 & \cdots & b_n & 0 & \cdots & 0 \\ 0 & \sigma(b_0) & \sigma(b_1) & \cdots & \sigma(b_{n-1}) & \sigma(b_n) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \sigma^{m-1}(b_0) & \sigma^{m-1}(b_1) & \cdots & \sigma^{m-1}(b_n) \end{pmatrix}.$$

Noting that the first n rows of the above matrix are multiplied on the left by $c, \sigma(c), \sigma^2(c)$, ..., $\sigma^{n-1}(c)$, respectively, it follows that

$$R_{\mathbb{F}}^{\sigma,0}(cf, g) = \sigma^{n-1}(c) \cdots \sigma(c)c \ (\text{mod } [\mathbb{F}^*, \mathbb{F}^*]) R_{\mathbb{F}}^{\sigma,0}(f, g) = N_n^{\sigma,0}(c) \ (\text{mod } [\mathbb{F}^*, \mathbb{F}^*]) R_{\mathbb{F}}^{\sigma,0}(f, g) \ .$$

□

Remark 4.1.16. The known property of "factorization" of the classical resultants, that is, $R(f_1 f_2, g) = R(f_1, g) \cdot R(f_2, g)$, is not true in general for our notion of resultant. Indeed, if we consider the ring $\mathbb{C}[x; \sigma, \delta]$, with $\sigma(z) = \bar{z}$ and $\delta(z) = z - \bar{z}$, for all $z \in \mathbb{C}$ and the skew polynomials $f_1 = x^2 + 1$, $f_2 = x^2 + i$ and $g = 2x^2 + x + 1$, we have

$$R_{\mathbb{C}}^{\sigma,\delta}(f_1, g) \cdot R_{\mathbb{C}}^{\sigma,\delta}(f_2, g) = \det \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 2 \end{pmatrix} \cdot \det \begin{pmatrix} i & 0 & 1 & 0 \\ 2i & -i & 0 & 1 \\ 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 2 \end{pmatrix} = 10 + 10i$$

However,

$$R_{\mathbb{C}}^{\sigma,\delta}(f_1 f_2, g) = \det \begin{pmatrix} 5i & -4i & 1+i & 0 & 1 & 0 \\ 10i & -13i & 6i & 1-i & 0 & 1 \\ 1 & 1 & 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 2 \end{pmatrix} = 650 + 90i.$$

This shows that in general $R_{\mathbb{F}}^{\sigma,\delta}(f_1 f_2, g) \neq R_{\mathbb{F}}^{\sigma,\delta}(f_1, g) \cdot R_{\mathbb{F}}^{\sigma,\delta}(f_2, g)$, also when $\delta = 0$.

Lemma 4.1.17 (Cramer's Rule)**.** *Let A be a non-singular square matrix $n \times n$ with entries in $\mathbb{F}$ and consider the linear system $A \cdot \overline{x} = \overline{b}$ for some column vector $\overline{b}$, where $\overline{x}$ is the transpose of the unknown vector $(x_1, x_2, \ldots, x_n)$. If we write $A = [\overline{v_1} | \ldots | \overline{v_n}]$, where the $\overline{v_i}$'s are the columns of A, then we have for $i = 1, \ldots, n$*

$$x_i \ (mod \ [\mathbb{F}^*, \mathbb{F}^*]) = (Ddet(A))^{-1} Ddet(A_i),$$

where $A_i := [\overline{v_1} | \ldots | \overline{b} | \ldots | \overline{v_n}]$ is the matrix A with the i-th column $\overline{v_i}$ replaced by $\overline{b}$.

Proof. Write $A^{-1}\overline{v_j} = \overline{e_j}$ for $j = 1, \ldots, n$, where the $\overline{e_j}$'s are the canonical column vectors. Then we have

$$A^{-1} \cdot \left[\overline{v_1} | \cdots | \overline{b} | \cdots | \overline{v_n}\right] = [\overline{e_1} | \cdots | \overline{x} | \cdots | \overline{e_n}] \ .$$

Therefore, by [7, Theorem 4.5] we deduce that

$$x_i \pmod{[\mathbb{F}^*, \mathbb{F}^*]} = \mathrm{Ddet}\left[\overline{e_1}|\cdots|\overline{x}|\cdots|\overline{e_n}\right] = \mathrm{Ddet}\left(A^{-1}\right)\mathrm{Ddet}\left[\overline{v_1}|\cdots|\overline{b}|\cdots|\overline{v_n}\right] \ ,$$

obtaining the formula of the statement having in mind that $\mathrm{Ddet}\,(A^{-1}) = (\mathrm{Ddet}A)^{-1}$. □

Remark 4.1.18. In a similar way as in Lemma 4.1.17, one can obtain the following row version of the Cramer's Rule. Let B be a square matrix $n \times n$ with entries in $\mathbb{F}$ and consider the linear system $\overline{y} \cdot B = \overline{c}$ for some row vector $\overline{c}$, where $\overline{y}$ is the unknown vector $(y_1, y_2, \ldots, y_n)$. If we denote by $\overline{w_j}$ the j-th row of B, then by [7, Theorems 3.9 and 4.5] we have for $j = 1, \ldots, n$

$$y_j \pmod{[\mathbb{F}^*, \mathbb{F}^*]} = \mathrm{Ddet}B_j(\mathrm{Ddet}B)^{-1} \ ,$$

where B_j is the matrix B with the j-th row $\overline{w_j}$ replaced by $\overline{c}$.

Proposition 4.1.19. *Let $f, g \in \mathcal{R}$ be two skew polynomials of positive degree. Then, there are $A, B \in \mathcal{R}$ such that*

$$Af + Bg = R_{\mathbb{F}}^{\sigma,\delta}(f, g) \ ,$$

where the coefficients of A and B (mod $[\mathbb{F}^*, \mathbb{F}^*]$) are integer polynomials in the entries of $Sylv_{\mathbb{F}}^{\sigma,\delta}(f, g)$.

Proof. Assume that $R_{\mathbb{F}}^{\sigma,\delta}(f, g) \neq 0$, otherwise we are done by choosing $A = B = 0$. Let

$$f = a_0x^l + \cdots + a_l \ , \quad a_0 \neq 0 \ ,$$

$$g = b_0x^m + \cdots + b_m \ , \quad b_0 \neq 0 \ ,$$

$$A' = c_0x^{m-1} + \cdots + c_{m-1} \ ,$$

$$B' = d_0x^{l-1} + \cdots + d_{l-1} \ ,$$

such that $A'f + B'g = 1$, where the coefficients $c_0, \ldots, c_{m-1}, d_0, \ldots, d_{l-1}$ are unknowns in $\mathbb{F}$. If we compare coefficients of powers of x in the formula $A'f + B'g = 1$, then we get the following system of linear equations similar to (4.1) with unknowns c_i, d_i:

$$(c_{m-1}, \ldots, c_0, d_{l-1}, \ldots, d_0) \cdot \mathrm{Sylv}_{\mathbb{F}}^{\sigma,\delta}(f, g) = (0, \ldots, 0, 1) \ . \tag{4.4}$$

By applying Remark 4.1.18 to the square linear system (4.4), we obtain that all the c_i's

and the d_i's are as follow:

$$c_i \pmod{[\mathbb{F}^*,\mathbb{F}^*]} = R_{\mathbb{F}}^{\sigma,\delta}(f,g)^{-1}\text{Ddet Sylv}_{\mathbb{F}}^{\sigma,\delta}(f,g)_{m-i}\ ,\ \text{for } i=0,\cdots,m-1\ ,$$

$$d_j \pmod{[\mathbb{F}^*,\mathbb{F}^*]} = R_{\mathbb{F}}^{\sigma,\delta}(f,g)^{-1}\text{Ddet Sylv}_{\mathbb{F}}^{\sigma,\delta}(f,g)_{m+l-j}\ ,\ \text{for } j=0,\cdots,l-1\ ,$$

where $\text{Sylv}_{\mathbb{F}}^{\sigma,\delta}(f,g)_k$ is the matrix $\text{Sylv}_{\mathbb{F}}^{\sigma,\delta}(f,g)$ with the k-th row replaced by the row vector $(0,\ldots,0,1)$. Defining $A := R_{\mathbb{F}}^{\sigma,\delta}(f,g)A'$, $B := R_{\mathbb{F}}^{\sigma,\delta}(f,g)B'$, we see that $Af+Bg = R_{\mathbb{F}}^{\sigma,\delta}(f,g)$ and the coefficients of A and B $(\text{mod } [\mathbb{F}^*,\mathbb{F}^*])$ are given by expressions of type $\text{Ddet Sylv}_{\mathbb{F}}^{\sigma,\delta}(f,g)_h$ for some $h=1,\ldots,m+l$. We conclude by noting that these latest expressions are simply integer polynomials in the entries of $\text{Sylv}_{\mathbb{F}}^{\sigma,\delta}(f,g)$. □

Now, let us show that under certain conditions, it is possible to add a sixth equivalent condition in Theorem 4.1.6. To do that, we first need to introduce the following definition.

