# Decomposing matrices into quadratic ones

Clément de Seguins Pazzis

Université de Versailles Saint-Quentin-en-Yvelines (France)

ILAS 2022, NUI Galway

# Quadratic objects

Setting: $\mathbb{F}$ an arbitrary field, $\mathcal{A}$ an $\mathbb{F}$-algebra (unital, associative).

$x \in \mathcal{A}$ is **quadratic** iff

$$\exists(\alpha, \beta) \in \mathbb{F}^2 : \; x^2 = \alpha\, 1_{\mathcal{A}} + \beta\, x.$$

i.e. $x$ annihilated by $p(t) \in \mathbb{F}[t]$ of degree 2.

For $p \in \mathbb{F}[t]$ of degree 2,

$x \in \mathcal{A}$ is ***p*-quadratic** iff $p(x) = 0$.

# Examples of quadratic objects

| | |
|---|---|
| Idempotents | $x^2 = x$ |
| Involutions | $x^2 = 1_{\mathcal{A}}$ |
| Square-zero elements | $x^2 = 0_{\mathcal{A}}$ |
| Unipotent elements of index 2 | $(x - 1_{\mathcal{A}})^2 = 0_{\mathcal{A}}$ |
| Quarter turns | $x^2 = -1_{\mathcal{A}}$ |

# Very general decomposition problems (1)

Let $r \geq 1$ and $p_1, \dots, p_r \in \mathbb{F}[t]$ all monic w/ degree 2.

**Definition**

$x \in \mathcal{A}$ is a $(p_1, \dots, p_r)$**-sum** when

$$\exists (a_1, \dots, a_r) \in \mathcal{A}^r : \; x = a_1 + \cdots + a_r$$

and

$$p_1(a_1) = 0, \; p_2(a_2) = 0, \quad \dots \quad p_r(a_r) = 0.$$

**Remark:** Set of all $(p_1, \dots, p_r)$-sums stable under conjugation $x \mapsto axa^{-1}$ in $\mathcal{A}$ for all $a \in \mathcal{A}^\times$.

**Q:** Can we characterize the $(p_1, \dots, p_r)$-sums?

**Remark:** This could require a precise knowledge of conjugacy classes in $\mathcal{A}$!

# Very general decomposition problems (2)

Let $r \geq 1$ and $p_1, \dots, p_r \in \mathbb{F}[t]$ all monic w/ degree 2.

**Definition**

$x \in \mathcal{A}$ is a $(p_1, \dots, p_r)$**-product** when

$$\exists (a_1, \dots, a_r) \in \mathcal{A}^r : \; x = a_1 a_2 \cdots a_r$$

and

$$p_1(a_1) = 0, \; p_2(a_2) = 0, \quad \dots \quad p_r(a_r) = 0.$$

**Remark:** Set of all $(p_1, p_2, \dots, p_r)$-products stable under conjugation $x \mapsto axa^{-1}$ in $\mathcal{A}$ for all $a \in \mathcal{A}^\times$.

**Q:** Can we characterize the $(p_1, p_2, \dots, p_r)$-products?

**Non-degenerate case:** $p_1(0)\, p_2(0) \cdots p_r(0) \neq 0$.

# A rare general solution: products of idempotents!

**Q:** With $r \geq 1$ *fixed*, which $M \in \mathrm{M}_n(\mathbb{F})$ decompose as

$$M = P_1 \cdots P_r \quad \text{with } P_1, \dots, P_r \text{ idempotents?}$$

(i.e. $(t^2 - t, \dots, t^2 - t)$-products).

**A:** (C.S. Ballantine, 1978): necessary and sufficient condition:

$$\operatorname{rank}(M - I) \leq r \dim \operatorname{Ker} M.$$

*Idea for necessity:* if $\operatorname{rk} M$ is large, then $\dim \operatorname{Ker}(P_i - I) = \operatorname{rk} P_i$ is large, and hence $\bigcap_i \operatorname{Ker}(P_i - I) \subset \operatorname{Ker}(M - I)$ has large dimension.

**A:** (J. Erdos, 1967) Matrices that are products of idempotents (unspecified number of factors): $I$ and singular matrices.

