Adv. Appl. Clifford Algebras (2022) 32:54

0188-7009/050001-43
published online September 4, 2022
https://doi.org/10.1007/s00006-022-01241-z

Advances in Applied Clifford Algebras

The Sum and the Product of Two Quadratic Matrices: Regular Cases

Clément de Seguins Pazzis*

Communicated by Uwe Kaehler

Abstract. Let p and q be polynomials with degree 2 over an arbitrary field $\mathbb{F}$, and M be a square matrix over $\mathbb{F}$. Thanks to the study of an algebra that is deeply connected to quaternion algebras, we give a necessary and sufficient condition for M to split into $A+B$ for some pair (A,B) of square matrices over $\mathbb{F}$ such that $p(A)=0$ and $q(B)=0$, provided that no eigenvalue of M splits into the sum of a root of p and a root of q. Provided that $p(0)q(0)\neq 0$ and no eigenvalue of M is the product of a root of p with a root of q, we also give a necessary and sufficient condition for M to split into AB for some pair (A,B) of square matrices over $\mathbb{F}$ such that $p(A)=0$ and $q(B)=0$. In further articles, we will complete the study by lifting the assumptions on the eigenvalues of M.

Mathematics Subject Classification. Primary 15A24, 15B33.

Keywords. Quadratic matrices, Rational canonical form, Companion matrices, Quaternion algebras, Decomposition.

1. Introduction

1.1. The Starting Point: A Strange 4-Dimensional Algebra

The main point of the article is the following. Starting from two monic polynomials p and q of degree 2 over a field $\mathbb{F}$, from a commutative unital $\mathbb{F}$-algebra R, and from an element x of R, we define an R-algebra, denoted by $\mathcal{W}(p,q,x)_R$, which has an additional structure of 4-dimensional free R-module. Precisely, $\mathcal{W}(p,q,x)_R$ is isomorphic to the quotient algebra of the unital free noncommutative R-algebra in two generators a and b by the two-sided ideal generated by $p(a), q(b)$ and $a(\mu 1_R - b) + b(\lambda 1_R - a) - x\,1_R$, where $p(t) = t^2 - \lambda t + p(0)$ and $q(t) = t^2 - \mu t + q(0)$; however, for convenience it

*Corresponding author.

turns out that it is better to define this algebra as a subalgebra of the algebra $\mathrm{M}_4(R)$ of 4-by-4 matrices with entries in R (see Sect. 2.2). It turns out that there is a very specific anti-automorphism $x \mapsto x^\star$ (the conjugation) of $\mathcal{W}(p,q,x)_R$, and a norm $N : \mathcal{W}(p,q,x)_R \rightarrow R$ such that $hh^\star = h^\star h = N(h).e$ for all $h \in \mathcal{W}(p,q,x)_R$, where e stands for the unity of $\mathcal{W}(p,q,x)_R$ (the construction of those mappings will be carried out in Sect. 2.3).

This is of course very reminiscent of quaternion algebras, and indeed it turns out that $\mathcal{W}(p,q,x)_R$ is a quaternion algebra whenever R is a field extension of $\mathbb{F}$ and unless x satisfies a very specific property with respect to p and q. If R is a field extension of $\mathbb{F}$, then the norm N is a 4-dimensional quadratic form on $\mathcal{W}(p,q,x)_R$. The degeneracy of N has a simple characterization in terms of the triple (p,q,x) (see Proposition 2.3 in Sect. 2.4), but it would be a distraction to state it now. Here is our first main result:

Theorem 1.1. *Let $\mathbb{L}$ be a field extension of $\mathbb{F}$. Let $x \in \mathbb{L}$, and assume that the norm of $\mathcal{W}(p,q,x)_{\mathbb{L}}$ is non-degenerate. Then $\mathcal{W}(p,q,x)_{\mathbb{L}}$ is a quaternion algebra over $\mathbb{L}$ and its norm of quaternion algebra is N.*

In particular, if the norm of $\mathcal{W}(p,q,x)_{\mathbb{L}}$ is both non-degenerate and isotropic, then $\mathcal{W}(p,q,x)_{\mathbb{L}}$ is isomorphic to the $\mathbb{L}$-algebra $\mathrm{M}_2(\mathbb{L})$ of 2-by-2 matrices over $\mathbb{L}$. Key to our article will be the following extension of this result to the case where R is the local residue ring $\mathbb{F}[t]/(r^n)$ for some monic irreducible polynomial r over $\mathbb{F}$:

Theorem 1.2. *Let r be an irreducible monic polynomial of $\mathbb{F}[t]$, and $n \in \mathbb{N}^*$ be a non-zero integer. Set $R := \mathbb{F}[t]/(r^n)$ and let x be the class of some polynomial of $\mathbb{F}[t]$ in R, and $\overline{x}$ be the class of the same polynomial in the residue field $\mathbb{L} := \mathbb{F}[t]/(r)$. Assume finally that the norm of $\mathcal{W}(p,q,\overline{x})_{\mathbb{L}}$ is non-degenerate and isotropic. Then, the R-algebra $\mathcal{W}(p,q,x)_R$ is isomorphic to $\mathrm{M}_2(R)$.*

At the point, the bottom line is that we start from a quirky 4-dimensional algebra with a strange set of parameters and, in many interesting cases we end up with the familiar situation of quaternion algebras, a special case of our beloved Clifford algebras.

The $\mathcal{W}(p,q,x)_R$ algebra is not an artificial construction: it appears naturally in trying to solve two long-standing decomposition problems in linear algebra. Not only will it help solve those problems, but it will unify many special cases of those problems that, prior to this paper, had been given scattered proofs, another tribute to the unifying power of Clifford algebras. The full study of the $\mathcal{W}(p,q,x)_R$ algebra is carried out in Sect. 2. In the meantime, we turn to explain the decomposition problems we aim at solving, along with a couple of basic technical issues that are not directly connected to the $\mathcal{W}(p,q,x)_R$ algebra (so the reader who is interested by the $\mathcal{W}(p,q,x)_R$ algebra for itself can directly jump to Sect. 2).

1.2. Quadratic Elements in an Algebra Over a Field

Let $\mathbb{F}$ be an arbitrary field and $\overline{\mathbb{F}}$ be an algebraic closure of it. We denote by $\mathrm{char}(\mathbb{F})$ the characteristic of $\mathbb{F}$. We denote by $\mathrm{M}_n(\mathbb{F})$ the algebra of all square matrices with n rows and entries in $\mathbb{F}$, and by I_n its unity. The similarity of two square matrices A and B is denoted by $A \simeq B$. We denote by $\mathbb{N}$ the set of all non-negative integers, and by $\mathbb{N}^*$ the set of all positive ones. Given a polynomial $p \in \mathbb{F}[t]$, we denote by $\mathrm{Root}(p)$ the set of all roots of p in $\overline{\mathbb{F}}$, and, if p is non-constant and monic with degree n, we denote by $\mathrm{tr}(p)$ the opposite of the coefficient of p on t^{n-1}, which we call the trace of p.

An element of an $\mathbb{F}$-algebra $\mathcal{A}$ is called **quadratic** when it is annihilated by a polynomial of degree 2 of $\mathbb{F}[t]$. Basic special cases of such elements are the idempotents ($a^2 = a$), the involutions ($a^2 = 1_{\mathcal{A}}$) and the square-zero elements ($a^2 = 0$). Given an element a of an $\mathbb{F}$-algebra $\mathcal{A}$ together with a polynomial $p \in \mathbb{F}[t]$ with degree 2 such that $p(a) = 0$, we set $a^\star := (\mathrm{tr}\, p)\, 1_{\mathcal{A}} - a$, which we call the p-**conjugate** of a, and we note that $aa^\star = a^\star a = p(0)1_{\mathcal{A}}$ (in this notation, the polynomial should normally be specified because of the possibility that a be a scalar multiple of $1_{\mathcal{A}}$, but it will always be clear from the context). Note that if p is irreducible then a and $a^\star$ are its roots in the quadratic extension $\mathbb{F}[a]$.

The following basic result will be used throughout the article so we state it and prove it right away.

Lemma 1.3. (Basic Commutation Lemma). *Let p and q be monic polynomials of $\mathbb{F}[t]$ with degree 2. Let a, b be elements of an $\mathbb{F}$-algebra $\mathcal{A}$ such that $p(a) = q(b) = 0$, and denote respectively by $a^\star$ and $b^\star$ the p-conjugate of a and the q-conjugate of b. Then, a and b commute with $ab^\star + ba^\star$.*

Note also that

$$ab^\star + ba^\star = \mathrm{tr}(q)\, a + \mathrm{tr}(p)\, b - (ab + ba) = a^\star b + b^\star a.$$

Proof. On the one hand

$$(ab^\star + ba^\star)a = ab^\star a + p(0)b,$$

and on the other hand, $ab^\star + ba^\star = b^\star a + a^\star b$, whence

$$a(ab^\star + ba^\star) = a(b^\star a + a^\star b) = ab^\star a + p(0)b.$$

Thus, a commutes with $ab^\star + ba^\star$. Symmetrically, so does b. □

1.3. The (p, q)-Sums (or Difference) Decomposition Problem

Let p and q be monic polynomials of degree 2 over $\mathbb{F}$. An element x of an $\mathbb{F}$-algebra $\mathcal{A}$ is called a (p, q)-**sum** (respectively, a (p, q)-**difference**) whenever it splits as $x = a + b$ (respectively, $x = a - b$) where a, b are elements of $\mathcal{A}$ that satisfy $p(a) = 0$ and $q(b) = 0$. In particular, by taking $\mathcal{A} = \mathrm{M}_n(\mathbb{F})$ or $\mathcal{A} = \mathrm{End}(V)$ for some vector space V over $\mathbb{F}$, we have the notion of a (p, q)-sum and of a (p, q)-difference for square matrices over $\mathbb{F}$ and for endomorphisms of V. Those two notions are easily connected: an element of $\mathcal{A}$ is a (p, q)-sum if and only if it is a $(p, q(-t))$-difference.

We will focus only on (p, q)-differences, as many results turn out to have a more elegant formulation when expressed in terms of (p, q)-differences rather than in terms of (p, q)-sums. Here is the first problem we will address here:

When is a square matrix a (p, q)-difference?

Since the set of all matrices $A \in \mathrm{M}_n(\mathbb{F})$ such that $p(A) = 0$ is a union of similarity classes, and ditto for q instead of p, the set of all matrices in $\mathrm{M}_n(\mathbb{F})$ that are (p, q)-differences is a union of similarity classes. Hence, in theory it should be possible to find necessary and sufficient conditions for being a (p, q)-difference in terms of either the Jordan normal form or the rational canonical form.

Special cases in the above problem were solved starting in the early nineteen nineties. First, Hartwig and Putcha [11] solved the case where $p = q = t^2 - t$ over the field of complex numbers, i.e. they determined the matrices that can be written as the difference of two idempotent complex matrices, and they also determined those that can be written as the sum of two idempotent complex matrices (those problems are easily seen to be equivalent by noting that a matrix A of $\mathrm{M}_n(\mathbb{F})$ is idempotent if and only if $I_n - A$ is idempotent). Later, Wang and Wu [18] obtained similar characterizations for sums of two square-zero complex matrices, and Wang alone [16] obtained a characterization of the matrices that are the sum of an idempotent matrix and a square-zero one, again over the field of complex numbers. In all those works, both the results and the methods can be generalized effortlessly to any algebraically closed field with characteristic not 2.

More recently, the results of the above authors were extended to arbitrary fields, even those with characteristic 2. In [9], we managed to obtain a description of all matrices that split into a linear combination of two idempotents with fixed nonzero coefficients, over an arbitrary field. It is easily seen that this yields a solution to the above problem in the slightly more general case where both p and q are split polynomials with simple roots. Botha [4] extended the classification of sums of two square-zero matrices to an arbitrary field (see also the appendix of [7] for an alternative proof). The case where both polynomials p and q are split was finally completed in [10], where Wang's result on the sum of an idempotent matrix and a square-zero one was extended to all fields.

Yet, to this day nothing was known on the case where one of the polynomials p and q is irreducible over $\mathbb{F}$. It is our ambition here to complete the study by giving a thorough treatment of the remaining cases: in the present article we will explain how this can be split into two subproblems, the regular and the exceptional cases, and we will completely solve the regular case but we will nevertheless state the results for the exceptional case (the proofs do not rely on quaternion algebras: they involve more traditional linear algebra along with basic Galois theory, and will be carried out in a subsequent article in a journal specialized in linear algebra).

1.4. The (p, q)-Products (or Quotients) Decomposition Problem

Let p and q be monic polynomials of degree 2 over $\mathbb{F}$. An element x of an $\mathbb{F}$-algebra $\mathcal{A}$ is called a (p, q)-**product** whenever it splits as $x = ab$ where a, b are elements of $\mathcal{A}$ that satisfy $p(a) = 0$ and $q(b) = 0$. In particular, by taking $\mathcal{A} = \mathrm{M}_n(\mathbb{F})$ or $\mathcal{A} = \mathrm{End}(V)$ for some vector space V over $\mathbb{F}$, we have the notion of a (p, q)-product for square matrices with entries in $\mathbb{F}$ and for endomorphisms of a vector space over $\mathbb{F}$.

Here is the second problem we will tackle:

When is a square matrix a (p, q)-product?

Since the set of all matrices $A \in \mathrm{M}_n(\mathbb{F})$ such that $p(A) = 0$ is a union of similarity classes, and ditto for q instead of p, the set of all matrices in $\mathrm{M}_n(\mathbb{F})$ that are (p, q)-products is a union of similarity classes. Hence, in theory it should be possible to find necessary and sufficient conditions for a matrix to be a (p, q)-product in terms of either its Jordan normal form or its rational canonical form.

Note that, in $\mathrm{M}_n(\mathbb{F})$, the (p, q)-products are the (q, p)-products, since it is known that every square matrix over a field is similar to its transpose.

Before we go on, we also need to note that the problem remains essentially unchanged should p or q be replaced with one of its *homothetic* polynomials:

Notation 1. Given $d \in \mathbb{F} \setminus \{0\}$, we set

$$H_d(p) := d^{-2} p(dt),$$

which is a monic polynomial of $\mathbb{F}[t]$ with degree 2.

Note also that if $p(0)q(0) \neq 0$, then a (p, q)-product must be invertible.

The topic of (p, q)-products has a long history that started in the nineteen sixties:

- The first result was due to Wonenburger [19] who, over a field with characteristic not 2, classified the $(t^2 - 1, t^2 - 1)$-products in $\mathrm{M}_n(\mathbb{F})$, i.e. the products of two involutions. Her result was shortly generalized to all fields by Djoković [6], and rediscovered independently by Hoffman and Paige [12]. Famously, the solutions are the invertible matrices that are similar to their inverse.
- Almost simultaneously, Ballantine [1] characterized the $(t^2 - t, t^2 - t)$-products in $\mathrm{M}_n(\mathbb{F})$ (where $\mathbb{F}$ is an arbitrary field). In other words, he classified the matrices that split into the product of two idempotents (he even classified the ones that split into the product of k idempotents for a given positive integer k).
- In a series of articles, Wang obtained an almost complete classification of the remaining cases when the field is the one of complex numbers (his proofs generalize effortlessly to any algebraically closed field). Wang and Wu [17] and him solved the case where both p and q have a nonzero double root (which reduces to the situation where $p = q = (t-1)^2$). Wang [14,16] considered the more general situation where $p(0)q(0) \neq 0$, with some stringent restrictions in the case where p or q has a double root (essentially, in that situation he only tackled the case where p has a double root and q has opposite distinct roots, and over an algebraically closed field with characteristic not 2). In [15], he tackled the case where $p(t) = t^2 - t$ and $q(0) \neq 0$.

- Novak [13] solved the case where $p(t) = q(t) = t^2$, over an arbitrary field.
- Botha [3] solved the case where $p(t) = t^2 - t$ and $q(t) = t^2$, over an arbitrary field.

Thus, even over an algebraically closed field, the general problem of classifying (p, q)-products is still partly open. Subsequent efforts were made to extend some of the above results to arbitrary fields:

- Bünger et al. [5] characterized the (p, p)-products when p splits over $\mathbb{F}$, $p(0) = 1$ and no fourth root of the unity is a root of p.
- Botha [2] generalized Wang's characterization of the $((t-1)^2, (t-1)^2)$-products to an arbitrary field.

Hence, before the present article no general solution to our problem was known. Even a full solution to the case where both polynomials p and q are split is missing from the literature. It is our ambition here to contribute to the problem by giving a treatment of the case where $p(0)q(0) \neq 0$, which essentially amounts to determining the *invertible* (p, q)-products.

Assume now that $p(0)q(0) \neq 0$. An element x of an $\mathbb{F}$-algebra $\mathcal{A}$ is called a (p, q)-**quotient** (in $\mathcal{A}$) whenever there exist elements a and b of $\mathcal{A}$ such that $x = ab^{-1}$ and $p(a) = q(b) = 0$ (this is equivalent to x being a $(p, q^\sharp)$-product where $q^\sharp := q(0)^{-1}t^2 q(t^{-1})$ is the reciprocal polynomial of q). It turns out that the characterization of quotients is more easily expressed than the one of products, in particular in the case where p and q are irreducible. Therefore, in the remainder of the article we will only consider the problem of classifying the (p, q)-quotients among the automorphisms of a finite-dimensional vector space. From our results on quotients, giving the corresponding results on products is an elementary task that requires no further explanation.

1.5. Main Structure of the Article

The rest of the article is split into three parts. Section 2 is devoted to the study of the $\mathcal{W}(p, q, x)_R$ algebras and their connection to quaternion algebras.

The structural results for this algebra will then help us obtain the classification of so-called *d-regular* (p, q)-differences (Sect. 3) and of *q-regular* (p, q)-quotients (Sect. 4) (in short, a (p, q)-difference is d-regular (the letter d standing for "difference") when it has no eigenvalue in $\mathrm{Root}(p) - \mathrm{Root}(q)$, and, when $p(0)q(0) \neq 0$, a (p, q)-quotient is q-regular (the letter q standing for "quotient") when it has no eigenvalue in $\mathrm{Root}(p)\,\mathrm{Root}(q)^{-1}$).

1.6. A Reminder on the Rational Canonical form of a Square Matrix Over a Field

Throughout the article, we need some notation and standard results from the representation theory for one endomorphism.

Let u be an endomorphism of a finite-dimensional vector space V (over the field $\mathbb{F}$). Then we can endow V with a structure of $\mathbb{F}[t]$-module by putting $r\,x := r(u)[x]$ for all $r \in \mathbb{F}[t]$ and all $x \in V$. This is a torsion module of finite type. By the classification of modules of finite type over a principal ideal domain, this yields a unique list $(r_1,\dots,r_k)$ of monic polynomials in non-increasing order for divisibility, such that V is isomorphic to the $\mathbb{F}[t]$-module $\mathbb{F}[t]/(r_1)\oplus\cdots\oplus\mathbb{F}[t]/(r_k)$, and the elements $r_1,\dots,r_k$ are called the **invariant factors** of u.

