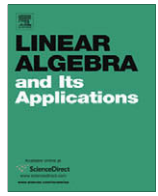
Linear Algebra and its Applications 433 (2010) 625–636

Contents lists available at ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa



On linear combinations of two idempotent matrices over an arbitrary field

Clément de Seguins Pazzis

Lycée Privé Sainte-Geneviève, 2, rue de l'École des Postes, 78029 Versailles Cedex, France

ARTICLE INFO

Article history:
Received 1 August 2009
Accepted 18 March 2010
Available online 10 April 2010

Submitted by H. Schneider

AMS classification:
15A24
15A23

Keywords:
Matrices
Idempotents
Decomposition
Elementary factors
Jordan reduction

ABSTRACT

Given an arbitrary field $\mathbb{K}$ and non-zero scalars α and β, we give necessary and sufficient conditions for a matrix $A \in M_n(\mathbb{K})$ to be a linear combination of two idempotents with coefficients α and β. This extends results previously obtained by Hartwig and Putcha in two ways: the field $\mathbb{K}$ considered here is arbitrary (possibly of characteristic 2), and the case $\alpha \neq \pm\beta$ is taken into account.

1. Introduction

In this article, $\mathbb{K}$ will denote an arbitrary field, $\mathrm{car}(\mathbb{K})$ its characteristic, and n a positive integer. We choose an algebraic closure of $\mathbb{K}$ which we denote by $\overline{\mathbb{K}}$. We let E denote a vector space of dimension n over $\mathbb{K}$, and $\mathrm{End}(E)$ denote the algebra of endomorphisms of E. We choose two scalars α and β in $\mathbb{K}^*$.

An idempotent matrix of $M_n(\mathbb{K})$ is a matrix P verifying $P^2 = P$, i.e. idempotent matrices represent projectors in finite-dimensional vector spaces. Of course, any matrix similar to an idempotent is itself an idempotent.

Definition 1. Let $\mathcal{A}$ be a $\mathbb{K}$-algebra. An element $x \in \mathcal{A}$ will be called an (α, β)-**composite** when there are two idempotents p and q such that $x = \alpha \cdot p + \beta \cdot q$.

E-mail address: dsp.prof@gmail.com

0024-3795/$ - see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2010.03.023

The purpose of this paper is to give necessary and sufficient conditions on a matrix $A \in M_n(\mathbb{K})$ to be an (α, β)-composite, both in terms of Jordan reduction and elementary factors. This will generalize the two cases $(\alpha, \beta) = (1, -1)$ and $(\alpha, \beta) = (1, 1)$ already discussed in [3] when the field $\mathbb{K}$ is algebraically closed and $\mathrm{car}(\mathbb{K}) \neq 2$.

Remark 1

(i) Any matrix similar to an (α, β)-composite is an (α, β)-composite itself.
(ii) If $A \in M_n(\mathbb{K})$ and $B \in M_p(\mathbb{K})$ are (α, β)-composites, then the block-diagonal matrix $\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$ is clearly an (α, β)-composite itself.
(iii) The matrix $A \in M_n(\mathbb{K})$ is an (α, β)-composite iff $A - \alpha \cdot I_n$ is a $(-\alpha, \beta)$-composite.

Notation 2. When A is a matrix of $M_n(\mathbb{K})$, $\lambda \in \overline{\mathbb{K}}$ and $k \in \mathbb{N}^*$, we denote by

$$n_k(A, \lambda) := \dim \mathrm{Ker}(A - \lambda \cdot I_n)^k - \dim \mathrm{Ker}(A - \lambda \cdot I_n)^{k-1},$$

i.e. $n_k(A, \lambda)$ is the number of blocks of size greater or equal to k for the eigenvalue λ in the Jordan reduction of A (in particular, it is zero when λ is not an eigenvalue of A). We extend this notation to an endomorphism of E provided $\lambda \in \mathbb{K}$. We also denote by $j_k(A, \lambda)$ the number of size k for the eigenvalue λ in the Jordan reduction of A.

Definition 3. Two sequences $(u_k)_{k \geqslant 1}$ and $(v_k)_{k \geqslant 1}$ are said to be **intertwined** when:

$$\forall k \in \mathbb{N}^*, \quad v_k \leqslant u_{k+1} \quad \text{and} \quad u_k \leqslant v_{k+1}.$$

Notation 4. Let $u \in \mathrm{End}(E)$ and Λ be a subset of $\mathbb{K}$. The minimal polynomial of u splits as $\mu_u(X) = P(X)\,Q(X)$, where P is a monic polynomial with all its roots in Λ, and Q is monic and has no root in Λ. We then set

$$u_\Lambda := u_{|\mathrm{Ker}P(u)} \in \mathrm{End}(\mathrm{Ker}P(u)) \quad \text{and} \quad u_{-\Lambda} := u_{|\mathrm{Ker}Q(u)} \in \mathrm{End}(\mathrm{Ker}Q(u)).$$

Thus u_Λ is triangularizable with all eigenvalues in Λ, whereas $u_{-\Lambda}$ has no eigenvalue in Λ. The kernel decomposition theorem ensures that $u = u_\Lambda \oplus u_{-\Lambda}$. Finally, with $n = \dim E$, the map u_Λ is an endomorphism of $\bigoplus_{\lambda \in \Lambda} \mathrm{Ker}(u - \lambda \cdot \mathrm{id}_E)^n$.

We are now ready to state our main theorems. We will start by generalizations of the Hartwig and Putcha results on differences of idempotents:

Theorem 1. *Assume* $\mathrm{car}(\mathbb{K}) \neq 2$ *and let* $A \in M_n(\mathbb{K})$. *Then* A *is an* $(\alpha, -\alpha)$*-composite iff all the following conditions hold*:

(*i*) *The sequences* $(n_k(A, \alpha))_{k \geqslant 1}$ *and* $(n_k(A, -\alpha))_{k \geqslant 1}$ *are intertwined*.
(*ii*) $\forall \lambda \in \overline{\mathbb{K}} \setminus \{0, \alpha, -\alpha\}$, $\forall k \in \mathbb{N}^*$, $j_k(A, \lambda) = j_k(A, -\lambda)$.