# Sums of idempotents - unlimited number of summands

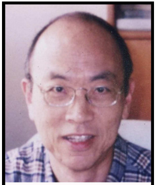
**Q:** Which $M \in \mathrm{M}_n(\mathbb{F})$ decompose as

$$M = P_1 + \cdots + P_r \quad \text{with } P_1, \dots, P_r \text{ idempotents?}$$

($r$ unlimited)

**A:** (P.-Y. Wu, 1990) fields of characteristic 0.
Necessary and sufficient condition:

$$\operatorname{tr} M \in \mathbb{Z} \quad \text{and} \quad \operatorname{rank} M \leq \operatorname{tr} M$$



Pei Yuan Wu

**A:** (fields of characteristic $p > 0$). Necessary and sufficient condition: $\operatorname{tr} M = k.1_{\mathbb{F}}$ with $k \in \mathbb{Z}$.

# Sums of idempotents - fixed number of summands

**Q:** With $r$ fixed, which $M \in \mathrm{M}_n(\mathbb{F})$ decompose as

$$M = P_1 + \cdots + P_r \quad \text{with } P_1, \dots, P_r \text{ idempotents?}$$

Answer unknown for general $r$!

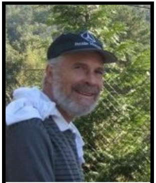
**A:** (J.-H. Wang, 1995) Solution for complex matrices of *small size*.

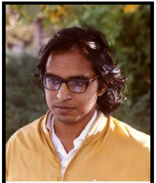
Jin-Hsien Wang

Some results for fields of positive characteristic (dSP, 2010)

# Sums of idempotents - few summands

- **2 summands:** R. Hartwig and M. Putcha (1990) over $\mathbb{C}$ (more generally, alg. closed field $\mathbb{F}$ with $\chi(\mathbb{F}) \neq 2$). Characterization in terms of the Jordan normal form.


Robert Hartwig


Mohan Putcha

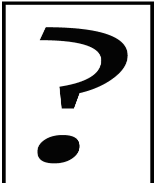
- Generalized to all fields (dSP, 2010).

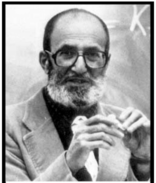
- **3 summands:** no known characterization!

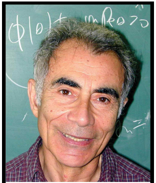
# Products of involutions in $\mathrm{GL}_n(\mathbb{F})$

$M \in \mathrm{GL}_n(\mathbb{F})$ is a product of involutions iff $\det M = \pm 1$
(very old result!)

**Q:** Least number of necessary factors in general?
**A:** Four! (Gustafson, Halmos and Radjavi - 1976)


William Gustafson


Paul Halmos


Heydar Rajdavi

**Counter-example for** 3 **factors:**
$\alpha I_n$ where $\alpha \in \mathbb{C}$ s.t. $\alpha^n = \pm 1$ and $\alpha^4 \neq 1$.

**Products of 3 involutions:** no known characterization
("Halmos problem").

$M \in \mathrm{GL}_n(\mathbb{F})$ product of two involutions iff

$$\exists P \in \mathrm{GL}_n(\mathbb{F}) : \; M^{-1} = PMP^{-1}$$

(Wonenburger, Djokovic ; 1966-1967).



**Remark:** in a group $G$, if $g = ab$ with $a^2 = b^2 = 1$, then

$$g^{-1} = b^{-1}a^{-1} = ba = b(ab)b^{-1} = bgb^{-1}.$$

# Sums of square-zero matrices

**Q:** Which matrices are sums of square-zero matrices?
**A:** Matrices $M$ with $\operatorname{tr} M = 0$.

**Q:** How many summands at most?
**A:** Four suffice! (Wang and Wu - 1991)

**3 summands** do not suffice in general

**Characterization of sums of** 3 **square-zero matrices:**
hopeless in general

# Sums of 2 square-zero matrices

**Q:** Which matrices are sums of 2 square-zero matrices?

**A1:** (Wang-Wu-Botha) If $\chi(\mathbb{F}) \neq 2$, the matrices $M$ such that

$$\exists P \in \mathrm{GL}_n(\mathbb{F}) : \; -M = PMP^{-1}.$$

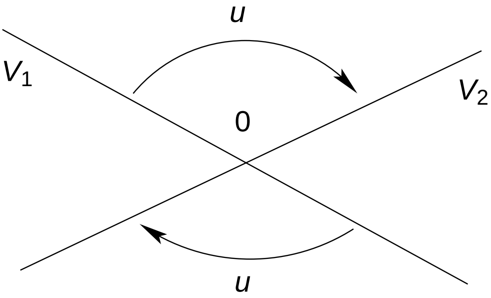
**A2:** (J.D. Botha, 2012) For general fields, matrices $M$ that have the exchange property.

