COMPOSITIO MATHEMATICA

J.-H. EVERTSE
R. TIJDEMAN

Singular differences of powers of 2×2-matrices

Compositio Mathematica, tome 104, n° 2 (1996), p. 199-216
<http://www.numdam.org/item?id=CM_1996__104_2_199_0>

Compositio Mathematica **104:** 199–216, 1996.

Singular differences of powers of 2×2-matrices

J.-H. EVERTSE and R. TIJDEMAN
University of Leiden, Department of Mathematics and Computer Science, P.O. Box 9512, 2300 RA Leiden, The Netherlands
e-mail: evertse@wi.leidenuniv.nl. tijdeman@wi.leidenuniv.nl

Received 30 June 1995; accepted in final form 17 October 1995

Abstract. We describe the pairs of non-singular 2×2-matrices (A, B) with complex entries such that the set of pairs of integers m, n for which $A^m - B^n$ is singular is infinite.

Key words: Matrices, exponential polynomial equations

1. Introduction

Suppose A and B are non-singular 2×2 matrices with rational integral entries. A. D. Pollington asked whether the following two statements are correct:

(a) Assume that for every large N there are at least $N^2/(\log N)^2$ pairs of positive integers m, n with $\max(m, n) \leqslant N$ such that $A^m - B^n$ is singular. Then one of the eigenvalues of A, B is a root of unity.

(b) Assume that A and B have non-real eigenvalues and that for every $\varepsilon > 0$ and for every N exceeding some bound in terms of ε, there are at least $N^{1-\varepsilon}$ pairs of positive integers m, n with $\max(m, n) \leqslant N$ such that $A^m - B^n$ is singular. Then there are integers r, s, not both zero, such that $A^r = B^s$.

Brown, Moran and Pollington [3] needed such results for their research on a conjecture of Schmidt [6] on normality with respect to matrices. Some further work on this conjecture of Schmidt was done by Brown and Moran [1, 2].

In the present paper we show that statements (a) and (b) are correct. More generally, in statement (a) we allow A, B to have complex entries, $N^2/(\log N)^2$ may be replaced by $Nf(N)$ for any function f which is unbounded in N, and we show that either both A and B have an eigenvalue equal to a root of unity or one of the matrices A, B has two eigenvalues equal to a root of unity. In statement b), the conclusion remains valid if A, B are any real 2×2-matrices with non-real eigenvalues such that $A^m - B^n$ is singular for infinitely many pairs (m, n).

Let A, B be two matrices in $\mathrm{GL}_k(\mathbb{C})$, i.e. the group of non-singular $k \times k$-matrices with complex entries. Define

$$\mathcal{S}_{A,B} := \{(m, n) \in \mathbb{Z}^2 : A^m - B^n \text{ is singular}\}.$$

Denote the transpose of a matrix C by C^T. It is obvious that $\mathcal{S}_{A^T,B^T} = \mathcal{S}_{A,B}$. Two pairs $(A, B), (A_1, B_1)$ of matrices in $\mathrm{GL}_k(\mathbb{C})$ are called *similar* if

$$A_1 = JAJ^{-1},\ B_1 = JBJ^{-1} \text{ for some } J \in \mathrm{GL}_k(\mathbb{C}). \tag{1.1}$$

Since (1.1) implies that $A_1^m - B_1^n = J(A^m - B^n)J^{-1}$ we have $\mathcal{S}_{A,B} = \mathcal{S}_{A_1,B_1}$ for similar pairs $(A, B), (A_1, B_1)$.

We are interested in the problem to determine the matrices A, B for which $\mathcal{S}_{A,B}$ is infinite. Clearly, if $(A, B), (A_1, B_1)$ are pairs in $\mathrm{GL}_k(\mathbb{C})$ such that

$$(A, B) \text{ is similar to } (A_1, B_1), (B_1, A_1), (A_1^T, B_1^T) \text{ or } (B_1^T, A_1^T) \tag{1.2}$$

then $\mathcal{S}_{A,B}$ is infinite if and only if $\mathcal{S}_{A_1,B_1}$ is infinite. For pairs of matrices (A, B), (A_1, B_1) satisfying (1.2) we say that (A, B) is *related* to (A_1, B_1).

In this paper we restrict our attention to 2×2-matrices. We describe four types of pairs of matrices (A_1, B_1) in $\mathrm{GL}_2(\mathbb{C})$ for which $\mathcal{S}_{A_1,B_1}$ is infinite.

(I) $A_1^r = \left(\begin{smallmatrix} \theta & * \\ 0 & * \end{smallmatrix}\right)$, $B_1^s = \left(\begin{smallmatrix} \theta & * \\ 0 & * \end{smallmatrix}\right)$ for certain integers r, s, not both zero and some nonzero $\theta \in \mathbb{C}$. Then $A_1^{rt} - B_1^{rt} = \left(\begin{smallmatrix} \theta^t - \theta^t & * \\ 0 & * \end{smallmatrix}\right)$ is singular for every $t \in \mathbb{Z}$.

(II) $A_1^r = \left(\begin{smallmatrix} \theta & 0 \\ 0 & \kappa \end{smallmatrix}\right)$, $B_1^s = \left(\begin{smallmatrix} 0 & \lambda \\ \lambda & 0 \end{smallmatrix}\right)$ for certain integers r, s with $rs \neq 0$ and for some nonzero $\theta, \kappa, \lambda \in \mathbb{C}$ with $\theta\kappa = \lambda^2$. Then $A_1^{r(2t+1)} - B_1^{s(2t+1)} = \left(\begin{smallmatrix} \theta^{2t+1} & -\lambda^{2t+1} \\ -\lambda^{2t+1} & \kappa^{2t+1} \end{smallmatrix}\right)$ is singular for every $t \in \mathbb{Z}$.

(III) $A_1^r = \left(\begin{smallmatrix} \theta & 0 \\ 0 & \kappa \end{smallmatrix}\right)$, $B_1^s = \left(\begin{smallmatrix} 2\lambda+\theta & 2(\lambda+\theta) \\ -(\lambda+\theta) & -2\theta-\lambda \end{smallmatrix}\right)$ for certain integers r, s with $rs \neq 0$ and for some nonzero $\theta, \kappa, \lambda \in \mathbb{C}$ with $\theta^2 = \kappa\lambda$. Then $A_1^{r(2t+1)} - B_1^{s(2t+1)} = \left(\begin{smallmatrix} \theta^{2t+1} - 2\lambda^{2t+1} - \theta^{2t+1} & -2(\lambda^{2t+1} + \theta^{2t+1}) \\ \lambda^{2t+1} + \theta^{2t+1} & \kappa^{2t+1} + 2\theta^{2t+1} + \lambda^{2t+1} \end{smallmatrix}\right)$ is singular for every $t \in \mathbb{Z}$.

(IV) $A_1 = \left(\begin{smallmatrix} \alpha & \alpha \\ 0 & \alpha \end{smallmatrix}\right)$, $B_1 = \left(\begin{smallmatrix} (1-\sqrt{\lambda\mu})\rho & \lambda\rho \\ -\mu\rho & (1+\sqrt{\lambda\mu})\rho \end{smallmatrix}\right)$ where $\alpha, \rho, \lambda, \mu$ are complex numbers such that

$$\begin{cases} (\alpha^m - \rho^n)^2 = \mu mn \alpha^m \rho^n \text{ for infinitely many } (m, n) \in \mathbb{Z}^2, \\ \mu \neq 0, \alpha \text{ and } \rho \text{ are not roots of unity.} \end{cases} \tag{1.3}$$

The equality in (1.3) is equivalent to $\det(A_1^m - B_1^n) = 0$. Hence for every pair $(m, n) \in \mathbb{Z}^2$ satisfying (1.3) we have that $A_1^m - B_1^n$ is singular.

It is easy to check that there are pairs of matrices (A_1, B_1) of type I, II or III. We do not know, whether there are pairs of type IV. We have been able to prove only (cf. Section 3, Lemma 8) that (1.3) implies

$$\begin{cases} \alpha^r = \rho^s =: \varepsilon \text{ is a real quadratic unit for certain } r, s \in \mathbb{Z} \text{ and} \\ \mu \in \mathbb{Q}. \end{cases} \tag{1.4}$$

Our main result is as follows:

THEOREM 1. *Let* (A, B) *be a pair of matrices in* $\mathrm{GL}_2(\mathbb{C})$ *for which* $\mathcal{S}_{A,B} = \{(m,n) \in \mathbb{Z}^2 : A^m - B^n$ *is singular*$\}$ *is infinite. Then* (A, B) *is related to a pair* (A_1, B_1) *of type I, II, III or IV.*

Remark. From (1.4) it follows that if (A, B) is related to a pair of type IV then both A and B have a double, irrational eigenvalue. This implies that a pair of matrices with entries in $\mathbb{Q}$ cannot be related (over $\mathbb{C}$) to a pair of type IV.

From Theorem 1 we shall derive the positive answer to question (b) of Pollington:

COROLLARY. *Let* (A, B) *be a pair of nonsingular* 2×2*-matrices with real entries and with non-real eigenvalues for which the set* $\mathcal{S}_{A,B}$ *is infinite. Then there are integers* r, s*, not both zero, such that* $A^r = B^s$.

We now consider the case that $\mathcal{S}_{A,B}$ has 'large density.' Define the maximum norm of $\mathbf{h} = (h_1, \ldots, h_r) \in \mathbb{C}^r$ by

$$|\mathbf{h}| = \max(|h_1|, \ldots, |h_r|)$$

and for $\mathcal{T} \subseteq \mathbb{Z}^r$, $N \in \mathbb{Z}, N > 0$, put

$$\mathcal{T}(N) := \{\mathbf{h} \in \mathcal{T} : |\mathbf{h}| \leqslant N\}.$$

Note that if (A, B) is related to a pair (A_1, B_1) of type I, II or III, then

$$\limsup_{N \to \infty} \frac{\#\mathcal{S}_{A,B}(N)}{N} > 0.$$

We now consider the pairs (A, B) of matrices in $\mathrm{GL}_2(\mathbb{C})$ for which $\limsup_{N\to\infty} \frac{1}{N} \cdot \#\mathcal{S}_{A,B}(N) = \infty$. We describe two types of pairs (A_1, B_1) with this property:

(V) $A_1^r = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$, $B_1^s = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ for certain nonzero integers r, s. Then $A_1^{rt} - B_1^{su} = \begin{pmatrix} 0 & * \\ 0 & * \end{pmatrix}$ is singular for every $t, u \in \mathbb{Z}$. Note that at least one of the eigenvalues of A_1 and at least one of the eigenvalues of B_1 is a root of unity.