Theorem 2. *Assume* $\mathrm{car}(\mathbb{K}) \neq 2$ *and let* u *be an endomorphism of* E. *Then* u *is an* $(\alpha, -\alpha)$*-composite iff all the following conditions hold*:

(*i*) *The sequences* $(n_k(u, \alpha))_{k \geqslant 1}$ *and* $(n_k(u, -\alpha))_{k \geqslant 1}$ *are intertwined*.
(*ii*) *The elementary factors of* $u_{-\{0,\alpha,-\alpha\}}$ *are all* **even** *polynomials* (*i.e. polynomials of* X^2).

Using Remark 1.(iii), the previous theorems lead to a characterization of (α, α)-composites when $\mathrm{car}(\mathbb{K}) \neq 2$.

Theorem 3. *Assume* $\mathrm{car}(\mathbb{K}) \neq 2$ *and let* $A \in M_n(\mathbb{K})$. *Then* A *is an* (α, α)*-composite iff all the following conditions hold*:

(*i*) *The sequences* $(n_k(A,0))_{k\geqslant 1}$ *and* $(n_k(A,2\alpha))_{k\geqslant 1}$ *are intertwined*.
(*ii*) $\forall \lambda \in \overline{\mathbb{K}} \setminus \{0,\alpha,2\alpha\},\ \forall k \in \mathbb{N}^*,\ j_k(A,\lambda) = j_k(A,2\alpha-\lambda)$.

Theorem 4. *Assume* $\mathrm{car}(\mathbb{K}) \neq 2$ *and let* $u \in \mathrm{End}(E)$. *Then* u *is an* (α,α)*-composite iff both of the following conditions hold*:

(*i*) *The sequences* $(n_k(u,0))_{k\geqslant 1}$ *and* $(n_k(u,2\alpha))_{k\geqslant 1}$ *are intertwined*.
(*ii*) *The elementary factors of* $u_{-\{0,\alpha,2\alpha\}}$ *are polynomials of* $(X-\alpha)^2$.

The case $\mathrm{car}(\mathbb{K}) = 2$ works rather differently in terms of Jordan reduction:

Theorem 5. *Assume* $\mathrm{car}(\mathbb{K}) = 2$ *and let* $A \in M_n(\mathbb{K})$. *Then* A *is an* $(\alpha,-\alpha)$*-composite iff for every* $\lambda \in \overline{\mathbb{K}} \setminus \{0,\alpha\}$, *all blocks in the Jordan reduction of* A *with respect to* λ *have an even size*.

Theorem 6. *Assume* $\mathrm{car}(\mathbb{K}) = 2$ *and let* $u \in \mathrm{End}(E)$. *Then* u *is an* $(\alpha,-\alpha)$*-composite iff the elementary factors of* $u_{-\{0,\alpha\}}$ *are even polynomials*.

The remaining cases are handled by our two last theorems:

Theorem 7. *Let* $A \in M_n(\mathbb{K})$ *and* $(\alpha,\beta) \in (\mathbb{K}^*)^2$ *such that* $\alpha \neq \pm\beta$. *Then* A *is an* (α,β)*-composite iff all the following conditions hold*:

(*i*) *The sequences* $(n_k(A,0))_{k\geqslant 1}$ *and* $(n_k(A,\alpha+\beta))_{k\geqslant 1}$ *are intertwined*.
(*ii*) *The sequences* $(n_k(A,\alpha))_{k\geqslant 1}$ *and* $(n_k(A,\beta))_{k\geqslant 1}$ *are intertwined*.
(*iii*) $\forall \lambda \in \overline{\mathbb{K}} \setminus \{0,\alpha,\beta,\alpha+\beta\},\ \forall k \in \mathbb{N}^*,\ j_k(A,\lambda) = j_k(A,\alpha+\beta-\lambda)$.
(*iv*) *If in addition* $\mathrm{car}(\mathbb{K}) \neq 2$, *then* $\forall k \in \mathbb{N}^*,\ j_{2k+1}\left(A, \frac{\alpha+\beta}{2}\right) = 0$.

Theorem 8. *Let* $u \in \mathrm{End}(E)$ *and* $(\alpha,\beta) \in (\mathbb{K}^*)^2$ *such that* $\alpha \neq \pm\beta$. *Then* u *is an* (α,β)*-composite iff all the following conditions hold*:

(*i*) *The sequences* $(n_k(u,0))_{k\geqslant 1}$ *and* $(n_k(u,\alpha+\beta))_{k\geqslant 1}$ *are intertwined*.
(*ii*) *The sequences* $(n_k(u,\alpha))_{k\geqslant 1}$ *and* $(n_k(u,\beta))_{k\geqslant 1}$ *are intertwined*.
(*iii*) *The elementary factors of* $u_{-\{0,\alpha,\beta,\alpha+\beta\}}$ *are polynomials of* $(X-\alpha)(X-\beta)$.

Remark 2. A striking consequence of the previous theorems is that being an (α,β)-composite is invariant under extension of scalars. More precisely, given a matrix $A \in M_n(\mathbb{K})$, an extension $\mathbb{L}$ of $\mathbb{K}$ and non-zero scalars α and β in $\mathbb{K}$, the matrix A is an (α,β)-composite in $M_n(\mathbb{K})$ iff it is an (α,β)-composite in $M_n(\mathbb{L})$.