Another way to see this is through the Frobenius canonical form, which involves companion matrices: the **companion matrix** of a monic polynomial $r(t)=t^n-\sum_{k=0}^{n-1}a_k t^k$ of $\mathbb{F}[t]$ is defined as

$$C(r):=\begin{bmatrix} 0 & & & (0) & a_0 \\ 1 & 0 & & & a_1 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & & 0 & a_{n-2} \\ (0) & \cdots & 0 & 1 & a_{n-1} \end{bmatrix}\in \mathrm{M}_n(\mathbb{F}).$$

Classically, its minimal polynomial and characteristic polynomial equal r. Conversely, every n-by-n matrix whose minimal polynomial equals r is similar to $C(r)$. Moreover, when $r_1,\dots,r_p$ are pairwise coprime monic polynomials, this observation leads one to see that

$$C(r_1\cdots r_p)\simeq C(r_1)\oplus\cdots\oplus C(r_p),$$

where $\oplus$ stands for the direct sum of two matrices, i.e. $A\oplus B=\begin{bmatrix} A & 0 \\ 0 & B\end{bmatrix}$. Then, the invariants factors $r_1,\dots,r_k$ of u are characterized by the combination of the following three properties:

(i) They are non-constant monic polynomials.
(ii) The polynomial r_{i+1} divides r_i for all $i\in[\![1,k-1]\!]$.
(iii) The endomorphism u is represented in some basis by $C(r_1)\oplus\cdots\oplus C(r_k)$.

We extend this finite sequence into an infinite one $(r_i)_{i\geq 1}$ by setting $r_i:=1$ whenever $i>k$, and convene that $C(1)$ denotes the 0-by-0 matrix.

Another useful viewpoint is the *primary decomposition*: given a monic polynomial $r\in\mathbb{F}[t]$, we can split $r=t_1^{n_1}\cdots t_p^{n_p}$ into irreducible monic factors (with $t_1,\dots,t_p$ monic, irreducible, and pairwise distinct), to the effect that

$$C(r)\simeq C(t_1^{n_1})\oplus\cdots\oplus C(t_p^{n_p}).$$

Using this, one can prove that there exists a sequence $(s_1,\dots,s_\ell)$ of non-constant polynomials over $\mathbb{F}$, each of which is a power of some monic irreducible polynomial of $\mathbb{F}[t]$, such that u is represented in some basis by $C(s_1)\oplus\cdots\oplus C(s_\ell)$. This sequence is uniquely determined by u up to a permutation of its terms. The polynomials $s_1,\dots,s_\ell$ are called the **elementary invariants** of u. Once again, this is a special case of the primary decomposition of a torsion module over a principal ideal domain.

2. The Key 4-Dimensional Algebra

Throughout this section, we let R be a commutative unital $\mathbb{F}$-algebra, and we let $p(t)=t^2-\lambda t+\alpha$, $q(t)=t^2-\mu t+\beta$ be monic polynomials with degree 2 over $\mathbb{F}$, and x be an element of R.

2.1. Heuristics

Let us start from the associative unital R-algebra $R\{y,z\}$ of polynomials in two *non-commuting* indeterminates y and z, and let us consider the quotient R-algebra $\mathcal{A}$ of $R\{y,z\}$ by the two-sided ideal generated by the elements $p(y)$, $q(z)$ and $\mu\, y + \lambda\, z - zy - yz - x\, 1_{R\{y,z\}}$. Denoting by a and b the respective classes of y and z in $\mathcal{A}$, we have the relations $p(a) = 0$, $q(b) = 0$ and $ab + ba = \mu\, a + \lambda\, b - x\, 1_{\mathcal{A}}$. Setting $a^\star := \lambda 1_{\mathcal{A}} - a$ and $b^\star := \mu 1_{\mathcal{A}} - b$, the third identity then reads $ab^\star + ba^\star = x\, 1_{\mathcal{A}}$, whereas the first and second one read $aa^\star = a^\star a = \alpha\, 1_{\mathcal{A}}$ and $bb^\star = b^\star b = \beta\, 1_{\mathcal{A}}$.

Now, taking a small leap of faith and assuming that $\mathcal{A}$ is a free R-module with basis $\mathcal{B} = (1_{\mathcal{A}}, a, b, ab)$, one finds from the relations $aa = \lambda a - \alpha 1_{\mathcal{A}}$ and $a(ab) = a^2 b = (\lambda a - \alpha 1_{\mathcal{A}})b = \lambda ab - \alpha b$ that the matrix of the R-module endomorphism $u \in \mathcal{A} \mapsto au \in \mathcal{A}$ in the basis $\mathcal{B}$ equals

$$A := \begin{bmatrix} 0 & -\alpha & 0 & 0 \\ 1 & \lambda & 0 & 0 \\ 0 & 0 & 0 & -\alpha \\ 0 & 0 & 1 & \lambda \end{bmatrix} \in \mathrm{M}_4(R).$$

Likewise, we have $b^2 = \mu b - \beta 1_{\mathcal{A}}$, $ba = \mu\, a + \lambda\, b - x\, 1_{\mathcal{A}} - ab$ and

$$\begin{aligned} b(ab) &= (ba)b = (\lambda b - ba^\star)\, b = (\lambda b + ab^\star - x\, 1_{\mathcal{A}})\, b \\ &= \lambda b^2 + \beta a - x\, b = \lambda(\mu b - \beta 1_{\mathcal{A}}) + \beta\, a - x\, b. \end{aligned}$$

Hence, the matrix of $u \in \mathcal{A} \mapsto bu \in \mathcal{A}$ in the basis $\mathcal{B}$ equals

$$B := \begin{bmatrix} 0 & -x & -\beta & -\lambda\beta \\ 0 & \mu & 0 & \beta \\ 1 & \lambda & \mu & \lambda\mu - x \\ 0 & -1 & 0 & 0 \end{bmatrix}.$$

We conclude that the matrix of $u \in \mathcal{A} \mapsto abu \in \mathcal{A}$ in the basis $\mathcal{B}$ equals

$$C := AB = \begin{bmatrix} 0 & -\alpha\mu & 0 & -\alpha\beta \\ 0 & \lambda\mu - x & -\beta & 0 \\ 0 & \alpha & 0 & 0 \\ 1 & 0 & \mu & \lambda\mu - x \end{bmatrix}.$$

Still taking the above leap of faith, we would deduce the relations $p(A) = 0$, $q(B) = 0$ and $A(\mu I_4 - B) + B(\lambda I_4 - A) = x\, I_4$ in the R-algebra $\mathrm{M}_4(R)$.

2.2. Actual Definition of $\mathcal{W}(p,q,x)_R$

Here, we will put things differently and simply start from the above three matrices of $\mathrm{M}_4(R)$, that is

$$A := \begin{bmatrix} 0 & -\alpha & 0 & 0 \\ 1 & \lambda & 0 & 0 \\ 0 & 0 & 0 & -\alpha \\ 0 & 0 & 1 & \lambda \end{bmatrix}, \quad B := \begin{bmatrix} 0 & -x & -\beta & -\lambda\beta \\ 0 & \mu & 0 & \beta \\ 1 & \lambda & \mu & \lambda\mu - x \\ 0 & -1 & 0 & 0 \end{bmatrix}$$

and

$$C := AB = \begin{bmatrix} 0 & -\alpha\mu & 0 & -\alpha\beta \\ 0 & \lambda\mu - x & -\beta & 0 \\ 0 & \alpha & 0 & 0 \\ 1 & 0 & \mu & \lambda\mu - x \end{bmatrix}.$$

From the previous heuristics, the reader will now be entirely confident in believing that a routine check yields, with $A^\star := \lambda I_4 - A$ and $B^\star := \mu I_4 - B$, the relations

$$AB^\star + BA^\star = xI_4, \quad p(A) = 0 \quad \text{and} \quad q(B) = 0. \tag{1}$$

From these identities, the first of which can be read $BA = -AB + \mu A + \lambda B - xI_4$, one derives that $\operatorname{span}_R(I_4, A, B, C)$ is stable under multiplication. Moreover, for all $(u, v, w, t) \in R^4$, the first column of $u\,I_4 + v\,A + w\,B + t\,C$ is the transpose of $\begin{bmatrix} u & v & w & t \end{bmatrix}$, which yields that $\operatorname{span}_R(I_4, A, B, C)$ is a free R-module with basis (I_4, A, B, C).

Definition 2. We define $\mathcal{W}(p, q, x)_R$ as the set $\operatorname{span}_R(I_4, A, B, C)$ equipped with its structure of R-algebra inherited from that of $\mathrm{M}_4(R)$, and we will simply write $\mathcal{W}(p, q, x)$ instead of $\mathcal{W}(p, q, x)_R$ when the ring R under consideration is obvious from the context.

It is noteworthy that $\mathcal{W}(p, q, x)_R$ is precisely isomorphic to the quotient algebra $\mathcal{A}$ we started from in building our heuristics:

Proposition 2.1. *The R-algebra $\mathcal{W}(p, q, x)_R$ is isomorphic to the R-algebra $\mathcal{A}$ which is the quotient of $R\{y, z\}$ by the two-sided ideal generated by $p(y)$, $q(z)$ and $yz^\star + zy^\star - x\,1_{R\{y,z\}}$, where $y^\star := \lambda 1_{R\{y,z\}} - y$ and $z^\star := \mu 1_{R\{y,z\}} - z$.*

Proof. Since the identities $p(A) = 0$, $q(B) = 0$ and $A(\mu I_4 - B) + B(\lambda I_4 - A) = x\,I_4$ are satisfied, we obtain a homomorphism $\varphi : \mathcal{A} \to \mathcal{W}(p, q, x)$ of R-algebras that takes the class a of y to A and the class b of z to B. Since $\mathcal{W}(p, q, x)$ is a free-R-module with basis

$$(I_4, A, B, AB) = (\varphi(1_{\mathcal{A}}), \varphi(a), \varphi(b), \varphi(ab)),$$

the bijectivity of φ will be obtained as soon as we know that $(1_{\mathcal{A}}, a, b, ab)$ generates the R-module $\mathcal{A}$. Yet:

- We can use the identity $ba = -ab + \mu a + \lambda b - x\,1_{\mathcal{A}}$ to obtain that every n-word in a and b is a linear combination of k-words in a and b, with $k < n$, and of words of the form $a^\ell b^{n-\ell}$ with $\ell \in [\![0, n]\!]$.
- By using one of the identities $a^2 = \lambda a - \alpha 1_{\mathcal{A}}$ and $b^2 = \mu b - \beta 1_{\mathcal{A}}$, every word of the form $a^m b^n$, with $m \geq 2$ or $n \geq 2$, can be turned into a linear combination of k-words in a and b with $k < m + n$.
- Then, by induction on n, we deduce that every n-word in a and b is a linear combination of $1_{\mathcal{A}}$, a, b and ab.

Therefore, φ is an isomorphism of R-modules, and we conclude that it is also an isomorphism of R-algebras. □

2.3. Trace, Conjugation, and Norm in $\mathcal{W}(p, q, x)$

We will now define the trace on $\mathcal{W}(p, q, x)$. An option would be to simply consider the trace of the elements of $\mathcal{W}(p, q, x)$ seen as matrices of $\mathrm{M}_4(R)$: however, with this viewpoint the traces of I_4, A, B, AB respectively equal $4.1_R, 2\lambda, 2\mu, 2(\lambda\mu - x)$, and all those traces equal zero if the characteristic of $\mathbb{F}$ (and hence of R) equals 2, rendering the trace useless in that situation.

To obtain a more interesting object, we will "halve" those traces. This is natural if we take the viewpoint of quadratic objects: indeed, if a denotes a quadratic object in an $\mathbb{F}$-algebra $\mathcal{A}$, and a is no scalar multiple of $1_{\mathcal{A}}$, we naturally want to define the trace of a, as a quadratic object, as the trace of the multiplication by a in the $\mathbb{F}$-vector space $\mathbb{F}[a]$: this trace equals the trace of the unique monic polynomial $r \in \mathbb{F}[t]$ of degree 2 such that $r(a) = 0$. Here, since $A^2 = \lambda A - \alpha I_4$ and $B^2 = \mu B - \beta I_4$, the trace of A and B should be λ and μ, respectively. Finally

$$\begin{aligned}(AB)^2 &= AB(\lambda I_4 - A^\star)B = A(\lambda B - BA^\star)B \\ &= A(\lambda B + AB^\star - xI_4)B \\ &= \lambda AB^2 + \beta A^2 - xAB \\ &= \lambda A(\mu B - \beta I_4) + \beta(\lambda A - \alpha I_4) - xAB \\ &= (\lambda\mu - x)AB - \alpha\beta I_4.\end{aligned}$$

Hence, AB has trace $\lambda\mu - x$ as a quadratic object.

From there, the following definition is entirely natural:

Definition 3. We define

$$\mathrm{Tr} : \mathcal{W}(p, q, x) \to R$$

as the unique R-linear mapping such that $\mathrm{Tr}(I_4) = 2.1_R$, $\mathrm{Tr}(A) = \lambda$, $\mathrm{Tr}(B) = \mu$ and $\mathrm{Tr}(C) = \lambda\mu - x$.

Our next step is the definition of the conjugation in $\mathcal{W}(p, q, x)$. Naturally, and again from the viewpoint of quadratic objects, we want the conjugate of A to be $\lambda I_4 - A$ and the conjugate of B to be $\mu I_4 - B$. Now, let us come back to the algebra $Z := R\{y, z\}$ of polynomials in non-commuting indeterminates y and z. On this algebra, we can define an anti-endomorphism ψ that takes y to $y^\star := \lambda 1_Z - y$ and z to $z^\star := \mu 1_Z - z$. Note that $\psi(y^\star) = y$ and $\psi(z^\star) = z$. Noting that $p(y) = -yy^\star + \alpha 1_Z = -y^\star y + \alpha 1_Z$ and $q(z) = -zz^\star + \beta 1_Z = -z^\star z + \beta 1_Z$ it is clear that $\psi(p(y)) = p(\psi(y)) = p(y)$ and $\psi(q(z)) = q(\psi(z)) = q(z)$, whereas

$$\psi(yz^\star + zy^\star - x\,1_Z) = \psi(z^\star)y^\star + \psi(y^\star)z^\star - x\,1_Z = zy^\star + yz^\star - x\,1_Z.$$

It follows that ψ stabilizes the two-sided ideal generated by $p(y)$, $q(z)$ and $yz^\star + zy^\star - x\,1_Z$. With the help of Proposition 2.1, we recover a (unique) anti-endomorphism

$$h \in \mathcal{W}(p, q, x) \mapsto h^\star \in \mathcal{W}(p, q, x)$$

of the R-algebra $\mathcal{W}(p, q, x)$ that takes A to $\lambda I_4 - A$ and B to $\mu I_4 - B$. We say that $h^\star$ is the **conjugate** of the element h of $\mathcal{W}(p, q, x)$.

Noting that $(A^\star)^\star = A$ and $(B^\star)^\star = B$ and that $M \mapsto (M^\star)^\star$ is an endomorphism of the R-algebra $\mathcal{W}(p, q, x)$ (being the product of two anti-endomorphisms), we deduce that

$$\forall h \in \mathcal{W}(p, q, x),\ (h^\star)^\star = h.$$

Next, noting that

$$\begin{aligned} AB + (AB)^\star &= AB + B^\star A^\star \\ &= A(\mu I_4 - B^\star) + (\mu I_4 - B)A^\star \\ &= \mu(A + A^\star) - (AB^\star + BA^\star) \\ &= (\lambda\mu - x)\, I_4, \end{aligned}$$

we find by linearity that

$$\forall h \in \mathcal{W}(p, q, x),\ h + h^\star = \mathrm{Tr}(h)\, I_4.$$

Applying this to $h_1 h_2^\star$ yields the identity

$$\forall (h_1, h_2) \in \mathcal{W}(p, q, x)^2,\ h_1 h_2^\star + h_2 h_1^\star = \mathrm{Tr}(h_1 h_2^\star)\, I_4. \tag{2}$$

Lemma 2.2. *The mapping*

$$h \in \mathcal{W}(p, q, x) \mapsto h h^\star$$

takes its values among the scalar multiples of I_4.

Proof. Denote by Φ the said mapping, and note that

$$\Phi(h_1 + h_2) = \Phi(h_1) + \Phi(h_2) + \mathrm{Tr}(h_1 h_2^\star)\, I_4$$

for all h_1, h_2 in $\mathcal{W}(p, q, x)$, whereas $\Phi(\lambda h) = \lambda^2 \Phi(h)$ for all $\lambda \in R$ and all $h \in \mathcal{W}(p, q, x)$. Combining this with identity (2), one sees that it suffices to prove that Φ takes every element of $\{I_4, A, B, C\}$ to a scalar multiple of I_4. However, this is already known for I_4, A and B (which are respectively mapped to I_4, αI_4 and βI_4). Finally, $CC^\star = ABB^\star A^\star = A(\beta I_4)A^\star = \alpha\beta I_4$. □

Definition 4. The norm of $\mathcal{W}(p, q, x)$ is defined as the unique mapping

$$N_{\mathcal{W}(p,q,x)} : \mathcal{W}(p, q, x) \longrightarrow R$$

such that

$$\forall h \in \mathcal{W}(p, q, x),\ N_{\mathcal{W}(p,q,x)}(h).I_4 = h h^\star = h^\star h. \tag{3}$$

The norm will simply be denoted by N when the four-tuple (p, q, x, R) is obvious from the context.

Note that the commutation of h with $h^\star$ is obvious from the formula $h^\star = \mathrm{Tr}(h)\, I_4 - h$.

We can view the norm N as a quadratic mapping with polar form

$$b_N : (h_1, h_2) \in \mathcal{W}(p, q, x)^2 \mapsto N(h_1 + h_2) - N(h_1) - N(h_2),$$

so that

$$\forall (h_1,h_2) \in \mathcal{W}(p,q,x)^2,\ \begin{cases} h_1 h_2^\star + h_2 h_1^\star = b_N(h_1,h_2)\, I_4 \\ b_N(h_1,h_2) = \operatorname{Tr}(h_1 h_2^\star). \end{cases}$$

Moreover, using the fact that $h_2 h_2^\star$ is central in $\mathcal{W}(p,q,x)$ for all $h_2 \in \mathcal{W}(p,q,x)$, we obtain that the norm is multiplicative, i.e.

$$\forall (h_1,h_2) \in \mathcal{W}(p,q,x)^2,\ N(h_1 h_2) = N(h_1) N(h_2).$$

In a certain way, every element of $\mathcal{W}(p,q,x)$ is R-quadratic: for all $h \in \mathcal{W}(p,q,x)$, we have indeed

$$h^2 = h(\operatorname{Tr}(h)\, I_4 - h^\star) = \operatorname{Tr}(h)\, h - hh^\star = \operatorname{Tr}(h)\, h - N(h)\, I_4.$$

In the prospect of studying (p,q)-differences and (p,q)-quotients, some special cases will be interesting. For $h = A - B$, we have $\operatorname{Tr}(h) = \operatorname{Tr}(A) - \operatorname{Tr}(B) = \lambda - \mu$ and $N(h) = N(A) + N(B) - b_N(A,B) = \alpha + \beta - x$, leading to

$$(A-B)^2 - (\lambda - \mu)(A-B) = (x - \alpha - \beta)\, I_4. \tag{4}$$

For $h = AB^{-1}$, we have $N(h) = N(A)N(B)^{-1} = \alpha\beta^{-1}$ and $\operatorname{Tr}(h) = \operatorname{Tr}(\beta^{-1} AB^\star) = \beta^{-1} b_N(A,B) = \beta^{-1} x$, leading to

$$(AB^{-1})^2 = -\alpha\beta^{-1} I_4 + \beta^{-1} x\, (AB^{-1}). \tag{5}$$

We finish this section by giving an explicit formula for the norm of an element of $\mathcal{W}(p,q,x)$. Let a,b,c,d in $\mathbb{F}$. We can view the norm of $M := aI_4 + bA + cB + dC$ as the entry of the matrix $MM^\star$ at the $(1,1)$-spot. Noting that the first column of $M^\star$ equals $\begin{bmatrix} a + \lambda b + \mu c + (\lambda\mu - x)d & -b & -c & -d \end{bmatrix}^T$ while the first row of M equals $\begin{bmatrix} a & -\alpha b - xc - \alpha\mu d & -\beta c & -\lambda\beta c - \alpha\beta d \end{bmatrix}$, we obtain

$$\begin{aligned} N(aI_4 + bA + cB + dC) &= a\,\big(a + \lambda b + \mu c + (\lambda\mu - x)d\big) + b\,(\alpha b + xc + \alpha\mu d) \\ &\quad + c\,\big(\beta c + \beta\lambda d\big) + \alpha\beta\, d^2. \end{aligned} \tag{6}$$

Remark 1. If one of the polynomials p and q splits over $\mathbb{F}$, then N is isotropic, i.e. it vanishes at some non-zero element of $\mathcal{W}(p,q,x)$. Indeed, if p has a root z in $\mathbb{F}$, then one checks that $N(A - zI_4) = 0$ since, denoting by z' the second root of p, we see that

$$\begin{aligned} (A - zI_4)(A - zI_4)^\star &= (A - zI_4)(A^\star - zI_4) = (A - zI_4)(z' I_4 - A) \\ &= -p(A) = 0. \end{aligned}$$

Likewise if q has a root y in $\mathbb{F}$, then $N(B - yI_4) = 0$.