Definition 4.1.20. We say that $\tilde{\mathbb{F}}[x;\tilde{\sigma},\tilde{\delta}]$ is a *polynomial ring extension* of $\mathcal{R}$ if $\mathbb{F}$ is a subring of $\tilde{\mathbb{F}}$, $\tilde{\sigma}_{|\mathbb{F}} = \sigma$ and $\tilde{\delta}_{|\mathbb{F}} = \delta$.

Remark 4.1.21. Since $\mathcal{R} \subseteq \tilde{\mathbb{F}}[x;\tilde{\sigma},\tilde{\delta}]$, $\tilde{\sigma}_{|\mathbb{F}} = \sigma$ and $\tilde{\delta}_{|\mathbb{F}} = \delta$, it is evident that $\mathcal{R}$ is closed with respect to the sum and the product of polynomials in $\tilde{\mathbb{F}}[x;\tilde{\sigma},\tilde{\delta}]$. Moreover, since $\mathcal{R}$ contains the multiplicative identity of $\tilde{\mathbb{F}}[x;\tilde{\sigma},\tilde{\delta}]$ (because $\mathbb{F}$ is a subring of $\tilde{\mathbb{F}}$), it follows that $\mathcal{R}$ is a subring of $\tilde{\mathbb{F}}[x;\tilde{\sigma},\tilde{\delta}]$.

Definition 4.1.20 is motivated by the following situation.

Consider $\mathbb{C}[x,\sigma,\delta]$, where σ is the complex conjugation and δ is an inner derivation given by $\delta(z) = z - \sigma(z) = 2\text{Im}(z)i$, for all $z \in \mathbb{C}$. Note that the skew polynomial $f = x^2 + i$ has no right roots in $\mathbb{C}$. In fact, for all $z \in \mathbb{C}$, we have

$$f(z) = N_2(z) + iN_0(z) = |z|^2 + (2\text{Im}(z)+1)i \neq 0.$$

The natural question is then the following: where does f have a right root? Unlike the classical case, i.e. when $\sigma = \text{Id}$ and $\delta = 0$, it will not be sufficient to extend $\mathbb{C}$ to find a right root of f, but it will be necessary to extend also the maps σ and δ, because the evaluation of f at such a root will depend on the action of these new functions. Therefore, we need to construct a polynomial ring extension of $\mathbb{C}[x;\sigma,\delta]$ for finding a right root of f. More in general, we will construct a polynomial ring extension $\tilde{\mathbb{F}}[x;\tilde{\sigma},\tilde{\delta}]$ of $\mathbb{C}[x;\sigma,\delta]$ such that any irreducible skew polynomial $g \in \mathbb{C}[x;\sigma,\delta]$ has a right root in $\tilde{\mathbb{F}}[x;\tilde{\sigma},\tilde{\delta}]$. Let $\mathbb{H}$ be the division ring of real quaternions. If we define over $\mathbb{H}$ the maps $\tilde{\sigma}(t) := a - bi + cj - dk$ and $\tilde{\delta}(t) := t - \tilde{\sigma}(t)$, for all $t := a + bi + cj + dk \in \mathbb{H}$, it follows

that $\tilde{\sigma}$ is an automorphism of $\mathbb{H}$ such that $\tilde{\sigma}_{|\mathbb{C}} = \sigma$ and $\tilde{\delta}$ is a $\tilde{\sigma}$-derivation such that $\tilde{\delta}_{|\mathbb{C}} = \delta$. Thus, $\mathbb{H}[x; \tilde{\sigma}, \tilde{\delta}]$ is a polynomial ring extension of $\mathbb{C}[x; \sigma, \delta]$. Moreover, since every non-constant skew polynomial $g \in \mathbb{H}[x; \sigma, \delta]$ splits into linear factors in $\mathbb{H}[x; \sigma, \delta]$ independently of σ and δ (see [28, Corollary 3]), it follows that g has all its roots in $\mathbb{H}[x; \sigma, \delta]$. In particular, the skew polynomial $f = x^2 + i \in \mathbb{C}[x; \sigma, \delta]$ will have its roots in $\mathbb{H}[x; \tilde{\sigma}, \tilde{\delta}]$. Therefore, $\mathbb{H}[x; \tilde{\sigma}, \tilde{\delta}]$ it looks like as a "*closure*" of $\mathbb{C}[x; \sigma, \delta]$.

Remark 4.1.22. Let $\mathbb{F} = \mathbb{F}_q$ be a finite field with q elements, where $q = p^m$ for some prime p and $m \in \mathbb{Z}_{\geq 1}$. Given any field extension $\tilde{\mathbb{F}}/\mathbb{F}_q$ and any automorphism σ of $\mathbb{F}_q$, that is, $\sigma(a) := a^{p^j}$ for any $a \in \mathbb{F}_q$ and some integer j such that $1 \leq j \leq m$, we see that one can always extend trivially σ to an automorphism $\tilde{\sigma} : \tilde{\mathbb{F}} \to \tilde{\mathbb{F}}$ such that $\tilde{\sigma}|_{\mathbb{F}_q} = \sigma$ by defining $\tilde{\sigma}(b) := b^{p^j}$ for any $b \in \tilde{\mathbb{F}}_q$. Moreover, since any σ-derivation δ is an inner derivation (see Proposition 1.1.4), that is, $\delta_\beta(a) := \beta(\sigma(a) - a)$ for any $a \in \mathbb{F}_q$ and some $\beta \in \mathbb{F}_q$, we can also extend trivially δ_β to a $\tilde{\sigma}$-derivation $\tilde{\delta}_\beta : \tilde{\mathbb{F}} \to \tilde{\mathbb{F}}$ such that $\tilde{\delta}_{\beta|\mathbb{F}_q} = \delta_\beta$ by defining $\tilde{\delta}_\beta(b) := \beta(\tilde{\sigma}(b) - b)$ for any $b \in \tilde{\mathbb{F}}$. This gives a special polynomial ring extension $\tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$ of $\mathbb{F}_q[x; \sigma, \delta]$ such that $N_i^{\tilde{\sigma}, \tilde{\delta}}(y) = N_i^{\sigma, \delta}(y)$ for any $y \in \tilde{\mathbb{F}}$ and $i \in \mathbb{Z}_{\geq 0}$.

The above remark shows that if $\mathbb{F}$ is a finite division ring (i.e. a finite field), then we can always construct a suitable polynomial ring extension. So, by Remark 4.1.22 we can obtain the following result.