Johan D. Botha

# Sums of 2 square-zero matrices (continued): Exchange property

$u \in \mathrm{End}(V)$ has the **exchange property** iff

$$\exists V_1, V_2 : V = V_1 \oplus V_2, \quad u(V_1) \subset V_2 \quad \text{and} \quad u(V_2) \subset V_1.$$



# Back to the general problem

**Q:** Is characterizing $(p_1, \dots, p_r)$-sums (or products) feasible in general?
**A:** No!

**Q:** Are there general methods?
**A:** Yes.

**Q:** What is the state of the art for the general case?
**A:** The complete solution for $r = 2$ (sums and products alike) (dSP, 2017)! Complete ... up to the degenerate case for products (minor issue).

# Why $r = 2$ is interesting?

**A1:** Challenging problem!

- Uses a wide variety of normal forms.
- Nontrivial problem, surprising results.

**A2:** Seems indispensable for decompositions of small length.

# Some applications of the case $r = 2$

$\to$ Every $M \in \mathrm{GL}_n(\mathbb{F})$ with $\det M = \pm 1$ is the product of 4 involutions.
Decomposes $M = AB$ where $A, B$ are products of two involutions.

$\to$ Every matrix $M \in \mathrm{M}_n(\mathbb{C})$ with trace 0 is the sum of 4 square-zero matrices (Wang-Wu; 1991).
Split $M = A + B$ with $A$ and $B$ the sum of two square-zero.

$\to$ Every matrix $M \in \mathrm{M}_n(\mathbb{F})$ is a *linear combination* of 3 idempotents. (dSP; 2010)
Requires a fine knowledge of matrices of the form $\alpha P + \beta Q$, with $\alpha, \beta$ fixed ($\neq 0$), and $P, Q$ variable idempotents. Amounts to consider $(t^2 - \alpha t, t^2 - \beta t)$-sums.

# Some applications of the case $r = 2$ (continued): stable results

$\rightarrow$ Let $M \in \mathrm{M}_n(\mathbb{F})$ with $\operatorname{tr} M = 0$.
Then $\begin{bmatrix} M & 0_n \\ 0_n & 0_n \end{bmatrix}$ is the sum of 3 square-zero matrices! (dSP, 2017)

$\rightarrow$ Let $M \in \mathrm{GL}_n(\mathbb{F})$ with $\det M = \pm 1$.
Then $\begin{bmatrix} M & 0_n \\ 0_n & I_n \end{bmatrix}$ is the product of 3 involutions! (dSP, 2019)

# Main ideas for the $r = 2$ problem

Here

$$p(t) = t^2 - (\operatorname{tr} p)\, t + p(0) \quad \text{and} \quad q(t) = t^2 - (\operatorname{tr} q)\, t + q(0).$$

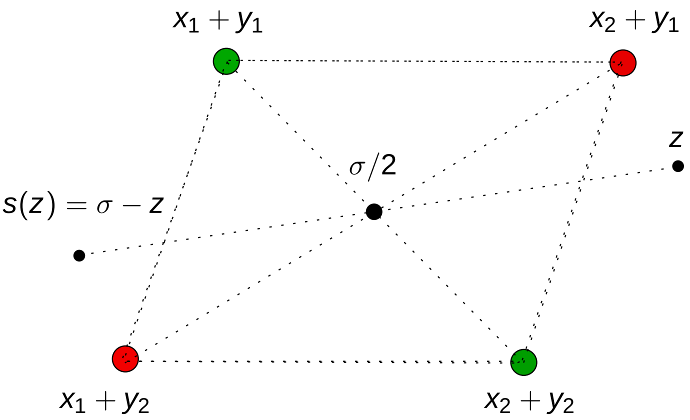
**Problem:** characterize the $(p, q)$-sums (w/ invariant factors)

**Five main ideas:**

1. Sums of roots of $p$ and $q$.
2. Regular/exceptional dichotomy.
3. Commutation trick.
4. Invariant factors for regular $(p, q)$-sums.
5. Construction of “simple" exceptional $(p, q)$-sums?

# Sums of roots of $p$ and $q$ (1)

Split $p(t) = (t - x_1)(t - x_2)$ and $q(t) = (t - y_1)(t - y_2)$ in $\overline{\mathbb{F}}[t]$.




Important object: $\sigma := x_1 + x_2 + y_1 + y_2 = \mathrm{tr}(p) + \mathrm{tr}(q) \in \mathbb{F}$.