The rest of the paper is laid out as follows:

(i) In Section 3, we show how the odd-labeled theorems can be derived from the even-labeled ones, e.g. how one can deduce Theorem 1 from Theorem 2.
(ii) In Section 4, we will establish a reduction principle that will show us that we can limit ourselves to three particular cases for $u \in \mathrm{End}(E)$: the case u has no eigenvalue in $\{0,\alpha,\beta,\alpha+\beta\}$, the case u has all its eigenvalues in $\{\alpha,\beta\}$ and the case it has all its eigenvalues in $\{0,\alpha+\beta\}$.
(iii) The case u has no eigenvalue in $\{0,\alpha,\beta,\alpha+\beta\}$ is handled in Section 5 by using the reduction to a canonical form and considerations of cyclic matrices.
(iv) In Section 6, we reduce the remaining cases to the sole case $\alpha \neq \beta$ and u has all its eigenvalues in $\{\alpha,\beta\}$, and show how Theorems 2, 4, 6 and 8 can be proven if that case is solved.
(v) Finally, in Section 7, we solve the case $\alpha \neq \beta$ and u has all its eigenvalues in $\{\alpha,\beta\}$.

2. Additional notations

Similarity of two matrices A and B of $M_n(\mathbb{K})$ will be written $A \sim B$. The rank of a matrix M will be written $\mathrm{rk}(M)$, and its spectrum $\mathrm{Sp}(M)$. Given a list $(A_1, \dots, A_p)$ of square matrices, we will denote by

$$D(A_1, \dots, A_p) := \begin{bmatrix} A_1 & 0 & & 0 \\ 0 & A_2 & & \vdots \\ \vdots & & \ddots & \\ 0 & \dots & & A_p \end{bmatrix}$$

the block-diagonal matrix with diagonal blocks $A_1, \dots, A_p$.

Notation 5. Given a monic polynomial $P = X^n - a_{n-1}X^{n-1} - \cdots - a_1X - a_0$, we let

$$C(P) := \begin{bmatrix} 0 & 0 & \dots & & 0 & a_0 \\ 1 & 0 & & & 0 & a_1 \\ 0 & 1 & 0 & \dots & 0 & a_2 \\ & & \ddots & \ddots & & \vdots \\ \vdots & & & 1 & 0 & a_{n-2} \\ 0 & \dots & \dots & 0 & 1 & a_{n-1} \end{bmatrix}$$

denote its companion matrix.

Given $n \in \mathbb{N}^*$ and $\lambda \in \mathbb{K}$, we set $J_n := (\delta_{i+1,j})_{1 \leqslant i,j \leqslant n}$, i.e.

$$J_n = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & \ddots & \\ 0 & \dots & & 0 & 1 \\ 0 & \dots & & & 0 \end{bmatrix}$$

and

$$J_\lambda(n) := \lambda \cdot I_n + J_n \quad \text{(the Jordan block of size } n \text{ associated to } \lambda).$$

3. Elementary factors vs. Jordan reduction

Derivation of Theorem 1 from Theorem 2 (resp. of Theorem 3 from Theorem 4, resp. of Theorem 5 from Theorem 6, resp. of Theorem 7 from Theorem 8) can be easily obtained by using the following result and the simple remark that polynomials of $(X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + \alpha\beta$ are polynomials of $X(X - \alpha - \beta)$.

Proposition 9. *Let $A \in M_n(\mathbb{K})$ and $t \in \mathbb{K}$. The following conditions are then equivalent*:

(*i*) *The elementary factors of M are polynomials of $X(X - t)$.*
(*ii*) *For every $\lambda \in \overline{\mathbb{K}}$,*

- *if $\lambda \neq t - \lambda$, then $\forall k \in \mathbb{N}^*$, $j_k(A, \lambda) = j_k(A, t - \lambda)$;*
- *if $\lambda = t - \lambda$, then $\forall k \in \mathbb{N}$, $j_{2k+1}(A, \lambda) = 0$.*

Proof

- Assume (i). By reduction to an elementary rational canonical form, it suffices to prove condition (ii) when A is the companion matrix of some polynomial $P = Q(X(X - t))$, with $Q = (Y -$

$\lambda)^r \in \overline{\mathbb{K}}[Y]$ for some $\lambda \in \overline{\mathbb{K}}$ (remark that when Q_1 and Q_2 are mutually prime polynomials, the polynomials $Q_1(X(X-t))$ and $Q_2(X(X-t))$ are mutually prime by the Bezout identity).

- $\rightarrow$ Assume $X^2 - tX - \lambda$ has only one root u in $\overline{\mathbb{K}}$, so it can be written $(X-u)^2$, hence $A = C((X-u)^{2r})$ has only one Jordan block: this block is even-sized, corresponds to the eigenvalue u, and one has $u = t-u$: this proves that A satisfies condition (ii).
- $\rightarrow$ Assume $X^2 - tX - \lambda$ has two roots in $\overline{\mathbb{K}}$, let v denote one such root, the other one being $t-v$. One has then $v \neq t-v$ and

$$A = C\left((X-v)^N(X-(t-v))^N\right) \sim \begin{bmatrix} C((X-v)^N) & 0 \\ 0 & C((X-t+v)^N) \end{bmatrix}.$$

In this case, A has only two Jordan blocks, they have the same size and are associated respectively to v and $t-v$, so A satisfies condition (ii).

- Assume now condition (ii) holds. Let μ_A denote the minimal polynomial of A. We will first prove that μ_A is a polynomial of $X(X-t)$. Since $\delta \mapsto t-\delta$ is an involution, we can split $\mathrm{Sp}(A)$ as a disjoint union

$$\mathrm{Sp}(A) = \mathcal{B} \cup \mathcal{C} \cup \mathcal{C}',$$

where $\mathcal{B} = \{\delta \in \mathrm{Sp}(A) : \delta = t-\delta\}$ and $\delta \mapsto t-\delta$ is a bijection from $\mathcal{C}$ to $\mathcal{C}'$. For $\delta \in \mathrm{Sp}(A)$, set $r_\delta = \max\{k \in \mathbb{N}^* : j_k(A,\delta) \neq 0\}$. Then the Jordan reduction theorem shows that

$$\mu_A = \prod_{\delta \in \mathrm{Sp}(A)} (X-\delta)^{r_\delta}.$$

Condition (ii) then entails that $r_\delta = r_{t-\delta}$ for every $\delta \in \mathcal{C}$ and r_δ is even when $\delta \in \mathcal{B}$, hence we may write:

$$\begin{aligned} \mu_A &= \prod_{\delta \in \mathcal{B}} (X-\delta)^{2(r_\delta/2)} \prod_{\delta \in \mathcal{C}} (X-\delta)^{r_\delta}(X-t+\delta)^{r_\delta} \\ &= \prod_{\delta \in \mathcal{B}} (X^2 - tX + \delta^2)^{r_\delta/2} \prod_{\delta \in \mathcal{C}} \left(X^2 - tX + \delta(t-\delta)\right)^{r_\delta}, \end{aligned}$$

hence μ_A is a polynomial of $X(X-t)$.