Theorem 4.1.23. *Two non-constant skew polynomials $f, g \in \mathbb{F}_q[x; \sigma, \delta]$ have a common right root in some polynomial ring extension $\tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$ of $\mathbb{F}_q[x; \sigma, \delta]$ if and only if $R_{\mathbb{F}_q}^{\sigma, \delta}(f, g) = 0$.*

Proof. If $f(x)$ and $g(x)$ have a common right root α in some polynomial ring extension $\tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$ of $\mathbb{F}_q[x; \sigma, \delta]$, then $f(x) = f_1(x)(x - \alpha)$ and $g(x) = g_1(x)(x - \alpha)$, for some $f_1(x), g_1(x) \in \tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$. By Theorem 4.1.6, since $f(x)$ and $g(x)$ have a common (non-unit) right factor $(x - \alpha)$ in $\tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$ it follows that $\mathrm{R}_{\tilde{\mathbb{F}}}^{\tilde{\sigma}, \tilde{\delta}}(f, g) = 0$. However, since $\tilde{\sigma}_{|\mathbb{F}_q} = \sigma$ and $\tilde{\delta}_{|\mathbb{F}_q} = \delta$, we obtain that $\mathrm{R}_{\mathbb{F}_q}^{\sigma, \delta}(f, g) = \mathrm{R}_{\tilde{\mathbb{F}}}^{\tilde{\sigma}, \tilde{\delta}}(f, g) = 0$. Conversely, if $\mathrm{R}_{\mathbb{F}_q}^{\sigma, \delta}(f, g) = 0$ then f and g have a common (non-unit) right factor $h(x) := \sum_i h_i x^i \in \mathbb{F}_q[x; \sigma, \delta]$. Thus, we can write $f(x) = f'(x)h(x)$ and $g(x) = g'(x)h(x)$, for some $f'(x), g'(x) \in \mathbb{F}_q[x; \sigma, \delta]$. If $h(x)$ has a right root in $\mathbb{F}_q$ then we are done. Otherwise, since any endomorphism σ of $\mathbb{F}_q$ is an automorphism of the form $\sigma(a) = a^{p^j}$ for some integer j such that $1 \leq j \leq m$ and each δ is an inner derivation, observe that $\sum_i h_i N_i^{\sigma, \delta}(y) \in \mathbb{F}_q[y]$. Therefore, from classical field theory it follows that there exists a field extension $\tilde{\mathbb{F}}$ of $\mathbb{F}_q$ such that $\sum_i h_i N_i^{\sigma, \delta}(\tilde{y}) = 0$ for some $\tilde{y} \in \tilde{\mathbb{F}}$. So considering

the special polynomial ring extension $\tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$ of $\mathbb{F}_q[x; \sigma, \delta]$ of Remark 4.1.22 with $\tilde{\mathbb{F}}$ as above, we have $h(\tilde{y}) = \sum_i h_i N_i^{\tilde{\sigma}, \tilde{\delta}}(\tilde{y}) = \sum_i h_i N_i^{\sigma, \delta}(\tilde{y}) = 0$ in $\tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$. Since $\mathbb{F}_q[x; \sigma, \delta] \subseteq \tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$, we can conclude by Theorem 1.1.18 that there exists $\tilde{y} \in \tilde{\mathbb{F}}$ such that $f(\tilde{y}) = g(\tilde{y}) = 0$ in $\tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$, that is, f and g have a common right root in some polynomial ring extension of $\mathcal{R}$. □

Corollary 4.1.24. *Let $\mathbb{F}$ be a division ring and let $f, g \in \mathcal{R}$ be two non-constant skew polynomials. If f and g have a common right root in some polynomial ring extension $\tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$ of $\mathcal{R}$, then $R_{\mathbb{F}}^{\sigma, \delta}(f, g) = 0$.*

Proof. It follows easily from the first part of the proof of Theorem 4.1.23. □

An interesting problem would be to determine, in general, when the reciprocal of Corollary 4.1.24 is true. We know that if $\mathrm{R}_{\mathbb{F}}^{\sigma, \delta}(f, g) = 0$ then f and g have a common (non-unit) right factor $h \in \mathcal{R}$. Then, the existence of a common right root between f and g is reduced to guarantee the existence of some polynomial ring extension where h has a right root. If $\mathbb{F} = \mathbb{F}_q$ is a finite field, then we have seen in Theorem 4.1.23 that for any skew polynomial $h \in \mathbb{F}_q[x; \sigma, \delta]$ we can find a polynomial ring extension where h has a right root. If $\mathbb{F} = \mathbb{C}$, then for the case $\mathbb{C}[x; \sigma, \delta]$ with σ the complex conjugation and δ an inner derivation, we know that $\mathbb{H}[x; \sigma, \delta]$ is a "closure" of $\mathbb{C}[x; \sigma, \delta]$. Therefore, every irreducible skew polynomial $h \in \mathbb{C}[x; \sigma, \delta]$ has a right root in $\mathbb{H}[x; \sigma, \delta]$ and then the reciprocal of Corollary 4.1.24 is true also in this case.

Thus, one could ask in which other cases the reciprocal of Corollary 4.1.24 is true. The following result gives a partial answer when $\mathbb{F}$ is an infinite division ring.

Proposition 4.1.25. *Let $\mathbb{F}$ be an infinite division ring and let σ be an inner automorphism of $\mathbb{F}$. Skew polynomials $f, g \in \mathbb{F}[x; \sigma] = \mathbb{F}[x; \sigma, 0]$ have a common right root in some polynomial ring extension $\tilde{\mathbb{F}}[x; \tilde{\sigma}]$ of $\mathbb{F}[x; \sigma]$ if and only if $R_{\mathbb{F}}^{\sigma, 0}(f, g) = 0$.*

Proof. By Corollary 4.1.24, the left-to-right implication is true. Conversely, suppose that $\mathrm{R}_{\mathbb{F}}^{\sigma, 0}(f, g) = 0$. Then $f(x) = a(x)h(x)$ and $g(x) = b(x)h(x)$, for some $a(x), b(x), h(x) \in \mathbb{F}[x; \sigma]$ with $h(x) := \sum_{i=0}^{n} h_i x^i \in \mathbb{F}[x; \sigma]$ of positive degree. If $h(x)$ has a right root in $\mathbb{F}$, then we are done. Otherwise, since σ is an inner automorphism, that is, $\sigma(a) := g^{-1}ag$ for all $a \in \mathbb{F}$ and $g \in \mathbb{F}^*$, we have

$$N_i^{\sigma, 0}(a) := N_i(a) = g^{1-i}(ag)^i g^{-1}, \text{ for all } a \in \mathbb{F},\ i \in \mathbb{Z}_{\geq 0}.$$

Then, we get

$$\textstyle\sum_{i=0}^{n} h_i N_i(a) = \sum_{i=0}^{n} h_i g^{1-i}(ag)^i g^{-1} = (\sum_{i=0}^{n} h_i g^{1-i}(ag)^i) g^{-1} = (\sum_{i=0}^{n} h_i' b^i) g^{-1}$$

where $b := ag$ and $h'_i := h_i g^{1-i}$ for all $i = 0, 1, ..., n$. Since $\sum_{i=0}^{n} h_i N_i(a) = 0$ if and only if $\sum_{i=0}^{n} h'_i b^i = 0$, it is sufficient to guarantee the existence of a right root of $p(y) := \sum_{i=0}^{n} h'_i b^i \in \mathbb{F}[y]$. By [10, Theorem 8.5.1], there exists a division ring extension (or skew field extension) $\tilde{\mathbb{F}}$ of $\mathbb{F}$ such that p has a right root, say $p(\alpha) = \sum_{i=0}^{n} h'_i \alpha^i = 0$ for some $\alpha \in \tilde{\mathbb{F}}$. Thus, defining $\tilde{\sigma}(z) := g^{-1} z g$ for all $z \in \tilde{\mathbb{F}}$ and putting $\beta := \alpha g^{-1} \in \tilde{\mathbb{F}}$, we have

$$h(\beta) = \sum_{i=0}^{n} h_i N_i^{\tilde{\sigma},0}(\beta) = \sum_{i=0}^{n} h_i N_i(\beta) = \left(\sum_{i=0}^{n} h'_i (\beta g)^i \right) g^{-1} = p(\beta g) g^{-1} = p(\alpha) g^{-1} = 0$$

in $\tilde{\mathbb{F}}[x; \tilde{\sigma}]$. Since $\mathbb{F}[x; \sigma] \subseteq \tilde{\mathbb{F}}[x; \tilde{\sigma}]$, we can conclude again by Theorem 1.1.18 that there exists $\beta \in \tilde{\mathbb{F}}$ such that $f(\beta) = g(\beta) = 0$ in $\tilde{\mathbb{F}}[x; \tilde{\sigma}]$, that is, f and g have a common right root in some polynomial ring extension of $\mathbb{F}[x; \sigma]$. □

Remark 4.1.26. Let $\mathbb{F}$ be an infinite division ring. If $\mathbb{F}$ is finite dimensional over its center Z, then every automorphism of $\mathbb{F}$ over Z is inner (see [10, Corollary 3.3.6]). Therefore, under this hypothesis, the result of Proposition 4.1.25 still holds.