(VI) $A_1^r = \begin{pmatrix} \theta & 0 \\ 0 & \kappa \end{pmatrix}$, $B_1^s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ for certain nonzero integers r, s and for $\theta, \kappa \in \mathbb{C}$ with $\theta\kappa = 1$. Then $A_1^{r(2t+1)} - B_1^{s(2u+1)} = \begin{pmatrix} \theta^{2t+1} & -1 \\ -1 & \kappa^{2t+1} \end{pmatrix}$ is singular for every $t, u \in \mathbb{Z}$. Note that both A_1, B_1 can be diagonalised, that both eigenvalues of B_1 are roots of unity and that the product of the eigenvalues of A_1 is a root of unity.

The following result implies Pollington's statement (a):

THEOREM 2. *Let* (A, B) *be a pair of matrices in* $\mathrm{GL}_2(\mathbb{C})$ *for which the sequence*

$$\frac{\#\mathcal{S}_{A,B}(N)}{N} \quad (N = 1, 2, \ldots) \quad \textit{is unbounded.} \tag{1.5}$$

Then (A, B) is related to a pair (A_1, B_1) of type V or VI.

Note that $\mathcal{S}_{A,B}$ is the set of solutions of the equation $\det(A^m - B^n) = 0$ in $(m, n) \in \mathbb{Z}^2$. This is a special type of exponential polynomial equation. We derive our results stated above from a theorem of Laurent ([4], Théorème 1) on the structure of the set of solutions of exponential polynomial equations. In Section 2 we recall Laurent's theorem and refine this a little bit and in Section 3 we prove our results.

2. Exponential polynomial equations

Let n be a positive integer. For $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ with $\alpha_1 \ldots \alpha_n \neq 0$ and $\mathbf{h} = (h_1, \ldots, h_n) \in \mathbb{Z}^n$ we write $\underline{\alpha}^{\mathbf{h}} := \alpha_1^{h_1} \ldots \alpha_n^{h_n}$. We consider the so-called exponential polynomial equation

$$\sum_{i \in I} f_i(\mathbf{h}) \underline{\alpha}_i^{\mathbf{h}} = 0 \quad \text{in } \mathbf{h} \in \mathbb{Z}^n, \tag{2.1}$$

where I is a finite index set and for each $i \in I$, $f_i(\mathbf{X})$ is a nonzero polynomial in $\mathbb{C}[X_1, \ldots, X_n]$, and $\underline{\alpha}_i = (\alpha_{i1}, \ldots, \alpha_{in})$ is a vector with nonzero complex coordinates.

For each solution of (2.1), the left-hand side of (2.1) can be split into vanishing subsums which are minimal in the sense that each proper subsum of any of the vanishing subsums is non-zero. We shall deal with all solutions corresponding to a given splitting into minimal vanishing subsums. More precisely, let $\mathcal{P}$ be a partition of I, i.e. a collection of non-empty, pairwise disjoint sets $\{P_1, \ldots, P_t\}$ with $P_1 \cup \cdots \cup P_t = I$. For a set P we write $P \prec \mathcal{P}$ if P is a subset of one of $P_1, \ldots, P_t$, and $P \precneqq \mathcal{P}$ if P is a proper subset of one of $P_1, \ldots, P_t$. We shall deal with the subset of solutions of (2.1),

$$U_{\mathcal{P}} = \left\{ \mathbf{h} \in \mathbb{Z}^n : \begin{array}{ll} \sum_{i \in P_j} f_i(\mathbf{h}) \underline{\alpha}_i^{\mathbf{h}} = 0 & \text{for } j = 1, \ldots, t, \\ \sum_{i \in P} f_i(\mathbf{h}) \underline{\alpha}_i^{\mathbf{h}} \neq 0 & \text{for each non-empty } P \precneqq \mathcal{P} \end{array} \right\}. \tag{2.2}$$

To $\mathcal{P}$ we associate two other sets. A pair $i \overset{\mathcal{P}}{\sim} j$ is a pair $i, j \in I$ such that i, j belong to the same set of $\mathcal{P}$. Define the abelian subgroup of $\mathbb{Z}^n$,

$$H_{\mathcal{P}} = \{\mathbf{h} \in \mathbb{Z}^n : \underline{\alpha}_i^{\mathbf{h}} = \underline{\alpha}_j^{\mathbf{h}} \text{ for each pair } i \overset{\mathcal{P}}{\sim} j\}.$$

(If $\mathcal{P}$ consists of singletons, i.e. sets of cardinality 1, then $H_{\mathcal{P}} = \mathbb{Z}^n$.) Let $r = r_{\mathcal{P}} := \operatorname{rank} H_{\mathcal{P}}$. As is well known, $\mathbb{Z}^n$ has a basis $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ such that for certain positive integers $d_1, \ldots, d_r$, $\{d_1 \mathbf{a}_1, \ldots, d_r \mathbf{a}_r\}$ is a basis of $H_{\mathcal{P}}$. Now let

$$S_{\mathcal{P}} = \left\{ \sum_{i=1}^{n} \xi_i \mathbf{a}_i : \xi_i \in \mathbb{Z} \text{ for } i = 1, \ldots, n,\ 0 \leqslant \xi_i < d_i \text{ for } i = 1, \ldots, r \right\}.$$

Then clearly, every $\mathbf{h} \in \mathbb{Z}^n$ can be expressed uniquely as

$$\mathbf{h} = \mathbf{h}' + \mathbf{h}'' \text{ with } \mathbf{h}' \in S_{\mathcal{P}},\ \mathbf{h}'' \in H_{\mathcal{P}}. \tag{2.3}$$

In what follows, for given $\mathbf{h} \in \mathbb{Z}^n$, $\mathbf{h}', \mathbf{h}''$ will always denote the vectors defined by (2.3).

In this section, we write $A \ll B$ or $B \gg A$ if $A \leqslant c \cdot (B+1)$ for some positive constant c depending only on the polynomials f_i and the vectors $\underline{\alpha}_i$ appearing in (2.1). We shall use frequently that for $\mathbf{h} = \sum_{i=1}^n \xi_i \mathbf{a}_i$ with $\underline{\xi} = (\xi_1, \ldots, \xi_n) \in \mathbb{Z}^n$ we have

$$|\mathbf{h}| \gg\ll |\underline{\xi}|, \tag{2.4}$$

with $|\cdot|$ denoting the maximum norm.

LEMMA 1. *Let $\mathbf{h} \in U_{\mathcal{P}}$. Then for the vector $\mathbf{h}' \in S_{\mathcal{P}}$ defined by* (2.3) *we have*

$$|\mathbf{h}'| \ll \log |\mathbf{h}|. \tag{2.5}$$

Proof. This is a straightforward consequence of Laurent [4], Théorème 1. By this theorem, we have $\mathbf{h} = \mathbf{h}'_1 + \mathbf{h}''_1$ with $\mathbf{h}''_1 \in H_{\mathcal{P}}$ and $|\mathbf{h}'_1| \ll \log |\mathbf{h}|$ (Laurent proves this only under the hypothesis that the partition $\mathcal{P}$ does not contain singletons. If $\mathcal{P}$ does contain singletons, $\{i_1\}, \ldots, \{i_s\}$, say, then we can reduce to the case that there are no singletons by removing $i_1, \ldots, i_s$ from I and $\{i_1\}, \ldots, \{i_s\}$ from $\mathcal{P}$, which makes the set $U_{\mathcal{P}}$ larger but does not affect $H_{\mathcal{P}}$). We have $\mathbf{h}'_1 = \mathbf{h}'_2 + \mathbf{h}''_2$ with $\mathbf{h}'_2 \in S_{\mathcal{P}}$, $\mathbf{h}''_2 \in H_{\mathcal{P}}$. This gives $\mathbf{h} = \mathbf{h}'_2 + (\mathbf{h}''_2 + \mathbf{h}''_1)$ with $\mathbf{h}''_2 + \mathbf{h}''_1 \in H_{\mathcal{P}}$. Hence $\mathbf{h}'_2 = \mathbf{h}'$. As $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ is a basis of $\mathbb{Z}^n$ we have

$$\mathbf{h}'_1 = \sum_{i=1}^n \xi_i \mathbf{a}_i \quad \text{with} \quad \underline{\xi} = (\xi_1, \ldots, \xi_n) \in \mathbb{Z}^n,$$

$$\mathbf{h}'_2 = \sum_{i=1}^n \eta_i \mathbf{a}_i \quad \text{with} \quad \underline{\eta} = (\eta_1, \ldots, \eta_n) \in \mathbb{Z}^n,$$

and since $\mathbf{h}'_1 - \mathbf{h}'_2 \in H_{\mathcal{P}}$, i.e. is a linear combination of $\mathbf{a}_1, \ldots, \mathbf{a}_r$, we have $\xi_i = \eta_i$ for $i = r+1, \ldots, n$. Together with (2.4) and $|\xi_i| < d_i, |\eta_i| < d_i$ for $i = 1, \ldots, r$ this implies that

$$|\mathbf{h}'| = |\mathbf{h}'_2| \ll |\underline{\eta}| \ll |\underline{\xi}| \ll |\mathbf{h}'_1| \ll \log |\mathbf{h}|,$$

which is (2.5). □

We need some more precise information about the set $U_{\mathcal{P}}$. To this end we need the following lemma.

