A MODEL THEORETIC PERSPECTIVE ON MATRIX RINGS

IGOR KLEP AND MARCUS TRESSL

ABSTRACT. In this paper natural necessary and sufficient conditions for quantifier elimination of matrix rings $M_n(K)$ in the language of rings expanded by two unary functions, naming the trace and transposition, are identified. This is used together with invariant theory to prove quantifier elimination when K is an intersection of real closed fields. On the other hand, it is shown that finding a natural definable expansion with quantifier elimination of the theory of $M_n(\mathbb{C})$ is closely related to the infamous simultaneous conjugacy problem in matrix theory. Finally, for various natural structures describing dimension-free matrices it is shown that no such elimination results can hold by establishing undecidability results.

Contents

1.	. Introduction			
2.	Elimination theory of matrix rings		3	
	2.1.	Naming matrix units	3	
	2.2.	Quantifier elimination with trace and transposition	6	
	2.3.	Trace and transposition are needed	12	
	2.4.	The simultaneous conjugacy problem	13	
3.	Undecidability of dimension-free matrices		14	
	3.1.	The universal Horn theory of finite groups	14	
	3.2.	Applications to dimension-free matrices	15	
References				

1. Introduction

This article grew out of an attempt to understand the model theory of full matrix rings in connection with their use in what is called *Free Analysis*. Free Analysis provides a framework for dealing with quantities with the highest degree of non-commutativity, such as large random matrices, see for example [AM16, KVV14, HKM11, Voi10]. Our focus lies in the geometry attached to algebraic functions in this context, meaning noncommutative polynomials over \mathbb{K} (= \mathbb{R} or \mathbb{C}). Here,

Date: April 28, 2020.

²⁰¹⁰ Mathematics Subject Classification. Primary: 03C10, 16R30, 16W22; Secondary: 15A21. Key words and phrases. Model theory, quantifier elimination, matrix rings, trace, decidability, free analysis, simultaneous conjugacy problem.

The first author is supported by the Slovenian Research Agency grants J1-8132, P1-0222. Part of this work was partially supported by the Marsden Fund Council of the Royal Society of New Zealand.

The second author is supported by the MIMS, The Depart of Mathematics, The University of Manchester.

matrices take on the role of field elements when polynomials (=noncommutative polynomials) are considered as functions. For example the polynomial xy - yx can only be distinguished from 0 by evaluating at matrices, say of size 2×2 . If $P(\bar{x})$ is an arbitrary noncommutative polynomial in finitely many variables, then P is 0 if and only if $P(\bar{X}) = 0$ for all tuples \bar{X} of square matrices of any size. Thus, matrices in this context are not restricted to a specific size and we may refer to "dimension-free" matrices when we want to stress this point of view.

There is ongoing interest (cf. [DNT17, Put07]) in the question of whether some form of elimination theory or decidability from the classical case of the field $\mathbb K$ can be rescued in the noncommutative context. This article contributes to these questions in two ways. To explain how, first note that these questions have obvious negative answers if we ask them for the common theory of all matrix rings $M_n(\mathbb K)$; this theory is not model complete in the language of rings as $M_n(\mathbb K)$ is not elementary in $M_{n+1}(\mathbb K)$ for any n, and it is indeed hereditarily undecidable because every non-principal ultraproduct of the $M_n(\mathbb K)$ interprets true arithmetic.

A less naive way to tackle the problem is to consider first order structures that interpret all $M_n(\mathbb{K})$ and then to try to approach elimination theory and decidability questions for such structures. We show that the most commonly used structures that are used in Free Analysis, interpret all matrix ring $M_n(\mathbb{K})$ and are undecidable. This is done in Section 3. (We point out that the community has not agreed on the exact structure to be used for dimension-free matrices yet.) This already implies that quantifier elimination results similar to those for algebraically closed fields or real closed fields cannot be expected to hold true for structures interpreting all $M_n(\mathbb{K})$. However it is unclear if a weakened elimination result like model-completeness holds true in a suitable language.

In this context it is important to understand the elimination theory of matrix rings of fixed size, which, surprisingly, is strongly tied to the well-known simultaneous conjugacy problem for matrices. To be more precise, let \mathcal{L} be the first-order language of rings. The question about the elimination theory of $M_n(\mathbb{K})$ in this language, a priori, seems to be all answered by the classical results for the field \mathbb{K} . (Contemporary model theory might even identify the bi-interpretable structures \mathbb{K} and $M_n(\mathbb{K})$.) However, already $M_n(\mathbb{C})$ does not have quantifier elimination in \mathcal{L} (cf. 2.1.8) and it admits quantifier elimination only if invariants for the simultaneous conjugacy problem are named in an extended language. This is done in Section 2.4.