However, the theory of elementary factors shows there is a square matrix B such that:

$$A \sim \begin{bmatrix} B & 0 \\ 0 & C(\mu_A) \end{bmatrix},$$

and it now suffices to show that the elementary factors of B are polynomials of $X(X-t)$. However, $j_k(B,\delta) = j_k(A,\delta) - j_k(C(\mu_A),\delta)$ for every $k \in \mathbb{N}^*$ and $\delta \in \overline{\mathbb{K}}$, and A and $C(\mu_A)$ satisfy (ii) (for that last matrix, we can use the first part of the proof or simply compute its Jordan form), so clearly B satisfies (ii). We can thus conclude by downward induction on the size of the matrices. □

4. Reducing the problem

The first key lemma is a classical one:

Lemma 10. *Let P and Q be two idempotents in a $\mathbb{K}$-algebra $\mathcal{A}$. Then P and Q commute with $(P-Q)^2$.*

Proof. Indeed $(P-Q)^2 = P+Q-PQ-QP$, so $P(P-Q)^2 = P - PQP = (P-Q)^2P$. By the same argument, Q commutes with $(Q-P)^2 = (P-Q)^2$. □

Corollary 11. *Let P and Q be two idempotents in a $\mathbb{K}$-algebra $\mathcal{A}$, and set $M := \alpha \cdot P + \beta \cdot Q$. Then P and Q commute with $(M - \alpha \cdot I_n)(M - \beta \cdot I_n)$.*

Proof. Indeed, a straightforward computation shows that

$$(M-\alpha\cdot I_n)(M-\beta\cdot I_n)=\alpha\beta\left(I_n-(P-Q)^2\right).\ \square$$

Let now u be an endomorphism of E and assume there are idempotents p and q such that $u=\alpha\cdot p+\beta\cdot q$.

We decompose the minimal polynomial of u as

$$\mu_u=X^a(X-\alpha)^b(X-\beta)^c(X-\alpha-\beta)^dP(X)$$

so that P has no root in $\{0,\alpha,\beta,\alpha+\beta\}$ (in case $\alpha+\beta=0$, we simply take $d=0$). Since $F:=\mathrm{Ker}P(u)$ is stabilized by $v:=(u-\alpha\cdot\mathrm{id})\circ(u-\beta\cdot\mathrm{id})$, we can define Q as the minimal polynomial of $v_{|F}$: then $F=\mathrm{Ker}Q(v)$ and $u_{|F}$ has no eigenvalue in $\{0,\alpha,\beta,\alpha+\beta\}$.

By Corollary 11, p and q commute with v and therefore stabilize the three subspaces:

- $\mathrm{Ker}v^n=\mathrm{Ker}(u-\alpha\cdot\mathrm{id}_E)^n\oplus\mathrm{Ker}(u-\beta\cdot\mathrm{id}_E)^n$;
- $\mathrm{Ker}(v-\alpha\beta\cdot\mathrm{id}_E)^n=\mathrm{Ker}u^n\oplus\mathrm{Ker}(u-(\alpha+\beta)\cdot\mathrm{id}_E)^n$;
- $\mathrm{Ker}Q(v)=\mathrm{Ker}P(u)$.

Since $u=\alpha\cdot p+\beta\cdot q$, restricting to those three subspaces shows that the three endomorphisms $u_{\{\alpha,\beta\}}$, $u_{\{0,\alpha+\beta\}}$ and $u_{-\{0,\alpha,\beta,\alpha+\beta\}}$ are themselves (α,β)-composites. Using Remark 1.(ii), we deduce the following reduction principle:

Proposition 12 (Reduction principle)**.** *Let $u\in\mathrm{End}(E)$. Then u is an (α,β)-composite iff both $u_{\{0,\alpha+\beta\}}, u_{\{\alpha,\beta\}}$ and $u_{-\{0,\alpha,\beta,\alpha+\beta\}}$ are (α,β)-composites.*

We are now reduced to the three special cases that follow:

- u has no eigenvalue in $\{0,\alpha,\beta,\alpha+\beta\}$;
- u is triangularizable with all eigenvalues in $\{\alpha,\beta\}$;
- u is triangularizable with all eigenvalues in $\{0,\alpha+\beta\}$.

5. When no eigenvalue belongs to $\{0,\alpha,\beta,\alpha+\beta\}$

In this section, u still denotes an endomorphism of E. We assume that u has no eigenvalue in $\{0,\alpha,\beta,\alpha+\beta\}$.