LEMMA 2. *Let $f(\mathbf{X}) \in \mathbb{C}[X_1, \ldots, X_n]$ be a polynomial of total degree d that does not vanish identically on $H_{\mathcal{P}}$.*

(i) *For every* $N \in \mathbb{N}$ *we have* $\#\{\mathbf{h} \in H_{\mathcal{P}} : |\mathbf{h}| \leqslant N, f(\mathbf{h}) = 0\} \ll_d N^{r-1}$.
(ii) *There is an* $\mathbf{h} \in H_{\mathcal{P}}$ *with* $|\mathbf{h}| \ll_d 1$ *and* $f(\mathbf{h}) \neq 0$.

Here $r = \text{rank } H_{\mathcal{P}}$ *and the constants implied by* $\ll_d$ *depend only on* d *and* $H_{\mathcal{P}}$.

Proof. We claim that for every non-zero polynomial $g(Y_1, \ldots, Y_r) \in \mathbb{C}[Y_1, \ldots, Y_r]$ of total degree d we have (a) $\#\{\mathbf{y} \in \mathbb{Z}^r : |\mathbf{y}| \leqslant N, g(\mathbf{y}) = 0\} \leqslant dN^{r-1}$ and (b) there is an $\mathbf{y} \in \mathbb{Z}^r$ with $|\mathbf{y}| \leqslant d$ and $g(\mathbf{y}) \neq 0$. We obtain Lemma 2 by applying (a), (b) to $g(\mathbf{Y}) := f(Y_1 a_1 \mathbf{a}_1 + \cdots + Y_r d_r \mathbf{a}_r)$ and using (2.4). We prove (a), (b) by induction on r. For $r = 1$, (a) and (b) are obvious since then g has at most d zeros. Suppose that $r \geqslant 2$ and that (a), (b) are true for polynomials in fewer than r variables. Write $g(\mathbf{Y}) = \sum_{i=0}^{s} g_i(Y_1, \ldots, Y_{r-1}) Y_r^i$ where $s \leqslant d$, $g_i \in \mathbb{C}[Y_1, \ldots, Y_{r-1}]$ is a polynomial of total degree $\leqslant d - i$ for $i = 0, \ldots, s$ and g_s is not identically zero. We express $\mathbf{y} \in \mathbb{Z}^r$ as $(\tilde{\mathbf{y}}, y_r)$ with $\tilde{\mathbf{y}} = (y_1, \ldots, y_{r-1}) \in \mathbb{Z}^{r-1}$. The set $S := \{\mathbf{y} \in \mathbb{Z}^r : |\mathbf{y}| \leqslant N, g(\mathbf{y}) = 0\}$ can be divided into $S_1 := \{\mathbf{y} \in S : g_s(\tilde{\mathbf{y}}) = 0\}$ and $S_2 := \{\mathbf{y} \in S : g_s(\tilde{\mathbf{y}}) \neq 0\}$. By the induction hypothesis, the set $\{\tilde{\mathbf{y}} \in \mathbb{Z}^{r-1} : |\tilde{\mathbf{y}}| \leqslant N, g_s(\tilde{\mathbf{y}}) = 0\}$ has cardinality $\leqslant (d - s)N^{r-2}$. Together with the $\leqslant N$ possibilities for y_r this implies that $\#S_1 \leqslant (d - s)N^{r-1}$. For each $\tilde{\mathbf{y}} \in \mathbb{Z}^{r-1}$ with $|\tilde{\mathbf{y}}| \leqslant N$ and $g_s(\tilde{\mathbf{y}}) \neq 0$ there are at most s values $y_r \in \mathbb{Z}$ with $g(\mathbf{y}) = \sum_{i=0}^{s} g_i(\tilde{\mathbf{y}}) y_r^i = 0$. Hence $\#S_2 \leqslant sN^{r-1}$. It follows that $\#S \leqslant dN^{r-1}$ which is (a). Again by the induction hypothesis, there is a $\tilde{\mathbf{y}} \in \mathbb{Z}^{r-1}$ with $|\tilde{\mathbf{y}}| \leqslant d - s$ and $g_s(\tilde{\mathbf{y}}) \neq 0$ and there is an $y_r \in \mathbb{Z}$ with $|y_r| \leqslant s$ and $g(\mathbf{y}) = \sum_{i=0}^{s} g_i(\tilde{\mathbf{y}}) y_r^i \neq 0$. This implies (b). □

For every $\mathbf{h}' \in S_{\mathcal{P}}$ and each set $P \prec \mathcal{P}$, define the polynomial

$$g_{\mathbf{h}',P}(\mathbf{X}) = \sum_{i \in P} f_i(\mathbf{h}' + \mathbf{X}) \underline{\alpha}_i^{\mathbf{h}'}.$$

From (2.2) and from $\underline{\alpha}_i^{\mathbf{h}''} = \underline{\alpha}_j^{\mathbf{h}''}$ for every $\mathbf{h}'' \in H_{\mathcal{P}}$ and for each pair $i \overset{\mathcal{P}}{\sim} j$, it follows that

$$U_{\mathcal{P}} = \left\{ \mathbf{h} \in \mathbb{Z}^n : \begin{array}{l} g_{\mathbf{h}',P_j}(\mathbf{h}'') = 0 \text{ for } j = 1, \ldots, t, \\ g_{\mathbf{h}',P}(\mathbf{h}'') \neq 0 \text{ for each non-empty } P \precneqq \mathcal{P} \end{array} \right\}, \tag{2.6}$$

where $\mathbf{h}' \in S_{\mathcal{P}}$, $\mathbf{h}'' \in H_{\mathcal{P}}$ are the vectors with $\mathbf{h} = \mathbf{h}' + \mathbf{h}''$ defined by (2.3). We divide $U_{\mathcal{P}}$ into

$$\begin{aligned} U_{\mathcal{P}}^{(1)} = \{&\mathbf{h} \in U_{\mathcal{P}} : \text{ at least one of the polynomials} \\ &g_{\mathbf{h}',P_j} \ (j = 1, \ldots, t) \text{is not identically zero on } H_{\mathcal{P}}\}, \\ U_{\mathcal{P}}^{(2)} = \{&\mathbf{h} \in U_{\mathcal{P}} : \text{ the polynomial } g_{\mathbf{h}',P_j} \text{ is identically zero on} \\ &H_{\mathcal{P}} \text{ for } j = 1, \ldots, t\}. \end{aligned} \tag{2.7}$$

LEMMA 3. *Letting* $U_{\mathcal{P}}^{(1)}(N) = \{\mathbf{h} \in U_{\mathcal{P}}^{(1)} : |\mathbf{h}| \leqslant N\}$ *we have* $\#U_{\mathcal{P}}^{(1)}(N) \ll N^{r-1}(\log N)^{n-r}$ *for* $N > 1$ *if* $0 < r := \text{rank } H_{\mathcal{P}} \leqslant n$ *and* $U_{\mathcal{P}}^{(1)} = \emptyset$ *if* $r = 0$ *or if all polynomials* f_i $(i \in I)$ *are constant on* $H_{\mathcal{P}}$.

Proof. If all polynomials f_i $(i \in I)$ are constant on $H_{\mathcal{P}}$ or if $r = 0$ then for every $\mathbf{h}' \in S_{\mathcal{P}}$, $j = 1, \ldots, t$ the polynomial $g_{\mathbf{h}', P_j}$ is constant on $H_{\mathcal{P}}$, the constancy being trivial if $r = 0$. Hence $g_{\mathbf{h}', P_j}$ is either identically zero on $H_{\mathcal{P}}$ or has no zeros in $H_{\mathcal{P}}$ and from (2.6) it follows that in both cases $U_{\mathcal{P}}^{(1)} = \emptyset$. Suppose that $r > 0$ and that not all polynomials f_i are constant on $H_{\mathcal{P}}$. By Lemma 1 we have for $\mathbf{h} \in U_{\mathcal{P}}^{(1)}(N)$ that $|\mathbf{h}'| \ll \log N$. We can express $\mathbf{h}'$ as $\sum_{i=1}^{n} \xi_i \mathbf{a}_i$ with $(\xi_1, \ldots, \xi_n) \in \mathbb{Z}^n$ where $0 \leqslant \xi_i < d_i$ for $i = 1, \ldots, r$ by the definition of $S_{\mathcal{P}}$ and $|\xi_i| \ll |\mathbf{h}'| \ll \log N$ for $i = r+1, \ldots, n$ by (2.4). Hence the set $S := \{\mathbf{h}' \in S_{\mathcal{P}} : \exists \mathbf{h}'' \in H_{\mathcal{P}} \text{ with } \mathbf{h}' + \mathbf{h}'' \in U_{\mathcal{P}}^{(1)}(N)\}$ has cardinality $\ll (\log N)^{n-r}$. Further, Lemma 2(i) implies that for each $\mathbf{h}' \in S$ the set $\{\mathbf{h}'' \in H_{\mathcal{P}} : |\mathbf{h}''| \leqslant N, g_{\mathbf{h}' P_j}(\mathbf{h}'') = 0 \text{ for } j = 1, \ldots, t\}$ has cardinality $\ll N^{r-1}$. It follows that $\#U_{\mathcal{P}}^{(1)}(N) \ll \#S \cdot N^{r-1} \ll N^{r-1}(\log N)^{n-r}$. □

For a set $S \subseteq \mathbb{Z}^n$ and an abelian subgroup H of $\mathbb{Z}^n$, we define $S + H = \{\mathbf{a} + \mathbf{h} : \mathbf{a} \in S, \mathbf{h} \in H\}$.

LEMMA 4. *There is a finite set* $S \subseteq S_{\mathcal{P}}$ *such that:*

(i) $U_{\mathcal{P}}^{(2)} \subseteq S + H_{\mathcal{P}}$;
(ii) *Every* $\mathbf{h} \in S + H_{\mathcal{P}}$ *satisfies* $\sum_{i \in P_j} f_i(\mathbf{h}) \underline{\alpha}_i^{\mathbf{h}} = 0$ *for* $j = 1, \ldots, t$.