We now explain our main contribution, namely the elimination theory of matrix rings of fixed size $n \times n$. We switch to an arbitrary field K. A classical comparison of the field K and the matrix ring $M_n(K)$ in terms of how the bi-interpretation is done reveals a more subtle elimination theory of $M_n(K)$. For an example, consider polynomials P(x,y), Q(x,y). The solution set in $M_n(K)^2$ of $P(x,y) = 0, Q(x,y) \neq 0$, seen as a subset of $K^{2 \cdot n^2}$, is closed under simultaneous conjugation. The question of whether the projection onto the X-coordinate(s) has this property is not answered within the elimination theory of K. The issue is that the quantifier-free definable sets in $M_n(K)$ (in the language of rings for now) single out certain K-definable sets and not all K-varieties can be described quantifier-free in $M_n(K)$. The ring $M_n(K)$ is quantifier-free definable in the field K. Conversely, K is universally definable in the ring $M_n(K)$ as its center¹ and in 2.1.4 we see an existential definition. However

¹It should also be noted that for any field K, the ring $M_n(K)$ is already interpretable in the monoid $(M_n(K), \cdot)$ when $n \geq 3$. The reason is that $(M_n(K), \cdot)$ interprets the poset of vector subspaces of K^n and one can then invoke incidence geometry, see [Tre17, 5.1]. For the interpretation

there is no field K that is quantifier-free definable in the ring $M_n(K)$ as its center, see 2.3.

In Section 2 we identify natural necessary and sufficient conditions for quantifier elimination of $M_n(K)$ in the language of rings expanded by two unary functions, naming the trace and transposition. This is obtained for formally real Pythagorean fields (see 2.2.4) and it says that $M_n(K)$ has quantifier elimination in the extended language if and only if there is some $D \in \mathbb{N}$ depending only on n such that for all d and any two d-tuples of $n \times n$ matrices $X, Y \in M_n(K)^d$ with

$$tr(w(X, X^t)) = tr(w(Y, Y^t))$$

for all words w in x, x^t of length $\leq D$, there is some $O \in M_n(K)$ with $OO^t = I_n$ and $O^tX_iO = Y_i$ for all i, i.e., the tuples X and Y are orthogonally equivalent over K.

This condition is satisfied for the field of real numbers and more generally for every intersection of real closed fields, see 2.2.5. A similar result holds for the complex field, however the involution properly expands the matrix ring to include the reals. As mentioned above, quantifier elimination of a natural *definable* expansion of $M_n(\mathbb{C})$ is closely related to the simultaneous conjugacy problem; see 2.4.

For the theory of matrix rings and more generally, C*-algebras from a continuous logic perspective we refer the reader to e.g. [FHS14]. We use basic model theory and standard notations as explained for example in [Hod93]. For generalities on decidability in first order logic see [Rau10]. All rings and algebras in this paper are associative but not necessarily commutative or unital. Fields are commutative.

2. Elimination theory of matrix rings

In this section we are concerned with the elimination theory of matrix rings of fixed size. The first subsection is of preliminary nature and deals with model-completeness in the ring language and with quantifier elimination after naming matrix units. After that, in the main part, we study natural expansions by trace and transposition (or adjoint). In particular, we prove quantifier elimination of the ring $M_n(\mathbb{R})$ expanded by the trace, transposition and the order on its center, see 2.2.6.

- 2.1. Naming matrix units. In this subsection we show that model complete expansions of fields have model complete matrix rings in their natural language, see 2.1.7. If we name matrix units, the same is true for quantifier elimination, see 2.1.11.
- 2.1.1. On matrix units. Let A be a ring, $n \in \mathbb{N}$ and for $i, j \in \{1, ..., n\}$ let $a_{ij} \in A$. Suppose for all $i, j, s, t \in \{1, ..., n\}$ we have $a_{ij} \cdot a_{st} = \delta_{js} a_{it}$. The following properties are easily verified.
 - (1) For $i, j, s, t \in \{1, ..., n\}$ we have $a_{ss}a_{ij}a_{tt} = \delta_{is}\delta_{jt}a_{ij}$.
- (2) If $a_{ij} = 0$ for some i, j, then $a_{st} = a_{si} \cdot a_{ij} \cdot a_{jt} = 0$ for all s, t. Now assume all $a_{ij} \neq 0$. Then the a_{ij} $(1 \leq i, j \leq n)$ are linearly independent over any central subfield F of A.
- (3) For $(x_{ij})_{i,j\in\{1,...,n\}}$, $(y_{ij})_{i,j\in\{1,...,n\}} \in M_n(F)$, we have

$$\left(\sum_{i,j=1}^{n} x_{ij} a_{ij}\right) \cdot \left(\sum_{i,j=1}^{n} y_{ij} a_{ij}\right) = \sum_{i,j=1}^{n} \left(\sum_{k=1}^{n} x_{ik} y_{kj}\right) a_{ij}.$$

we code a subspace as the range of a matrix and note that $ran(A) \subseteq ran(B) \iff \exists C \in M_n(K) : A = BC$.