# Sums of roots of $p$ and $q$ (2)

**Rough idea:** If $u$ is a $(p,q)$-sum, then $\mathrm{Sp}(u) \setminus (\mathrm{Root}(p) + \mathrm{Root}(q))$ invariant under $s$ (and same Jordan cells for $z$ and $s(z)$).
Yet:

- This condition is not sufficient.
- Additional nontrivial condition if $s(z) = z$ and $z \notin \mathrm{Root}(p) + \mathrm{Root}(q)$.
- Eigenvalues in $\mathrm{Root}(p) + \mathrm{Root}(q)$ can fail to have the symmetry property.
- “Quasi-symmetry" between Jordan cells of $z$ and $s(z)$ if $z \in \mathrm{Root}(p) + \mathrm{Root}(q)$.

# Regular/exceptional dichotomy (1)

Let $u \in \mathrm{End}(V)$ ($V$ vector space of finite dimension).

- $u$ **regular** (w/ respect to $(p,q)$) when it has *no* eigenvalue in $\mathrm{Root}(p)+\mathrm{Root}(q)$ (in $\overline{\mathbb{F}}$)
- $u$ **exceptional** (w/ respect to $(p,q)$) when it has *all its* eigenvalues in $\mathrm{Root}(p)+\mathrm{Root}(q)$ (in $\overline{\mathbb{F}}$).

Basic principle: unique splitting

$$u = u_r \oplus u_e$$

with $u_r$ regular and $u_e$ exceptional.

*Idea:* Fitting decomposition of $F_{p,q}(u)$ where

$$F_{p,q}(t) := \prod_{i,j} (t-(x_i+y_j)) \in \mathbb{F}[t].$$

# Regular/exceptional dichotomy (2)

**Theorem**

*Let $u \in \mathrm{End}(V)$. Then $u$ is a $(p,q)$-sum iff both $u_r$ and $u_e$ are $(p,q)$-sums.*

**Proof.** If $u = a + b$ where $p(a) = q(b) = 0$, then:

- $a$ and $b$ commute with $F_{p,q}(u)$ (to be explained later);
- $a$ and $b$ stabilize the Fitting decomposition of $F_{p,q}(u)$;
- resulting endomorphisms yield that $u_r$ and $u_e$ are $(p,q)$-sums.

**Warning:** in general a $(p,q)$-sum can split $u = u_1 \oplus u_2$ without $u_1$ and $u_2$ being $(p,q)$-sums.

Basic example: $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ is a $(t^2, t^2)$-sum but not $\begin{bmatrix} 1 \end{bmatrix}$!

In an $\mathbb{F}$-algebra $\mathcal{A}$, let $a, b$ with $p(a) = q(b) = 0$. Quadratic conjugates:

$$a^\star = (\operatorname{tr} p)1_{\mathcal{A}} - a \quad \text{and} \quad b^\star = (\operatorname{tr} q)1 - b,$$

so that

$$aa^\star = a^\star a = p(0)1_{\mathcal{A}} \quad \text{and} \quad bb^\star = b^\star b = q(0)1_{\mathcal{A}}.$$

Note that $p(a^\star) = q(b^\star) = 0$.

An important element:

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

**Lemma (Commutation lemma)**

*$a$ and $b$ commute with $ab^\star + ba^\star$.*

**Pseudo-conjugate** of $u = a + b$:

$$u^\star := a^\star + b^\star = \sigma\, 1_{\mathcal{A}} - u$$

**Pseudo-norm** of $u$:

$$uu^\star = ab^\star + ba^\star + aa^\star + bb^\star = ab^\star + ba^\star + (p(0) + q(0))\, 1_{\mathcal{A}}$$

commutes w/ $a$ and $b$.
That is, $u(u - \sigma 1_{\mathcal{A}})$ commutes w/ $a, b$.

**Application:**

$$F_{p,q}(t) = \prod_{i,j} (t - x_i - y_j) = Q(t^2 - \sigma t)$$

for

$$Q = \bigl(t + (x_1 + y_1)(x_2 + y_2)\bigr)\bigl(t + (x_1 + y_2)(x_2 + y_1)\bigr) \in \mathbb{F}[t].$$

**Conclusion:** $a$ and $b$ commute with $F_{p,q}(u)$.

**Frobenius normal form.**

Companion matrix of monic polynomial $r(t) = t^n - \sum_{k=0}^{n-1} a_k t^k$:

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

**Theorem (Frobenius)**

*Let $u \in \mathrm{End}(V)$ ($V$ vector space of finite dimension). Then $u$ represented by block-diagonal $C(R_1) \oplus \cdots \oplus C(R_s)$ for a unique list $(R_1, \dots, R_s)$ of monic polynomials s.t. $R_{i+1}$ divides $R_i$.*
*$R_1, \dots, R_s$: the **invariant factors** of $u$.*

**Theorem**

*Let $u \in \mathrm{End}(V)$ regular $(p, q)$-sum. Then each invariant factor of $u$ reads $R(t^2 - \sigma t)$.*

*Starting idea of proof for alg. closed fields:* if $u = a + b$ with $p(a) = q(b) = 0$ then $a, b$ have no common eigenvector.