Proof. Let $S = \{\mathbf{h}' \in S_{\mathcal{P}} : \exists \mathbf{h}'' \in H_{\mathcal{P}} \text{ with } \mathbf{h}' + \mathbf{h}'' \in U_{\mathcal{P}}^{(2)}\}$. Obviously $U_{\mathcal{P}}^{(2)} \subseteq S + H_{\mathcal{P}}$. Further, by (2.7) we have for $\mathbf{h}' \in S, \mathbf{h}'' \in H_{\mathcal{P}}$ that

$$\sum_{i \in P_j} f_i(\mathbf{h}' + \mathbf{h}'') \underline{\alpha}_i^{\mathbf{h}' + \mathbf{h}''} = \underline{\alpha}_{i_j}^{\mathbf{h}''} g_{\mathbf{h}', P_j}(\mathbf{h}'') = 0$$

for $j = 1, \ldots, t$ where $i_j \in P_j$. Hence it suffices to show that S is finite. Take $\mathbf{h}' \in S$. Since there is an $\mathbf{h}'' \in H_{\mathcal{P}}$ with $\mathbf{h}' + \mathbf{h}'' \in U_{\mathcal{P}}^{(2)} \subseteq U_{\mathcal{P}}$, the polynomial $g(\mathbf{X}) := \prod_{P \precneqq \mathcal{P}} g_{\mathbf{h}', P}(\mathbf{X})$ is not identically zero on $H_{\mathcal{P}}$. By Lemma 2, there is an $\mathbf{h}'' \in H_{\mathcal{P}}$ with $|\mathbf{h}''| \ll 1$, $g(\mathbf{h}'') \neq 0$, i.e. $g_{\mathbf{h}', P}(\mathbf{h}'') \neq 0$ for each $P \precneqq \mathcal{P}$. Together with (2.8), (2.2) this implies that $\mathbf{h}' + \mathbf{h}'' \in U_{\mathcal{P}}$. But then, by Lemma 1

$$|\mathbf{h}'| \ll \log |\mathbf{h}' + \mathbf{h}''| \ll \log |\mathbf{h}'|.$$

This implies that $|\mathbf{h}'|$ is bounded, i.e. that S is finite. □

We need the following result for exponential polynomial equations in one variable

$$\sum_{i\in I} f_i(h)\alpha_i^h = 0 \quad \text{in } h \in \mathbb{Z}, \tag{2.8}$$

where as before, I is a finite index set and for each $i \in I$, $f_i(X) \in \mathbb{C}[X]$ is non-zero and $\alpha_i \in \mathbb{C}$ is non-zero.

LEMMA 5. *Assume that* (2.9) *has infinitely many solutions. Then there is a partition $\mathcal{P}$ of I, consisting of sets of cardinality $\geqslant 2$, such that for each pair i, j contained in one of the sets of $\mathcal{P}$, α_i/α_j is a root of unity.*

Proof. This result was proved by Skolem–Mahler–Lech, cf. [5]. It is a straightforward consequence of our Lemmas 3 and 4. Since the set of solutions of (2.9) is the union of finitely many sets $U_{\mathcal{P}}$, there is a partition $\mathcal{P}$ of I for which $U_{\mathcal{P}}$ is infinite. There are no singletons in $\mathcal{P}$ since $f_i(h)\alpha_i^h$ has only finitely many zeros. By Lemmas 3 and 4, rank $H_{\mathcal{P}} = 0$ implies that $U_{\mathcal{P}}^{(1)} = \emptyset$ and $U_{\mathcal{P}}^{(2)}$ is finite, hence that $U_{\mathcal{P}}$ is finite. Therefore, $H_{\mathcal{P}} = \{h \in \mathbb{Z}\colon \alpha_i^h = \alpha_j^h \text{ for each pair } i \overset{\mathcal{P}}{\sim} j\}$ has rank 1. This implies Lemma 5. □

3. Proofs of the results

We first prove Theorems 1 and 2 simultaneously, and then derive the Corollary.

A matrix $N \in \mathrm{GL}_2(\mathbb{C})$ is said to be in *normal form* if either $N = \left(\begin{smallmatrix}\alpha & 0\\ 0 & \beta\end{smallmatrix}\right)$ with $\alpha, \beta \in \mathbb{C}^*$ or $N = \left(\begin{smallmatrix}\alpha & \alpha\\ 0 & \alpha\end{smallmatrix}\right)$ with $\alpha \in \mathbb{C}^*$. It is well-known that every $A \in \mathrm{GL}_2(\mathbb{C})$ can be expressed as JNJ^{-1}, with $J \in \mathrm{GL}_2(\mathbb{C})$ and N in normal form. Let (A, B) be the pair of matrices from Theorems 1 and 2. Then $A = J_1N_1J_1^{-1}, B = J_2N_2J_2^{-1}$ with $J_1, J_2 \in \mathrm{GL}_2(\mathbb{C})$ and N_1, N_2 in normal form. (A, B) is related to $(J_1^{-1}AJ_1, J_1^{-1}BJ_1)$. Hence it suffices to prove Theorems 1 and 2 with

$$\begin{aligned} &A \text{ in normal form,}\\ &B = JNJ^{-1} \text{ with } J \in \mathrm{GL}_2(\mathbb{C}) \text{ and } N \text{ in normal form.}\end{aligned} \tag{3.1}$$

In what follows, (A, B) is a pair of matrices satisfying (3.1) and we write $J = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$. Thus, $ad - bc = \det J \neq 0$. Note that

$$\begin{aligned} A^m - B^n \text{ is singular} &\iff A^m - JN^nJ^{-1} \text{ is singular}\\ &\iff A^mJ - JN^n \text{ is singular.}\end{aligned}$$

Hence $\mathcal{S}_{A,B} = \{(m, n) \in \mathbb{Z}^2\colon A^m - B^n \text{ is singular}\}$ is the set of solutions of

$$\det(A^mJ - JN^n) = 0 \quad \text{in} \quad (m, n) \in \mathbb{Z}^2. \tag{3.2}$$

We distinguish the following cases:

(a) $A = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}, N = \begin{pmatrix} \rho & 0 \\ 0 & \sigma \end{pmatrix}$. Then (3.2) becomes (noting that $A^m = \begin{pmatrix} \alpha^m & 0 \\ 0 & \beta^m \end{pmatrix}$, etc.),

$$ad(\alpha^m - \rho^n)(\beta^m - \sigma^n) - bc(\alpha^m - \sigma^n)(\beta^m - \rho^n) =$$

$$(ad - bc)(\alpha\beta)^m + (ad - bc)(\rho\sigma)^n$$

$$-ad\alpha^m\sigma^n - ad\beta^m\rho^n + bc\alpha^m\rho^n + bc\beta^m\sigma^n = 0. \tag{3.2a}$$

(b) $A = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}, N = \begin{pmatrix} \rho & \rho \\ 0 & \rho \end{pmatrix}$. Then (3.2) becomes (noting that $N^n = \begin{pmatrix} \rho^n & n\rho^n \\ 0 & \rho^n \end{pmatrix}$),

$$(ad - bc)(\alpha^m - \rho^n)(\beta^m - \rho^n) - acn\rho^n(a^m - \beta^m) =$$

$$(ad - bc)(\alpha\beta)^m + (ad - bc)\rho^{2n}$$

$$+\{-(ad - bc) - acn\}\alpha^m\rho^n + \{-(ad - bc) + acn\}\beta^m\rho^n = 0. \tag{3.2b}$$

(c) $A = \begin{pmatrix} \alpha & \alpha \\ 0 & \alpha \end{pmatrix}, N = \begin{pmatrix} \rho & \rho \\ 0 & \rho \end{pmatrix}$. Then (3.2) gives

$$(ad - bc)(\alpha^m - \rho^n)^2 - c^2mn\alpha^m\rho^n =$$

$$(ad - bc)\alpha^{2m} + (ad - bc)\rho^{2n} + \{-2(ad - bc) - c^2mn\}\alpha^m\rho^n = 0. \tag{3.2c}$$

In the proof of Theorems 1 and 2 we have to consider all partitions of the left-hand sides of (3.2a), (3.2b) and (3.2c) into vanishing subsums. We can reduce the number of cases by using the following 'symmetry considerations,' which are consequences of the fact that in the proofs of our results (A, B) may be replaced by any related pair satisfying (3.1):

(1) in case (a), $(\alpha, \beta, \rho, \sigma, a, b, c, d)$ may be replaced by $(\rho, \sigma, \alpha, \beta, -d, b, c, -a)$ and in case c), $(\alpha, \rho, a, b, c, d)$ may be replaced by $(\rho, \alpha, -d, b, c, -a)$. Namely, (A, B) is related to $(N, J^{-1}AJ) = (N, \begin{pmatrix} -d & b \\ c & -a \end{pmatrix} A \begin{pmatrix} -d & b \\ c & -a \end{pmatrix}^{-1})$.

(2) in case (a), $(\rho, \sigma, a, b, c, d)$ may be replaced by $(\sigma, \rho, b, -a, d, -c)$. Namely, $B = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix} \begin{pmatrix} \sigma & 0 \\ 0 & \rho \end{pmatrix} \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}^{-1}$.

(3) in cases (a) and (b), $(\alpha, \beta, a, b, c, d)$ may be replaced by $(\beta, \alpha, -c, -d, a, b)$. Namely, (A, B) is related to $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} A \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} B \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1}) =$ $(\begin{pmatrix} \beta & 0 \\ 0 & \alpha \end{pmatrix}, \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} N \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}^{-1})$.

(4) in case (a), $(\alpha, \beta, \rho, \sigma, a, b, c, d)$ may be replaced by $(\beta, \alpha, \sigma, \rho, a, -b, -c, d)$ and in case (b), $(\alpha, \beta, a, b, c, d)$ may be replaced by $(\beta, \alpha, a, -b, -c, d)$. Namely, (A, B) is related to $(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} A^T \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} B^T \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}) = (\begin{pmatrix} \beta & 0 \\ 0 & \alpha \end{pmatrix},$

$\left(\begin{smallmatrix} a & -b \\ -c & d \end{smallmatrix}\right) N' \left(\begin{smallmatrix} a & -b \\ -c & d \end{smallmatrix}\right)^{-1}$), where $N' = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) N^T \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \sigma & 0 \\ 0 & \rho \end{smallmatrix}\right)$ in case (a) and $\left(\begin{smallmatrix} \rho & \rho \\ 0 & \rho \end{smallmatrix}\right)$ in case (b).