Assume further that there are idempotents p and q such that $u=\alpha\cdot p+\beta\cdot q$. The assumption on the spectra of u implies that p and q have no common eigenvector, hence

$$\mathrm{Ker}p\cap\mathrm{Ker}q=\mathrm{Ker}p\cap\mathrm{Im}q=\mathrm{Im}p\cap\mathrm{Ker}q=\mathrm{Im}p\cap\mathrm{Im}q=\{0\}.$$

As a consequence $\dim\mathrm{Ker}p=\dim\mathrm{Ker}q=\dim\mathrm{Im}p=\dim\mathrm{Im}q$ and n is even. It follows that the various kernels and images of p and q all have dimension $m:=\frac{n}{2}$. By gluing together a basis of $\mathrm{Ker}q$ and one of $\mathrm{Ker}p$, we obtain a basis $\mathbf{B}$ of E, together with square matrices $A\in M_m(\mathbb{K})$ and $B\in M_m(\mathbb{K})$ such that

$$M_{\mathbf{B}}(p)=\begin{bmatrix}I_m & 0\\ A & 0\end{bmatrix}\quad\text{and}\quad M_{\mathbf{B}}(q)=\begin{bmatrix}0 & B\\ 0 & I_m\end{bmatrix}.$$

Since $\mathrm{Im}p\cap\mathrm{Ker}q=\{0\}$, the matrix A is non-singular. By a change of basis, we can reduce the situation to the case

$$M_{\mathbf{B}}(p)=\begin{bmatrix}I_m & 0\\ \frac{1}{\alpha}I_m & 0\end{bmatrix}\quad\text{and}\quad M_{\mathbf{B}}(q)=\begin{bmatrix}0 & \frac{1}{\beta}C\\ 0 & I_m\end{bmatrix}$$

for some $C\in M_m(\mathbb{K})$, so that

$$M_{\mathbf{B}}(u)=\begin{bmatrix}\alpha\cdot I_m & C\\ I_m & \beta\cdot I_m\end{bmatrix}.$$

Conversely, for every $C \in M_m(\mathbb{K})$, the matrix

$$\begin{bmatrix} \alpha \cdot I_m & C \\ I_m & \beta \cdot I_m \end{bmatrix} = \alpha \cdot \begin{bmatrix} I_m & 0 \\ \frac{1}{\alpha} I_m & 0 \end{bmatrix} + \beta \cdot \begin{bmatrix} 0 & \frac{1}{\beta} C \\ 0 & I_m \end{bmatrix}$$

is an (α, β)-composite.

We have thus proven that, for every $M \in M_n(\mathbb{K})$ with no eigenvalue in $\{0, \alpha, \beta, \alpha + \beta\}$, the following conditions are equivalent:

(i) M is an (α, β)-composite;
(ii) The integer n is even and there exists $C \in M_{n/2}(\mathbb{K})$ such that

$$M \sim \begin{bmatrix} \alpha \cdot I_{n/2} & C \\ I_{n/2} & \beta \cdot I_{n/2} \end{bmatrix}.$$

We will now characterize this situation in terms of elementary factors:

Proposition 13. *Let $M \in M_n(\mathbb{K})$ with no eigenvalue in $\{0, \alpha, \beta, \alpha + \beta\}$. The following conditions are then equivalent*:

(i) *The elementary factors of M are all polynomials of $(X - \alpha)(X - \beta)$.*
(ii) *The integer n is even and there exists $N \in M_{n/2}(\mathbb{K})$ such that*

$$M \sim \begin{bmatrix} \alpha \cdot I_{n/2} & N \\ I_{n/2} & \beta \cdot I_{n/2} \end{bmatrix}.$$

(iii) *M is an (α, β)-composite.*
Also (ii) implies (iii) without any assumption on the eigenvalues of M.

We will start with a simple situation:

Lemma 14. *Let $P \in \mathbb{K}[X]$ be a monic polynomial of degree $n \geqslant 1$, and set $Y = (X - \alpha)(X - \beta)$. Then*

$$\begin{bmatrix} \alpha \cdot I_n & C(P) \\ I_n & \beta \cdot I_n \end{bmatrix} \sim C\left(P(Y)\right).$$

Proof. Setting $M := \begin{bmatrix} \alpha \cdot I_n & C(P) \\ I_n & \beta \cdot I_n \end{bmatrix}$, it will suffice to prove that $P(Y)$, which has degree $2n$, is the minimal polynomial of M. Simple computation shows that

$$(M - \alpha \cdot I_n)(M - \beta \cdot I_n) = \begin{bmatrix} C(P) & 0 \\ 0 & C(P) \end{bmatrix},$$

which proves that $P(Y)$ is an annihilator polynomial of M.

Conversely, let $Q \in \mathbb{K}[X]$ be an annihilator polynomial of M. The sequence

$$\left(1, X - \alpha, (X - \alpha)(X - \beta), \ldots, (X - \alpha)^k (X - \beta)^k, (X - \alpha)^{k+1} (X - \beta)^k, \ldots\right)$$

is clearly a basis of $\mathbb{K}[X]$, so we may split

$$Q = Q_1(Y) + (X - \alpha) Q_2(Y)$$

for some polynomials Q_1 and Q_2 in $\mathbb{K}[X]$. Hence

$$\begin{aligned} Q(M) &= \begin{bmatrix} Q_1\left(C(P)\right) & 0 \\ 0 & Q_1\left(C(P)\right) \end{bmatrix} + \begin{bmatrix} 0 & C(P) \\ I_n & (\beta - \alpha) \cdot I_n \end{bmatrix} \times \begin{bmatrix} Q_2\left(C(P)\right) & 0 \\ 0 & Q_2\left(C(P)\right) \end{bmatrix} \\ &= \begin{bmatrix} Q_1\left(C(P)\right) & ? \\ Q_2\left(C(P)\right) & ? \end{bmatrix}. \end{aligned}$$

Since $Q(M) = 0$, we deduce that P divides Q_1 and Q_2, so Q is a multiple of $P(Y)$. This proves that $P(Y)$ is the minimal polynomial of M. □

Proof of Proposition 13. We have already proven that (ii) is equivalent to (iii) and also that it implies (iii) with no assumption on the eigenvalues of M. For $A \in M_m(\mathbb{K})$, set

$$\varphi(A) := \begin{bmatrix} \alpha \cdot I_m & A \\ I_m & \beta \cdot I_m \end{bmatrix}.$$