Corollary 4.1.27. *Let $\mathbb{F}$ be an infinite division ring, σ an inner automorphism and δ an inner derivation of $\mathbb{F}$. Skew polynomials $f, g \in \mathbb{F}[x; \sigma, \delta]$ have a common right root in some polynomial ring extension $\tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$ of $\mathbb{F}[x; \sigma, \delta]$ if and only if $R_{\mathbb{F}}^{\sigma,\delta}(f, g) = 0$.*

Proof. By Corollary 4.1.24, the left-to-right implication is true. Conversely, if $\mathrm{R}_{\mathbb{F}}^{\sigma,\delta}(f, g) = 0$, then by Theorem 4.1.6 $f(x)$ and $g(x)$ have a common (non-unit) right factor in $\mathbb{F}[x; \sigma, \delta]$. Since σ, δ are inner, i.e. $\sigma(a) := g^{-1} a g$ and $\delta(a) := \sigma(a) v - v a$ with $g \in \mathbb{F}^*$ and $v \in \mathbb{F}$ for all $a \in \mathbb{F}$, then by the change of variable $x' := x + v$, we have a ring isomorphism between $\mathbb{F}[x; \sigma, \delta]$ and $\mathbb{F}[x'; \sigma]$ (see [9, p. 295]). Then it follows that $f(x' - v), g(x' - v)$ have a common (non-unit) right factor in $\mathbb{F}[x'; \sigma]$ and therefore $\mathrm{R}_{\mathbb{F}}^{\sigma,\delta}(f(x' - v), g(x' - v)) = 0$. Thus, by Proposition 4.1.25 $f(x' - v)$ and $g(x' - v)$ have a common right root in some polynomial ring extension $\tilde{\mathbb{F}}[x'; \tilde{\sigma}]$ of $\mathbb{F}[x'; \sigma]$, where $\tilde{\sigma}(z) := g^{-1} z g$ for all $z \in \tilde{\mathbb{F}}$. Now, constructing the ring isomorphism $\tilde{\varphi}$ between $\tilde{\mathbb{F}}[x', \tilde{\sigma}]$ and $\tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$ (by the change of variable $x := x' - v$), where $\tilde{\delta}(z) := \tilde{\sigma}(z) v - v a$ for all $z \in \tilde{\mathbb{F}}$, it follows that $f(x), g(x)$ have a common right root in $\tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$.

$$\begin{array}{ccc} \mathbb{F}[x; \sigma, \delta] & \xleftrightarrow{\varphi} & \mathbb{F}[x'; \sigma] \\ \big\downarrow i & & \big\downarrow j \\ \tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}] & \xleftrightarrow{\tilde{\varphi}} & \tilde{\mathbb{F}}[x'; \tilde{\sigma}] \end{array}$$

□

4.2 Left (σ, δ)-Resultant

In Examples 4.1.10 and 4.1.11 we have seen that in general the condition $\mathrm{R}_{\mathbb{F}}^{\sigma,\delta}(f, g) = 0$ is not related with the existence of common (non-unit) left factor of f and g. From this, it seems interesting to study the possibility of defining a left (σ, δ)-resultant which allows us to guarantee the existence of a common (non-unit) left factor for two skew polynomials. Since not every endomorphism σ over a division ring $\mathbb{F}$ is an automorphism (see Remark 1.1.3), we would like to emphasize the fact that in general the left-hand division of two skew polynomials cannot be performed in $\mathcal{R}$ (see e.g. [27]). On the other hand, under the assumption that σ is an automorphism, one can give a left-hand version of some of the main results shown in § 4.1.

Keeping in mind that if σ is an automorphism then $\mathcal{R}$ is a left Euclidean domain and hence a RPID (see [27, Theorem 6]), it is possible to give a left version of Lemma 4.1.2 as follows.

Lemma 4.2.1. *Let σ be an automorphism of $\mathbb{F}$. Two non-constant skew polynomials $f, g \in \mathcal{R}$ of respective degrees m and n, have a common (non-unit) left factor in $\mathcal{R}$ if and only if there exist skew polynomials $c, d \in \mathcal{R}$ such that $fc + gd = 0$, $\deg(c) < n$ and $\deg(d) < m$.*

By Lemmas 1.1.12 and 4.2.1, we can define a left (σ, δ)-resultant as follows. Let

$$f = a_m x^m + \ldots + a_1 x + a_0, a_m \neq 0\ , \quad g = b_n x^n + \ldots + b_1 x + b_0, b_n \neq 0\ ,$$
$$c = c_{n-1} x^{n-1} + \ldots + c_1 x + c_0\ , \quad d = d_{m-1} x^{m-1} + \ldots + d_1 x + d_0$$

be skew polynomials as in Lemma 4.2.1. By Lemma 1.1.12, we can write

$$f = x^m A_m + \ldots + x A_1 + A_0, A_m \neq 0\ , \quad g = x^n B_n + \ldots + x B_1 + B_0, B_n \neq 0\ ,$$
$$c = x^{n-1} C_{n-1} + \ldots + x C_1 + C_0\ , \quad d = x^{m-1} D_{m-1} + \ldots + x D_1 + D_0$$

where A_i, B_i, C_i, D_i are given by (1.7). Then, by (1.5) we have

$$fc = \sum_{i=0}^{m} \sum_{j=0}^{n-1} \left(\sum_{k=0}^{j} x^{i+j-k} (-1)^k \mathcal{T}_{k,j-k}(A_i) \cdot C_j \right)$$
$$gd = \sum_{i=0}^{n} \sum_{j=0}^{m-1} \left(\sum_{k=0}^{j} x^{i+j-k} (-1)^k \mathcal{T}_{k,j-k}(B_i) \cdot D_j \right)$$

Thus the equation $fc + gd = 0$ of Lemma 4.2.1 gives a homogeneous system of $m + n$

linear equations with $m+n$ unknowns $C_0, ..., C_{n-1}, D_0, ..., D_{m-1}$, that is

$$M \cdot (C_0, ..., C_{n-1}, D_0, ..., D_{m-1})^T = (0, ..., 0) \ , \tag{4.5}$$

where M is the following $(m+n) \times (m+n)$ matrix:

$$M = \begin{pmatrix}
A_0 & A_1 & A_2 & \cdots & A_m & 0 & 0 & 0 & \cdots & 0 \\
-\mathcal{T}_{1,0}(A_0) & \sum_{i=0}^{1}(-1)^{1+i}\mathcal{T}_{1-i,i}(A_{1-i}) & \sum_{i=0}^{1}(-1)^{1+i}\mathcal{T}_{1-i,i}(A_{2-i}) & \cdots & \sum_{i=0}^{1}(-1)^{1+i}\mathcal{T}_{1-i,i}(A_{m-i}) & \mathcal{T}_{0,1}(A_m) & 0 & 0 & \cdots & 0 \\
\mathcal{T}_{2,0}(A_0) & \sum_{i=0}^{1}(-1)^{2+i}\mathcal{T}_{2-i,i}(A_{1-i}) & \sum_{i=0}^{2}(-1)^{2+i}\mathcal{T}_{2-i,i}(A_{2-i}) & \cdots & \sum_{i=0}^{2}(-1)^{2+i}\mathcal{T}_{2-i,i}(A_{m-i}) & \sum_{i=1}^{2}(-1)^{2+i}\mathcal{T}_{2-i,i}(A_{m+1-i}) & \mathcal{T}_{0,2}(A_m) & 0 & \cdots & 0 \\
-\mathcal{T}_{3,0}(A_0) & \sum_{i=0}^{1}(-1)^{3+i}\mathcal{T}_{3-i,i}(A_{1-i}) & \sum_{i=0}^{2}(-1)^{3+i}\mathcal{T}_{3-i,i}(A_{2-i}) & \cdots & \sum_{i=0}^{3}(-1)^{3+i}\mathcal{T}_{3-i,i}(A_{m-i}) & \sum_{i=1}^{3}(-1)^{3+i}\mathcal{T}_{3-i,i}(A_{m+1-i}) & \sum_{i=2}^{3}(-1)^{3+i}\mathcal{T}_{3-i,i}(A_{m+1-i}) & \mathcal{T}_{0,3}(A_m) & \cdots & 0 \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\
(-1)^{n-1}\mathcal{T}_{n-1,0}(A_0) & \sum_{i=0}^{1}(-1)^{n-1+i}\mathcal{T}_{n-1-i,i}(A_{1-i}) & \sum_{i=0}^{2}(-1)^{n-1+i}\mathcal{T}_{n-1-i,i}(A_{2-i}) & \cdots & \sum_{i=0}^{m}(-1)^{n-1+i}\mathcal{T}_{n-1-i,i}(A_{m-i}) & \sum_{i=1}^{n-1}(-1)^{n-1+i}\mathcal{T}_{n-1-i,i}(A_{m+1-i}) & \sum_{i=2}^{n-1}(-1)^{n-1+i}\mathcal{T}_{n-1-i,i}(A_{m+2-i}) & \sum_{i=3}^{n-1}(-1)^{n-1+i}\mathcal{T}_{n-1-i,i}(A_{m+3-i}) & \cdots & \mathcal{T}_{0,n-1}(A_m) \\
B_0 & B_1 & B_2 & \cdots & B_n & 0 & 0 & 0 & \cdots & 0 \\
-\mathcal{T}_{1,0}(B_0) & \sum_{i=0}^{1}(-1)^{1+i}\mathcal{T}_{1-i,i}(B_{1-i}) & \sum_{i=0}^{1}(-1)^{1+i}\mathcal{T}_{1-i,i}(B_{2-i}) & \cdots & \sum_{i=0}^{1}(-1)^{1+i}\mathcal{T}_{1-i,i}(B_{n-i}) & \mathcal{T}_{0,1}(B_n) & 0 & 0 & \cdots & 0 \\
\mathcal{T}_{2,0}(B_0) & \sum_{i=0}^{1}(-1)^{2+i}\mathcal{T}_{2-i,i}(B_{1-i}) & \sum_{i=0}^{2}(-1)^{2+i}\mathcal{T}_{2-i,i}(B_{2-i}) & \cdots & \sum_{i=0}^{2}(-1)^{2+i}\mathcal{T}_{2-i,i}(B_{n-i}) & \sum_{i=1}^{2}(-1)^{2+i}\mathcal{T}_{2-i,i}(B_{n+1-i}) & \mathcal{T}_{0,2}(B_n) & 0 & \cdots & 0 \\
-\mathcal{T}_{3,0}(B_0) & \sum_{i=0}^{1}(-1)^{3+i}\mathcal{T}_{3-i,i}(B_{1-i}) & \sum_{i=0}^{2}(-1)^{3+i}\mathcal{T}_{3-i,i}(B_{2-i}) & \cdots & \sum_{i=0}^{3}(-1)^{3+i}\mathcal{T}_{3-i,i}(B_{n-i}) & \sum_{i=1}^{3}(-1)^{3+i}\mathcal{T}_{3-i,i}(B_{n+1-i}) & \sum_{i=2}^{3}(-1)^{3+i}\mathcal{T}_{3-i,i}(B_{n+1-i}) & \mathcal{T}_{0,3}(A_m) & \cdots & 0 \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\
(-1)^{m-1}\mathcal{T}_{m-1,0}(B_0) & \sum_{i=0}^{1}(-1)^{m-1+i}\mathcal{T}_{m-1-i,i}(B_{1-i}) & \sum_{i=0}^{2}(-1)^{m-1+i}\mathcal{T}_{m-1-i,i}(B_{2-i}) & \cdots & \sum_{i=0}^{n}(-1)^{m-1+i}\mathcal{T}_{m-1-i,i}(B_{n-i}) & \sum_{i=1}^{m-1}(-1)^{m-1+i}\mathcal{T}_{m-1-i,i}(B_{n+1-i}) & \sum_{i=2}^{m-1}(-1)^{m-1+i}\mathcal{T}_{m-1-i,i}(B_{n+2-i}) & \sum_{i=3}^{m-1}(-1)^{m-1+i}\mathcal{T}_{m-1-i,i}(B_{n+3-i}) & \cdots & \mathcal{T}_{0,m-1}(B_n)
\end{pmatrix}$$

The first n rows involve the A_i's and the last m rows involve the B_j's.

From the preceding $(m+n)\times(m+n)$ matrix M, we can define the left (σ, δ)-resultant.

Definition 4.2.2. Let $f, g \in \mathcal{R}$ be skew polynomials of non-negative degrees m and n, respectively, with σ an automorphism. The above matrix M will be called the *left* (σ, δ)-*Sylvester matrix* of f and g, we will denote by $\text{Sylv}^{\sigma,\delta}_{\mathbb{F},L}(f, g)$. Finally, we define the *left* (σ, δ)-*resultant* of f and g (over $\mathbb{F}$), denoted by $R^{\sigma,\delta}_{\mathbb{F},L}(f, g)$, as the Dieudonné determinant of M.

Remark 4.2.3. If $\delta = 0$, then formula (1.7) can be written as $\mathcal{A}_i = \sigma^{-i}(a_i)$ for all

$i = 1, ..., m$, and $\mathcal{A}_0 = a_0$. Hence $R^{\sigma,0}_{\mathbb{F},L}(f, g) = \text{Ddet}(M)$ with

$$M = \begin{pmatrix} a_0 & \sigma^{-1}(a_1) & \sigma^{-2}(a_2) & \cdots & \sigma^{-m}(a_m) & 0 & \cdots & 0 \\ 0 & \sigma^{-1}(a_0) & \sigma^{-2}(a_1) & \cdots & \sigma^{-m}(a_{m-1}) & \sigma^{-(m+1)}(a_m) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \sigma^{-(n-1)}(a_0) & \sigma^{-n}(a_1) & \cdots & \sigma^{-(n-1+m)}(a_m) \\ b_0 & \sigma^{-1}(b_1) & \sigma^{-2}(b_2) & \cdots & \sigma^{-n}(b_n) & 0 & \cdots & 0 \\ 0 & \sigma^{-1}(b_0) & \sigma^{-2}(b_1) & \cdots & \sigma^{-n}(b_{n-1}) & \sigma^{-(n+1)}(b_n) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \sigma^{-(m-1)}(b_0) & \sigma^{-m}(b_1) & \cdots & \sigma^{-(m-1+n)}(b_n) \end{pmatrix}$$

To obtain an algorithm that allows us to compute the left (σ, δ)-Sylvester matrix (see Definition 4.2.2), we will need first the Algorithm 9 below.

Algorithm 9 Computation of $\mathcal{A}_i$

Input: $f(x) = \sum_{i=0}^{m} a_i x^i$ and $i \in \{0, \ldots, m\}$
Output: $\mathcal{A}_i$

$A_i \leftarrow 0$
for $j \leftarrow 0$ to $m + 1 - i$ **do**
    $A_i \leftarrow A_i + (-1)^j \cdot \mathcal{T}_{j,i}(a_{j+i-1})$
end for
return $\mathcal{A}_i$

By Algorithms 2 and 9, we can produce now the following algorithm which allows us to compute $\text{Sylv}^{\sigma,\delta}_{\mathbb{F},L}(f, g)$.

Algorithm 10 Computation of the left (σ, δ)-Sylvester matrix of $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ and $g(x) = b_0 + b_1 x + \cdots + b_n x^n$.

Input: $f, g \in \mathcal{R}$.
Output: Left (σ, δ)-Sylvester matrix M of f and g.

$M_1 \leftarrow \begin{pmatrix} \mathcal{A}_0 & \mathcal{A}_1 & \mathcal{A}_2 & \cdots & \mathcal{A}_{n+m} \end{pmatrix}$
$M_2 \leftarrow \begin{pmatrix} \mathcal{B}_0 & \mathcal{B}_1 & \mathcal{B}_2 & \cdots & \mathcal{B}_{n+m} \end{pmatrix}$
for $p \leftarrow 1$ to $n - 1$ **do**
    $M_3 \leftarrow \begin{pmatrix} (-1)^p \cdot \mathcal{T}_{p,0}(\mathcal{A}_0) \end{pmatrix}$
    for $q \leftarrow 1$ to $n + m - 1$ **do**
        $Z_1 \leftarrow 0$
        for $l \leftarrow 0$ to p **do**
            if $0 \leq q - l \leq m$ **then**
                $Z_1 \leftarrow Z_1 + \mathcal{T}_{p-l,l}(\mathcal{A}_{q-l})$
            end if

11: **end for**
12: $M_3 \leftarrow \left(\begin{array}{c|c} M_3 & Z_1 \end{array} \right)$
13: **end for**
14: $M_1 \leftarrow \left(\dfrac{M_1}{M_3} \right)$
15: **end for**
16: **for** $p \leftarrow 1$ to $m-1$ **do**
17: $M_4 \leftarrow \left(\mathcal{T}_{p,0}(\mathcal{B}_0) \right)$
18: **for** $q \leftarrow 1$ to $n+m-1$ **do**
19: $Z_2 \leftarrow 0$
20: **for** $l \leftarrow 0$ to p **do**
21: **if** $0 \leq q-l \leq n$ **then**
22: $Z_2 \leftarrow Z_2 + \mathcal{T}_{p-l,l}(\mathcal{B}_{q-l})$
23: **end if**
24: **end for**
25: $M_4 \leftarrow \left(\begin{array}{c|c} M_4 & Z_2 \end{array} \right)$
26: **end for**
27: $M_2 \leftarrow \left(\dfrac{M_2}{M_4} \right)$
28: **end for**
29: $M \leftarrow \left(\dfrac{M_1}{M_2} \right)$
30: **return** M

As an application of the above algorithms, we can calculate in Magma the left (σ, δ)-Sylvester matrix of $f = x^2 + wx$ and $g = x^2 + w^2x + 1$ in $\mathbb{F}_4[x; \sigma, \delta]$, where $\mathbb{F}_4 = \{0, 1, w, w^2\}, \sigma(a) = a^2, \delta(a) = w(\sigma(a) + a)$ for every $a \in \mathbb{F}_4$. Note that in this situation $\sigma^{-1} = \sigma$.