Each of the above replacements leads to a permutation of the terms in (3.2a, b, c), provided that with replacement (1), m and n are interchanged.

We deal with a simple case first:

LEMMA 6. *Assume that* $abcd = 0$ *in case* (a), *or* $ac = 0$ *in case* (b), *or* $c = 0$ *in case* (c). *If* $\mathcal{S}_{A,B}$ *is infinite then* (A, B) *is related to a pair of type I. If the sequence* $\#\mathcal{S}_{A,B}(N)/N$ $(N = 1, 2, \ldots,)$ *is unbounded, then* (A, B) *is related to a pair of type V.*

Proof. By symmetry consideration 3, it is no loss of generality to assume $bc = 0$ in case (a) and $c = 0$ in case (b). Further, since in case (a), (A, B) is related to the transposed pair $(A^T, B^T) = (\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right), \left(\begin{smallmatrix} -d & c \\ b & -a \end{smallmatrix}\right) \left(\begin{smallmatrix} \rho & 0 \\ 0 & \sigma \end{smallmatrix}\right) \left(\begin{smallmatrix} -d & c \\ b & -a \end{smallmatrix}\right)^{-1})$, we may assume that $c = 0$ in cases (a), (b) and (c). By substituting $c = 0$ and using that $ad - bc = \det J \neq 0$, (3.2a,b,c) become $(\alpha^m - \rho^n)(\beta^m - \sigma^n) = 0, (\alpha^m - \rho^n)(\beta^m - \rho^n) = 0, \alpha^m - \rho^n = 0$, respectively. In view of symmetry consideration 4, it suffices to prove Lemma 6 with the hypotheses $\mathcal{S}_{A,B}$ infinite, $\#\mathcal{S}_{A,B}(N)/N$ $(N = 1, 2, \ldots,)$ unbounded being replaced by

$$\mathcal{S}' := \{(m, n) \in \mathbb{Z}^2 : \alpha^m = \rho^n\} \quad \text{is infinite} \tag{3.3}$$

$$\#\mathcal{S}'(N)/N \ (N = 1, 2, \ldots) \quad \text{is unbounded,} \tag{3.4}$$

respectively, for all three cases (a), (b), (c). If (3.3) holds, then take $(r, s) \in \mathcal{S}'$ with $(r, s) \neq (0, 0)$. Then $A^r = \left(\begin{smallmatrix} \alpha^r & * \\ 0 & * \end{smallmatrix}\right), B^s = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \left(\begin{smallmatrix} \rho^s & * \\ 0 & * \end{smallmatrix}\right) \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} \rho^s & * \\ 0 & * \end{smallmatrix}\right)$, hence (A, B) is of type I with $\alpha^r = \rho^s = \theta$. If (3.4) holds then take linearly independent $(r_1, s_1), (r_2, s_2) \in \mathcal{S}'$ (these exist since for each 'line' $\mathcal{T} = \{t(r, s) : t \in \mathbb{Z}\} \subseteq \mathcal{S}'$ we have $\#\mathcal{T}(N) \ll N$). Then $\alpha^{r_1 s_2 - r_2 s_1} = \rho^{r_1 s_2 - r_2 s_1} = 1, A^{r_1 s_2 - r_2 s_1} = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right), B^{r_1 s_2 - r_2 s_1} = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$, whence (A, B) is of type V. □

In the sequel we assume that $abcd \neq 0$ in case (a), $ac \neq 0$ in case (b), $c \neq 0$ in case (c). We write $\mathbf{h} = (m, n)$ and in the left-hand sides of (3.2a,b,c) we denote the ith term from the left by $f_i(\mathbf{h})\underline{\alpha}_i^{\mathbf{h}}$. For instance, in (3.2a) we have $f_1(\mathbf{h})\underline{\alpha}_1^{\mathbf{h}} = (ad - bc) \cdot (\alpha\beta)^m 1^n$ with $f_1(\mathbf{h}) = ad - bc, \underline{\alpha}_1 = (\alpha\beta, 1)$, $f_2(\mathbf{h})\underline{\alpha}_2^{\mathbf{h}} = (ad - bc) \cdot 1^m (\rho\sigma)^n, \ldots,$ $f_6(\mathbf{h})\underline{\alpha}_6^{\mathbf{h}} = bc \cdot \beta^m \sigma^n$. Thus, (3.2a, b, c) can be rewritten as $\sum_{i \in I} f_i(\mathbf{h})\underline{\alpha}_i^{\mathbf{h}} = 0$ with $I = \{1, \ldots, 6\}$ in (3.2.a), $I = \{1, \ldots, 4\}$ in (3.2b) and $I = \{1, 2, 3\}$ in (3.2c). By our assumptions on a, b, c, d we have that $f_i(\mathbf{h})$ is not identically zero for $i \in I$. By applying the theory of Section 2 to exponential polynomials in $n = 2$ variables we infer that Theorems 1 and 2 follow from:

PROPOSITION. (i) *Suppose that in cases* (a), (b) *or* (c) *there is a partition* $\mathcal{P}$ *of* I *for which rank* $H_{\mathcal{P}} \geqslant 1$ *and* $U_{\mathcal{P}}$ *is infinite. Then* (A, B) *is related to a pair of type I, II, III or IV.*

(ii) *Suppose that for some partition* $\mathcal{P} = \{P_1, \dots, P_t\}$ *of* I *and some* $\mathbf{a} \in \mathbb{Z}^2$ *we have rank* $H_{\mathcal{P}} = 2$ *and every* $\mathbf{h} \in \mathbf{a} + H_{\mathcal{P}}$ *satisfies* $\sum_{i \in P_j} f_i(\mathbf{h}) \underline{\alpha}_i^{\mathbf{h}} = 0$ *for* $j = 1, \dots, t$. *Then* (A, B) *is related to a pair of type V or VI.*

Namely, if $\mathcal{S}_{A,B}$ is infinite, then there is a partition $\mathcal{P}$ of I for which $U_{\mathcal{P}}$ is infinite. By Lemmas 3 and 4 this is possible only if rank $H_{\mathcal{P}} \geqslant 1$. Since $\#(S + H_{\mathcal{P}})(N) \ll N^{\operatorname{rank} H_{\mathcal{P}}}$ for any finite set S, we have by Lemmas 3 and 4 that $\#U_{\mathcal{P}}^{(1)}(N) \ll \log N, \#U_{\mathcal{P}}^{(2)}(N) \ll N$ if rank $H_{\mathcal{P}} = 1$ and $\#U_{\mathcal{P}}^{(1)}(N) \ll N$ if rank $H_{\mathcal{P}} = 2$. Hence if $\#\mathcal{S}_{A,B}(N)/N$ $(N = 1, 2, \dots)$ is unbounded then there must be a partition $\mathcal{P}$ of I with rank $H_{\mathcal{P}} = 2$ and $U_{\mathcal{P}}^{(2)} \neq \emptyset$. Then Lemma 4 implies that for some $\mathbf{a} \in \mathbb{Z}^2$, every $\mathbf{h} \in \mathbf{a} + H_{\mathcal{P}}$ satisfies $\sum_{i \in P_j} f_i(\mathbf{h}) \underline{\alpha}_i^{\mathbf{h}} = 0$ for $j = 1, \dots, t$. □

The following situation will occur frequently:

LEMMA 7. *Let* $\mathcal{P}$ *be a partition of* I *such that for some positive integer* k, $H_{\mathcal{P}}$ *is contained in one of the groups* $\{\alpha^{km} = \beta^{km} = \rho^{kn}\}^\star$ *(in cases* (a), (b)*),* $\{\alpha^{km} = \beta^{km} = \sigma^{kn}\}$, $\{\alpha^{km} = \rho^{kn} = \sigma^{kn}\}$, $\{\beta^{km} = \rho^{kn} = \sigma^{kn}\}$ *(in case* (a)*). If rank* $H_{\mathcal{P}} \geqslant 1$ *then* (A, B) *is related to a pair of type I and if rank* $H_{\mathcal{P}} = 2$ *then* (A, B) *is related to a pair of type V.*

Proof. By the symmetry considerations, it suffices to consider the case $H_{\mathcal{P}} \subseteq \{\alpha^{km} = \beta^{km} = \rho^{kn}\}$. Recall that (A, B) is related to (A_1, B_1) with $A_1 = J^{-1}AJ, B_1 = J^{-1}BJ = N$. If rank $H_{\mathcal{P}} \geqslant 1$ then for $(r, s) \in H_{\mathcal{P}} \backslash \{(0, 0)\}$ we have

$$A_1^{kr} = J^{-1} \begin{pmatrix} \alpha^{kr} & 0 \\ 0 & \beta^{kr} \end{pmatrix} J = \begin{pmatrix} \alpha^{kr} & 0 \\ 0 & \alpha^{kr} \end{pmatrix},$$

$$B_1^{ks} = N^{ks} = \begin{pmatrix} \rho^{ks} & * \\ 0 & * \end{pmatrix} = \begin{pmatrix} \alpha^{kr} & * \\ 0 & * \end{pmatrix},$$

i.e. (A_1, B_1) is of type I. If rank $H_{\mathcal{P}} = 2$ then there are linearly independent $(r_1, s_1), (r_2, s_2) \in H_{\mathcal{P}}$ and from $\alpha^{kr_i} = \beta^{kr_i} = \rho^{ks_i}$ for $i = 1, 2$ it follows that $\alpha^{k(r_1 s_2 - r_2 s_1)} = \beta^{k(r_1 s_2 - r_2 s_1)} = \rho^{k(r_1 s_2 - r_2 s_1)} = 1$, hence

$$A_1^{k(r_1 s_2 - r_2 s_1)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B_1^{k(r_1 s_2 - r_2 s_1)} = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix},$$

i.e. (A_1, B_1) is of type V. □

---

* short hand for $\{(m, n) \in \mathbb{Z}^2 \colon \alpha^{km} = \beta^{km} = \rho^{kn}\}$

Proof of the Proposition. We first deal with case (a). Recall that the left-hand side of (3.2a) has six terms $f_i(\mathbf{h})\underline{\alpha}_i^{\mathbf{h}}$ $(i \in I = \{1,\dots,6\})$, $f_i(\mathbf{h})\underline{\alpha}_i^{\mathbf{h}}$ being the ith term from the left. If the partition $\mathcal{P}$ of I contains singletons then $U_{\mathcal{P}} = \emptyset$ since each f_i is constant. Therefore we consider only partitions of I without singletons. To each such partition $\mathcal{P}$ we associate a graph G as follows: the vertices of G are $V_1 = \{1,2\}, V_2 = \{3,4\}, V_3 = \{5,6\}$ and $[V_i, V_j]$ with $i \neq j$ is an edge of G if there are $k \in V_i$, $l \in V_j$ belonging to the same set of $\mathcal{P}$. Note that if $[V_1, V_2]$ is an edge of G then $H_{\mathcal{P}} \subseteq \{\alpha^m = \rho^n\}$ or $H_{\mathcal{P}} \subseteq \{\beta^m = \sigma^n\}$, if $[V_1, V_3]$ is an edge then $H_{\mathcal{P}} \subseteq \{\alpha^m = \sigma^n\}$ or $H_{\mathcal{P}} \subseteq \{\beta^m = \rho^n\}$ and if $[V_2, V_3]$ is an edge then $H_{\mathcal{P}} \subseteq \{\alpha^m = \beta^m\}$ or $H_{\mathcal{P}} \subseteq \{\rho^n = \sigma^n\}$.