2.4. A Deeper Study of the Algebra $\mathcal{W}(p,q,x)$: When R is a Field

Here, we assume that R is a field extension of $\mathbb{F}$, and we denote it by $\mathbb{L}$. The norm of $\mathcal{W}(p,q,x)_{\mathbb{L}}$ is still denoted by N: it is a quadratic form on the $\mathbb{L}$-vector space $\mathcal{W}(p,q,x)_{\mathbb{L}}$, and we will now analyze when this form is degenerate.

Proposition 2.3. *Consider an algebraic closure $\overline{\mathbb{L}}$ of $\mathbb{L}$. The quadratic form N is degenerate if and only if there exist elements x_1, x_2, y_1, y_2 of $\overline{\mathbb{L}}$ such that $p(t) = (t - x_1)(t - x_2)$, $q(t) = (t - y_1)(t - y_2)$, and $x = x_1 y_1 + x_2 y_2$.*

Proof. Note from formula (6) that the matrix of b_N in the basis (I_4, A, B, C) is unchanged when $\mathbb{L}$ is extended to $\overline{\mathbb{L}}$, and the invertibility of this matrix is the same in $\mathrm{M}_4(\mathbb{L})$ and in $\mathrm{M}_4(\overline{\mathbb{L}})$. Hence, it suffices to prove the statement when $\mathbb{L}$ is already algebraically closed: in the rest of the proof we assume that so is $\mathbb{L}$.

Let us then split $p(t) = (t - x_1)(t - x_2)$ and $q(t) = (t - y_1)(t - y_2)$ in $\mathbb{L}[t]$. Then, take $X := A - x_1 I_4$ and $Y := B - y_1 I_4$ and note that $XY = AB - x_1 B - y_1 A + x_1 y_1 I_4$. It is clear then that (I_4, X, Y, XY) is a basis of the $\mathbb{L}$-vector space $\mathcal{W}(p, q, x)$. Next, we see that $N(X) = 0$ and $N(Y) = 0$ (see Remark 1, at the end of Sect. 2.3), leading to $N(XY) = N(X)N(Y) = 0$. Note finally that

$$b_N(X, XY)\, I_4 = X(Y + Y^\star)X^\star = \mathrm{Tr}(Y)N(X)\, I_4 = 0$$

and

$$b_N(Y, XY)\, I_4 = YY^\star X^\star + XYY^\star = N(Y)\mathrm{Tr}(X)\, I_4 = 0.$$

It follows that the matrix of b_N in the basis (I_4, X, Y, XY) reads

$$\begin{bmatrix} ? & ? & ? & b_N(I_4, XY) \\ ? & ? & b_N(X, Y) & 0 \\ ? & b_N(Y, X) & 0 & 0 \\ b_N(XY, I_4) & 0 & 0 & 0 \end{bmatrix}.$$

Therefore, b_N is degenerate if and only if one of the four anti-diagonal elements vanishes, i.e. $b_N(I_4, XY) = 0$ or $b_N(X, Y) = 0$. Next, we compute

$$\begin{aligned} b_N(X, Y) &= b_N(A, B) - y_1 b_N(A, I_4) - x_1 b_N(I_4, B) + x_1 y_1 b_N(I_4, I_4) \\ &= x - y_1(x_1 + x_2) - x_1(y_1 + y_2) + 2x_1 y_1 \\ &= x - (x_2 y_1 + x_1 y_2). \end{aligned}$$

Noting that $Y^\star = \mathrm{Tr}(Y)\, I_4 - Y = -(B - y_2\, I_4)$, the same computation yields

$$b_N(I_4, XY) = b_N(Y^\star, X) = -b_N(X, B - y_2 I_4) = x_1 y_1 + x_2 y_2 - x.$$

We conclude that N is degenerate if and only if x equals $x_1 y_1 + x_2 y_2$ or $x_1 y_2 + x_2 y_1$. The claimed result follows. □

Next, in the situation where N is non-degenerate, we further analyze the structure of $\mathcal{W}(p, q, x)_{\mathbb{L}}$. This restates Theorem 1.1:

Theorem 2.4. *Assume that the quadratic form N is non-degenerate. Then, $\mathcal{W}(p, q, x)_{\mathbb{L}}$ is a quaternion algebra over $\mathbb{L}$ and its norm of quaternion algebra is N.*

Proof. First of all, we note that the linear form Tr on $\mathcal{W}(p, q, x)$ is nonzero. Indeed, if $\mathrm{Tr} = 0$, we would find that $\mathrm{char}(\mathbb{F}) = 2$ and $\lambda = \mu = x = 0$, but then $p(t) = (t - x_1)^2$ and $q(t) = (t - y_1)^2$ for some scalars x_1 and y_1 in $\overline{\mathbb{L}}$, leading to $x = 0 = x_1 y_1 + x_1 y_1$ and contradicting the non-degeneracy of N (see Proposition 2.3).

Next, we consider the linear hyperplane $H := \mathrm{Ker}\, \mathrm{Tr}$ of the $\mathbb{L}$-vector space $\mathcal{W}(p, q, x)$. The radical of the restriction of N to H has dimension at most 1, whence we can find a 2-dimensional subspace P of H on which N

is regular. It follows that $\forall h \in P,\ h^2 = -N(h)\, I_4$. Hence, the identity of P yields a morphism $\varphi : C(-N_{|P}) \to \mathcal{W}(p,q,x)$ of $\mathbb{L}$-algebras whose domain is the Clifford algebra $C(-N_{|P})$ over $\mathbb{L}$, and whose range includes P. Yet, since P has dimension 2 and $N_{|P}$ is non-degenerate, it is known (for fields with characteristic not 2, see [8] p.528 Theorem 1.1.5, otherwise see [8] p.744 Theorem 2.2.3) that the $\mathbb{L}$-algebra $C(-N_{|P})$ is simple. It follows that φ is injective, and since $\dim_{\mathbb{L}} C(-N_{|P}) = 4 = \dim_{\mathbb{L}} \mathcal{W}(p,q,x)$, we deduce that φ is an isomorphism. Hence, $\mathcal{W}(p,q,x)$ is a quaternion algebra.

Yet, in a quaternion algebra C over $\mathbb{L}$, the set of all $z \in C$ such that $z^2 \in \mathbb{L}1_C$ splits uniquely as the union $(\mathbb{L}1_C) \cup H'$ for some linear hyperplane H' of C whose elements are called the pure quaternions, and there is a unique antiautomorphism $h \mapsto \overline{h}$ of the $\mathbb{L}$-algebra C, called the conjugation, whose restriction to H' is $h \mapsto -h$. Yet, in $\mathcal{W}(p,q,x)$, for every element h, we have both $hh^\star = \mathrm{Tr}(h)h - h^2$ and $hh^\star \in \mathbb{L}1_{\mathcal{W}(p,q,x)}$, whence $h^2 \in \mathbb{L}1_{\mathcal{W}(p,q,x)}$ if and only if $h \in \mathbb{L}1_{\mathcal{W}(p,q,x)}$ or $\mathrm{Tr}(h) = 0$. Hence, in the quaternion algebra $\mathcal{W}(p,q,x)$, the pure quaternions are the elements of H. Since $h^\star = -h$ for all such quaternions, and $h \mapsto h^\star$ is an antiautomorphism of $\mathcal{W}(p,q,x)$, we conclude that $h \mapsto h^\star$ is the conjugation of the quaternion algebra $\mathcal{W}(p,q,x)$. Hence, Formula (3) entails that the norm of the quaternion algebra $\mathcal{W}(p,q,x)$ is N. □

From the classification of quaternion algebras (for fields with characteristic not 2, see [8] p.528 Theorem 1.1.5, otherwise see [8] p.744 Theorem 2.2.3), we can conclude on the structure of $\mathcal{W}(p,q,x)$ when N is non-degenerate.

Corollary 2.5. *Assume that the quadratic form $N_{\mathcal{W}(p,q,x)}$ is non-degenerate. If it is non-isotropic, then $\mathcal{W}(p,q,x)_{\mathbb{L}}$ is a skew field.*
Otherwise, the $\mathbb{L}$-algebra $\mathcal{W}(p,q,x)_{\mathbb{L}}$ is isomorphic to $\mathrm{M}_2(\mathbb{L})$.

2.5. A Deeper Study of the Algebra $\mathcal{W}(p,q,x)$: When R is a Local Quotient of $\mathbb{F}[t]$

The following result generalizes the last statement of Corollary 2.5. This restates Theorem 1.2:

Proposition 2.6. *Let r be an irreducible polynomial of $\mathbb{F}[t]$, and $n \in \mathbb{N}^*$ be a non-zero integer. Set $R := \mathbb{F}[t]/(r^n)$ and let x be the class of some polynomial of $\mathbb{F}[t]$ in R, and $\overline{x}$ be the class of the same polynomial in the residue field $\mathbb{L} := \mathbb{F}[t]/(r)$. Assume finally that the norm of $\mathcal{W}(p,q,\overline{x})_{\mathbb{L}}$ is non-degenerate and isotropic. Then, the R-algebra $\mathcal{W}(p,q,x)_R$ is isomorphic to $\mathrm{M}_2(R)$.*

Proof. Denote by ϵ the class of r in $\mathbb{F}[t]/(r^n)$. With the construction from Sect. 2.2, it is obvious that $\mathcal{W}(p,q,\overline{x})_{\mathbb{L}}$ is naturally isomorphic to the quotient of $\mathcal{W}(p,q,x)_R$ by the two-sided ideal $\epsilon\mathcal{W}(p,q,x)_R$, and we shall make this identification throughout the proof. We will denote by $\overline{N}$ the norm of $\mathcal{W}(p,q,\overline{x})_{\mathbb{L}}$, while N still denotes the one of $\mathcal{W}(p,q,x)_R$.

By Corollary 2.5, we know that there exists an isomorphism

$$\varphi : \mathcal{W}(p,q,\overline{x})_{\mathbb{L}} \xrightarrow{\simeq} \mathrm{M}_2(\mathbb{L})$$

of $\mathbb{L}$-algebras. Moreover, such an isomorphism must be compatible with the enriched structure of quaternion algebra (with its conjugation and norm).

Yet, in $\mathrm{M}_2(\mathbb{L})$ the conjugation is the classical adjunction $M \mapsto M^{\mathrm{ad}}$ (where M^{ad} is the transpose of the comatrix of M), and the norm is the determinant.

Given an arbitrary commutative $\mathbb{F}$-algebra $\mathcal{M}$ and an element u of it, we say that a pair (X, Y) of elements of $\mathcal{W}(p,q,u)_{\mathcal{M}}$ is **adapted** whenever it satisfies the following two conditions:

(i) $b_N(I_4, X) = b_N(I_4, Y) = 0$, $N(X) = N(Y) = 0$ and $b_N(X, Y) = -1$.
(ii) (I_4, X, Y, XY) is a basis of the $\mathcal{M}$-module $\mathcal{W}(p,q,u)_{\mathcal{M}}$.

Denote by $E_{i,j}$ the elementary matrix of $\mathrm{M}_2(\mathbb{L})$ with zero entries everywhere except the entry at the (i,j)-spot, which equals 1. In the quaternion algebra $\mathrm{M}_2(\mathbb{L})$, we see that $I_2 E_{1,2}^{\mathrm{ad}} + E_{1,2} I_2^{\mathrm{ad}} = -E_{1,2} + E_{1,2} = 0$ and likewise with $E_{2,1}$ instead of $E_{1,2}$. Moreover $\det(E_{1,2}) = 0 = \det(E_{2,1})$, and finally $E_{1,2}E_{2,1}^{\mathrm{ad}} + E_{2,1}E_{1,2}^{\mathrm{ad}} = -E_{1,2}E_{2,1} - E_{2,1}E_{1,2} = -I_2$. Finally, $(I_2, E_{1,2}, E_{2,1}, E_{1,2}E_{2,1})$ is a basis of the $\mathbb{L}$-vector space $\mathrm{M}_2(\mathbb{L})$. Hence, the pair $\big(\varphi^{-1}(E_{1,2}), \varphi^{-1}(E_{2,1})\big)$ is adapted in $\mathcal{W}(p,q,\overline{x})_{\mathbb{L}}$.

Assuming for a moment that we have an adapted pair (X,Y) in the algebra $\mathcal{W}(p,q,x)_R$, we claim that $\mathcal{W}(p,q,x)_R$ is isomorphic to $\mathrm{M}_2(R)$. Indeed, first of all we note that $b_N(I_4, X) = b_N(I_4, Y) = 0$ means that $X^\star = -X$ and $Y^\star = -Y$. Then, it follows from $N(X) = N(Y) = 0$ that $X^2 = Y^2 = 0$. Finally, $b_N(X,Y) = -1$ reads $XY^\star + YX^\star = -I_4$, that is $XY + YX = I_4$. Thus, condition (ii) yields an isomorphism $\psi : \mathcal{W}(p,q,x)_R \to \mathrm{M}_2(R)$ of R-modules that maps I_4, X, Y, XY respectively to $I_2, E_{1,2}, E_{2,1}, E_{1,1}$, and the identities $X^2 = Y^2 = 0$ and $YX = I_4 - XY$ show that ψ is actually a ring homomorphism.

It remains to prove that there exists an adapted pair in $\mathcal{W}(p,q,x)_R$. To do so, we shall use Hensel's method. Given $M \in \mathcal{W}(p,q,x)_R$, we denote by $\overline{M}$ its class modulo ϵ, and we shall see $\overline{M}$ as an element of the ring $\mathcal{W}(p,q,\overline{x})_{\mathbb{L}}$. Let $k \in [\![1, n-1]\!]$, and $(X_k, Y_k) \in \mathcal{W}(p,q,x)_R^2$ be such that:

(a) $b_N(I_4, X_k) = 0 \mod \epsilon^k$, $b_N(I_4, Y_k) = 0 \mod \epsilon^k$, $N(X_k) = 0 \mod \epsilon^k$, $N(Y_k) = 0 \mod \epsilon^k$ and $b_N(X_k, Y_k) = -1 \mod \epsilon^k$.
(b) The family $(I_4, \overline{X_k}, \overline{Y_k}, \overline{X_k Y_k})$ is a basis of the $\mathbb{L}$-vector space $\mathcal{W}(p,q,\overline{x})_{\mathbb{L}}$.

Then, we construct a pair $(X_{k+1}, Y_{k+1}) \in \mathcal{W}(p,q,x)_R$ such that $X_{k+1} = X_k \mod \epsilon^k$, $Y_{k+1} = Y_k \mod \epsilon^k$, and the pair $(X_{k+1}, Y_{k+1}) \in \mathcal{W}(p,q,x)_R$ satisfies the above conditions at the step $k+1$. To do so, let $Z \in \mathcal{W}(p,q,x)_R$ be arbitrary, and set $X_{k+1} := X_k + \epsilon^k Z$. We write $b_N(I_4, X_k) = \epsilon^k h_1$ and $N(X_k) = \epsilon^k h_2$ for some h_1, h_2 in $\mathcal{W}(p,q,x)_R$. Then, $b_N(I_4, X_{k+1}) = \epsilon^k(h_1 + b_N(I_4, Z))$ and $N(X_{k+1}) = \epsilon^k(h_2 + b_N(X_k, Z)) \mod \epsilon^{k+1}$. Since $b_{\overline{N}}$ is non-degenerate and $\overline{I_4}, \overline{X_k}$ are linearly independent over $\mathbb{L}$, the linear forms $b_{\overline{N}}(\overline{I_4}, -)$ and $b_{\overline{N}}(\overline{X_k}, -)$ are independent, which shows that the linear system of equations

$$\begin{cases} b_{\overline{N}}(\overline{I_4}, U) = -\overline{h_1} \\ b_{\overline{N}}(\overline{X_k}, U) = -\overline{h_2} \end{cases}$$

has a solution U in $\mathcal{W}(p,q,\overline{x})_{\mathbb{L}}$. Lifting U, we recover that $Z \in \mathcal{W}(p,q,x)_R$ can be chosen so as to have $b_N(I_4, Z) = -h_1 \mod \epsilon$ and $b_N(X_k, Z) = -h_2 \mod \epsilon$. We choose such a Z from now on, and hence we have $b_N(I_4, X_{k+1}) = 0$

mod ϵ^{k+1} and $N(X_{k+1}) = 0 \bmod \epsilon^{k+1}$. Note that $b_N(X_{k+1}, Y_k) = b_N(X_k, Y_k) \bmod \epsilon^k$ whence $b_N(X_{k+1}, Y_k) = -1 \bmod \epsilon^k$.

Next, let $T \in \mathcal{W}(p, q, x)_R$ and set $Y_{k+1} := Y_k + \epsilon^k T$. We find three elements h_3, h_4 and h_5 of $\mathcal{W}(p, q, x)_R$ such that $b_N(I_4, Y_k) = \epsilon^k h_3$, $N(Y_k) = \epsilon^k h_4$ and $b_N(X_{k+1}, Y_k) = -1+\epsilon^k h_5$. As before, the linear system of equations

$$\begin{cases} b_{\overline{N}}(\overline{I_4}, V) = -\overline{h_3} \\ b_{\overline{N}}(\overline{Y_k}, V) = -\overline{h_4} \\ b_{\overline{N}}(\overline{X_{k+1}}, V) = -\overline{h_5} \end{cases}$$

has a solution V in $\mathcal{W}(p, q, \overline{x})_{\mathbb{L}}$, and hence T can be chosen as a representative of it, in which case we find $b_N(I_4, Y_{k+1}) = 0 \bmod \epsilon^{k+1}$, $N(Y_{k+1}) = 0 \bmod \epsilon^{k+1}$ and $b_N(X_{k+1}, Y_{k+1}) = -1 \bmod \epsilon^{k+1}$. Hence, condition (a) is satisfied at the rank $k+1$ by (X_{k+1}, Y_{k+1}). On the other hand, since condition (b) is satisfied at the rank k by (X_k, Y_k), while X_k and X_{k+1} have the same reduction modulo ϵ, and Y_k and Y_{k+1} have the same reduction modulo ϵ, we obtain that condition (b) is also satisfied by (X_{k+1}, Y_{k+1}).