- Assume (i) holds, and let $P_1, \ldots, P_N$ denote the elementary factors of M. For $k \in [\![1, N]\!]$, write $P_k = Q_k((X-\alpha)(X-\beta))$ for some $Q_k \in \mathbb{K}[X]$. Hence
$$M \sim D\left(C(P_1), \ldots, C(P_N)\right)$$
and, for every $k \in [\![1, N]\!]$, the companion matrix $C(P_k) \sim \varphi(C(Q_k))$ is an (α, β)-composite, so M is an (α, β)-composite, which in turn proves (ii).
- Assume (ii) holds, and let $A \in M_{n/2}(\mathbb{K})$ such that $\varphi(A) \sim M$. Let $Q_1, \ldots, Q_N$ denote the elementary factors of A, so $A \sim D\left(C(Q_1), \ldots, C(Q_N)\right)$. Set $P_k := Q_k((X-\alpha)(X-\beta))$ for $k \in [\![1, N]\!]$. A simple permutation of the basis shows then that
$$M \sim \varphi(A) \sim D\left(\varphi(C(Q_1)), \ldots, \varphi(C(Q_n))\right) \sim D\left(C(P_1)), \ldots, C(P_n)\right).$$
Since P_i divides P_{i+1} for every suitable i, the P_k's are the elementary factors of M, which proves (i). □

6. When all eigenvalues belongs to $\{0, \alpha, \beta, \alpha + \beta\}$

Recall first Proposition 1 of [3], the proof of which holds regardless of the field $\mathbb{K}$:

Proposition 15. *Any nilpotent matrix is a difference of two idempotents.*

From this, we easily derive:

Proposition 16. *Every nilpotent matrix is an $(\alpha, -\alpha)$-composite.*

The next proposition will be the last key to our theorems:

Proposition 17. *Let $M \in M_n(\mathbb{K})$ be a triangularizable matrix with all eigenvalues in $\{\alpha, \beta\}$. Assume $\alpha \neq \beta$. The following conditions are then equivalent:*

(i) *M is an (α, β)-composite;*
(ii) *The sequences $(n_k(M, \alpha))_{k \geqslant 1}$ and $(n_k(M, \beta))_{k \geqslant 1}$ are intertwined.*

By Remark 1(iii), this proposition has the following corollary:

Corollary 18. *Assume $\alpha + \beta \neq 0$, and let $M \in M_n(\mathbb{K})$ denote a triangularizable matrix with all eigenvalues in $\{0, \alpha + \beta\}$. The following conditions are then equivalent:*

(i) *M is an (α, β)-composite;*
(ii) *The sequences $(n_k(M, 0))_{k \geqslant 1}$ and $(n_k(M, \alpha + \beta))_{k \geqslant 1}$ are intertwined.*

Assuming temporarily that Proposition 17 holds, we can then prove the theorems with even numbers listed in Section 1.

- Assume $\mathrm{car}(\mathbb{K}) \neq 2$ and $\alpha \neq \pm\beta$. Then Theorem 8 follows directly from Propositions 12, 17 and 18.

- Assume $\mathrm{car}(\mathbb{K}) \neq 2$ and $\beta = -\alpha$. Notice that the polynomials of $(X-\alpha)(X+\alpha) = X^2 - \alpha^2$ are simply the even polynomials.
  The "only if" part of Theorem then follows from Propositions 12, 13 and 17. For the "if" part, we use the same results in conjunction with Proposition 16.
- Assume $\mathrm{car}(\mathbb{K}) = 2$ and $\beta = \alpha$. The "only if" part of Theorem 6 then follows from Propositions 12 and 13. For the "if" part, we use the same results in conjunction with Proposition 16 and the fact that for every nilpotent matrix N, the matrix $\alpha \cdot I_n + N$ is an (α, α)-composite since N is an $(\alpha, -\alpha)$ composite.

It now only remains to prove Proposition 17: this will be done in the last section.

7. Proof of Proposition 17

Our proof will differ from that of Hartwig and Putcha in [3]. More precisely, we will not rely upon the results of Flanders featured in [1], but will try instead to prove the equivalence by elementary means. We will need a few notations first.

Notation 6. When p, q, r, s denote non-negative integers such that $p \geqslant r$ and $q \geqslant s$, we set

$$K_{p,q} := \begin{bmatrix} \alpha \cdot I_p & 0 \\ 0 & \beta \cdot I_q \end{bmatrix} \in M_{p+q}(\mathbb{K}) \quad \text{and} \quad J_{p,q,r,s} := \begin{bmatrix} I_r & 0_{r,s} \\ 0_{p-r,r} & 0_{p-r,s} \\ 0_{s,r} & -I_s \\ 0_{q-s,r} & 0_{q-s,s} \end{bmatrix} \in M_{p+q,r+s}(\mathbb{K}).$$

For the entire proof, we set a triangularizable matrix M with all eigenvalues in $\{\alpha, \beta\}$. We will simply write $n_k := n_k(M, \alpha)$ and $m_k := n_k(M, \beta)$ for $k \in \mathbb{N}^*$.

7.1. Proof that (i) implies (ii)

Assume that $M = \alpha \cdot P + \beta \cdot Q$ for some idempotents P and Q. The Jordan reduction theorem shows, after permuting the basis vectors, that the matrix M is similar to some block-triangular matrix

$$M' = \begin{bmatrix} K_{n_1,m_1} & J_{n_1,m_1,n_2,m_2} & 0 & \cdots & 0 \\ 0 & K_{n_2,m_2} & J_{n_2,m_2,n_3,m_3} & & 0 \\ 0 & 0 & K_{n_3,m_3} & \ddots & \vdots \\ \vdots & & & \ddots & \\ 0 & \cdots & & 0 & K_{n_N,m_N} \end{bmatrix}$$

where N denotes the index of the nilpotent matrix $(M - \alpha \cdot I)(M - \beta \cdot I)$. Since the problem is invariant under similarity, we may assume that $M = M'$.