Subcase (a1). G has at least two edges.
Then $H_{\mathcal{P}}$ satisfies the conditions of Lemma 7 with $k = 1$ and the Proposition follows.

Subcase (a2). G has no edges.
Then $\mathcal{P} = \{\{1,2\},\{3,4\},\{5,6\}\}$. Hence $H_{\mathcal{P}} = \{(\alpha\beta)^m = (\rho\sigma)^n, \alpha^m\sigma^n = \beta^m\rho^n, \alpha^m\rho^n = \beta^m\sigma^n\}$. For $(m,n) \in H_{\mathcal{P}}$ we have $\alpha^m\sigma^n \cdot \alpha^m\rho^n = \beta^m\rho^n \cdot \beta^m\sigma^n$, whence $\alpha^{2m} = \beta^{2m}$ and $\alpha^m\rho^n \cdot \beta^m\rho^n = \beta^m\sigma^n \cdot \alpha^m\sigma^n$, whence $\rho^{2n} = \sigma^{2n}$. This implies $\alpha^{4m} = (\alpha\beta)^{2m} = (\rho\sigma)^{2n} = \rho^{4n}$. So $H_{\mathcal{P}} \subseteq \{\alpha^{4m} = \beta^{4m} = \rho^{4n}\}$. Therefore, we can again apply Lemma 7 and derive the Proposition.

Subcase (a3). $[V_2, V_3]$ is the only edge of G.
Then $\mathcal{P} = \{\{1,2\},\{3,5\},\{4,6\}\}$ or $\mathcal{P} = \{\{1,2\},\{3,6\},\{4,5\}\}$. We consider only $\mathcal{P} = \{\{1,2\},\{3,5\},\{4,6\}\}$; the other possibility can be reduced to this one by our symmetry considerations. With this $\mathcal{P}$ we have

$$H_{\mathcal{P}} = \{(\alpha\beta)^m = (\rho\sigma)^n,\ \rho^n = \sigma^n\},$$
$$U_{\mathcal{P}} = \{(\alpha\beta)^m + (\rho\sigma)^n = 0,\ ad\sigma^n = bc\rho^n,\ ad\rho^n = bc\sigma^n\}.$$

Assuming that $U_{\mathcal{P}} \neq \emptyset$, we have $ad/bc = bc/ad = (\rho/\sigma)^n$ for some $n \in \mathbb{N}$, hence $ad/bc = \pm 1$. But $ad - bc = \det J \neq 0$, so $ad = -bc$. Now (A, B) is related to (A_1, B_1) with

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & b/d \end{pmatrix} A \begin{pmatrix} 1 & 0 \\ 0 & b/d \end{pmatrix}^{-1} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix},$$

$$B_1 = \begin{pmatrix} 1 & 0 \\ 0 & b/d \end{pmatrix} B \begin{pmatrix} 1 & 0 \\ 0 & b/d \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ -a & b \end{pmatrix} \begin{pmatrix} \rho & 0 \\ 0 & \sigma \end{pmatrix} \begin{pmatrix} a & b \\ -a & b \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} \frac{1}{2}(\rho+\sigma) & \frac{1}{2}(\sigma-\rho) \\ \frac{1}{2}(\sigma-\rho) & \frac{1}{2}(\rho+\sigma) \end{pmatrix}.$$

For $(r,s) \in U_{\mathcal{P}}$ we have $\rho^s = -\sigma^s$, $(\alpha\beta)^r = -(\rho\sigma)^s = \rho^{2s}$, and

$$A_1^r = \begin{pmatrix} \alpha^r & 0 \\ 0 & \beta^r \end{pmatrix}, \quad B_1^s = \begin{pmatrix} \frac{1}{2}(\rho^s+\sigma^s) & \frac{1}{2}(\sigma^s-\rho^s) \\ \frac{1}{2}(\sigma^s-\rho^s) & \frac{1}{2}(\rho^s+\sigma^s) \end{pmatrix} = \begin{pmatrix} 0 & \sigma^s \\ \sigma^s & 0 \end{pmatrix}.$$

Hence (A_1, B_1) is of type II, with $\theta = \alpha^r, \kappa = \beta^r, \lambda = \sigma^s$.

Now suppose that rank $H_{\mathcal{P}} = 2$. For linearly independent pairs $(m_1, n_1), (m_2, n_2) \in H_{\mathcal{P}}$ we have $(\alpha\beta)^{m_1 n_2 - m_2 n_1} = (\rho\sigma)^{m_1 n_2 - m_2 n_1} = 1$, $(\rho/\sigma)^{n_1} = (\rho/\sigma)^{n_2} = 1$, hence $\alpha\beta$, ρ and σ are roots of unity. Now choose $(r, s) \in U_{\mathcal{P}}$ and let A_1, B_1 be as above. Let u be an odd integer with $\sigma^u = \pm 1$. (A, B) is related to (A_2, B_2) with

$$A_2 = \begin{pmatrix} (\pm 1)^s & 0 \\ 0 & 1 \end{pmatrix} A_1 \begin{pmatrix} (\pm 1)^s & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix},$$

$$B_2 = \begin{pmatrix} (\pm 1)^s & 0 \\ 0 & 1 \end{pmatrix} B_1 \begin{pmatrix} (\pm 1)^s & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2}(\rho + \sigma) & (\pm 1)^s \cdot \frac{1}{2}(\sigma - \rho) \\ (\pm 1)^s \cdot \frac{1}{2}(\sigma - \rho) & \frac{1}{2}(\rho + \sigma) \end{pmatrix}$$

and we have $\alpha^{ru} \cdot \beta^{ru} = \sigma^{2su} = 1$,

$$A_2^{ru} = \begin{pmatrix} \alpha^{ru} & 0 \\ 0 & \beta^{ru} \end{pmatrix}, \quad B_2^{su} = \begin{pmatrix} 0 & (\pm 1)^s \sigma^{su} \\ (\pm 1)^s \sigma^{su} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Hence (A_2, B_2) is a pair of type VI.

Subcase (a4). $[V_1, V_2]$ or $[V_1, V_3]$ is the only edge of G.
Then $\mathcal{P} = \{\{1,3\},\{2,4\},\{5,6\}\}$ or $\{\{1,4\},\{2,3\},\{5,6\}\}$ or $\{\{1,5\},\{2,6\},\{3,4\}\}$, or $\{\{1,6\},\{2,5\},\{3,4\}\}$. We deal only with $\mathcal{P} = \{\{1,3\},\{2,4\},\{5,6\}\}$; the other possibilities can be reduced to this one by our symmetry considerations. With this $\mathcal{P}$ we have

$$\begin{aligned} H_{\mathcal{P}} &= \{\beta^m = \sigma^n,\ \alpha^m \rho^n = \beta^m \sigma^n\}, \\ U_{\mathcal{P}} &= \{(ad - bc)\beta^m = ad\sigma^n, (ad - bc)\sigma^n = ad\beta^m, \alpha^m \rho^n + \beta^m \sigma^n = 0\}. \end{aligned}$$

Assuming that $U_{\mathcal{P}} \neq \emptyset$ we have $(ad - bc)/ad = ad/(ad - bc)$. Together with $bc \neq 0$ this implies that $(ad - bc)/ad = -1$, i.e. $bc = 2ad$. Now (A, B) is related to (A_1, B_1) with

$$A_1 = \begin{pmatrix} 0 & -b/d \\ 1 & 0 \end{pmatrix} A \begin{pmatrix} 0 & -b/d \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} \beta & 0 \\ 0 & \alpha \end{pmatrix},$$

$$\begin{aligned} B_1 &= \begin{pmatrix} 0 & -b/d \\ 1 & 0 \end{pmatrix} B \begin{pmatrix} 0 & -b/d \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} -2a & -b \\ a & b \end{pmatrix} \begin{pmatrix} \rho & 0 \\ 0 & \sigma \end{pmatrix} \begin{pmatrix} -2a & -b \\ a & b \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 2\rho - \sigma & 2(\rho - \sigma) \\ \sigma - \rho & 2\sigma - \rho \end{pmatrix}. \end{aligned}$$

Take $(r, s) \in U_{\mathcal{P}}$. Then $\beta^r = -\sigma^s$, $\alpha^r \rho^s = -\beta^r \sigma^s = \sigma^{2s}$ and

$$A_1^r = \begin{pmatrix} \beta^r & 0 \\ 0 & \alpha^r \end{pmatrix}, \quad B_1^s = \begin{pmatrix} 2\rho^s - \sigma^s & 2(\rho^s - \sigma^s) \\ \sigma^s - \rho^s & 2\sigma^s - \rho^s \end{pmatrix},$$

hence (A_1, B_1) is a pair of type III with $\theta = \beta^r, \kappa = \alpha^r, \rho^s = \lambda, \sigma^s = -\theta$.