As we have shown that there exists an adapted pair in $\mathcal{W}(p, q, \overline{x})_{\mathbb{L}}$, this construction yields, by induction, a pair $(X, Y) \in \mathcal{W}(p, q, x)_R^2$ that satisfies condition (i) and for which $(I_4, \overline{X}, \overline{Y}, \overline{XY})$ is a basis of the $\mathbb{L}$-vector space $\mathcal{W}(p, q, \overline{x})_{\mathbb{L}}$. Since R is a local ring with residue class field $\mathbb{L}$ and $\mathcal{W}(p, q, x)_R$ is a free R-module with dimension 4, this shows that (I_4, X, Y, XY) is a basis of the R-module $\mathcal{W}(p, q, x)_R$. Therefore, (X, Y) is an adapted pair in $\mathcal{W}(p, q, x)_R$, and a previous remark helps us conclude that the R-algebra $\mathcal{W}(p, q, x)_R$ is isomorphic to $\mathrm{M}_2(R)$. □

Having the above results, we are now ready to tackle the two decomposition issues that were raised in Sects. 1.3 and 1.4 .

3. The Difference of Two Quadratic Matrices

3.1. The Basic Splitting

Let u be an endomorphism of a finite-dimensional vector space V over $\mathbb{F}$. Let p and q be monic polynomials with degree 2 over $\mathbb{F}$, which we write

$$p(t) = t^2 - \lambda t + \alpha \quad \text{and} \quad q(t) = t^2 - \mu t + \beta.$$

Let us set

$$\delta := \lambda - \mu = \mathrm{tr}(p) - \mathrm{tr}(q).$$

Let us fix an indeterminate t, and consider the polynomials $p(x)$ and $q(x-t)$, seen as monic polynomials with coefficients in the ring $\mathbb{F}[t]$ with respect to the indeterminate x. Hence, we can consider their resultant $\mathrm{res}_{\mathbb{F}[t]}\big(p(x), q(x-t)\big)$, which is an element of the ring $\mathbb{F}[t]$. The **d-fundamental polynomial** of the pair (p, q) is defined as this resultant

$$F_{p,q}(t) := \mathrm{res}_{\mathbb{F}[t]}\big(p(x), q(x-t)\big) \in \mathbb{F}[t],$$

which is a polynomial of degree 4. More explicitly, if we split $p(z) = (z - x_1)(z - x_2)$ and $q(z) = (z - y_1)(z - y_2)$ in $\overline{\mathbb{F}}[z]$, then

$$F_{p,q}(t) = \prod_{1 \leq i,j \leq 2} \big(t - (x_i - y_j)\big) = p(t + y_1)\, p(t + y_2) = q(x_1 - t)\, q(x_2 - t).$$

We set

$$E_{p,q}(u) := \bigcup_{n \in \mathbb{N}} \operatorname{Ker} F_{p,q}(u)^n \quad \text{and} \quad R_{p,q}(u) := \bigcap_{n \in \mathbb{N}} \operatorname{Im} F_{p,q}(u)^n.$$

Hence, $V = E_{p,q}(u) \oplus R_{p,q}(u)$, and the endomorphism u stabilizes both linear subspaces $E_{p,q}(u)$ and $R_{p,q}(u)$. The endomorphism u is called **d-exceptional** with respect to (p, q) (respectively, **d-regular** with respect to (p, q)) whenever $E_{p,q}(u) = V$ (respectively, $R_{p,q}(u) = V$). In other words, u is d-exceptional (respectively, d-regular) with respect to (p, q) if and only all the eigenvalues of u in $\overline{\mathbb{F}}$ belong to $\operatorname{Root}(p) - \operatorname{Root}(q)$ (respectively, no eigenvalue of u in $\overline{\mathbb{F}}$ belongs to $\operatorname{Root}(p) - \operatorname{Root}(q)$).

The endomorphism of $E_{p,q}(u)$ (respectively, of $R_{p,q}(u)$) induced by u is always d-exceptional (respectively, always d-regular) with respect to (p, q) and we call it the **d-exceptional part** (respectively, the **d-regular part**) of u with respect to (p, q).

Next, we expand

$$F_{p,q}(t) = \big(t - (x_1 - y_1)\big)\big(t - (x_2 - y_2)\big)\big(t - (x_1 - y_2)\big)\big(t - (x_2 - y_1)\big).$$

Noting that

$$\big(t - (x_1 - y_1)\big)\big(t - (x_2 - y_2)\big) = t^2 - \delta t + (x_1 - y_1)(x_2 - y_2)$$

and

$$\big(t - (x_1 - y_2)\big)\big(t - (x_2 - y_1)\big) = t^2 - \delta t + (x_1 - y_2)(x_2 - y_1),$$

we find that

$$F_{p,q}(t) = \Lambda_{p,q}(t^2 - \delta t), \tag{7}$$

where

$$\begin{aligned} \Lambda_{p,q}(t) &:= \big(t + (x_1 - y_1)(x_2 - y_2)\big)\big(t + (x_2 - y_1)(x_1 - y_2)\big) & (8)\\ &= t^2 + \big((x_1 - y_1)(x_2 - y_2) + (x_2 - y_1)(x_1 - y_2)\big)\, t + F_{p,q}(0). & (9) \end{aligned}$$

Finally,

$$(x_1 - y_1)(x_2 - y_2) + (x_2 - y_1)(x_1 - y_2) = 2\,(x_1 x_2 + y_1 y_2) - (x_1 + x_2)(y_1 + y_2),$$

whence

$$\Lambda_{p,q}(t) = t^2 + \big(2(\alpha + \beta) - \lambda\mu\big)\, t + F_{p,q}(0) \in \mathbb{F}[t],$$

and

$$F_{p,q}(u) = \Lambda_{p,q}(u^2 - \delta u).$$

Remark 2. Let $\mathcal{A}$ be an $\mathbb{F}$-algebra, and let a, b be elements of $\mathcal{A}$ such that $p(a) = q(b) = 0$. Denote by $a^\star$ the p-conjugate of a and by $b^\star$ the q-conjugate of b. Then,

$$(a-b)^2 = (a-b)(\delta 1_{\mathcal{A}} - a^\star + b^\star) = \delta\,(a-b) + (ab^\star + ba^\star) - aa^\star - bb^\star,$$

and hence

$$(a-b)^2 - \delta(a-b) = ab^\star + ba^\star - (\alpha+\beta)\,1_{\mathcal{A}}. \tag{10}$$

Our first basic result follows:

Proposition 3.1. *The endomorphism u is a (p,q)-difference if and only if both its d-exceptional part and its d-regular part are (p,q)-differences.*

The proof of this result will use the following corollary of the Basic Commutation Lemma (Lemma 1.3):

Lemma 3.2. (Commutation Lemma). *Let p and q be monic polynomials of $\mathbb{F}[t]$ with degree 2, and let a and b be endomorphisms of a vector space V such that $p(a) = q(b) = 0$. Then, both a and b commute with $(a-b)^2 - (\operatorname{tr}(p) - \operatorname{tr}(q))(a-b)$.*

Proof. This follows from the Basic Commutation Lemma and from identity (10). ☐

Proof of Proposition 3.1. The "if" part is obvious. Conversely, assume that u is a (p,q)-difference, and split $u = a - b$ where a and b are endomorphisms of V such that $p(a) = 0$ and $q(b) = 0$. By the Commutation Lemma, both a and b commute with $v := u^2 - \delta u$. Hence, a and b commute with $\Lambda_{p,q}(v) = F_{p,q}(u)$, and it follows that both stabilize $E_{p,q}(u)$ and $R_{p,q}(u)$. Denote by a' and b' (respectively, by a'' and b'') the endomorphisms of $E_{p,q}(u)$ (respectively, of $R_{p,q}(u)$) induced by a and b. Then, the d-exceptional part of u is $a' - b'$, and the d-regular part of u is $a'' - b''$. Obviously, p annihilates a' and a'', and q annihilates b' and b'', which yields that both the d-exceptional and the d-regular part of u are (p,q)-differences. ☐

From there, it is clear that classifying (p,q)-differences amounts to classifying the d-exceptional ones and the d-regular ones. The easier classification is the latter: as we shall see, it involves little discussion on the specific polynomials p and q under consideration (whether they are split or not over $\mathbb{F}$, separable or not over $\mathbb{F}$, etc). In contrast, the classification of d-exceptional (p,q)-differences involves a tedious case-by-case study which will not be carried out in the present article: we will state the results for reference purpose, but we will not prove them.

The following result will be useful for the study of the regular case:

Proposition 3.3. *Let $r \in \mathbb{F}[t]$ be irreducible. The following conditions are equivalent:*

(i) *No root of $r(t^2 - \delta t)$ belongs to* $\operatorname{Root}(p) - \operatorname{Root}(q)$.
(ii) *For $\mathbb{L} := \mathbb{F}[t]/(r)$ and y the class of t in $\mathbb{L}$, the norm of $\mathcal{W}(p, q, y+\alpha+\beta)_{\mathbb{L}}$ is nondegenerate.*

Proof. Note first by (8) that the roots of $\Lambda_{p,q}$ in $\overline{\mathbb{F}}$ are $-\alpha-\beta+x_1y_1+x_2y_2$ and $-\alpha-\beta+x_1y_2+x_2y_1$.

Assume that some root of $r(t^2-\delta t)$ belongs to $\mathrm{Root}(p)-\mathrm{Root}(q)$, choose such a root and denote it by z. Then, $z^2-\delta z$ is a common root of r with $\Lambda_{p,q}$. Since r is irreducible, it follows that r divides $\Lambda_{p,q}$, and hence y is a root of $\Lambda_{p,q}$. Consequently, $y+\alpha+\beta$ equals $x_1y_1+x_2y_2$ or $x_1y_2+x_2y_1$. By Proposition 2.3, this yields that the norm of $\mathcal{W}(p,q,y+\alpha+\beta)_{\mathbb{L}}$ is degenerate.

Conversely, assume that the norm of $\mathcal{W}(p,q,y+\alpha+\beta)_{\mathbb{L}}$ is degenerate. Then, $y+\alpha+\beta$ equals $x_1y_1+x_2y_2$ or $x_1y_2+x_2y_1$, and hence y is one of the roots of $\Lambda_{p,q}$. We can choose $z\in\overline{\mathbb{F}}$ such that $z^2-\delta z=y$, and it follows from (7) that $F_{p,q}(z)=\Lambda_{p,q}(y)=0$, to the effect that $z\in\mathrm{Root}(p)-\mathrm{Root}(q)$. We conclude that $r(t^2-\delta t)$ has a root in $\mathrm{Root}(p)-\mathrm{Root}(q)$ (namely, z). □

3.2. Statement of the Results

We are now ready to state our results. We shall frame them in terms of direct-sum decomposability.

Let u be an endomorphism of a nonzero finite-dimensional vector space V. Assume that V splits into $V_1\oplus V_2$, and that each linear subspace V_1 and V_2 is stable under u and nonzero, and both induced endomorphisms $u_{|V_1}$ and $u_{|V_2}$ are (p,q)-differences. Then, u is obviously a (p,q)-difference. In the event when such a decomposition exists we shall say that u is a **decomposable** (p,q)-difference, otherwise and if u is a (p,q)-difference, we shall say that u is an **indecomposable** (p,q)-difference. Obviously, if V is nonzero then every (p,q)-difference in $\mathrm{End}(V)$ is the direct sum of indecomposable ones. Hence, it suffices to describe the indecomposable (p,q)-differences.

Moreover, if a (p,q)-difference is indecomposable then by Proposition 3.1 it is either d-regular or d-exceptional.

In each one of the following tables, we give a set of matrices. Each matrix represents an indecomposable (p,q)-difference, and every indecomposable (p,q)-difference in $\mathrm{End}(V)$ is represented by one of those matrices, in some basis. Throughout the classification, we set

$$\delta:=\operatorname{tr}p-\operatorname{tr}q.$$

We start with d-regular (p,q)-differences. In that situation the classification is rather simple (Table 1).

Remember, by Remark 1, that the norm of the quaternion algebra $\mathcal{W}(p,q,x)_R$ is isotropic whenever one of p and q splits in $\mathbb{F}[t]$.

Next, we tackle the indecomposable d-exceptional (p,q)-differences. We give these results only for future reference: they will not be proved here, but in a future article. We start with the known classifications, in which both p and q are split over $\mathbb{F}$. The three situations are described in the following tables (see [4] for Table 2, [9] for Table 3, and [10] for Table 4).

Now, we state new results on the d-exceptional (p,q)-differences. We start with the case where p is irreducible but q is split. There are two cases to consider, whether the two polynomials obtained by translating p along the roots of q are equal or not (Tables 5, 6).

Table 1. The classification of indecomposable d-regular (p,q)-differences

Representing matrix	Associated data
$C\big(r^n(t^2-\delta t)\big)$	$n \in \mathbb{N}^*$, $r \in \mathbb{F}[t]$ irreducible and monic, $r(t^2-\delta t)$ has no root in $\operatorname{Root}(p)-\operatorname{Root}(q)$ $N_{\mathcal{W}(p,q,y+p(0)+q(0))_{\mathbb{L}}}$ isotropic over $\mathbb{L} := \mathbb{F}[t]/(r)$ for $y := \overline{t}$ in $\mathbb{L}$
$C\big(r^n(t^2-\delta t)\big) \oplus C\big(r^n(t^2-\delta t)\big)$	$n \in \mathbb{N}^*$, $r \in \mathbb{F}[t]$ irreducible and monic, $r(t^2-\delta t)$ has no root in $\operatorname{Root}(p)-\operatorname{Root}(q)$ $N_{\mathcal{W}(p,q,y+p(0)+q(0))_{\mathbb{L}}}$ non-isotropic over $\mathbb{L} := \mathbb{F}[t]/(r)$ for $y := \overline{t}$ in $\mathbb{L}$

Table 2. The classification of indecomposable d-exceptional (p,q)-differences: When both p and q are split with a double root

Representing matrix	Associated data
$C\big((t-x)^n\big)$	$n \in \mathbb{N}^*$, $x \in \operatorname{Root}(p)-\operatorname{Root}(q)$

Table 3. The classification of indecomposable d-exceptional (p,q)-differences: When both p and q are split with simple roots

Representing matrix	Associated data
$C\big((t-x)^n\big) \oplus C\big((t-\delta+x)^n\big)$	$n \in \mathbb{N}^*$, $x \in \operatorname{Root}(p)-\operatorname{Root}(q)$ such that $x \neq \delta - x$
$C\big((t-x)^{n+1}\big) \oplus C\big((t-\delta+x)^n\big)$	$n \in \mathbb{N}$, $x \in \operatorname{Root}(p)-\operatorname{Root}(q)$ such that $x \neq \delta - x$
$C\big((t-x)^n\big)$	$n \in \mathbb{N}^*$, $x \in \operatorname{Root}(p)-\operatorname{Root}(q)$ such that $x = \delta - x$

Table 4. The classification of indecomposable d-exceptional (p,q)-differences: When one of p and q is split with a double root and the other one is split with simple roots

Representing matrix	Associated data
$C\big((t-x)^n\big) \oplus C\big((t-\delta+x)^n\big)$	$n \in \mathbb{N}^*$, $x \in \operatorname{Root}(p)-\operatorname{Root}(q)$
$C\big((t-x)^{n+1}\big) \oplus C\big((t-\delta+x)^n\big)$	$n \in \mathbb{N}$, $x \in \operatorname{Root}(p)-\operatorname{Root}(q)$
$C\big((t-x)^{n+2}\big) \oplus C\big((t-\delta+x)^n\big)$	$n \in \mathbb{N}$, $x \in \operatorname{Root}(p)-\operatorname{Root}(q)$

TABLE 5. The classification of indecomposable d-exceptional (p,q)-differences: When p is irreducible, $q=(t-y_1)(t-y_2)$ for some y_1,y_2 in $\mathbb{F}$, and $p(t+y_1)=p(t+y_2)$

Representing matrix	Associated data
$C\big(p(t+y)^n\big)$	$n\in\mathbb{N}^*$, $y\in\operatorname{Root}(q)$

TABLE 6. The classification of indecomposable d-exceptional (p,q)-differences: When p is irreducible, $q=(t-y_1)(t-y_2)$ for some y_1,y_2 in $\mathbb{F}$, and $p(t+y_1)\neq p(t+y_2)$

Representing matrix	Associated data
$C\big(p(t+y_1)^n\big)\oplus C\big(p(t+y_2)^n\big)$	$n\in\mathbb{N}^*$
$C\big(p(t+y_1)^{n+1}\big)\oplus C\big(p(t+y_2)^n\big)$	$n\in\mathbb{N}$
$C\big(p(t+y_2)^{n+1}\big)\oplus C\big(p(t+y_1)^n\big)$	$n\in\mathbb{N}$

TABLE 7. The classification of indecomposable d-exceptional (p,q)-differences: When p and q are irreducible with the same splitting field $\mathbb{L}$

Representing matrix	Associated data
$C\Big(\big(t^2-\delta t+N_{\mathbb{L}/\mathbb{F}}(x-y)\big)^n\Big)$ $\oplus$ $C\Big(\big(t^2-\delta t+N_{\mathbb{L}/\mathbb{F}}(x-y)\big)^n\Big)$	$n\in\mathbb{N}^*$, $x\in\operatorname{Root}(p)$, $y\in\operatorname{Root}(q)$ with $x-y\notin\mathbb{F}$
$C\Big(\big(t^2-\delta t+N_{\mathbb{L}/\mathbb{F}}(x-y)\big)^{n+1}\Big)$ $\oplus$ $C\Big(\big(t^2-\delta t+N_{\mathbb{L}/\mathbb{F}}(x-y)\big)^n\Big)$	$n\in\mathbb{N}$, $x\in\operatorname{Root}(p)$, $y\in\operatorname{Root}(q)$ with $x-y\notin\mathbb{F}$
$C\big((t-(x-y))^n\big)\oplus C\big((t-(x-y))^n\big)$	$n\in\mathbb{N}^*$, $x\in\operatorname{Root}(p)$, $y\in\operatorname{Root}(q)$ with $x-y\in\mathbb{F}$

Note that there are cases where $p(t+y_1)=p(t+y_2)$ even with $y_1\neq y_2$. Indeed, it is not difficult to see that $p(t+y_1)=p(t+y_2)$ if and only if either one of the following conditions holds:

- $y_1=y_2$
- $\mathbb{F}$ has characteristic 2 and $\operatorname{tr} p=\operatorname{tr} q$.

Next, we consider the situation where p and q are both irreducible in $\mathbb{F}[t]$, with the same splitting field (Table 7).

Table 8. The classification of indecomposable d-exceptional (p, q)-differences: When p and q are irreducible with distinct splitting fields and distinct discriminants

Representing matrix	Associated data
$C(F_{p,q}^n) \oplus C(F_{p,q}^n)$	$n \in \mathbb{N}^*$
$C(F_{p,q}^{n+1}) \oplus C(F_{p,q}^n)$	$n \in \mathbb{N}$

Table 9. The classification of indecomposable d-exceptional (p, q)-differences: When p and q are irreducible with distinct splitting fields and the same discriminant

Representing matrix	Associated data
$C\Big(\big(t^2-(\operatorname{tr} p)\,t+p(0)+q(0)\big)^n\Big) \oplus C\Big(\big(t^2-(\operatorname{tr} p)\,t+p(0)+q(0)\big)^n\Big)$	$n \in \mathbb{N}^*$

We finish with the case where p and q are both irreducible, with distinct splitting fields. There are two subcases to consider, whether p and q have the same discriminant or not. Note that the case where p and q have the same discriminant and distinct splitting fields can occur only if $\mathbb{F}$ has characteristic 2 (Tables 8, 9).

3.3. An Example: The Difference of Two Quarter Turns Over the Reals

Here, we consider the case where $\mathbb{F}$ is the field $\mathbb{R}$ of real numbers, and $p = q = t^2+1$. In other words, we determine the endomorphisms of a finite-dimensional real vector space V that split into the difference of two endomorphisms a and b such that $a^2 = b^2 = -\mathrm{id}_V$.