Remark that the flag of linear subspaces which gives the previous block-decomposition of M consists precisely of the iterated kernels of $(M - \alpha \cdot I)(M - \beta \cdot I)$. Since the matrices P and Q commute with $(M - \alpha \cdot I)(M - \beta \cdot I)$, they stabilize these subspaces, which proves that P and Q themselves decompose as block-triangular matrices:

$$P = \begin{bmatrix} P_{1,1} & P_{1,2} & \cdots & P_{1,N} \\ 0 & P_{2,2} & \cdots & P_{2,N} \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & P_{N,N} \end{bmatrix} \quad \text{and} \quad Q = \begin{bmatrix} Q_{1,1} & Q_{1,2} & \cdots & Q_{1,N} \\ 0 & Q_{2,2} & \cdots & Q_{2,N} \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & Q_{N,N} \end{bmatrix}.$$

It is then clear that, for every $k \in [\![1, N-1]\!]$, the matrices $\begin{bmatrix} P_{k,k} & P_{k,k+1} \\ 0 & P_{k+1,k+1} \end{bmatrix}$ and $\begin{bmatrix} Q_{k,k} & Q_{k,k+1} \\ 0 & Q_{k+1,k+1} \end{bmatrix}$ are idempotents, which in turn proves that the matrix

$\begin{bmatrix} K_{n_k,m_k} & J_{n_k,m_k,n_{k+1},m_{k+1}} \\ 0 & K_{n_{k+1},m_{k+1}} \end{bmatrix}$ is an (α,β)-composite.

That the sequences $(n_k)_{k\geqslant 1}$ and $(m_k)_{k\geqslant 1}$ are intertwined can then be deduced from the following lemma:

Lemma 19 (Intertwinement lemma)**.** *Let p, q, r, s be non-negative integers such that $p \geqslant r$ and $q \geqslant s$. Assume the block matrix $M = \begin{bmatrix} K_{p,q} & J_{p,q,r,s} \\ 0 & K_{r,s} \end{bmatrix}$ is an (α,β)-composite. Then $q \geqslant r$ and $p \geqslant s$.*

In order to prove this, we will extract two matrices A_1 and A_2 such that

$r \leqslant rk(A_1) + rk(A_2) \leqslant q$.

Proof. Set $K_1 := K_{p,q}$, $K_2 := K_{r,s}$ and $K_3 := J_{p,q,r,s}$, so that $M = \begin{bmatrix} K_1 & K_3 \\ 0 & K_2 \end{bmatrix}$. We choose two idempotents P and Q such that $M = \alpha \cdot P + \beta \cdot Q$. Remark foremost that

$$(M - \alpha \cdot I_{p+q})(M - \beta \cdot I_{p+q}) = \begin{bmatrix} 0 & I' \\ 0 & 0 \end{bmatrix},$$

$$\text{with } I' = \begin{bmatrix} (\alpha-\beta)\cdot I_r & 0_{r,s} \\ 0_{p-r,r} & 0_{p-r,s} \\ 0_{s,r} & (\alpha-\beta)\cdot I_s \\ 0_{q-s,r} & 0_{q-s,s} \end{bmatrix} \in M_{p+q,r+s}(\mathbb{K}).$$

The commutation argument already used earlier proves that there are three matrices $A \in M_{p+q}(\mathbb{K})$, $B \in M_{p+q,r+s}(\mathbb{K})$ and $C \in M_{r+s}(\mathbb{K})$ such that

$$P = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}.$$

The idempotent Q also has a decomposition of this type. Consequently, both A and $\frac{1}{\beta}(K_1 - \alpha A)$ are idempotents, so

$$\beta(K_1 - \alpha A) = (K_1 - \alpha A)^2 = K_1^2 - \alpha(AK_1 + K_1A) + \alpha^2A^2 = K_1^2 - \alpha(AK_1 + K_1A) + \alpha^2 A.$$

From the definition of K_1, it is clear that $K_1^2 = (\alpha+\beta)\cdot K_1 - \alpha\beta \cdot I_{p+q}$, and we deduce that

$$\alpha \cdot K_1 - \alpha(AK_1 + K_1A) + \alpha(\alpha+\beta)\cdot A = \alpha\beta \cdot I_{p+q}.$$

From this identity and the fact that $\alpha(\alpha-\beta) \neq 0$, we derive that there are matrices $A_1 \in M_{q,p}(\mathbb{K})$ and $A_2 \in M_{p,q}(\mathbb{K})$ such that $A = \begin{bmatrix} I_p & A_2 \\ A_1 & 0 \end{bmatrix}$. Identity $A^2 = A$ then entails that $A_2A_1 = 0$, hence

$$rkA_1 + rkA_2 \leqslant q.$$

We will now try to prove that $r \leqslant rkA_1 + rkA_2$.

Commutation of P with $(M - \alpha \cdot I_n)(M - \beta \cdot I_n)$ yields that there are matrices $D_1 \in M_{s,r}(\mathbb{K})$, $L_1 \in M_{s,p-r}(\mathbb{K})$, $N_1 \in M_{q-s,p-r}(\mathbb{K})$, $D_2 \in M_{r,s}(\mathbb{K})$, $L_2 \in M_{r,q-s}(\mathbb{K})$, and $N_2 \in M_{p-r,q-s}(\mathbb{K})$ such that

$$A_1 = \begin{bmatrix} D_1 & L_1 \\ 0 & N_1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} D_2 & L_2 \\ 0 & N_2 \end{bmatrix} \quad \text{and} \quad C = \begin{bmatrix} I_r & D_2 \\ D_1 & 0 \end{bmatrix}.$$

Using again the identity $P^2 = P$, we obtain:

$$AB + BC = B.$$

Since $Q = \frac{1}{\beta}(M - \alpha \cdot P)$ and Q is also idempotent, the corresponding identity for Q yields:

$$\frac{1}{\beta}(K_1 - \alpha\cdot A)\frac{1}{\beta}(K_3 - \alpha\cdot B) + \frac{1}{\beta}(K_3 - \alpha\cdot B)\frac{1}{\beta}(K_2 - \alpha\cdot C) = \frac{1}{\beta}(K_3 - \alpha\cdot B),$$

therefore

$$\beta K_3 = K_1K_3 + K_3K_2 - \alpha(K_1B + BK_2) - \alpha(K_3C + AK_3) + \alpha(\alpha + \beta)B.$$