**Remark:** $M := C(R(t^2 - \sigma t))$ always similar to $\sigma I - M$.

Condition sufficient when $p$ or $q$ has a root in $\mathbb{F}$; not in general!

# Regular $(p, q)$-sums: a necessary condition (3)

**Counterexample for sufficiency:** $p = q = t^2 + 1$ over reals.

The companion matrix $M := C(t^2 + 2)$ is *not* a $(p, q)$-sum!

Otherwise $M = A + B$ with $A^2 = B^2 = -I$, hence

$$M^2 = (A + B)^2 = A^2 + B^2 + AB + BA = -2I + AB + BA$$

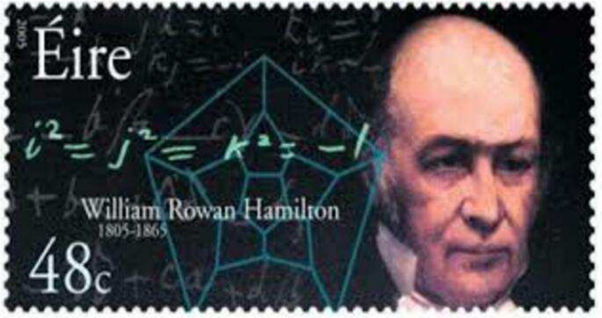
and so

$$BA = -AB.$$

Then $\mathbb{R}[A, B]$ isomorphic to $\mathbb{H}$ (quaternions).
$\rightarrow$ Structure of left $\mathbb{H}$-vector space on $\mathbb{R}^2$!
Impossible (dimension constraints)!

# Regular $(p, q)$-sums: necessary and sufficient condition

The full characterization of regular $(p, q)$-sums (dSP 2017) requires deep results on **quaternion algebras**, a generalization of quaternions . . .



# Exceptional $(p, q)$-sums: the basic construction (1)

Old trick (dates back to Hartwig, Putcha, Wang, Wu).

*Assume $p, q$ split over $\mathbb{F}$.*

**First matrix:**

$$A = \begin{cases} \begin{bmatrix} x_1 & 0 \\ 1 & x_2 \end{bmatrix} \oplus \begin{bmatrix} x_1 & 0 \\ 1 & x_2 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} x_1 & 0 \\ 1 & x_2 \end{bmatrix} & (n \text{ even}) \\ \begin{bmatrix} x_1 & 0 \\ 1 & x_2 \end{bmatrix} \oplus \begin{bmatrix} x_1 & 0 \\ 1 & x_2 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} x_1 & 0 \\ 1 & x_2 \end{bmatrix} \oplus \begin{bmatrix} x_1 \end{bmatrix} & (n \text{ odd}) \end{cases}$$

**Second matrix:**

$$B = \begin{cases} \begin{bmatrix} y_1 \end{bmatrix} \oplus \begin{bmatrix} y_2 & 0 \\ 1 & y_1 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} y_2 & 0 \\ 1 & y_1 \end{bmatrix} \oplus \begin{bmatrix} y_2 \end{bmatrix} & (n \text{ even}) \\ \begin{bmatrix} y_1 \end{bmatrix} \oplus \begin{bmatrix} y_2 & 0 \\ 1 & y_1 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} y_2 & 0 \\ 1 & y_1 \end{bmatrix} \oplus \begin{bmatrix} y_2 & 0 \\ 1 & y_1 \end{bmatrix} & (n \text{ odd}) \end{cases}$$

# Exceptional $(p, q)$-sums: the basic construction (2)

$$A + B = \begin{bmatrix} x_1 + y_1 & & & & & & (0) \\ 1 & x_2 + y_2 & & & & & \\ 0 & 1 & x_1 + y_1 & & & & \\ \vdots & 0 & 1 & \ddots & & & \\ \vdots & & & \ddots & \ddots & & \\ & & & & & \ddots & \\ (0) & & \cdots & \cdots & 0 & 1 & ? \end{bmatrix}$$