Suppose that rank $H_{\mathcal{P}} = 2$. Choose linearly independent $(m_1, n_1), (m_2, n_2) \in H_{\mathcal{P}}$. Then $\beta^{m_i} = \sigma^{n_i}, (\alpha/\beta)^{m_i} = (\sigma/\rho)^{n_i}$ for $i = 1, 2$, hence $\beta^{m_1 n_2 - m_2 n_1} = \sigma^{m_1 n_2 - m_2 n_1} = 1$, $(\alpha/\beta)^{m_1 n_2 - m_2 n_1} = (\sigma/\rho)^{m_1 n_2 - m_2 n_1} = 1$, which implies that $\alpha, \beta, \rho, \sigma$ are roots of unity. Letting k be a nonzero integer with $\alpha^k = \beta^k = \rho^k = \sigma^k = 1$, we infer that $H_{\mathcal{P}} \subseteq \{\alpha^{km} = \beta^{km} = \rho^{kn}\}$. Together with Lemma 7 this implies that (A, B) is related to a pair of type V.

We continue with case (b). Recall that the left-hand side of (3.2b) has four terms, the ith from the left being denoted by $f_i(\mathbf{h})\underline{\alpha}_i^{\mathbf{h}}$. Again we have to consider some possibilities for $\mathcal{P}$.

Subcase (b1). $\mathcal{P}$ contains singletons.
$f_1(\mathbf{h}), f_2(\mathbf{h})$ are constants, $f_3(\mathbf{h}) = 0$ implies that $n = -(ad-bc)/ac$ and $f_4(\mathbf{h}) = 0$ implies that $n = (ad - bc)/ac$. Hence if $U_{\mathcal{P}} \neq \emptyset$ then $\mathcal{P}$ does not contain $\{1\}$ or $\{2\}$ and at most one of $\{3\}, \{4\}$. Thus, $\mathcal{P} = \{\{1,2,4\},\{3\}\}$ or $\{\{1,2,3\},\{4\}\}$ and in both cases we have $H_{\mathcal{P}} = \{\alpha^m = \beta^m = \rho^n\}$. Now the Proposition follows from Lemma 7.

Subcase (b2). $\mathcal{P} = \{\{1,2\},\{3,4\}\}$ or $\{\{1,2,3,4\}\}$.
Then $H_{\mathcal{P}} \subseteq \{(\alpha\beta)^m = \rho^{2n},\ \alpha^m\rho^n = \beta^m\rho^n\} \subseteq \{\alpha^{2m} = \beta^{2m} = \rho^{2n}\}$. Again the Proposition follows from Lemma 7.

Subcase (b3). $\mathcal{P} = \{\{1,3\},\{2,4\}\}$ or $\{\{1,4\},\{2,3\}\}$.
We deal only with $\mathcal{P} = \{\{1,4\},\{2,3\}\}$ as the other possibility can be reduced to this one by our symmetry considerations. For this $\mathcal{P}$ we have

$$U_{\mathcal{P}} = \{\ (ad-bc)(\alpha\beta)^m + (-(ad-bc) + acn)\beta^m\rho^n = 0,$$
$$(ad-bc)\rho^{2n} + (-(ad-bc) - acn)\alpha^m\rho^n = 0\}.$$

For $(m,n) \in U_{\mathcal{P}}$ we have

$$(1 - acn/(ad-bd)) \cdot (1 + acn/(ad-bc)) = (\alpha^m/\rho^n) \cdot (\rho^n/\alpha^m) = 1,$$

hence $n = 0$. Therefore, $U_{\mathcal{P}} = \{\alpha^m = 1, n = 0\}$. If $U_{\mathcal{P}}$ is infinite then there is a positive integer r with $\alpha^r = 1$; hence $A^r = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right), B^0 = \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ and (A, B) is of type I. Recall that $\mathcal{P} = \{P_1, P_2\}$ with $P_1 = \{1,4\}, P_2 = \{2,3\}$ and that $U_{\mathcal{P}}$ is the set of solutions of $(*)$ $\sum_{i \in P_j} f_i(\mathbf{h})\underline{\alpha}_i^{\mathbf{h}} = 0$ for $j = 1, 2$. So if rank $H_{\mathcal{P}} = 2$ then there is no $\mathbf{a} \in \mathbb{Z}^2$ such that every $\mathbf{h} \in \mathbf{a} + H_{\mathcal{P}}$ satisfies $(*)$, i.e. $\mathcal{P}$ cannot satisfy the hypothesis of part (ii) of the Proposition.

Finally, we deal with case (c). For each partition $\mathcal{P}$ of $\{1,2,3\}$ containing a singleton, $U_{\mathcal{P}}$ is finite; namely $f_1(\mathbf{h}), f_2(\mathbf{h})$ are constants and $f_3(\mathbf{h}) = -2(ad - bc) - c^2mn$ has only finitely many zeros $(m,n) \in \mathbb{Z}^2$. Therefore, we have to deal only with the case $\mathcal{P} = \{1,2,3\}$. (3.2c) can be rewritten as

$$(\alpha^m - \rho^n)^2 - \mu mn\alpha^m\rho^n = \alpha^{2m} + \rho^{2n} + (-2 - \mu mn)\alpha^m\rho^n = 0, \quad (3.5)$$

where $\mu = c^2/(ad - bc)$. We have $\mu \neq 0$ since we assumed that $c \neq 0$. Further,

$$H_{\mathcal{P}} = \{\alpha^m = \rho^n\}.$$

The hypothesis of part (ii) of the Proposition cannot be satisfied. Namely, suppose that rank $H_{\mathcal{P}} = 2$ and that for some $\mathbf{a} = (a, b) \in \mathbb{Z}^2$ every $(m, n) \in \mathbf{a} + H_{\mathcal{P}}$ satisfies (3.5). We have $H_{\mathcal{P}} \supseteq d\mathbb{Z}^2$ for some positive integer d, hence $(a+du, b+dv)$ satisfies (3.5), i.e.

$$\begin{aligned}&(\alpha^a - \rho^b)^2 - \mu(a + du)(b + dv)\alpha^a\rho^b \\ &\quad = \alpha^{-du}\rho^{-dv}\{(\alpha^{a+du} - \rho^{b+dv})^2 - \mu(a + du)(b + dv)\alpha^{a+du}\rho^{b+dv}\} = 0\end{aligned}$$

for every $(u, v) \in \mathbb{Z}^2$. But this is clearly impossible. So we have to prove only part (i) of the Proposition. If one of α, ρ, which by our symmetry considerations we may assume to be α, is a root of unity then (A, B) is related to a pair of type I: namely, if $\alpha^r = 1$ for some positive integer r then $A^r = \begin{pmatrix} \alpha^r & * \\ 0 & * \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ and $B^0 = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$.

Assume that α and ρ are not roots of unity, that rank $H_{\mathcal{P}} = 1$, and that $U_{\mathcal{P}}$, i.e. the set of solutions of (3.5) is infinite. We recall that $\mu \neq 0$. Hence (1.3) holds. Further,

$$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \rho & \rho \\ 0 & \rho \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} (1 - \sqrt{\lambda\mu})\rho & \lambda\rho \\ -\mu\rho & (1 + \sqrt{\lambda\mu})\rho \end{pmatrix}$$

with $\lambda = a^2/(ad - bc), \mu = c^2/(ad - bc)$. Hence (A, B) is of type IV. This completes the proof of the Proposition. □

We now show that (1.3) implies (1.4):

LEMMA 8. *Let α, ρ, μ be nonzero complex numbers such that α and ρ are not roots of unity and such that $(\alpha^m - \rho^n)^2 = \mu mn\alpha^m\rho^n$ has infinitely many solutions in integers m, n. Then $\mu \in \mathbb{Q}$ and there are integers r, s such that $\alpha^r = \rho^s =: \varepsilon$ is a real quadratic unit.*

Proof. By Lemmas 3 and 4 (with $n = 2$) applied to (3.5) and by the fact that α and ρ are not roots of unity, we have that $H_{\mathcal{P}} = \{\alpha^m = \rho^n\}$ has rank 1, i.e.

$$H_{\mathcal{P}} = \{t(r_1, s_1) : t \in \mathbb{Z}\} \tag{3.6}$$

for some fixed $(r_1, s_1) \in \mathbb{Z}^2$ with $r_1 s_1 \neq 0$. Now $(m, n) \in \mathbb{Z}^2$ can be expressed uniquely as $t(r_1, s_1) + (u, p)$ with $t, u \in \mathbb{Z}, p \in \{0, \ldots, s_1 - 1\}$. So for some $p \in \{0, \ldots, s_1 - 1\}$, (3.5) has infinitely many solutions $(tr_1 + u, ts_1 + p)$. In what follows, we fix this p. Thus, there are infinitely many pairs $(u, t) \in \mathbb{Z}^2$ satisfying

$$(\alpha^{tr_1+u} - \rho^{ts_1+p})^2 = \mu(tr_1 + u)(ts_1 + p)\alpha^{tr_1+u}\rho^{ts_1+p}$$

or, dividing by $\alpha^{2r_1t} = \rho^{2s_1t} = \alpha^{r_1t}\rho^{s_1t}$,

$$\frac{\alpha^u}{\rho^p} + \frac{\rho^p}{\alpha^u} - 2 = \mu(tr_1 + u)(ts_1 + p). \tag{3.7}$$

We first show that α, ρ are algebraic. For given u, there are only finitely many t satisfying (3.7). Hence if (u, t) runs through all solutions of (3.7) then u runs through an infinite set. Choose solutions $(u_1, t_1), (u_2, t_2)$ of (3.7) with $u_1 \neq u_2, \alpha^{u_i} \neq \rho^p$ for $i = 1, 2$. Put $\delta := \alpha^{1/s_1}$. Then $\delta = \zeta\rho^{1/r_1}$ for some root of unity ζ. Hence

$$\frac{\zeta^{r_1p}\delta^{s_1u_1 - r_1p} + \zeta^{-r_1p}\delta^{r_1p - s_1u_1} - 2}{\zeta^{r_1p}\delta^{s_1u_2 - r_1p} + \zeta^{-r_1p}\delta^{r_1p - s_1u_2} - 2} = \frac{\mu(t_1r_1 + u_1)(t_1s_1 + p)}{\mu(t_2r_1 + u_2)(t_2s_1 + p)} =: a \in \mathbb{Q}.$$

This shows that δ is a zero of a non-identically zero polynomial with algebraic coefficients, i.e. δ is algebraic. It follows that indeed, α, ρ are algebraic.