First, write the following instructions in Magma:

```
F<w>:=GF(4);
\\ In this situation S must be the inverse of sigma
S:= map< F -> F | x :-> x^2 >;
D:= map< F -> F | x :-> w*(S(x)+x) >;
```

Then, by typing the next Magma program

Program 8.

```
PosComT:=function(i,j,a)
C:= [u: u in [VectorSpace(GF(2),i+j)!v : v in
VectorSpace(GF(2),i+j)]| Weight(u) eq i];
```

```
A:=0;
for k in [1..#C] do
 b:=a;
  for l in [1..i+j] do
   if C[k][l] eq 1 then
    b:=D(S(b));
    else
    b:=S(b);
   end if;
  end for;
 A:=A+b;
end for;
return A;
end function;

Ai:=function(f,i)
A:=0;
for j in [0..#f-i] do
 A:=A+(-1)^(j)*PosComT(j,i-1,f[j+i]);
end for;
return A;
end function;

SumPosComT:=function(f,i,j)
AA:=0;
for k in [0..i-1] do
 if j-k ge 1 and j-k le #f then
  if i-1 ne 0 then
   AA:=AA+(-1)^(i-1+k)*PosComT(i-1-k,k,Ai(f,j-k));
   else
   AA:=(-1)^(i-1+k)*Ai(f,j-k);
  end if;
 end if;
end for;
return AA;
end function;
```

```
LeftSylvesterMatrix:=function(f,g)
m:=#f-1;
n:=#g-1;
if n ne 0 then
 M1:= Matrix(F,1,n+m,[SumPosComT(f,s,t): s in {1}, t in {1..n+m}]);
  for p in [2..n] do
   X:=Matrix(F,1,n+m,[SumPosComT(f,s,t): s in {p}, t in {1..n+m}]);
   M1:=VerticalJoin(M1,X);
  end for;
 else
 M1:=RemoveRow(ZeroMatrix(F,1,n+m),1);
end if;
if m ne 0 then
 M2:= Matrix(F,1,n+m,[SumPosComT(g,s,t): s in {1}, t in {1..n+m}]);
  for p in [2..m] do
   X:=Matrix(F,1,n+m,[SumPosComT(g,s,t): s in {p}, t in {1..n+m}]);
   M2:=VerticalJoin(M2,X);
  end for;
 else
 M2:=RemoveRow(ZeroMatrix(F,1,n+m),1);
end if;
M:=VerticalJoin(M1,M2);
return M;
end function;
```

and writing the following instruction

```
LeftSylvesterMatrix([0,w,1],[1,w^2,1]);
```

we obtain

$$S := Sylv^{\sigma,\delta}_{\mathbb{F}_4,L}(f,g) = \begin{pmatrix} w & w^2 & 1 & 0 \\ w & 1 & w & 1 \\ w^2 & w & 1 & 0 \\ w & 0 & w^2 & 1 \end{pmatrix}. \tag{4.6}$$

By using $R^{\sigma,\delta}_{\mathbb{F},L}(f,g)$, we can give a left-hand version of Theorem 4.1.6 as follows.

Theorem 4.2.4. *Let σ be an automorphism of $\mathbb{F}$ and let $f, g \in \mathcal{R}$ be two skew polynomials of positive degree m and n, respectively. Then the following conditions are equivalent:*

1) $R^{\sigma,\delta}_{\mathbb{F},L}(f,g) = 0$;

2) *f and g have a common (non-unit) left factor in $\mathcal{R}$;*

3) *$gcld(f,g) \neq 1$ (where "gcld" means greatest common left divisor);*

4) *there are no polynomials $p, q \in \mathcal{R}$ such that $fp + gq = 1$;*

5) $f\mathcal{R} + g\mathcal{R} \subsetneq \mathcal{R}$.

Proof. Similar to Theorem 4.1.6. □

Example 4.2.5. Consider $\mathbb{F}_4[x; \sigma, \delta]$ with $\mathbb{F}_4 = \{0, 1, w, w^2\}$, where $w^2 + w + 1 = 0$, $\sigma(a) = a^2$ and $\delta(a) = w(\sigma(a) + a)$ for all $a \in \mathbb{F}_4$. In Example 4.1.10 we have seen that given $f := (x+1)(x+w) = x^2 + wx$ and $g := (x+1)(x+w^2) = x^2 + w^2x + 1$ we have $R^{\sigma,\delta}_{\mathbb{F}_4}(f,g) = w^2 \neq 0$, but $R^{\sigma,\delta}_{\mathbb{F}_4,L}(f,g) = \det S = 0$ with S as in (4.6), according to Theorem 4.2.4.

Let us continue here by giving left-hand versions of some previous results, whose proofs we omit because are similar to those of Theorem 4.1.8 and Proposition 4.1.19, respectively.

Theorem 4.2.6. *Let σ an automorphism of $\mathbb{F}$ and $\mathcal{P}_k(\mathbb{F})$ be the set of the polynomials in $\mathcal{R}$ of degree less than or equal to k with coefficients in $\mathbb{F}$. Let $f, g \in \mathcal{R}$ be two polynomials of positive degree m, n respectively. Consider the right $\mathbb{F}$-linear map*

$$\varphi : \mathcal{P}_{n-1}(\mathbb{F}) \oplus \mathcal{P}_{m-1}(\mathbb{F}) \to \mathcal{P}_{n+m-1}(\mathbb{F})$$

defined by $\varphi((a,b)) := fa + gb$. Then

$$\deg gcld(f,g) = \dim \ker \varphi = \dim \ker \phi = n + m - rr.rk(M) = n + m - lc.rk(M) \ ,$$

where $\phi : \mathbb{F}^{n+m} \to \mathbb{F}^{n+m}$ is the right $\mathbb{F}$-linear map given by $\phi(\vec{x}) := M \cdot \vec{x}^T$ with $M := Sylv^{\sigma,\delta}_{\mathbb{F},L}(f,g)$ the matrix defined in (4.5) and $rr.rk(M)$ ($lc.rk(M)$) is the right row (left column) rank of M which means the dimension of the $\mathbb{F}$-subspace spanned by the rows (columns) of M viewed as elements of the $n+m$-dimensional right (left) vector space $\mathcal{P}_{n+m-1}(\mathbb{F})$ over $\mathbb{F}$.

Proposition 4.2.7. *Let $f, g \in \mathcal{R}$ be two skew polynomials of positive degree. Then, there are $A, B \in \mathcal{R}$ such that*

$$fA + gB = R^{\sigma,\delta}_{\mathbb{F},L}(f, g) \ ,$$

where the coefficients of A and B $(mod\ [\mathbb{F}^*, \mathbb{F}^*])$ are integer polynomials in the entries of $Sylv^{\sigma,\delta}_{\mathbb{F},L}(f, g)$.

Moreover, we can reformulate Proposition 4.1.15, Theorem 4.1.23 and Corollary 4.1.24 as follows.

Proposition 4.2.8. *Let σ be an automorphism of $\mathbb{F}$ and let $f, g \in \mathcal{R}$ be two skew polynomials of non-negative degree m and n, respectively. The following properties hold:*

1) $R^{\sigma,\delta}_{\mathbb{F},L}(g, f) = (-1)^{mn} R^{\sigma,\delta}_{\mathbb{F},L}(f, g)$.