# Exceptional $(p,q)$-sums: the basic construction (3)

Set

$$z_1 := x_1 + y_1 \quad \text{and} \quad z_2 := x_2 + y_2,$$

$$n = 2q + \varepsilon \quad \text{(Euclidean division).}$$

Then

$$A + B \simeq C((t - z_1)^{q+\varepsilon}(t - z_2)^q)$$

If $z_1 = z_2$ then

$$A + B \simeq J_n(z_1) \quad \text{(Jordan cell).}$$

If $z_1 \neq z_2$, then

$$A + B \simeq J_{q+\varepsilon}(z_1) \oplus J_q(z_2).$$

# What about products?

Assume $p(0)q(0) \neq 0$ (non-degenerate case).
Correspondence table:

| $(p,q)$-sums | $(p,q)$-products |
|---|---|
| $x_i + y_j$ | $x_i y_j$ |
| $\sigma := x_1 + x_2 + y_1 + y_2$ | $\pi := x_1 x_2 y_1 y_2 = p(0)q(0)$ |
| $z \mapsto \sigma - z$ (symmetry) | $z \mapsto \pi z^{-1}$ (inversion) |
| $u = a + b$ | $u = ab$ |
| $u^\star = a^\star + b^\star$ | $u^\star = b^\star a^\star = \pi\, u^{-1}$ |
| $uu^\star$ | $u + u^\star = a(b^\star)^\star + (b^\star)a^\star$ |
| $R(t^2 - \sigma t)$ | $t^d R(t + \pi t^{-1})$ where $d = \deg R$ |

# Is it all over for $r = 2$?

Two possible directions of further research:

- endomorphisms of infinite-dimensional vector spaces;
- **the “double-quadratic" problem.**

# Endomorphisms of infinite-dimensional spaces

**Theorem (Breaz, Shitov, de Seguins Pazzis, (2016-2018))**

*Let $V$ vector space of infinite dimension. Let $p_1, p_2, p_3, p_4 \in \mathbb{F}[t]$ all split, monic w/ degree 2.*
*Every $u \in \mathrm{End}(V)$ is a $(p_1, p_2, p_3, p_4)$-sum!*
*If $(p_1 p_2 p_3 p_4)(0) \neq 0$, every $u \in \mathrm{GL}(V)$ a $(p_1, p_2, p_3, p_4)$-product!*

**Open problem:** can some or all the $p_i$'s be irreducible?

3 **summands/factors:** completed for the reasonable cases, probably little room for improvement

2 **summands/factors:** probably intractable without *drastic* assumptions on $u$
($V$ countable dimensional and $u$ locally finite).

# The quadratic-quadratic problem for sums

Equip $V$ (vector space of finite dimension with $\chi(\mathbb{F}) \neq 2$) with non-degenerate (symmetric or skewsymmetric) bilinear form

$$B : V \times V \to \mathbb{F}$$

Every $u \in \mathrm{End}(V)$ has a $B$-adjoint $u^\bullet$:

$$\forall (x,y) \in V^2,\ B(u^\bullet(x),y) = B(x,u(y)).$$

Let $p, q \in \mathbb{F}[t]$ (with degree 2).

**Quadratic-quadratic problem for sums:** characterize the $B$-selfadjoint $u$ s.t.

$$\exists\ B\text{-selfadjoint } a, b :\ u = a + b \quad \text{and} \quad p(a) = q(b) = 0.$$

**Example:** sum of two orthogonal projections!

# The quadratic-quadratic problem for sums and products

Same issue for skew-selfadjoint elements.

**Quadratic-quadratic problem for products:** characterize the $(p,q)$-products in $\operatorname{Isom}(B)$.

Same issues for Hermitian forms:

- sums of selfadjoints
- products of unitaries

# The quadratic-quadratic problem: the state of the art

| Decomposition | Context | Author (year) |
|---|---|---|
| Products of 2 involutions | Orthogonal groups | Wonenburger (1966) |
| Products of 2 involutions | Symplectic groups | Nielsen (unpublished) |
| Sums of 2 square-zeros | Selfadjoints or skew-selfadjoints | dSP (in preparation) |
| Products of 2 unipotents of index 2 | Orthogonal or symplectic groups | dSP (in preparation) |
| All $(p,q)$-sums | Selfadjoints symplectic form | dSP (in preparation) |

# Conclusion

Much remains to be done!