Here, $\operatorname{Root}(p) - \operatorname{Root}(q) = \{2i, -2i, 0\}$ and $\delta = 0$. Let us consider the indecomposable (p, q)-differences. Let $r \in \mathbb{R}[t]$ be an irreducible polynomial such that $r(t^2 - \delta t) = r(t^2)$ has no root in $\operatorname{Root}(p) - \operatorname{Root}(q)$. We set $\mathbb{L} := \mathbb{R}[t]/(r)$ and we note that the class $\overline{t}$ of t in $\mathbb{L}$ is a root of r. If r has degree 2, then $\mathbb{L}$ is isomorphic to $\mathbb{C}$, which is algebraically closed, and it follows that the norm of the quaternion algebra $\mathcal{W}(p, q, \overline{t}+2)_{\mathbb{L}}$ is isotropic (as is any quadratic form with dimension at least 2 over an algebraically closed field).

Assume now that r has degree 1, and denote by x its root. Since $r(t^2)$ has no root in $\operatorname{Root}(p) - \operatorname{Root}(q)$, we see that $x \notin \{-4, 0\}$. Using formula (6) (with here $\alpha = \beta = 1$ and $\lambda = \mu = 0$), we find that the norm of $\mathcal{W}(p, q, x+2)_{\mathbb{R}}$ reads

$$aI_4 + bA + cB + dC \mapsto a^2 + b^2 + c^2 + d^2 + (x+2)bc - (x+2)ad,$$

and hence it is equivalent to the orthogonal direct sum of two copies of the quadratic form

$$Q : (a, b) \mapsto a^2 + (x+2)ab + b^2.$$

TABLE 10. The classification of indecomposable (t^2+1, t^2+1)-differences over $\mathbb{R}$

Representing matrix	Associated data
$C\big((t^2-x)^n\big) \oplus C\big((t^2-x)^n\big)$	$n \in \mathbb{N}^*$, $x \in (-4,0)$
$C\big((t^2-x)^n\big)$	$n \in \mathbb{N}^*$, $x \in (-\infty,-4) \cup (0,+\infty)$
$C\big((t^4+\alpha t^2+\beta)^n\big)$	$n \in \mathbb{N}^*$, $(\alpha,\beta) \in \mathbb{R}^2$ with $\alpha^2 < 4\beta$
$C(t^n) \oplus C(t^n)$	$n \in \mathbb{N}^*$
$C((t^2+4)^n) \oplus C((t^2+4)^n)$	$n \in \mathbb{N}^*$
$C((t^2+4)^{n+1}) \oplus C((t^2+4)^n)$	$n \in \mathbb{N}$

We have $Q(1,0) > 0$, and the discriminant of Q equals $\frac{(x+2)^2-4}{4}$. Therefore, either $|x+2| < 2$ and hence Q is positive definite, or $|x+2| > 2$ and Q is isotropic. It follows that if $x \in (-4,0)$, then the norm of $\mathcal{W}(p,q,x+2)_{\mathbb{R}}$ is non-isotropic, otherwise it is isotropic.

Hence, Table 10 gives a complete list of indecomposable (t^2+1, t^2+1)-differences, where the d-exceptional ones (given in the last three rows) are obtained thanks to Table 7.

3.4. The Classification of d-Regular (p, q)-Differences

We start with a partial result on d-regular (p,q)-differences.

Proposition 3.4. *Let p and q be monic polynomials with degree 2 over $\mathbb{F}$, and set $\delta := \operatorname{tr} p - \operatorname{tr} q$. Let u be an endomorphism of a finite-dimensional vector space V and assume that u is a d-regular (p,q)-difference. Then:*

- (a) *Each invariant factor of u has the form $r(t^2-\delta t)$ for some monic polynomial r.*
- (b) *In some basis of V, the endomorphism u is represented by a block-diagonal matrix in which every diagonal block has the form $C\big(r^n(t^2-\delta t)\big)$ for some irreducible monic polynomial r and some positive integer n. We shall call such a matrix a (p,q)-**reduced canonical form** of u.*

It can easily be shown that a (p,q)-reduced canonical form is unique up to a permutation of the diagonal blocks.

Before we prove Proposition 3.4, we need the corresponding special case where both polynomials p and q are split over $\mathbb{F}$: this result can be obtained by collecting various results from [4,9,10], but we give a synthetic proof here (that uses the same technique as in those articles).

Proposition 3.5. *Let p and q be split monic polynomials with degree 2 over $\mathbb{F}$ and set $\delta := \operatorname{tr} p - \operatorname{tr} q$. Let u be an endomorphism of a finite-dimensional vector space V and assume that u is a d-regular (p,q)-difference. Then, each invariant factor of u is a polynomial in $t^2-\delta t$.*

The proof requires the following basic lemma, which is proved in [9] (see Lemma 14 there, in which the assumption that α and β be nonzero is unnecessary):

Lemma 3.6. *Let $r \in \mathbb{F}[t]$ be a monic polynomial with degree n, and let x and y be scalars. Then,*

$$\begin{bmatrix} xI_n & C(r) \\ I_n & yI_n \end{bmatrix} \simeq C\big(r((t-x)(t-y))\big)$$

Corollary 3.7. *Let N be an arbitrary matrix of $\mathrm{M}_n(\mathbb{F})$, and let x and y be scalars. Then, the invariant factors of*

$$K(N) := \begin{bmatrix} xI_n & N \\ I_n & yI_n \end{bmatrix}$$

are polynomials in $(t-x)(t-y)$.

Proof of Corollary 3.7. We note that the similarity class of $K(N)$ depends only on that of N: indeed, for all $P \in \mathrm{GL}_n(\mathbb{F})$, the invertible matrix $Q := P \oplus P$ satisfies $QK(N)Q^{-1} = K(PNP^{-1})$. Next, if N splits into $N = N_1 \oplus \cdots \oplus N_r$ for some square matrices $N_1, \dots, N_r$ then, by permuting the basis vectors, we gather that $K(N) \simeq K(N_1) \oplus \cdots \oplus K(N_r)$. Considering the rational canonical form $N \simeq C(r_1) \oplus \cdots \oplus C(r_k)$, we obtain

$$K(N) \simeq C\big(r_1\big((t-x)(t-y)\big)\big) \oplus \cdots \oplus C\big(r_k\big((t-x)(t-y)\big)\big).$$

Moreover, the polynomials $r_1\big((t-x)(t-y)\big), \dots, r_k\big((t-x)(t-y)\big)$ are all monic and $r_{i+1}\big((t-x)(t-y)\big)$ divides $r_i\big((t-x)(t-y)\big)$ for all $i \in [\![1, k-1]\!]$. Hence, we have found the invariant factors of $K(N)$, which proves the claimed result. □

Proof of Proposition 3.5. Let a and b be endomorphisms of V such that $p(a) = q(b) = 0$ and $u = a - b$. Denote by x (respectively, by y) an eigenvalue of a (respectively, of b) with maximal geometric multiplicity (the geometric multiplicity of an eigenvalue is the dimension of the corresponding eigenspace), and split $p(t) = (t-x)(t-x')$ and $q(t) = (t-y)(t-y')$. We claim that

$$\dim \operatorname{Ker}(a - x\,\mathrm{id}_V) \geq \frac{n}{2}\cdot$$

Indeed, since $p(a) = 0$ we have $\operatorname{Im}(a - x'\,\mathrm{id}_V) \subset \operatorname{Ker}(a - x\,\mathrm{id}_V)$, which yields $\dim \operatorname{Ker}(a - x\,\mathrm{id}_V) + \dim \operatorname{Ker}(a - x'\,\mathrm{id}_V) \geq n$. Since $\dim \operatorname{Ker}(a - x\,\mathrm{id}_V) \geq \dim \operatorname{Ker}(a - x'\,\mathrm{id}_V)$, the claimed inequality follows.

Likewise, $\dim \operatorname{Ker}(b - y\,\mathrm{id}_V) \geq \frac{n}{2}\cdot$ Since u is d-regular with respect to (p, q), any eigenspace of a is linearly disjoint from any eigenspace of b. In particular, $\operatorname{Ker}(a - x\mathrm{id}_V) \cap \operatorname{Ker}(b - y\,\mathrm{id}_V) = \{0\}$. It follows that $\dim \operatorname{Ker}(a - x\,\mathrm{id}_V) = \frac{n}{2} = \dim \operatorname{Ker}(b - y\,\mathrm{id}_V)$, n is even and $V = \operatorname{Ker}(a - x\mathrm{id}_V) \oplus \operatorname{Ker}(b - y\,\mathrm{id}_V)$. Next, we deduce that $\frac{n}{2} = \dim \operatorname{Im}(a - x\mathrm{id}_V)$ and $\dim \operatorname{Ker}(a - x'\mathrm{id}_V) \leq \frac{n}{2}$ by choice of x. However, $\operatorname{Im}(a - x\mathrm{id}_V) \subset \operatorname{Ker}(a - x'\mathrm{id}_V)$, and hence it follows that $\operatorname{Im}(a - x\mathrm{id}_V) = \operatorname{Ker}(a - x'\mathrm{id}_V)$. Likewise, $\operatorname{Im}(b - y\mathrm{id}_V) = \operatorname{Ker}(b - y'\mathrm{id}_V)$, and it follows that x' has geometric multiplicity $\frac{n}{2}$ with respect to a, and ditto for y' with respect to b. In turn, this shows that $\operatorname{Im}(a - x'\mathrm{id}_V) =$

$\mathrm{Ker}(a - x\mathrm{id}_V)$ and $\mathrm{Im}(b - y'\mathrm{id}_V) = \mathrm{Ker}(b - y\mathrm{id}_V)$, and any eigenspace of a is a complementary subspace of any eigenspace of b.

Let us write $s := \frac{n}{2}$ and choose a basis $(e_1, \dots, e_s)$ of $\mathrm{Ker}(b - y\mathrm{id}_V)$. Then, we have $V = \mathrm{Ker}(b - y\mathrm{id}_V) \oplus \mathrm{Ker}(a - x\mathrm{id}_V)$, whence $(e_{s+1}, \dots, e_n) := ((a - x\mathrm{id}_V)(e_1), \dots, (a - x\mathrm{id}_V)(e_s))$ is a basis of $\mathrm{Im}(a - x\mathrm{id}_V) = \mathrm{Ker}(a - x'\mathrm{id}_V)$. Since $\mathrm{Ker}(b - y\mathrm{id}_V) \oplus \mathrm{Ker}(a - x'\mathrm{id}_V) = V$, we deduce that $\mathbf{B} := (e_1, \dots, e_n)$ is a basis of V. Obviously

$$\mathrm{M}_{\mathbf{B}}(a) = \begin{bmatrix} xI_s & 0 \\ I_n & x'I_s \end{bmatrix}.$$

On the other hand, since $\mathrm{Ker}(b - y\mathrm{id}_V) = \mathrm{Im}(b - y'\mathrm{id}_V)$, we find

$$\mathrm{M}_{\mathbf{B}}(b) = \begin{bmatrix} yI_s & N \\ 0 & y'I_s \end{bmatrix}$$

for some matrix $N \in \mathrm{M}_s(\mathbb{F})$. Hence,

$$\mathrm{M}_{\mathbf{B}}(u) = \begin{bmatrix} (x-y)I_s & -N \\ I_n & (x'-y')I_s \end{bmatrix}.$$

Since $(t - (x - y))(t - (x' - y')) = t^2 - \delta t + (x - y)(x' - y')$, we conclude from Lemma 3.6 that all the invariant factors of u are polynomials in $t^2 - \delta t$. □

Proof of Proposition 3.4. We start with point (a). Let us extend the field of scalars to $\overline{\mathbb{F}}$. The resulting extension $\overline{u}$ of u is still a (p, q)-difference. Hence, by Corollary 3.7 its invariant factors are $p_1(t^2 - \delta t), \dots, p_r(t^2 - \delta t)$ for some monic polynomials $p_1, \dots, p_r$ of $\overline{\mathbb{F}}[t]$ such that p_{i+1} divides p_i for all $i \in [\![1, r-1]\!]$. Yet, the invariant factors of $\overline{u}$ are known to be the ones of u. Finally, given a monic polynomial $h \in \overline{\mathbb{F}}[t]$ such that $h(t^2 - \delta t) \in \mathbb{F}[t]$, we obtain by downward induction that all the coefficients of h belong to $\mathbb{F}$: indeed, if we write $h(t) = t^N - \sum_{i=0}^{N-1} \alpha_i\, t^i$ and we know that $\alpha_{N-1}, \dots, \alpha_{k+1}$ all belong to $\mathbb{F}$ for some $k \in [\![0, N-1]\!]$, then $\sum_{i=0}^{k} \alpha_i\, (t^2 - \delta t)^i = (t^2 - \delta t)^N - \sum_{i=k+1}^{N-1} \alpha_i\, (t^2 - \delta t)^i - h(t^2 - \delta t)$ belongs to $\mathbb{F}[t]$, and by considering the coefficient on t^{2k}, we gather that $\alpha_k \in \mathbb{F}$. It follows that $p_1, \dots, p_r$ all belong to $\mathbb{F}[t]$, which completes the proof of statement (a).

From point (a), we easily derive point (b): indeed, consider an invariant factor $r(t^2 - \delta t)$ of u for some monic polynomial $r \in \mathbb{F}[t]$. Then, we split $r = r_1^{n_1} \cdots r_k^{n_k}$ where $r_1, \dots, r_k$ are pairwise distinct irreducible monic polynomials of $\mathbb{F}[t]$, and $n_1, \dots, n_k$ are positive integers. Then, the polynomials $r_1^{n_1}(t^2 - \delta t), \dots, r_k^{n_k}(t^2 - \delta t)$ are pairwise coprime and their product equals $r(t^2 - \delta t)$, whence

$$C\big(r(t^2 - \delta t)\big) \simeq C\big(r_1^{n_1}(t^2 - \delta t)\big) \oplus \cdots \oplus C\big(r_k^{n_k}(t^2 - \delta t)\big).$$

Using point (a), we deduce that statement (b) holds true. □

We are now ready to complete our study of d-regular (p, q)-differences. An additional definition will be useful in this prospect:

Definition 5. Let p and q be monic polynomials with degree 2 in $\mathbb{F}[t]$. Set $\delta := \mathrm{tr}(p) - \mathrm{tr}(q)$. Let r be an irreducible monic polynomial of $\mathbb{F}[t]$, and set $\mathbb{L} := \mathbb{F}[t]/(r)$. Denote by $\overline{t}$ the class of t in $\mathbb{L}$. We say that r has:

- **Type** 1 **with respect to** (p,q) if $r(t^2-\delta t)$ has no root in $\operatorname{Root}(p)-\operatorname{Root}(q)$ and the norm of the quaternion algebra $\mathcal{W}\bigl(p,q,\overline{t}+p(0)+q(0)\bigr)_{\mathbb{L}}$ is isotropic.
- **Type** 2 **with respect to** (p,q) if $r(t^2-\delta t)$ has no root in $\operatorname{Root}(p)-\operatorname{Root}(q)$ and the norm of the quaternion algebra $\mathcal{W}\bigl(p,q,\overline{t}+p(0)+q(0)\bigr)_{\mathbb{L}}$ is nonisotropic.

First of all, we use the structural results on $\mathcal{W}(p,q,x)_R$ to obtain various (p,q)-differences. Our first result is actually not restricted to d-regular (p,q)-differences and will be used in a subsequent article.

Lemma 3.8. (Duplication Lemma). *Let p and q be monic polynomials of $\mathbb{F}[t]$ with degree 2, and set $\delta := \operatorname{tr} p - \operatorname{tr} q$. Let r be a nonconstant monic polynomial of $\mathbb{F}[t]$. Then, $C\bigl(r(t^2-\delta t)\bigr) \oplus C\bigl(r(t^2-\delta t)\bigr)$ is a (p,q)-difference.*

Proof. We work with the commutative $\mathbb{F}$-algebra $R := \mathbb{F}[C(r)]$, which is isomorphic to the quotient ring $\mathbb{F}[t]/(r)$, and with the element $x := \bigl(p(0)+q(0)\bigr)\,1_R + C(r)$. Using $q(B)=0$, it is easily seen that $\mathbf{B} := (I_2, A-B, B, (A-B)B)$ is still a basis of the free R-module $\mathcal{W}(p,q,x)$. Then, we consider the endomorphisms $a : X \mapsto AX$ and $b : X \mapsto BX$ of $\mathcal{W}(p,q,x)$. Since $p(A)=0$ and $q(B)=0$, we get $p(a)=0$ and $q(b)=0$. Denote by A' and B' the respective matrices of a and b in $\mathbf{B}$. Using $(A-B)^2 = \delta(A-B) + \bigl(x-p(0)-q(0)\bigr)I_4$, we get that

$$A'-B' = \begin{bmatrix} 0 & C(r) & 0 & 0 \\ 1_R & \delta\,1_R & 0 & 0 \\ 0 & 0 & 0 & C(r) \\ 0 & 0 & 1_R & \delta\,1_R \end{bmatrix},$$

whence the matrix $A'-B'$ of $\mathrm{M}_{4d}(\mathbb{F})$ (where d denotes the degree of r) is similar to $C\bigl(r(t(t-\delta))\bigr) \oplus C\bigl(r(t(t-\delta))\bigr)$ by Lemma 3.6. Since $p(A')=0$ and $q(B')=0$, the conclusion follows. □

Our next result deals with certain companion matrices that are associated with irreducible polynomials of Type 1.

Lemma 3.9. *Let p and q be monic polynomials of $\mathbb{F}[t]$ with degree 2, and set $\delta := \operatorname{tr} p - \operatorname{tr} q$. Let r be an irreducible monic polynomial of $\mathbb{F}[t]$ of Type 1 with respect to (p,q). Then, for all $n \in \mathbb{N}^*$, the companion matrix $C\bigl(r^n(t^2-\delta t)\bigr)$ is a (p,q)-difference.*

Proof. Denote by d the degree of r. Let $n \in \mathbb{N}^*$. Set $R := \mathbb{F}[C(r^n)]$, seen as a subalgebra of $\mathrm{M}_{nd}(\mathbb{F})$, and set $x := C(r^n) + \bigl(p(0)+q(0)\bigr)I_{nd}$. The $\mathbb{F}$-algebra R is isomorphic to $\mathbb{F}[t]/(r^n)$. By Proposition 2.6, it follows that $\mathcal{W}(p,q,x)_R$ is isomorphic to $\mathrm{M}_2(R)$. We choose an isomorphism $\varphi : \mathcal{W}(p,q,x)_R \xrightarrow{\simeq} \mathrm{M}_2(R)$, and we set $a := \varphi(A)$ and $b := \varphi(B)$. Note that $p(a)=q(b)=0$, whereas $c := a-b$ satisfies $c(c-\delta I_2) = \bigl(x-(p(0)+q(0))1_R\bigr)\, I_2$.

Denote by $\mathbb{L}$ the residue field of R. The mapping $X \in R^2 \mapsto cX \in R^2$ yields an endomorphism $\overline{c}$ of $\mathbb{L}^2$. Yet, $\overline{c}$ cannot be a scalar multiple of the identity (otherwise, (I_2, a, b, ab) would not be a basis of the R-module $\mathrm{M}_2(R)$).