2) $R^{\sigma,\delta}_{\mathbb{F},L}(-f, g) = (-1)^n R^{\sigma,\delta}_{\mathbb{F},L}(f, g)$ *and* $R^{\sigma,\delta}_{\mathbb{F},L}(f, -g) = (-1)^m R^{\sigma,\delta}_{\mathbb{F},L}(f, g)$.

3) *If $g = x - a$, then $R^{\sigma,\delta}_{\mathbb{F},L}(f, g) = 0$ if and only if $f_L(a) = 0$. In particular, if $a = 0$ we have $R^{\sigma,\delta}_{\mathbb{F},L}(f, g) = f_L(0)$ $(mod\ [\mathbb{F}^*, \mathbb{F}^*])$*

4) *If $g = b_0$, then $R^{\sigma,\delta}_{\mathbb{F},L}(f, g) = b_0\sigma^{-1}(b_0)\sigma^{-2}(b_0)\cdots\sigma^{-(m-1)}(b_0)$ $(mod\ [\mathbb{F}^*, \mathbb{F}^*])$.*

Proof. The proofs of the statements 1), 2) and 4) are similar to the proof of Proposition 4.1.15. Finally, statement 3) follows easily from equivalence between 1) and 2) of Theorem 4.2.4. □

Theorem 4.2.9. *Two non-constant skew polynomials $f, g \in \mathbb{F}_q[x; \sigma, \delta]$ have a common left root in some polynomial ring extension $\tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$ of $\mathbb{F}_q[x; \sigma, \delta]$ if and only if $R^{\sigma,\delta}_{\mathbb{F}_q,L}(f, g) = 0$.*

Proof. The left-to-right implication follows from Theorem 4.2.4 and the fact that $\mathrm{R}^{\tilde{\sigma},\tilde{\delta}}_{\tilde{\mathbb{F}},L}(f, g) = \mathrm{R}^{\sigma,\delta}_{\mathbb{F}_q,L}(f, g)$. Conversely, the proof it is analogous to the right-to-left implication of Theorem 4.1.23 by using [2, Theorem 3.2] and by exchanging the functions $N^{\sigma,\delta}_i$ with $M^{\sigma,\delta}_i$ of Lemma 1.1.14 together with slight modifications. □

Corollary 4.2.10. *Let $\mathbb{F}$ be a division ring and let $f, g \in \mathcal{R}$ be two non-constant skew polynomials. If f and g have a common left root in some polynomial ring extension $\tilde{\mathbb{F}}[x; \tilde{\sigma}, \tilde{\delta}]$ of $\mathcal{R}$, then $R^{\sigma,\delta}_{\mathbb{F},L}(f, g) = 0$.*

4.3 Right and left multiple roots

In this section, under the assumption that σ is an automorphism of $\mathbb{F}$, we will use the left and right (σ,δ)-resultants to analyse the existence of right and left multiple roots of a skew polynomial $f \in \mathcal{R}$, respectively.

First, let us give here the next classical definition of right (left) multiplicity of roots.

Definition 4.3.1. Consider $f \in \mathcal{R}$, $a \in \mathbb{F}$ and $r \in \mathbb{Z}_{\geq 1}$. If σ is an endomorphism (automorphism), we say that a is a *right (left) root of f of multiplicity $\geq r$* if the skew polynomial $(x-a)^r$ divides f on the right (left). Moreover, we say that a is a right (left) root of f of multiplicity r if the skew polynomial $(x-a)^r$ is the maximum power of $x-a$ which divides f on the right (left).

Example 4.3.2. Let $\mathbb{F}_9[x;\sigma,0]$ with $\sigma(z) := z^3$ for all $z \in \mathbb{F}_9$. If $x = a \in \mathbb{F}_9$ is a right root of $g(x) \in \mathbb{F}_9[x;\sigma,0]$ of multiplicity ≥ 2, then $\mathrm{R}^{\sigma,\delta}_{\mathbb{F}_9}(g, \Delta^1_a g) = 0$. On the other hand, consider $f(x) = (x+1)(x-1) \in \mathbb{F}_9[x;\sigma,0]$. Then $\Delta^1_1 f(x) = x+1$ and $R^{\sigma,0}_{\mathbb{F}_9}(f, \Delta^1_1 f) = 0$, because we can write $f(x) = (x-1)(x+1)$, but $x = 1$ is a right root of $f(x)$ of multiplicity one.

Keeping in mind the previous definition, we obtain the following result.

Theorem 4.3.3. *Consider $f \in \mathcal{R}$, $a \in \mathbb{F}$ and r a positive integer such that $r < \deg f$. If σ is an automorphism of $\mathbb{F}$, then the following are equivalent:*

1) *a is a right (left) root of f of multiplicity $\geq r$;*

2) *a is a common right (left) root of $f, \Delta^1_a f, \ldots, \Delta^{r-1}_a f$ $\left(f, \Delta^1_{a,L} f, \ldots, \Delta^{r-1}_{a,L} f\right)$;*

3) *$R^{\sigma,\delta}_{\mathbb{F},L}(\Delta^j_a f, \Delta^{j+1}_a f) = 0$ $\left(R^{\sigma,\delta}_{\mathbb{F}}(\Delta^j_{a,L} f, \Delta^{j+1}_{a,L} f) = 0\right)$ for $j = 0, \ldots, r-1$;*

4) *$gcld(\Delta^j_a f, \Delta^{j+1}_a f) \neq 1$ $\left(gcrd(\Delta^j_{a,L} f, \Delta^{j+1}_{a,L} f) \neq 1\right)$ for $j = 0, \ldots, r-1$,*

where $\Delta^0_a f(a) := f(a)$ $\left(\left(\Delta^0_{a,L} f\right)_L (a) := f_L(a)\right)$.

Proof. The equivalence between 1) and 2) follows from Definition 4.3.1 and the equalities

$$\Delta^i_a\left(g(x)(x-a)^t\right) = g(x)(x-a)^{t-i} \quad \left(\Delta^i_{a,L}\left((x-a)^t g(x)\right) = (x-a)^{t-i} g(x)\right),$$

$$(*)\ \ \Delta^i_a f(x) = \Delta^{i+1}_a f(x)(x-a) + \Delta^i_a f(a) \quad \left(\Delta^i_{a,L} f(x) = (x-a)\Delta^{i+1}_{a,L} f(x) + \left(\Delta^i_{a,L} f\right)_L (a)\right),$$

for $i = 0, \ldots, r-1$, where $\Delta^0_a f(x) = f(x)$ $\left(\Delta^0_{a,L} f(x) = f(x)\right)$, while the equivalences 2) $\Leftrightarrow$ 3) $\Leftrightarrow$ 4) follow from Theorems 4.1.6 and 4.2.4, and the fact that for every

$j = 0, \dots, r-1$, we have $\Delta_a^j f(a) = 0$ $(\Delta_{a,L}^j f(a) = 0) \iff \mathrm{R}_{\mathbb{F},L}^{\sigma,\delta}(\Delta_a^j f, \Delta_a^{j+1} f) = 0$ $(\mathrm{R}_{\mathbb{F}}^{\sigma,\delta}(\Delta_{a,L}^j f, \Delta_{a,L}^{j+1} f) = 0)$ by the equations $(*)$. □

Recently, in [26] the author proposed a definition of multiplicity distinct from the previous one, but which coincide in the commutative case (that is, when $\mathbb{F}$ is a field, $\sigma = Id$ and $\delta = 0$).

Definition 4.3.4. Let σ be an endomorphism (automorphism) of $\mathbb{F}$. For $r \in \mathbb{Z}_{>0}$, we say that a sequence $\mathbf{a} = (a_1, a_2, ..., a_r) \in \mathbb{F}^r$ is a *right (left)* (σ, δ)*-multiplicity sequence* if a_1 is the only right (left) root of the skew polynomial $P_{\mathbf{a}}$ $(P_{\mathbf{a},L})$. Moreover, given $f \in \mathcal{R}$, $r \in \mathbb{Z}_{>0}$ and a right (left) (σ, δ)-multiplicity sequence $\mathbf{a} = (a_1, ..., a_r) \in \mathbb{F}^r$ as before, we say that a_1 is a *right (left) zero of* f *of multiplicity* r *via* $\mathbf{a}$ if the skew polynomial $P_{\mathbf{a}}$ $(P_{\mathbf{a},L})$ divides f on the right (left).