Let K be a finite normal extension of $\mathbb{Q}$ containing α, ρ. Then $\mu \in K$. Let σ be an element of the Galois group G of $K/\mathbb{Q}$. Then every solution (u, t) of (3.7) satisfies

$$\mu^{-1}\left(\frac{\alpha^u}{\rho^p} + \frac{\rho^p}{\alpha^u} - 2\right) = \sigma(\mu)^{-1}\left(\frac{\sigma(\alpha)^u}{\sigma(\rho)^p} + \frac{\sigma(\rho)^p}{\sigma(\alpha)^u} - 2\right) \tag{3.8}$$

or

$$\begin{aligned}(\mu^{-1}\rho^{-p})\alpha^u + (\mu^{-1}\rho^p)\alpha^{-u} - (\sigma(\mu)^{-1}\sigma(\rho)^{-p})\sigma(\alpha)^u \\ -(\sigma(\mu)^{-1}\sigma(\rho)^p)\sigma(\alpha)^{-u} + 2(\sigma(\mu)^{-1} - \mu^{-1})1^u = 0.\end{aligned} \tag{3.9}$$

(3.9) is an exponential polynomial equation with infinitely many solutions $u \in \mathbb{Z}$. Suppose that $\sigma(\mu) \neq \mu$. By Lemma 5, there is a $\beta \in \{\alpha, \alpha^{-1}, \sigma(\alpha), \sigma(\alpha)^{-1}\}$ such that $\beta/1$ is a root of unity. Hence α is a root of unity but this is against our assumption. Therefore, $\sigma(\mu) = \mu$. This holds for every $\sigma \in G$; hence $\mu \in \mathbb{Q}$.

By inserting $\mu \in \mathbb{Q}$ in (3.8) we infer that for every solution (u, t) and for every $\sigma \in G$ we have

$$\rho^{-p}\alpha^u + \rho^p\alpha^{-u} - \sigma(\rho)^{-p}\sigma(\alpha)^u - \sigma(\rho)^p\sigma(\alpha)^{-u} = 0. \tag{3.10}$$

From Lemma 5 and the fact that α is not a root of unity, it follows that either $\alpha/\sigma(\alpha)$ or $\alpha\sigma(\alpha)$ is a root of unity. So there is a positive integer r_2 such that for each $\sigma \in G$ we have either $\sigma(\alpha^{r_2}) = \alpha^{r_2}$ or $\sigma(\alpha^{r_2}) = \alpha^{-r_2}$. Hence $G' := \{\sigma \in G : \sigma(\alpha^{r_2}) = \alpha^{r_2}\}$ is a subgroup of index $\leqslant 2$ in G and so its field of invariants $L = \mathbb{Q}(\alpha^{r_2})$ is either $\mathbb{Q}$ or a quadratic field. We infer that with $r = r_1r_2$, $s = s_1r_2$ we have $\alpha^r = \rho^s =: \varepsilon \in L$.

We show that ε is a real quadratic unit. Let $\mathfrak{p}$ be a prime ideal of K. The right-hand side of (3.7) is a rational number with a fixed denominator. Hence there is a

constant C such that $\mathrm{ord}_{\mathfrak{p}}(\alpha^u/\rho^p + \rho^p/\alpha^u - 2) \geqslant C$ for every solution (u,t) of (3.7). As we mentioned above, (3.7) has solutions with arbitrarily large u. Hence $\mathrm{ord}_{\mathfrak{p}}(\alpha) = 0$. This being the case for every prime ideal $\mathfrak{p}$, it follows that α, hence ε, is a unit in L. However, α, hence ε, is not a root of unity, and therefore ε is a real quadratic unit. This completes the proof of Lemma 8. □

Proof of the Corollary. Assume that A, B are non-singular matrices with real entries and non-real eigenvalues such that $A^m - B^n$ is singular for infinitely many pairs $(m,n) \in \mathbb{Z}^2$. The eigenvalues of A are complex conjugates, $\alpha, \overline{\alpha}$, say. Similarly, B has complex conjugate eigenvalues $\rho, \overline{\rho}$. By Theorem 1, (A,B) is related to a pair (A_1, B_1) of type I, II, III, or IV. After interchanging A, B or taking transposes, we may assume that $A = JA_1J^{-1}, B = JB_1J^{-1}$ for some $J \in \mathrm{GL}_2(\mathbb{C})$. We consider all possibilities.

Suppose (A_1, B_1) is of type I, i.e. $A_1^r = \left(\begin{smallmatrix} \theta & * \\ 0 & * \end{smallmatrix}\right), B_1^s = \left(\begin{smallmatrix} \theta & * \\ 0 & * \end{smallmatrix}\right)$ for some $r, s \in \mathbb{Z}$ not both zero and some nonzero $\theta \in \mathbb{C}$. After interchanging $\alpha, \overline{\alpha}$ or $\rho, \overline{\rho}$ if necessary, we have that $\theta = \alpha^r = \rho^s$. We have $A = J_1 \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{smallmatrix}\right) J_1^{-1}$ for some $J_1 \in \mathrm{GL}_2(\mathbb{C})$. If $\alpha^r = \overline{\alpha}^r$, then $A^r = J_1 \left(\begin{smallmatrix} \alpha^r & 0 \\ 0 & \alpha^r \end{smallmatrix}\right) J_1^{-1} = \left(\begin{smallmatrix} \alpha^r & 0 \\ 0 & \alpha^r \end{smallmatrix}\right)$. Further, it follows that $\rho^s = \overline{\rho}^s$, and so $B^s = \left(\begin{smallmatrix} \rho^s & 0 \\ 0 & \rho^s \end{smallmatrix}\right) = A^r$. Suppose that $\alpha^r \neq \overline{\alpha}^r$, i.e. $\theta \neq \overline{\theta}$. Note that θ is an eigenvalue of A^r and B^s with the same eigenvector, $\mathbf{a}$, say. By taking complex conjugates, we obtain a common eigenvector $\mathbf{a}'$ of A^r and B^s with eigenvalue $\overline{\theta}$. Hence A^r and B^s have the same action on two linearly independent vectors, i.e. $A^r = B^s$.

Suppose (A_1, B_1) is of type II, i.e. $A_1^r = \left(\begin{smallmatrix} \theta & 0 \\ 0 & \kappa \end{smallmatrix}\right), B_1^s = \left(\begin{smallmatrix} 0 & \lambda \\ \lambda & 0 \end{smallmatrix}\right)$ for some $r, s \in \mathbb{Z}$ and some nonzero $\theta, \kappa, \lambda \in \mathbb{C}$ with $\theta\kappa = \lambda^2$. Note that A^r, B^s have the same eigenvalues as A_1^r, B_1^s respectively. Hence $\theta\kappa = \alpha^r\overline{\alpha}^r > 0$, $\lambda^2 = -\rho^s\overline{\rho}^s < 0$. But this contradicts $\theta\kappa = \lambda^2$. Hence (A,B) is not related to a pair of type II.

Suppose (A_1, B_1) is of type III, i.e. $A_1^r = \left(\begin{smallmatrix} \theta & 0 \\ 0 & \kappa \end{smallmatrix}\right), B_1^s = \left(\begin{smallmatrix} 2\lambda+\theta & 2(\lambda+\theta) \\ -(\lambda+\theta) & -2\theta-\lambda \end{smallmatrix}\right)$ for some $r, s \in \mathbb{Z}$ with $rs \neq 0$ and some $\theta, \kappa, \lambda \in \mathbb{C}$ with $\theta^2 = \kappa\lambda$. Since A^r, B^s have the same eigenvalues as A_1^r, B_1^s, respectively, we may assume, after interchanging $\alpha, \overline{\alpha}$ or $\rho, \overline{\rho}$ if necessary, that $\alpha^r = \theta$, $\overline{\alpha}^r = \kappa$, $\rho^s = \theta, \overline{\rho}^s = -\lambda$. Thus, $\kappa = -\lambda = \overline{\theta}$, and therefore, $\theta^2 = \kappa\lambda = -\overline{\theta}^2$, $\theta^4 = \overline{\theta}^4$. This implies that $\alpha^{4r} = \overline{\alpha}^{4r} = \rho^{4s} = \overline{\rho}^{4s}$. Now as $A = J_1 \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{smallmatrix}\right) J_1^{-1}$ for some $J_1 \in \mathrm{GL}_2(\mathbb{C})$ we have $A^{4r} = J_1 \left(\begin{smallmatrix} \alpha^{4r} & 0 \\ 0 & \overline{\alpha}^{4r} \end{smallmatrix}\right) J_1^{-1} = \left(\begin{smallmatrix} \alpha^{4r} & 0 \\ 0 & \alpha^{4r} \end{smallmatrix}\right)$, and similarly, $B^{4s} = \left(\begin{smallmatrix} \rho^{4s} & 0 \\ 0 & \rho^{4s} \end{smallmatrix}\right) = A^{4r}$.

Finally, we mention that both A and B have two distinct eigenvalues. Hence (A,B) cannot be related to a pair (A_1, B_1) of type IV. This proves the Corollary. □

References

1. Brown, G. and Moran, W., Schmidt's conjecture on normality for commuting matrices, *Invent. Math.* 111 (1993), 449–463.
2. Brown, G. and Moran, W., Normality with respect to matrices, *Comptes Rendus*, to appear.
3. Brown, G., Moran, W. and Pollington, A. D., The Schmidt conjecture on normality in two dimensions, in preparation.
4. Laurent, M., Équations exponentielles-polynômes et suites récurrentes linéaires II, *J. Number Theory* 31 (1989), 24–53.
5. Lech, C., A note on recurring series, *Ark. Math.* 2 (1953), 417–421.
6. Schmidt, W. M., Normalität bezüglich Matrizen, *J. reine angew. Math.* 214/215 (1964), 227–260.