Hence, we find a vector e of $\mathbb{L}^2$ such that $\big(e, \overline{c}(e)\big)$ is a basis of $\mathbb{L}^2$. Lifting e to a vector E of R^2, we deduce that (E, cE) is a basis of the R-module R^2. Hence, composing φ with an additional interior automorphism of the R-algebra $\mathrm{M}_2(R)$, we see that no generality is lost in assuming that the first column of c reads $\begin{bmatrix} 0_R \\ 1_R \end{bmatrix}$. Then, $c(c - \delta I_2) = \big(x - (p(0) + q(0))1_R\big)\, I_2$ yields

$$c = \begin{bmatrix} 0 & C(r^n) \\ 1_R & \delta 1_R \end{bmatrix}.$$

It follows that the matrix $\begin{bmatrix} 0 & C(r^n) \\ I_{nd} & \delta I_{nd} \end{bmatrix}$ of $\mathrm{M}_{2nd}(\mathbb{F})$ is a (p,q)-difference. By Lemma 3.6, this matrix is similar to $C\big(r^n(t^2 - \delta t)\big)$, which completes the proof. □

Combining Lemma 3.8 with Lemma 3.9, we conclude that the implication (iii) ⇒ (i) in the following theorem holds true.

Theorem 3.10. (Classification of d-regular (p,q)-differences) *Let p and q be monic polynomials of degree 2 in $\mathbb{F}[t]$. Let u be an endomorphism of a finite-dimensional vector space V over $\mathbb{F}$. Assume that u is d-regular with respect to (p,q) and set $\delta := \operatorname{tr}(p) - \operatorname{tr}(q)$. The following conditions are equivalent:*

- (i) *The endomorphism u is a (p,q)-difference.*
- (ii) *The invariant factors of u read $p_1(t^2 - \delta t), \dots, p_{2n-1}(t^2 - \delta t), p_{2n}(t^2 - \delta t), \dots$ where, for every irreducible monic polynomial $r \in \mathbb{F}[t]$ that has Type 2 with respect to (p,q) and every positive integer n the polynomials p_{2n-1} and p_{2n} have the same valuation with respect to r.*
- (iii) *There is a basis of V in which u is represented by a block-diagonal matrix in which every diagonal block equals either $C\big(r^n(t^2 - \delta t)\big)$ for some irreducible monic polynomial $r \in \mathbb{F}[t]$ of Type 1 with respect to (p,q) and some $n \in \mathbb{N}^*$, or $C\big(r^n(t^2 - \delta t)\big) \oplus C\big(r^n(t^2 - \delta t)\big)$ for some irreducible monic polynomial $r \in \mathbb{F}[t]$ and some $n \in \mathbb{N}^*$.*

Note that this result, combined with the observation that $C\big(r^n(t^2 - \delta t)\big)$ is d-regular with respect to (p,q) for every monic polynomial $r \in \mathbb{F}[t]$ such that $r(t^2 - \delta t)$ has no root in $\operatorname{Root}(p) - \operatorname{Root}(q)$, yields the classification of indecomposable d-regular (p,q)-differences as given in Table 1. Moreover, by using the method from the last part of the proof of Proposition 3.4, it is easily seen that conditions (ii) and (iii) are equivalent.

In order to conclude on Theorem 3.10, it only remains to prove that condition (i) implies condition (ii), which we shall now do thanks to the structural results on $\mathcal{W}(p,q,x)_R$.

Proof. (Proof of the implication (i) ⇒ (ii)) Let us assume that u is a (p,q)-difference. Let r be an irreducible monic polynomial of $\mathbb{F}[t]$, with Type 2 with respect to (p,q). Let $n \in \mathbb{N}^*$. All we need is to prove that, in the canonical form of u from Proposition 3.4, the number m of diagonal blocks that equal $C\big(r^n(t^2 - \delta t)\big)$ is even.

Let us choose endomorphisms a and b of V such that $u = a - b$ and $p(a) = q(b) = 0$. By the Commutation Lemma (Lemma 3.2), we know that a and b

commute with $v := u^2 - \delta u$, and hence all three endomorphisms a, b, u yield endomorphisms $\overline{a}$, $\overline{b}$ and $\overline{u}$ of the vector space $E := \operatorname{Ker}\bigl(r^n(v)\bigr) / \operatorname{Ker}\bigl(r^{n-1}(v)\bigr)$ such that $\overline{u} = \overline{a} - \overline{b}$, and r annihilates $\overline{v} := \overline{u}^2 - \delta \overline{u}$. Again, $\overline{a}$ and $\overline{b}$ commute with $\overline{v}$, and hence they are endomorphisms of the $\mathbb{F}[\overline{v}]$-module E. Since r is irreducible, we have $\mathbb{F}[\overline{v}] \simeq \mathbb{F}[t]/(r)$, and $\mathbb{L} := \mathbb{F}[\overline{v}]$ is a field. We shall write $y := \overline{v}$, which we see as an element of $\mathbb{L}$.

Besides, $2m \deg(r)$ is the dimension of the $\mathbb{F}$-vector space E, and hence $2m$ is the dimension of the $\mathbb{L}$-vector space E.

Using the structure of $\mathbb{L}$-vector space, we can write $\overline{u}^2 - \delta \overline{u} = y \operatorname{id}_E$, and hence $\overline{a}$ and $\overline{b}$ yield a representation of the $\mathbb{L}$-algebra $\mathcal{W}\bigl(p, q, y + p(0) + q(0)\bigr)_{\mathbb{L}}$ on the $\mathbb{L}$-vector space E. By Corollary 2.5, the algebra $\mathcal{W}\bigl(p, q, y + p(0) + q(0)\bigr)_{\mathbb{L}}$ is a 4-dimensional skew-field over $\mathbb{L}$, whence the $\mathbb{L}$-vector space E is isomorphic to a power of $\mathcal{W}\bigl(p, q, y + p(0) + q(0)\bigr)_{\mathbb{L}}$, and it follows that its dimension over $\mathbb{L}$ is a multiple of 4. Therefore, m is a multiple of 2, which completes the proof. $\square$

The classification of d-regular (p, q)-differences is now completed.

4. The Quotient of Two Invertible Quadratic Matrices

4.1. The Basic Splitting

Let u be an automorphism of a finite-dimensional vector space V over $\mathbb{F}$. Let p and q be monic polynomials with degree 2 over $\mathbb{F}$, with $p(0)q(0) \neq 0$, which we write

$$p(t) = t^2 - \lambda t + \alpha \quad \text{and} \quad q(t) = t^2 - \mu t + \beta.$$

Taking an indeterminate x independent of t, we can view $p(x)$ and $\beta^{-1} t^2 q(x/t)$ as monic polynomials of degree 2 with coefficients in the ring $\mathbb{F}[t]$, with respect to the indeterminate x. We can therefore define the **q-fundamental polynomial** as their resultant

$$G_{p,q}(t) := \operatorname{res}_{\mathbb{F}[t]}\bigl(p(x), q(0)^{-1} t^2 q(x/t)\bigr) \in \mathbb{F}[t],$$

which is a monic polynomial of degree 4. More explicitly, if we split $p(t) = (t - x_1)(t - x_2)$ and $q(t) = (t - y_1)(t - y_2)$ in $\overline{\mathbb{F}}[t]$, then

$$G_{p,q}(t) = \prod_{1 \leq i,j \leq 2} \bigl(t - x_i y_j^{-1}\bigr) = \beta^{-2} p(y_1 t)\, p(y_2 t) = \beta^{-2}\, t^4\, q(x_1 t^{-1})\, q(x_2 t^{-1}).$$

We set

$$E'_{p,q}(u) := \bigcup_{n \in \mathbb{N}} \operatorname{Ker} G_{p,q}(u)^n \quad \text{and} \quad R'_{p,q}(u) := \bigcap_{n \in \mathbb{N}} \operatorname{Im} G_{p,q}(u)^n.$$

Hence, $V = E'_{p,q}(u) \oplus R'_{p,q}(u)$, and the endomorphism u stabilizes both linear subspaces $E'_{p,q}(u)$ and $R'_{p,q}(u)$. The endomorphism u is called **q-exceptional** with respect to (p, q) (respectively, **q-regular** with respect to (p, q)) whenever $E'_{p,q}(u) = V$ (respectively, $R'_{p,q}(u) = V$). In other words, u is q-exceptional (respectively, q-regular) with respect to (p, q) if and only if all the eigenvalues of u in $\overline{\mathbb{F}}$ belong to $\operatorname{Root}(p)\operatorname{Root}(q)^{-1}$ (respectively, no eigenvalue of u in $\overline{\mathbb{F}}$ belongs to $\operatorname{Root}(p)\operatorname{Root}(q)^{-1}$).

The endomorphism of $E'_{p,q}(u)$ (respectively, of $R'_{p,q}(u)$) induced by u is always q-exceptional (respectively, always regular) with respect to (p,q) and we call it the **q-exceptional part** (respectively, the **q-regular part**) of u with respect to (p,q).

Next, note that $\beta^2 G_{p,q}(t) = \prod_{1\leq i,j\leq 2} (y_j t - x_i)$, and

$$\begin{aligned}(y_1t-x_1)(y_2t-x_2) &= \beta t^2 - (x_1y_2+x_2y_1)\,t+\alpha \\ &= t\left(\beta t+\alpha t^{-1}-(x_1y_2+x_2y_1)\right)\end{aligned}$$

and likewise

$$(y_1t-x_2)(y_2t-x_1) = t\left(\beta t+\alpha t^{-1}-(x_1y_1+x_2y_2)\right).$$

Hence,

$$\beta^2 G_{p,q}(t) = t^2\,\Theta_{p,q}(\beta t+\alpha t^{-1})$$

where

$$\Theta_{p,q} := \left(t-(x_1y_1+x_2y_2)\right)\left(t-(x_1y_2+x_2y_1)\right).$$

We compute that

$$\Theta_{p,q} = t^2-\lambda\mu t+(x_1y_2+x_2y_1)(x_1y_1+x_2y_2)$$

and

$$\begin{aligned}(x_1y_2+x_2y_1)(x_1y_1+x_2y_2) &= x_1x_2(y_1^2+y_2^2)+y_1y_2(x_1^2+x_2^2) \\ &= \alpha(\mu^2-2\beta)+\beta(\lambda^2-2\alpha).\end{aligned}$$

We conclude that

$$\Theta_{p,q} = t^2-\lambda\mu t+(\alpha\mu^2+\beta\lambda^2-4\alpha\beta)\in\mathbb{F}[t]$$

and

$$\beta^2 G_{p,q}(u) = u^2\,\Theta_{p,q}(\beta u+\alpha u^{-1}).$$

Remark 3. Let $\mathcal{A}$ be an $\mathbb{F}$-algebra, and let a,b be elements of $\mathcal{A}$ such that $p(a)=q(b)=0$. Denote by $a^\star$ the p-conjugate of a and by $b^\star$ the q-conjugate of b. Then, $b^\star=\beta\,b^{-1}$ and $a^\star=\alpha\,a^{-1}$, whence

$$\beta\,ab^{-1}+\alpha\,(ab^{-1})^{-1} = \beta\,ab^{-1}+\alpha\,ba^{-1} = ab^\star+ba^\star.$$

Our first basic result follows:

Proposition 4.1. *The endomorphism u is a (p,q)-quotient if and only if both its q-exceptional part and its q-regular part are (p,q)-quotients.*

The proof of this result will use the following basic lemma, which is a straightforward corollary to the Basic Commutation Lemma (Lemma 1.3):

Lemma 4.2. (Commutation Lemma). *Let a and b be endomorphisms of a vector space V such that $p(a)=q(b)=0$. Then, both a and b commute with $\beta\,(ab^{-1})+\alpha\,(ab^{-1})^{-1}$.*

Now, we are ready to prove Proposition 4.1.

Proof of Proposition 4.1. The "if" part is obvious. Conversely, assume that u is a (p,q)-quotient, and split $u = ab^{-1}$ where a and b are automorphisms of V such that $p(a) = 0$ and $q(b) = 0$. By the Commutation Lemma, both a and b commute with $v := \beta u + \alpha u^{-1}$. Hence, a and b commute with $\Theta_{p,q}(v)$. Since u commutes with v and is an automorphism, we see that $G_{p,q}(u)^n = q(0)^{-2n} u^{2n} \Theta_{p,q}(v)^n = q(0)^{-2n} \Theta_{p,q}(v)^n u^{2n}$ for every positive integer n, and it follows that $\operatorname{Ker} G_{p,q}(u)^n = \operatorname{Ker} \Theta_{p,q}(v)^n$ and $\operatorname{Im} G_{p,q}(u)^n = \operatorname{Im} \Theta_{p,q}(v)^n$ for every such integer n. Hence, as a and b commute with v, we deduce that both stabilize $E_{p,q}(u)$ and $R_{p,q}(u)$ (and of course they induce automorphisms of those vector spaces). Denote by a' and b' (respectively, by a'' and b'') the automorphisms of $E_{p,q}(u)$ (respectively, of $R_{p,q}(u)$) induced by a and b. Then, the q-exceptional part of u is $a'(b')^{-1}$, and the q-regular part of u is $a''(b'')^{-1}$. As p annihilates a' and a'', and q annihilates b' and b'', both the q-exceptional and the q-regular part of u are (p,q)-quotients. □

From there, it is clear that classifying (p,q)-quotients amounts to classifying the q-exceptional ones and the q-regular ones. The easier classification is the latter: as we shall see, it involves little discussion on the specific polynomials p and q under consideration (whether they are split or not over $\mathbb{F}$, separable or not over $\mathbb{F}$, etc). In contrast, the classification of q-exceptional (p,q)-quotients involves a tedious case-by-case study: it will be carried out in a separate article.

4.2. The R_δ Transformation

Notation 6. Let r be a monic polynomial with degree d, and let δ be a nonzero scalar. We set

$$R_\delta(r) := t^d r(t + \delta t^{-1}),$$

which is a monic polynomial with degree $2d$ and valuation 0.

Some basic facts will be useful on the R_δ transformation:

- For all monic polynomials r and s, we have $R_\delta(r) R_\delta(s) = R_\delta(rs)$.
- Followingly, if r and s are monic polynomials such that r divides s, then $R_\delta(r)$ divides $R_\delta(s)$.
- Let r and s be coprime monic polynomials. Then, $R_\delta(r)$ and $R_\delta(s)$ are coprime: indeed if in some algebraic (field) extension of $\mathbb{F}$ those polynomials had a common root z (necessarily nonzero) then $z + \delta z^{-1}$ would be a common root of r and s.

In the study of q-regular (p,q)-quotients, the following lemma will be useful.

Proposition 4.3. *Let $r \in \mathbb{F}[t] \smallsetminus \{t\}$ be irreducible. Set $\delta := \alpha\beta^{-1}$. The following conditions are equivalent:*

(i) *No root of $R_\delta(r)$ (in $\overline{\mathbb{F}}$) belongs to* $\operatorname{Root}(p)\operatorname{Root}(q)^{-1}$.

(ii) *For $\mathbb{L} := \mathbb{F}[t]/(r)$ and y the class of t in $\mathbb{L}$, the norm of $\mathcal{W}(p,q,\beta y)_{\mathbb{L}}$ is nondegenerate.*

Proof. Assume that $R_\delta(r)$ has a root z in $\operatorname{Root}(p)\operatorname{Root}(q)^{-1}$. Noting that z is a root of $G_{p,q} = \beta^{-1}\Theta_{p,q}(\beta(t + \delta t^{-1}))$, we deduce that $z + \delta z^{-1}$ is a

Table 11. The classification of indecomposable q-regular (p,q)-quotients

Representing matrix	Associated data
$C\big(R_\delta(r)^n\big)$	$n \in \mathbb{N}^*$, $r \in \mathbb{F}[t]$ irreducible and monic, $R_\delta(r)$ has no root in $\operatorname{Root}(p)\operatorname{Root}(q)^{-1}$ $N_{\mathcal{W}(p,q,q(0)y)_{\mathbb{L}}}$ is isotropic over $\mathbb{L} := \mathbb{F}[t]/(r)$ for some root y of r in $\mathbb{L}$
$C\big(R_\delta(r)^n\big)$ $\oplus$ $C\big(R_\delta(r)^n\big)$	$n \in \mathbb{N}^*$, $r \in \mathbb{F}[t]$ irreducible and monic, $R_\delta(r)$ has no root in $\operatorname{Root}(p)\operatorname{Root}(q)^{-1}$ $N_{\mathcal{W}(p,q,q(0)y)_{\mathbb{L}}}$ is non-isotropic over $\mathbb{L} := \mathbb{F}[t]/(r)$ for some root y of r in $\mathbb{L}$

common root of r and of $\Theta_{p,q}(\beta t)$. Since r is irreducible, it follows that r divides $\Theta_{p,q}(\beta t)$, and hence y is a root of $\Theta_{p,q}(\beta t)$ in $\mathbb{L}$, that is βy equals $x_1y_1 + x_2y_2$ or $x_1y_2 + x_2y_1$. Hence the norm of $\mathcal{W}(p,q,\beta y)_{\mathbb{L}}$ is degenerate.

Conversely, assume that the norm of $\mathcal{W}(p,q,\beta y)_{\mathbb{L}}$ is degenerate. Then βy equals $x_1y_1 + x_2y_2$ or $x_1y_2 + x_2y_1$, to the effect that $\Theta_{p,q}(\beta y) = 0$. We can choose $z \in \overline{\mathbb{F}} \smallsetminus \{0\}$ such that $z + \delta z^{-1} = y$ (it suffices to take a root of $t^2 - yt + \delta$). Then, z is a common root of $R_\delta(r)$ and of $G_{p,q}$, whence $R_\delta(r)$ has a root in $\operatorname{Root}(p)\operatorname{Root}(q)^{-1}$. □

4.3. Statement of the Results

We are now ready to state our results. We shall frame them in terms of direct-sum decomposability.

Let u be an endomorphism of a nonzero finite-dimensional vector space V. Assume that V splits into $V_1 \oplus V_2$, and that each linear subspace V_1 and V_2 is stable under u and nonzero, and both induced endomorphisms $u_{|V_1}$ and $u_{|V_2}$ are (p,q)-quotients. Then, u is obviously a (p,q)-quotient. In the event when such a decomposition exists we shall say that u is a **decomposable** (p,q)-quotient, otherwise and if u is a (p,q)-quotient, we shall say that u is an **indecomposable** (p,q)-quotient. Obviously, every (p,q)-quotient in $\operatorname{End}(V)$ is the direct sum of indecomposable ones. Hence, it suffices to describe the indecomposable (p,q)-quotients.

Moreover, if a (p,q)-quotient is indecomposable then it is either q-regular or q-exceptional, owing to Proposition 4.1.

In each one of the following tables, we give a set of matrices. Each matrix represents an indecomposable (p,q)-quotient, and every indecomposable (p,q)-quotient in $\operatorname{End}(V)$ is represented by one of those matrices, in some basis. It is convenient to set

$$\delta := p(0)q(0)^{-1}.$$

We start with q-regular (p,q)-quotients. In that situation the classification is rather simple (Table 11):

Remember (see Remark 1), that the norm of the quaternion algebra $\mathcal{W}(p,q,x)$ is isotropic whenever one of p and q splits in $\mathbb{F}[t]$.