Using a block-decomposition of B, a simple computation allows us to deduce from the previous identity that there are matrices $B_1 \in M_{s,r}(\mathbb{K})$, $C_1 \in M_{q-s,r}(\mathbb{K})$ and $B_2 \in M_{r,s}(\mathbb{K})$ such that

$$B = \begin{bmatrix} \frac{1}{\alpha}I_r & B_2 \\ 0 & ? \\ B_1 & ? \\ C_1 & ? \end{bmatrix}.$$

Computation of the first $r \times r$ block in the identity $AB + BC = B$ then yields:

$$D_2B_1 + B_2D_1 + L_2C_1 = \frac{1}{\alpha}I_r.$$

For every $X \in \mathrm{Ker}D_1$, one has $D_2B_1X + L_2C_1X = \frac{1}{\alpha}X$, which proves that

$$\dim(\mathrm{Im}D_2 + \mathrm{Im}L_2) \geqslant \dim \mathrm{Ker}D_1,$$

hence

$$rk\begin{bmatrix} D_2 & L_2 \end{bmatrix} \geqslant r - rk(D_1).$$

It follows that

$$r \leqslant rk(D_1) + rk\begin{bmatrix} D_2 & L_2 \end{bmatrix} \leqslant rk(A_1) + rk(A_2).$$

This finally proves $r \leqslant q$. By an argument of symmetry, one also has $s \leqslant p$. □

7.2. Proof of (ii) ⇒ (i)

We start with three special cases:

Proposition 20. *Let $n \geqslant 1$. Then each one of the three matrices*

$$A := \begin{bmatrix} J_n(\alpha) & 0 \\ 0 & J_n(\beta) \end{bmatrix}, \quad B := \begin{bmatrix} J_n(\alpha) & 0 \\ 0 & J_{n+1}(\beta) \end{bmatrix} \quad \text{and} \quad B' := \begin{bmatrix} J_{n+1}(\alpha) & 0 \\ 0 & J_n(\beta) \end{bmatrix}$$

is an (α, β)-composite.

Proof

- Since A is similar to the companion matrix $C((X-\alpha)^n(X-\beta)^n)$, Proposition 13 proves that it is an (α, β)-composite.
- We can decompose

$$B = \begin{bmatrix} A & C \\ 0 & \beta \end{bmatrix}, \quad \text{where } C = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} \in M_{2n,1}(\mathbb{K}).$$

We have found two idempotents P and Q such that $A = \alpha \cdot P + \beta \cdot Q$. More precisely, the proof of Proposition 13 (see the beginning of Section 5) even provides P and Q with the additional constraint: $\mathrm{Im}P \oplus \mathrm{Ker}Q = \mathbb{K}^{2n}$. We can then find two column matrices C_1 and C_2 such that

$$C_1 \in \mathrm{Im}P, \quad C_2 \in \mathrm{Ker}Q \quad \text{and} \quad C = \alpha \cdot C_1 + \beta \cdot C_2.$$

The matrices

$$P_1 := \begin{bmatrix} P & C_1 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad Q_1 := \begin{bmatrix} Q & C_2 \\ 0 & 1 \end{bmatrix}$$

are then idempotents and satisfy $B = \alpha \cdot P_1 + \beta \cdot Q_1$.

- A similar argument proves that B' is an (α, β)-composite. □

Let now $M \in M_n(\mathbb{K})$ as in Proposition 17, and assume the two sequences $(n_k)_{k\geqslant 1} = (n_k(M,\alpha))_{k\geqslant 1}$ and $(m_k)_{k\geqslant 1} = (n_k(M,\beta))_{k\geqslant 1}$ are intertwined. Let N_α and N_β denote the respective nilpotency indices associated to the restriction of M to $\mathrm{Ker}(M-\alpha\cdot I_n)^n$ and $\mathrm{Ker}(M-\beta\cdot I_n)^n$. That the sequences $(n_k)_{k\geqslant 1}$ and $(m_k)_{k\geqslant 1}$ are intertwined shows that $-1\leqslant N_\alpha - N_\beta \leqslant 1$. If $N_\alpha = 0$ or $N_\beta = 0$, then $M = \beta\cdot I_n$ or $M = \alpha\cdot I_n$ so M is clearly an (α,β)-composite. Assume now that $N_\alpha \geqslant 1$ and $N_\beta \geqslant 1$. Whether $N_\beta = N_\alpha$, $N_\beta = N_\alpha + 1$ or $N_\beta = N_\alpha - 1$, there is some matrix M' such that M is similar to either

$$\begin{bmatrix} M' & 0 & 0 \\ 0 & J_{N_\alpha}(\alpha) & 0 \\ 0 & 0 & J_{N_\alpha}(\beta) \end{bmatrix}, \quad \begin{bmatrix} M' & 0 & 0 \\ 0 & J_{N_\alpha}(\alpha) & 0 \\ 0 & 0 & J_{N_\alpha+1}(\beta) \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} M' & 0 & 0 \\ 0 & J_{N_\alpha}(\alpha) & 0 \\ 0 & 0 & J_{N_\alpha-1}(\beta) \end{bmatrix}.$$

In any case, we are reduced to proving that M' is an (α,β)-composite, which follows easily by induction since M' has its eigenvalues in $\{\alpha,\beta\}$ and the sequences $(n_k(M',\alpha))_{k\geqslant 1}$ and $(n_k(M',\beta))_{k\geqslant 1}$ are easily shown to be intertwined. This finishes our proof of Proposition 17, and all the theorems claimed in Section 1 then follow.

References

[1] H. Flanders, Elementary divisors of *AB* and *BA*, Proc. Amer. Math. Soc. 2 (1951) 871–874.
[2] F.R. Gantmacher, The Theory of Matrices, vol. 1, Chelsea, New York, 1960.
[3] R.E. Hartwig, M.S. Putcha, When is a matrix a difference of two idempotents? Linear and Multilinear Algebra 26 (1990) 267–277.