Finally, with this new notion of multiplicity, we get also the next result.

Theorem 4.3.5. *Let* σ *be an automorphism of* $\mathbb{F}$. *Consider* $f \in \mathcal{R}$, $a \in \mathbb{F}$, r *a positive integer such that* $r < \deg f$ *and* $\mathbf{a} = (a_1, ..., a_r) \in \mathbb{F}^r$ *a right (left)* (σ, δ)*-multiplicity sequence. Then the following are equivalent:*

1) a_1 *is a right (left) root of* f *of multiplicity* r *via* $\mathbf{a}$*;*

2) $\Delta_{\mathbf{a_i}} f(a_{i+1}) = 0$ $\left((\Delta_{\mathbf{a_i},L} f)_L (a_{i+1}) = 0\right)$ *for all* $i = 0, 1, ..., r-1$, *where* $\mathbf{a_j} = (a_1, \dots, a_j)$ *for* $j = 1, 2, ..., r-1$, $\Delta_{\mathbf{a_0}} f(a_1) := f(a_1)$ $\left((\Delta_{\mathbf{a_0},L} f)_L (a_1) := f_L(a_1)\right)$*;*

3) $R_{\mathbb{F},L}^{\sigma,\delta}(\Delta_{\mathbf{a_i}} f, \Delta_{\mathbf{a_{i+1}}} f) = 0$ $\left(R_{\mathbb{F}}^{\sigma,\delta}(\Delta_{\mathbf{a_i},L} f, \Delta_{\mathbf{a_{i+1}},L} f) = 0\right)$ *for all* $i = 0, 1, ..., r-1$ *;*

4) $gcld(\Delta_{\mathbf{a_i}} f, \Delta_{\mathbf{a_{i+1}}} f) \neq 1$ $\left(gcrd(\Delta_{\mathbf{a_i},L} f, \Delta_{\mathbf{a_{i+1}},L} f) \neq 1\right)$ *for all* $i = 0, 1, ..., r-1$.

Proof. The equivalence between 1) and 2) follows from [26, Proposition 45] (a left-hand version of [26, Proposition 45] with suitable modifications) and Remark 2.2.3, while the equivalences 2) ⇔ 3) ⇔ 4) follow from Theorem 4.2.4 (Theorem 4.1.6) and the fact that for every $i = 0, \dots, r-1$, we have $\Delta_{\mathbf{a_i}} f(a_{i+1}) = 0$ $\left((\Delta_{\mathbf{a_i},L} f)_L (a_{i+1}) = 0\right) \iff \mathrm{R}_{\mathbb{F},L}^{\sigma,\delta}(\Delta_{\mathbf{a_i}} f, \Delta_{\mathbf{a_{i+1}}} f) = 0$ $\left(\mathrm{R}_{\mathbb{F}}^{\sigma,\delta}(\Delta_{\mathbf{a_i},L} f, \Delta_{\mathbf{a_{i+1}},L} f) = 0\right)$ because $\Delta_{\mathbf{a_i}} f(x) = \Delta_{\mathbf{a_{i+1}}} f(x)(x - a_{i+1}) + \Delta_{\mathbf{a_i}} f(a_{i+1})$ $\left(\Delta_{\mathbf{a_i},L} f(x) = (x - a_{i+1}) \Delta_{\mathbf{a_{i+1}},L} f(x) + (\Delta_{\mathbf{a_i},L} f)_L (a_{i+1})\right)$. □

Bibliography

[1] E. Artin, *Geometric algebra*, Interscience Publishers, Inc., New York-London, 1957.

[2] T. Baumbaugh, *Results on Common Left/Right Divisors of Skew Polynomials*, PhD thesis, Clemson University, 2016.

[3] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[4] D. Boucher, F. Ulmer, *Coding with skew polynomial rings*, J. Symbolic Comput. **44** (2009), no. 12, 1644–1656.

[5] D. Boucher D, P. Gaborit, W. Geiselmann, F. Ulmer, *Key exchange and encryption schemes based on non-commutative skew polynomials*, Proc. PQCrypto. **6061** (2010), 126–141.

[6] D. Boucher, W. Geiselmann, F.Ulmer, *Skew-cyclic codes*. Appl. Algebra Engrg. Comm. Comput. **18** (2007), no. 4, 379–389.

[7] J.L. Brenner, *Applications of the Dieudonné determinant*, Linear Algebra Appl. **1** (1968), 511–536.

[8] N. Buaphim, K. Onsaard , P. So-ngoen, and T. Rungratgasame, *Some reviews on ranks of upper triangular block matrices over a skew field*, International Mathematical Forum (2018), vol. 13, no. 7, pp. 323–335.

[9] P.M. Cohn, *Free Rings and Their Relations*, London Math. Soc. Monographs, No. 2. Academic Press, London-New York, 1971.

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

[11] J. Dieudonné, *Les déterminants sur un corps non commutatif*, Bull. Soc. Math. France **71** (1943), 27–45.

[12] P.K. Draxl, *Skew fields*, London Mathematical Society Lecture Note Series **81**, Cambridge University Press, Cambridge, 1983.

[13] P. Draxl, M. Kneser, SK_1 *von Schiefkörpern*, Seminar held at Bielefeld and Göttingen, 1976, Lecture Notes in Mathematics **778**, Springer, Berlin, 1980.

[14] A. Lj. Erić, *Polynomial interpolation problem for skew polynomials*, Appl. Anal. Disc. Math. **1** (2007), 403–414.

[15] A. Lj. Erić, *The resultant of non-commutative polynomials*, Mat. Vesnik **60** (2008), no. 1, 3–8.

[16] I.M. Gelfand, M.M. Kapranov and A.V. Zelevinsky, *Discriminants, resultants, and multidimensional determinants*, Birkhäuser Boston, Inc., Boston, 1994.

[17] I.N. Herstein, *Wedderburn's theorem and a theorem of Jacobson*, Amer. Math. Monthly **68** (1961), 249–251.

[18] N. Jacobson, *Finite-dimensional division algebras over fields*, Springer-Verlag, Berlin, 1996.

[19] M.A. Laidacker, *Another theorem relating Sylvester's matrix and the greatest common divisor*, Math. Mag. **42** (1969), 126–128.

[20] T.Y. Lam, *A first course in noncommutative rings*, Graduate Texts in Mathematics **131**, Springer-Verlag, New York, 1991.

[21] T.Y. Lam, A. Leroy, *Vandermonde and Wronskian matrices over division rings*, J. Algebra **119** (1988), no. 2, 308–336.

[22] S. Lang, *Algebra. Revised third edition*, Graduate Texts in Mathematics **211**, Springer-Verlag, New York, 2002.

[23] U. Martínez-Peñas, F. Kschischang, *Evaluation and interpolation over multivariate skew polynomial rings*, J. Algebra **525** (2019), 111–139.

[24] 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.

[25] U. Martínez-Peñas, *Sum-rank BCH codes and cyclic-skew-cyclic codes*, IEEE Trans. Inform. Theory **67** (2021), no. 8, 5149–5167.

[26] U. Martínez-Peñas, *Zeros with multiplicity, Hasse derivatives and linear factors of general skew polynomials*, ArXiv preprint arXiv: 2103.07239 (2021).

[27] O. Ore, *Theory of non-commutative polynomials*, Ann. of Math. (2) **34** (1933), no. 3, 480–508.

[28] S. Pumplün, *Factoring skew polynomials over Hamilton's quaternion algebra and the complex numbers*, J. Algebra **427** (2015), 20–29.

[29] B.L. Van der Waerden, *Modern Algebra, Vol. I*, Translated from the second revised German edition by Fred Blum. With revisions and additions by the author. Frederick Ungar Publishing Co., New York, N. Y., 1949.

[30] M. Voskoglou, *Derivations and Iterated Skew Polynomial Rings*, International journal of applied mathematics and informatics, Issue 2, Volume 5, 2011.

[31] R. Wilson, J. Gray, *Mathematical conversations: selections from The Mathematical Intelligencer*, Springer, 2001.

[32] X. Zhao, Y. Zhang, *Resultants of quaternion polynomials*, Hacet. J. Math. Stat. **48** (2019), no. 5, 1304–1311.