Table 12. The classification of indecomposable q-exceptional (p, q)-quotients: When both p and q are split with a double root

Representing matrix	Associated data
$C\big((t-x)^n\big)$	$x \in \operatorname{Root}(p)\operatorname{Root}(q)^{-1}$, $n \in \mathbb{N}^*$

Table 13. The classification of indecomposable q-exceptional (p, q)-quotients: When both p and q are split with simple roots

Representing matrix	Associated data
$C\big((t-x)^n\big) \oplus C\big((t-\delta x^{-1})^n\big)$	$n \in \mathbb{N}^*$, $x \in \operatorname{Root}(p)\operatorname{Root}(q)^{-1}$ such that $x \neq \delta x^{-1}$
$C\big((t-x)^{n+1}\big) \oplus C\big((t-\delta x^{-1})^n\big)$	$n \in \mathbb{N}$, $x \in \operatorname{Root}(p)\operatorname{Root}(q)^{-1}$ such that $x \neq \delta x^{-1}$
$C\big((t-x)^n\big)$	$n \in \mathbb{N}^*$, $x \in \operatorname{Root}(p)\operatorname{Root}(q)^{-1}$ such that $x = \delta x^{-1}$

Table 14. The classification of indecomposable q-exceptional (p, q)-quotients: When both p and q are split, p has simple roots and q has a double root

Representing matrix	Associated data
$C\big((t-x)^n\big) \oplus C\big((t-\delta x^{-1})^n\big)$	$x \in \operatorname{Root}(p)\operatorname{Root}(q)^{-1}$, $n \in \mathbb{N}^*$
$C\big((t-x)^{n+1}\big) \oplus C\big((t-\delta x^{-1})^n\big)$	$x \in \operatorname{Root}(p)\operatorname{Root}(q)^{-1}$, $n \in \mathbb{N}$
$C\big((t-x)^{n+2}\big) \oplus C\big((t-\delta x^{-1})^n\big)$	$x \in \operatorname{Root}(p)\operatorname{Root}(q)^{-1}$, $n \in \mathbb{N}$

Next, we tackle the q-exceptional indecomposable (p, q)-quotients. Here, there are many cases to consider. We start with the one when both p and q are split (Tables 12, 13, 14).

We now turn to the case where p is irreducible but q splits.

There are two subcases to consider, whether the two polynomials deduced from p by using the homotheties with ratio among the roots of q are equal or not. Here, we refer to Notation 1 on page 4 for $H_y(p)$ (Table 15, 16).

Next, we consider the situation where both p and q are irreducible in $\mathbb{F}[t]$, with the same splitting field (Table 17).

We finish with the case where p and q are both irreducible, with distinct splitting fields. There are two subcases to consider, whether both $\operatorname{tr} p$ and $\operatorname{tr} q$ equal zero or not (Table 18, 19).

Table 15. The classification of indecomposable q-exceptional (p,q)-quotients: When p is irreducible, $q=(t-y_1)(t-y_2)$ for some y_1,y_2 in $\mathbb{F}$, and $H_{y_1}(p)=H_{y_2}(p)$

Representing matrix	Associated data
$C\big(H_y(p)^n\big)$	$n\in\mathbb{N}^*$, $y\in\mathrm{Root}(q)$

Table 16. The classification of indecomposable q-exceptional (p,q)-quotients: When p is irreducible, $q=(t-y_1)(t-y_2)$ for some y_1,y_2 in $\mathbb{F}$, and $H_{y_1}(p)\neq H_{y_2}(p)$

Representing matrix	Associated data
$C\big(H_{y_1}(p)^n\big)\oplus C\big(H_{y_2}(p)^n\big)$	$n\in\mathbb{N}^*$
$C\big(H_{y_1}(p)^{n+1}\big)\oplus C\big(H_{y_2}(p)^n\big)$	$n\in\mathbb{N}$
$C\big(H_{y_2}(p)^{n+1}\big)\oplus C\big(H_{y_1}(p)^n\big)$	$n\in\mathbb{N}$

Table 17. The classification of indecomposable q-exceptional (p,q)-quotients: When p and q are irreducible with the same splitting field $\mathbb{L}$

Representing matrix	Associated data
$C\Big(\big(t^2-\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(xy^{-1})t+\delta\big)^n\Big)$ $\oplus$ $C\Big(\big(t^2-\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(xy^{-1})t+\delta\big)^n\Big)$	$n\in\mathbb{N}^*$, $x\in\mathrm{Root}(p)$, $y\in\mathrm{Root}(q)$ with $xy^{-1}\notin\mathbb{F}$
$C\Big(\big(t^2-\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(xy^{-1})t+\delta\big)^{n+1}\Big)$ $\oplus$ $C\Big(\big(t^2-\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(xy^{-1})t+\delta\big)^n\Big)$	$n\in\mathbb{N}$, $x\in\mathrm{Root}(p)$, $y\in\mathrm{Root}(q)$ with $xy^{-1}\notin\mathbb{F}$
$C\big((t-xy^{-1})^n\big)\oplus C\big((t-xy^{-1})^n\big)$	$n\in\mathbb{N}^*$, $x\in\mathrm{Root}(p)$, $y\in\mathrm{Root}(q)$ with $xy^{-1}\in\mathbb{F}$

Table 18. The classification of indecomposable q-exceptional (p,q)-quotients: When p and q are irreducible with distinct splitting fields and $(\mathrm{tr}\,p,\mathrm{tr}\,q)\neq(0,0)$

Representing matrix	Associated data
$C(G_{p,q}^n)\oplus C(G_{p,q}^n)$	$n\in\mathbb{N}^*$
$C(G_{p,q}^{n+1})\oplus C(G_{p,q}^n)$	$n\in\mathbb{N}$

Table 19. The classification of indecomposable q-exceptional (p,q)-quotients: When p and q are irreducible with distinct splitting fields and $\operatorname{tr} p = \operatorname{tr} q = 0$

Representing matrix	Associated data
$C\big((t^2-\delta)^n\big) \oplus C\big((t^2-\delta)^n\big)$	$n \in \mathbb{N}^*$

4.4. An Example: The Quotient of Two Quarter Turns Over the Reals

Here, we consider the case where $\mathbb{F}$ is the field $\mathbb{R}$ of real numbers and $p = q = t^2+1$. In other words, we determine the automorphisms of a finite-dimensional real vector space V that split into ab^{-1} for some automorphisms a and b such that $a^2 = b^2 = -\mathrm{id}_V$ (note that these automorphisms are also the (t^2+1, t^2+1)-products). Here, $\operatorname{Root}(p)\operatorname{Root}(q)^{-1} = \{1,-1\}$ and $\delta := p(0)q(0)^{-1}$ equals 1.

Let us investigate the indecomposable (p,q)-quotients. Let $r \in \mathbb{R}[t]$ be an irreducible monic polynomial. The fraction $r(t+\delta t^{-1}) = r(t+t^{-1})$ has no root in $\operatorname{Root}(p)\operatorname{Root}(q)^{-1}$ if and only if $r(2) \neq 0$ and $r(-2) \neq 0$.

From now on, we assume that $r \neq t-2$ and $r \neq t+2$. We set $\mathbb{L} := \mathbb{R}[t]/(r)$ and we denote by $\bar{t}$ the class of t in it. If r has degree 2, then $\mathbb{L}$ is isomorphic to $\mathbb{C}$, which is algebraically closed, and it follows that the norm of $\mathcal{W}(p,q,\bar{t})_{\mathbb{L}}$ is isotropic. Note that, for all $(a,b) \in \mathbb{R}^2$ such that $a^2 < 4b$, we have

$$\begin{aligned} R_\delta(t^2+at+b) &= t^2\big((t+t^{-1})^2 + a(t+t^{-1}) + b\big) \\ &= t^4 + at^3 + (b+2)t^2 + at + 1. \end{aligned}$$

Assume now that r has degree 1, and denote by x its root (so that $x \neq \pm 2$). The norm of $\mathcal{W}(p,q,x)_{\mathbb{R}}$ reads

$$aI_4 + bA + cB + dC \mapsto a^2 + b^2 + c^2 + d^2 + xbc - xad$$

which is equivalent to the orthogonal direct sum of two copies of the quadratic form

$$Q : (a,b) \mapsto a^2 + xab + b^2.$$

We have $Q(1,0) > 0$, and the discriminant of Q equals $\frac{x^2-4}{4}$. Hence, either $|x| < 2$ and Q is positive definite, or $|x| > 2$ and Q is isotropic. It follows that if $x \in (-2,2)$, then the norm of $\mathcal{W}(p,q,x)_{\mathbb{R}}$ is non-isotropic, otherwise it is isotropic.

Table 20 thus gives a complete list of indecomposable (t^2+1, t^2+1)-quotients, where the q-exceptional ones – given in the last two rows – are obtained thanks to Table 17.

4.5. The Classification of q-Regular (p,q)-Quotients

Proposition 4.4. *Let p and q be monic polynomials with degree 2 over $\mathbb{F}$ such that $p(0)q(0) \neq 0$, and set $\delta := p(0)q(0)^{-1}$. Let u be an endomorphism of*

TABLE 20. The classification of indecomposable (t^2+1, t^2+1)-quotients over $\mathbb{R}$

Representing matrix	Associated data
$C\big((t^2-xt+1)^n\big) \oplus C\big((t^2-xt+1)^n\big)$	$n \in \mathbb{N}^*$, $x \in (-2,2)$
$C\big((t^2-xt+1)^n\big)$	$n \in \mathbb{N}^*$, $x \in (-\infty,-2) \cup (2,+\infty)$
$C\big((t^4+at^3+(b+2)t^2+at+1)^n\big)$	$n \in \mathbb{N}^*$, $(a,b) \in \mathbb{R}^2$ with $a^2<4b$
$C((t-1)^n) \oplus C((t-1)^n)$	$n \in \mathbb{N}^*$
$C((t+1)^n) \oplus C((t+1)^n)$	$n \in \mathbb{N}^*$

a finite-dimensional vector space V and assume that u is a q-regular (p,q)-quotient. Then:

(a) *Each invariant factor of u has the form $R_\delta(r)$ for some monic polynomial r.*
(b) *In some basis of V, the endomorphism u is represented by a block-diagonal matrix in which every diagonal block has the form $R_\delta(r)^n$ for some irreducible monic polynomial r and some positive integer n. We call such a matrix a (p,q)-**reduced canonical form** of u.*

It is easily seen that a (p,q)-reduced canonical form is unique up to a permutation of the diagonal blocks.

Before we prove Proposition 4.4, we need the corresponding special case where both polynomials p and q are split over $\mathbb{F}$: this result will be obtained by following a similar method as for the study of (p,q)-differences.

Proposition 4.5. *Let p and q be split monic polynomials with degree 2 over $\mathbb{F}$ such that $p(0)q(0) \neq 0$, and set $\delta := p(0)q(0)^{-1}$. Let u be an endomorphism of a finite-dimensional vector space V and assume that u is a q-regular (p,q)-quotient. Then, each invariant factor of u has the form $R_\delta(r)$ for some monic polynomial r.*

The proof requires the following basic lemma:

Lemma 4.6. *Let $r \in \mathbb{F}[t]$ be a monic polynomial with degree $n>0$, and δ be a nonzero scalar. Then,*

$$\begin{bmatrix} 0_n & -\delta I_n \\ I_n & C(r) \end{bmatrix} \simeq C\big(R_\delta(r)\big).$$

Before we give the proof, we recall some known results on palindromials. Let $\delta \in \mathbb{F} \setminus \{0\}$. Given a non-negative integer m, a $(2m,\delta)$-**palindromial** is a polynomial $R(t)=\sum_{k=0}^{2m} a_k t^k$ in $\mathbb{F}_{2m}[t]$ such that $R(t)=t^{2m}\delta^{-m}R(\delta/t)$ or, in other words, $a_{2m-k}=\delta^{k-m}a_k$ for all $k \in [\![0,2m]\!]$. The $(2m,\delta)$-palindromials obviously constitute a linear subspace $P_{2m,\delta}(\mathbb{F})$ of $\mathbb{F}_{2m}[t]$ with dimension $m+1$, and the mapping

$$U \mapsto t^m U(t+\delta t^{-1})$$

is a linear injection from $\mathbb{F}_m[t]$ into $P_{2m,\delta}(\mathbb{F})$. Hence, because of the dimension of the source and target spaces we get that this map is a linear isomorphism.

Finally, given a positive integer m, every polynomial $R \in \mathbb{F}_{2m}[t]$ splits (uniquely) into $U+V$ for some $(2m,\delta)$-palindromial U and some $(2m-2,\delta)$-palindromial V. Indeed:

- We see that $\dim P_{2m,\delta}(\mathbb{F})+\dim P_{2m-2,\delta}(\mathbb{F}) = (m+1)+m = \dim \mathbb{F}_{2m}[t]$.
- On the other hand we have $P_{2m,\delta}(\mathbb{F}) \cap P_{2m-2,\delta}(\mathbb{F}) = \{0\}$: indeed, if $\sum_{k=0}^{2m} a_k t^k$ is both a $(2m,\delta)$-palindromial and a $(2m-2,\delta)$-palindromial, then, with the convention that $a_k = 0$ for every integer $k \in \mathbb{Z} \smallsetminus \{0,\dots,2m\}$ we see that $a_k = \delta^{m-k} a_{2m-k}$ and $a_k = \delta^{m-1-k} a_{2(m-1)-k}$ for all $k \in \mathbb{Z}$, which shows that $a_k = \delta^{-1} a_{k-2}$ for all $k \in \mathbb{Z}$. Since $(a_k)_{k\in\mathbb{Z}}$ ultimately vanishes, we deduce that $a_k = 0$ for all $k \in \mathbb{Z}$.

It follows that every polynomial of $\mathbb{F}_{2m}[t]$ has a (unique) splitting into

$$t^m P(t+\delta t^{-1}) + t^{m-1} Q(t+\delta t^{-1})$$

for some polynomials P and Q with $\deg P \leq m$ and $\deg Q \leq m-1$.

With this result in mind, we can now prove the above lemma.

Proof of Lemma 4.6. Set

$$N := \begin{bmatrix} 0_n & -\delta I_n \\ I_n & C(r) \end{bmatrix}.$$

By a straightforward computation, one checks that N is invertible and that

$$\delta N^{-1} = \begin{bmatrix} C(r) & \delta I_n \\ -I_n & 0_n \end{bmatrix},$$

whence

$$N + \delta N^{-1} = \begin{bmatrix} C(r) & 0_n \\ 0_n & C(r) \end{bmatrix}.$$

Hence, for every polynomial $P \in \mathbb{F}[t]$, we see that

$$P(N+\delta N^{-1}) = \begin{bmatrix} P\big(C(r)\big) & 0_n \\ 0_n & P\big(C(r)\big) \end{bmatrix}$$

and

$$NP(N+\delta N^{-1}) = \begin{bmatrix} 0_n & -\delta P\big(C(r)\big) \\ P\big(C(r)\big) & C(r)P\big(C(r)\big) \end{bmatrix}.$$

In particular, $R_\delta(r)$ annihilates N; note that this polynomial is monic with degree $2n$.

Let $u(t) \in \mathbb{F}[t]$ annihilate N with $\deg u(t) < 2n$. Then, as we have seen before the start of the proof, $u(t) = t^n P(t+\delta t^{-1}) + t^{n-1} Q(t+\delta t^{-1})$ for some pair (P,Q) of polynomials such that $\deg P \leq n$ and $\deg Q \leq n-1$. Since $\deg u(t) < 2n$ we must have $\deg P < n$. Since N is invertible, we have

$$NP(N+\delta N^{-1}) + Q(N+\delta N^{-1}) = 0.$$

By looking at the upper-left and lower-left n-by-n blocks in this identity, we get $P\big(C(r)\big) = 0$ and $Q\big(C(r)\big) = 0$, and hence r divides P and Q. Since $\deg P < n$ and $\deg Q < n$ we obtain $P = 0 = Q$, whence $u = 0$.

We conclude that $R_\delta(r)$ is the minimal polynomial of N, and since this polynomial is of degree $2n$ we conclude that N is similar to the companion matrix of $R_\delta(r)$. $\square$

Corollary 4.7. *Let N be an arbitrary matrix of $\mathrm{M}_n(\mathbb{F})$, and δ be a nonzero scalar. Denote by $r_1, \dots, r_a$ the invariant factors of N. Then, the invariant factors of*

$$K(N) := \begin{bmatrix} 0_n & -\delta I_n \\ I_n & N \end{bmatrix}$$

are $R_\delta(r_1), \dots, R_\delta(r_a)$.

Proof. We note that the similarity class of $K(N)$ depends only on that of N: indeed, for all $P \in \mathrm{GL}_n(\mathbb{K})$, the invertible matrix $Q := P \oplus P$ satisfies $QK(N)Q^{-1} = K(PNP^{-1})$. Hence,

$$K(N) \simeq K\big(C(r_1) \oplus \cdots \oplus C(r_a)\big).$$

By permuting the basis vectors, we find

$$K\big(C(r_1) \oplus \cdots \oplus C(r_a)\big) \simeq K\big(C(r_1)\big) \oplus \cdots \oplus K\big(C(r_a)\big).$$

Hence, by Lemma 4.6, we conclude that

$$K(N) \simeq C\big(R_\delta(r_1)\big) \oplus \cdots \oplus C\big(R_\delta(r_a)\big).$$

Finally, by the results of Sect. 4.2, we see that $R_\delta(r_{i+1})$ divides $R_\delta(r_i)$ for all $i \in [\![1, a-1]\!]$. Therefore, the monic polynomials $R_\delta(r_1), \dots, R_\delta(r_a)$ are the invariant factors of $K(N)$. $\square$

Proof of Proposition 4.5. Let a and b be automorphisms of V that satisfy $p(a) = q(b) = 0$ and $u = ab^{-1}$. Denote by x (respectively, by y) an eigenvalue of a (respectively, of b) with maximal geometric multiplicity, and split $p(t) = (t-x)(t-x')$ and $q(t) = (t-y)(t-y')$.

We claim that

$$\dim \operatorname{Ker}(a - x\,\mathrm{id}_V) \geq \frac{n}{2}\cdot$$

Indeed, since $p(a) = 0$ we have $\operatorname{Im}(a - x'\,\mathrm{id}_V) \subset \operatorname{Ker}(a - x\,\mathrm{id}_V)$, which yields $\dim \operatorname{Ker}(a - x\,\mathrm{id}_V) + \dim \operatorname{Ker}(a - x'\,\mathrm{id}_V) \geq n$. Since $\dim \operatorname{Ker}(a - x\,\mathrm{id}_V) \geq \dim \operatorname{Ker}(a - x'\,\mathrm{id}_V)$, the claimed inequality follows. Likewise, $\dim \operatorname{Ker}(b - y\,\mathrm{id}_V) \geq \frac{n}{2}\cdot$

Since u is q-regular with respect to (p, q), any eigenspace of a is linearly disjoint from any eigenspace of b: indeed if we had a common eigenvector of a and b, with corresponding eigenvalues x_i and y_j, then this vector would be an eigenvector of u with corresponding eigenvalue $x_i y_j^{-1}$, thereby contradicting the assumption that u has no eigenvalue in $\operatorname{Root}(p)\operatorname{Root}(q)^{-1}$. In particular, $\operatorname{Ker}(a - x\mathrm{id}_V) \cap \operatorname{Ker}(b - y\,\mathrm{id}_V) = \{0\}$. It follows that $\dim \operatorname{Ker}(a - x\,\mathrm{id}_V) = \frac{n}{2} = \dim \operatorname{Ker}(b - y\,\mathrm{id}_V)$, that n is even and that $V = \operatorname{Ker}(a - x\mathrm{id}_V) \oplus \operatorname{Ker}(b - y\,\mathrm{id}_V)$. Next, we deduce that $\frac{n}{2} = \dim \operatorname{Im}(a - x\mathrm{id}_V)$ and $\dim \operatorname{Ker}(a - x'\mathrm{id}_V) \leq \frac{n}{2}$ by choice of x. However, $\operatorname{Im}(a - x\mathrm{id}_V) \subset \operatorname{Ker}(a - x'\mathrm{id}_V)$, and hence it follows that $\operatorname{Im}(a - x\mathrm{id}_V) = \operatorname{Ker}(a - x'\mathrm{id}_V)$. Likewise, $\operatorname{Im}(b - y\mathrm{id}_V) = \operatorname{Ker}(b - y'\mathrm{id}_V)$, and it follows that x' has geometric multiplicity $\frac{n}{2}$ with respect to a, and ditto for y'

with respect to b. In turn, this shows that $\operatorname{Im}(a-x'\mathrm{id}_V)=\operatorname{Ker}(a-x\mathrm{id}_V)$ and $\operatorname{Im}(b-y'\mathrm{id}_V)=\operatorname{Ker}(b-y\mathrm{id}_V)$, and any eigenspace of a is a complementary subspace of any eigenspace of b.

Let us write $s:=\frac{n}{2}$ and choose a basis $(e_1,\dots,e_s)$ of $\operatorname{Ker}(b-y\mathrm{id}_V)$. Then, we have $V=\operatorname{Ker}(b-y\mathrm{id}_V)\oplus\operatorname{Ker}(a-x\mathrm{id}_V)$, whence $(e_{s+1},\dots,e_n):=\bigl(y^{-1}(a-x\mathrm{id}_V)(e_1),\dots,y^{-1}(a-x\mathrm{id}_V)(e_s)\bigr)$ is a basis of $\operatorname{Im}(a-x\mathrm{id}_V)=\operatorname{Ker}(a-x'\mathrm{id}_V)$. Since $\operatorname{Ker}(b-y\mathrm{id}_V)\oplus\operatorname{Ker}(a-x'\mathrm{id}_V)=V$, we deduce that $\mathbf{B}:=(e_1,\dots,e_n)$ is a basis of V. Obviously

$$\mathrm{M}_{\mathbf{B}}(a)=\begin{bmatrix}xI_s & 0\\ yI_s & x'I_s\end{bmatrix}.$$

On the other hand, since $\operatorname{Ker}(b-y\mathrm{id}_V)=\operatorname{Im}(b-y'\mathrm{id}_V)$, we find

$$\mathrm{M}_{\mathbf{B}}(b^{-1})=\begin{bmatrix}y^{-1}I_s & N\\ 0 & (y')^{-1}I_s\end{bmatrix}\quad\text{for some matrix } N\in\mathrm{M}_s(\mathbb{F}).$$

Hence,

$$\mathrm{M}_{\mathbf{B}}(u)=\begin{bmatrix}xy^{-1}I_s & xN\\ I_s & yN+x'(y')^{-1}I_s\end{bmatrix}.$$

Setting

$$P:=\begin{bmatrix}I_s & -xy^{-1}I_s\\ 0 & I_s\end{bmatrix},$$

we obtain

$$P\,\mathrm{M}_{\mathbf{B}}(u)P^{-1}=\begin{bmatrix}0 & -(xx')(yy')^{-1}I_s\\ I_s & N'\end{bmatrix}$$

for some matrix $N'\in\mathrm{M}_s(\mathbb{F})$. Since $\delta=p(0)q(0)^{-1}=(xx')(yy')^{-1}$, the claimed result is then readily deduced from Corollary 4.7. □

Proof of Proposition 4.4. We start with point (a). Let us extend the scalar field to $\overline{\mathbb{F}}$. The corresponding extension $\overline{u}$ of u is still a (p,q)-quotient. Hence, by Corollary 4.7 its invariant factors are $R_\delta(p_1),\dots,R_\delta(p_r)$ for some monic polynomials $p_1,\dots,p_r$ of $\overline{\mathbb{F}}[t]$ such that p_{i+1} divides p_i for all $i\in[\![1,r-1]\!]$.

Yet, the invariant factors of $\overline{u}$ are known to be the ones of u. Finally, given a monic polynomial $h\in\overline{\mathbb{F}}[t]$ (with degree N) such that $R_\delta(h)\in\mathbb{F}[t]$, we obtain by downward induction that all the coefficients of h belong to $\mathbb{F}$: indeed, if we write $h(t)=t^N-\sum_{i=0}^{N-1}\alpha_i\,t^i$ and we know that $\alpha_{N-1},\dots,\alpha_{k+1}$ all belong to $\mathbb{F}$ for some $k\in[\![0,N-1]\!]$, then $\sum_{i=0}^{k}\alpha_i\,t^N(t+\delta t^{-1})^i=t^N(t+\delta t^{-1})^N-\sum_{i=k+1}^{N-1}\alpha_i\,t^N(t+\delta t^{-1})^i-R_\delta(h)$ belongs to $\mathbb{F}[t]$, and by considering the coefficient on t^{N+k}, we gather that $\alpha_k\in\mathbb{F}$. It follows that $p_1,\dots,p_r$ all belong to $\mathbb{F}[t]$, which completes the proof of statement (a).

From point (a), we easily derive point (b): indeed, consider an invariant factor $R_\delta(r)$ of u with some monic polynomial $r\in\mathbb{F}[t]$. Then, we split $r=r_1^{n_1}\cdots r_k^{n_k}$ where $r_1,\dots,r_k$ are pairwise distinct irreducible monic polynomials of $\mathbb{F}[t]$, and $n_1,\dots,n_k$ are positive integers. By a previous remark (see

Sect. 4.2), the monic polynomials $R_\delta(r_1^{n_1}),\dots,R_\delta(r_k^{n_k})$ are pairwise coprime and their product equals $R_\delta(r)$, whence

$$C\big(R_\delta(r)\big)\simeq C\big(R_\delta(r_1^{n_1})\big)\oplus\cdots\oplus C\big(R_\delta(r_k^{n_k})\big).$$

Using point (a), we deduce that statement (b) holds true. □

An additional definition will now be useful:

Definition 7. Let p and q be monic polynomials with degree 2 in $\mathbb{F}[t]$ such that $p(0)q(0)\neq 0$. Set $\delta:=p(0)q(0)^{-1}$. Let r be an irreducible monic polynomial of $\mathbb{F}[t]$, and set $\mathbb{L}:=\mathbb{F}[t]/(r)$. Denote by x the class of t in $\mathbb{L}$. We say that r has:

- **Type** 1 **with respect to** (p,q) if $R_\delta(r)$ has no root in $\operatorname{Root}(p)\operatorname{Root}(q)^{-1}$ and the norm of the quaternion algebra $\mathcal{W}\big(p,q,q(0)x\big)_{\mathbb{L}}$ is isotropic.
- **Type** 2 **with respect to** (p,q) if $R_\delta(r)$ has no root in $\operatorname{Root}(p)\operatorname{Root}(q)^{-1}$ and the norm of the quaternion algebra $\mathcal{W}\big(p,q,q(0)x\big)_{\mathbb{L}}$ is non-isotropic.

First of all, we use the structural results on $\mathcal{W}(p,q,x)_R$ to obtain various (p,q)-quotients. Our first result is actually not restricted to q-regular (p,q)-quotients and will be used later in our study.

Lemma 4.8. (Duplication Lemma). *Let p and q be monic polynomials of $\mathbb{F}[t]$ with degree 2 such that $p(0)q(0)\neq 0$, and set $\delta:=p(0)q(0)^{-1}$. Let r be a nonconstant monic polynomial of $\mathbb{F}[t]$. Then, $C\big(R_\delta(r)\big)\oplus C\big(R_\delta(r)\big)$ is a (p,q)-quotient.*

Proof. Denote by d the degree of r. We work with the commutative $\mathbb{F}$-algebra $R:=\mathbb{F}[C(r)]$, which is isomorphic to the quotient ring $\mathbb{F}[t]/(r)$, and with the element $x:=C(r)$. Then, we consider the endomorphisms $a:X\mapsto AX$ and $b:X\mapsto BX$ of $\mathcal{W}(p,q,q(0)x)_R$. Since $p(A)=0$ and $q(B)=0$, we get $p(a)=0$ and $q(b)=0$. Moreover, since $B^{-1}=q(0)^{-1}(\operatorname{tr}q)I_4-q(0)^{-1}B$, we have $AB^{-1}=q(0)^{-1}(\operatorname{tr}q)A-q(0)^{-1}AB$ and hence (B,A,I_4,AB^{-1}) is a basis $\mathbf{B}$ of the free R-module $\mathcal{W}(p,q,q(0)x)_R$.

Denote by A' and B' the respective matrices of a and b in $\mathbf{B}$. Using identity (5) from page 11, we find $(AB^{-1})^2=-\delta I_4+x\,(AB^{-1})$, and it easily follows that

$$A'B'^{-1}=\begin{bmatrix}0 & -\delta\,1_R & 0 & 0\\ 1_R & x & 0 & 0\\ 0 & 0 & 0 & -\delta\,1_R\\ 0 & 0 & 1_R & x\end{bmatrix}.$$

Therefore, $A'B'^{-1}$, seen as a matrix of $\mathrm{M}_{4d}(\mathbb{F})$, is similar to $C\big(R_\delta(r)\big)\oplus C\big(R_\delta(r)\big)$ by Lemma 4.6. Since $p(A')=0$ and $q(B')=0$, the conclusion follows. □

Our next result deals with certain companion matrices that are associated with irreducible polynomials with Type 1 with respect to (p,q).

Lemma 4.9. *Let p and q be monic polynomials of $\mathbb{F}[t]$ with degree 2 such that $p(0)q(0) \neq 0$, and set $\delta := p(0)q(0)^{-1}$. Let r be an irreducible monic polynomial of $\mathbb{F}[t]$ of Type 1 with respect to (p,q). Then, for all $n \in \mathbb{N}^*$, the companion matrix $C\big(R_\delta(r^n)\big)$ is a (p,q)-quotient.*

Proof. Denote by k the degree of r. Let $n \in \mathbb{N}^*$. Set $R := \mathbb{F}[C(r^n)]$, seen as a subalgebra of $\mathrm{M}_{nd}(\mathbb{F})$, and set $x := C(r^n)$. The $\mathbb{F}$-algebra R is isomorphic to $\mathbb{F}[t]/(r^n)$. By Proposition 2.6, it follows that $\mathcal{W}(p,q,q(0)x)_R$ is isomorphic to $\mathrm{M}_2(R)$. We choose an isomorphism $\varphi : \mathcal{W}(p,q,q(0)x)_R \xrightarrow{\simeq} \mathrm{M}_2(R)$, and we set $a := \varphi(A)$ and $b := \varphi(B)$. Note that $p(a) = q(b) = 0$, whereas $d := ab^{-1}$ satisfies $q(0)d + p(0)d^{-1} = q(0)x\, I_2$, whence $d^2 = xd - \delta I_2$.

Denote by $\mathbb{L}$ the residue field of R. The endomorphism $X \mapsto dX$ of R^2 induces an endomorphism $\overline{d}$ of the $\mathbb{L}$-vector space $\mathbb{L}^2$. Since (I_2, a, b, ab^{-1}) is a basis of the R-module $\mathrm{M}_2(R)$, the endomorphism $\overline{d}$ is not a scalar multiple of the identity of $\mathbb{L}^2$. This yields a vector e of $\mathbb{L}^2$ such that $\big(e, \overline{d}(e)\big)$ is a basis of $\mathbb{L}^2$. Lifting e to a vector E of R^2, we deduce that (E, dE) is a basis of the R-module R^2. Hence, composing φ with an additional interior automorphism of the R-algebra $\mathrm{M}_2(R)$, we see that no generality is lost in assuming that the first column of d reads $\begin{bmatrix} 0_R \\ 1_R \end{bmatrix}$. Then, the equality $d^2 = xd - \delta I_2$ yields

$$d = \begin{bmatrix} 0 & -\delta 1_R \\ 1_R & x \end{bmatrix}.$$

It follows that the matrix $\begin{bmatrix} 0 & -\delta I_{nk} \\ I_{nk} & C(r^n) \end{bmatrix}$ of $\mathrm{M}_{2nk}(\mathbb{F})$ is a (p,q)-quotient. By Lemma 4.6, this matrix is similar to $C\big(R_\delta(r^n)\big)$, which completes the proof. □

Combining Lemma 4.8 with Lemma 4.9, we conclude that the implication (iii) ⇒ (i) in the following theorem holds true.

Theorem 4.10. (Classification of q-regular (p,q)-quotients) *Let p and q be monic polynomials of degree 2 in $\mathbb{F}[t]$ such that $p(0)q(0) \neq 0$. Let u be an endomorphism of a finite-dimensional vector space V over $\mathbb{F}$. Assume that u is q-regular with respect to (p,q) and set $\delta := p(0)q(0)^{-1}$. The following conditions are equivalent:*

- (i) *The endomorphism u is a (p,q)-quotient.*
- (ii) *The invariant factors of u read $R_\delta(p_1), \dots, R_\delta(p_{2n-1}), R_\delta(p_{2n}) \dots$ where, for every irreducible monic polynomial $r \in \mathbb{F}[t]$ that has Type 2 with respect to (p,q) and every positive integer n, the polynomials p_{2n-1} and p_{2n} have the same valuation with respect to r.*
- (iii) *There is a basis of V in which u is represented by a block-diagonal matrix where every diagonal block equals either $C\big(R_\delta(r^n)\big)$ for some irreducible monic polynomial $r \in \mathbb{F}[t]$ of Type 1 with respect to (p,q) and some $n \in \mathbb{N}^*$, or $C\big(R_\delta(r^n)\big) \oplus C\big(R_\delta(r^n)\big)$ for some irreducible monic polynomial $r \in \mathbb{F}[t]$ and some $n \in \mathbb{N}^*$.*

Note that this result, combined with the observation that $C\big(R_\delta(r^n)\big)$ is q-regular with respect to (p,q) for every monic polynomial $r \in \mathbb{F}[t]$ such that $R_\delta(r)$ has no root in $\operatorname{Root}(p)\operatorname{Root}(q)^{-1}$, yields the classification of indecomposable q-regular (p,q)-quotients as given in Table 11. Moreover, by using the same method as in the last part of the proof of Proposition 4.4, it is easily seen that condition (ii) is equivalent to condition (iii).

In order to conclude on Theorem 4.10, it only remains to prove that condition (i) implies condition (ii), which we shall now do thanks to the structural results on $\mathcal{W}(p,q,x)_R$.

Proof. (Proof of the implication (i) $\Rightarrow$ (ii)) Let us assume that u is a (p,q)-quotient. Let r be an irreducible monic polynomial of $\mathbb{F}[t]$ with Type 2 with respect to (p,q), and let $n \in \mathbb{N}^*$. All we need is to prove that, in the canonical form of u from Proposition 4.4, the number m of diagonal cells that equal $C\big(R_\delta(r)^n\big)$ is even.

Let us choose automorphisms a and b of V such that $u = ab^{-1}$ and $p(a) = q(b) = 0$. By the Commutation Lemma (i.e. Lemma 4.2), we know that a and b commute with $v := u + \delta u^{-1}$, and hence all three endomorphisms a, b, u yield endomorphisms $\overline{a}$, $\overline{b}$ and $\overline{u}$ of the vector space

$$E := \operatorname{Ker}\big(r^n(v)\big)/\operatorname{Ker}\big(r^{n-1}(v)\big) = \operatorname{Ker}(R_\delta(r^n)(u))/\operatorname{Ker}(R_\delta(r^{n-1})(u))$$

such that $\overline{u} = \overline{a}\overline{b}^{-1}$, and r annihilates $\overline{v} := \overline{u} + \delta\overline{u}^{-1}$. Again, $\overline{a}$ and $\overline{b}$ commute with $\overline{v}$, and hence they are endomorphisms of the $\mathbb{F}[\overline{v}]$-module E. Since r is irreducible, we have $\mathbb{F}[\overline{v}] \simeq \mathbb{F}[t]/(r)$, and $\mathbb{L} := \mathbb{F}[\overline{v}]$ is a field. We shall write $y := \overline{v}$, which we see as an element of $\mathbb{L}$. Using the structure of $\mathbb{L}$-vector space, we can write $\overline{u} + \delta\overline{u}^{-1} = y\,\mathrm{id}_E$; by combining this with $p(\overline{a}) = q(\overline{b}) = 0$, we deduce that $\overline{a}$ and $\overline{b}$ yield a representation of the $\mathbb{L}$-algebra $\mathcal{W}\big(p,q,q(0)y\big)_{\mathbb{L}}$ on the $\mathbb{L}$-vector space E.

Besides, $2m\deg(r)$ is the dimension of the $\mathbb{F}$-vector space E, and hence $2m$ is the dimension of the $\mathbb{L}$-vector space E.

By Proposition 2.4, the algebra $\mathcal{W}\big(p,q,q(0)y\big)_{\mathbb{L}}$ is a 4-dimensional skew-field over $\mathbb{L}$, whence the $\mathbb{L}$-vector space E is isomorphic to some power of $\mathcal{W}\big(p,q,q(0)y\big)_{\mathbb{L}}$ and it follows that its dimension is a multiple of 4. Therefore, m is a multiple of 2, which completes the proof. $\square$

This completes the classification of q-regular (p,q)-quotients.

Date availability statement The author acknowledges that the present manuscript has no associated data.

Declarations

Conflict of interest The author has no conflicts of interest to declare that are relevant to the content of this article.

References

[1] Ballantine, C.S.: Products of idempotent matrices. Linear Algebra Appl. **19**, 81–86 (1967)

[2] Botha, J.D.: Product of two unipotent matrices of index 2. Linear Algebra Appl. **433**, 1447–1451 (2010)

[3] Botha, J.D.: Products of idempotent and square-zero matrices. Linear Algebra Appl. **497**, 116–133 (2016)

[4] Botha, J.D.: Sums of two square-zero matrices over an arbitrary field. Linear Algebra Appl. **436**, 516–524 (2012)

[5] Bünger, F., Knüppel, F., Nielsen, K.: The product of two quadratic matrices. Linear Algebra Appl. **331**, 31–41 (2001)

[6] Djoković, D.Ž: Products of two involutions. Arch. Math. **18**, 582–584 (1967)

[7] de Seguins Pazzis, C.: A note on sums of three square-zero matrices. Linear Multilinear Algebra **65**, 787–807 (2017)

[8] de Seguins Pazzis, C.: Invitation Aux Formes Quadratiques. Calvage & Mounet, Paris (2011)

[9] de Seguins Pazzis, C.: On linear combinations of two idempotent matrices over an arbitrary field. Linear Algebra Appl. **433**, 625–636 (2010)

[10] de Seguins Pazzis, C.: Sums of two triangularizable quadratic matrices over an arbitrary field. Linear Algebra Appl. **436**, 3293–3302 (2012)

[11] Hartwig, R.E., Putcha, M.S.: When is a matrix a difference of two idempotents? Linear Multilinear Algebra **26**, 267–277 (1990)

[12] Hoffman, F., Paige, E.C.: Products of two involutions in the general linear group. Indiana Univ. Math. J. **20**, 1017–1020 (1971)

[13] Novak, N.: Products of square-zero operators. Linear Algebra Appl. **339**, 10–17 (2008)

[14] Wang, J.-H.: Factorization of matrices into quadratic ones II. Linear Algebra Appl. **231**, 111–152 (1995)

[15] Wang, J.-H.: Factorization of matrices into quadratic ones III. Linear Algebra Appl. **240**, 21–39 (1996)

[16] Wang, J.-H.: Sums and products of two quadratic matrices. Linear Algebra Appl. **129–1**, 127–149 (1995)

[17] Wang, J.-H., Wu, P.Y.: Products of unipotent matrices with index 2. Linear Algebra Appl. **149**, 111–123 (1991)

[18] Wang, J.-H., Wu, P.Y.: Sums of square zero operators. Stud. Math. **99–2**, 115–127 (1991)

[19] Wonenburger, M.J.: Transformations which are products of two involutions. J. Math. Mech. **16**, 327–338 (1966)

Clément de Seguins Pazzis
Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, avenue des États-Unis
78035 Versailles cedex
France
e-mail: dsp.prof@gmail.com

Received: August 4, 2021.
Accepted: August 17, 2022.