4

(4) Let F be a central subfield of A. The map

$$M_n(F) \longrightarrow A, \quad (u_{ij})_{i,j \in \{1,\dots,n\}} \longmapsto \sum_{i,j=1}^n u_{ij} a_{ij}$$

is a (not necessarily unital) F-algebra homomorphism, because it is clearly F-linear and it is a ring homomorphism by (3). If $a_{ij} \neq 0$ for all $i, j \in \{1, \ldots, n\}$, then by (2) this map is injective.

To see an example where the map is not unital, choose any field F, set n = 1 < m, $A = M_m(F)$ and take $a_{11} \in A \setminus \{0, I_m\}$ with $a_{11}^2 = a_{11}$.

- 2.1.2. **Defining matrix units.** The language of unital rings is denoted by $\mathcal{L}_{\text{ri}} = \{+,\cdot,-,0,1\}$. Let F be a field and let $M = M_n(F)$. The center $C = C_n$ of M is isomorphic to F, but we will work with C instead of F. For $N \in \mathbb{N}$ we consider $M_N(C)$ as a subset of M^{N^2} and as an F-algebra via the natural embedding $F \cong C \hookrightarrow M_N(C)$. Take $2N^2 + 2$ variables $\bar{u} = (u_{ij} \mid i, j \in \{1, \dots N\}), \ \bar{x} = (x_{ij} \mid i, j \in \{1, \dots N\}), \ y, \ v$. Consider the following \mathcal{L}_{ri} -formulas:
 - (1) Let $\varepsilon = \varepsilon_N(\bar{u})$ be the formula $\bigwedge_{i,j,t=1}^N u_{ij} \cdot u_{jt} = u_{it} \neq 0 \land \bigwedge_{i,j,s,t=1,j\neq s}^N u_{ij} \cdot u_{st} = 0$.
 - (2) Let $\delta = \delta_N(v, \bar{u})$ be the formula $\bigwedge_{s,t=1}^N v \cdot u_{st} = u_{st} \cdot v$.
 - (3) Let $\lambda_N(\bar{x}, y, \bar{u})$ be the formula $y = \sum_{i,j=1}^N x_{ij} \cdot u_{ij}$.

Finally let $\gamma = \gamma_N(\bar{x}, y, \bar{u})$ be the formula $\lambda(\bar{x}, y, \bar{u}) \wedge \varepsilon(\bar{u}) \wedge \bigwedge_{i,j=1}^N \delta(x_{ij}, \bar{u})$. By 2.1.1 we then obtain

- 2.1.3. **Proposition.** For $i, j \in \{1, ..., N\}$ let $E_{ij} \in M_N(C)$ be the $N \times N$ -matrix that has exactly one nonzero entry, namely $1 \in C$ at position (i, j).
- (1) If $\Theta: M_N(C) \longrightarrow M_n(F) = M$ is a (not necessarily unital) embedding of F-algebras, then the N^2 -tuple $\bar{a} := (\Theta(E_{ij}))_{i,j \in \{1,...N\}} \in M^{N^2}$ is a realization of $\varepsilon_N(\bar{u})$, and $\gamma_N(\bar{x}, y, \bar{a})$ defines the graph of Θ in the ring M.
- (2) For every realization $\bar{a} = (a_{ij})_{i,j \in \{1,...,N\}} \in M^{N^2}$ of ε_N in M, there is a unique (not necessarily unital) embedding of F-algebras $\Theta_{\bar{a}} : M_N(C) \longrightarrow M_n(F)$ such that $\Theta_{\bar{a}}(E_{ij}) = a_{ij} \ (i,j \in \{1,...,N\})$. Explicitly, the graph of $\Theta_{\bar{a}}$ is defined by $\gamma_N(\bar{x},y,\bar{a})$.

Consequently the family of all (not necessarily unital) embeddings of F-algebras $M_N(C) \longrightarrow M_n(F)$ is quantifier-free definable in M by $\gamma(\bar{x}, y, \bar{u})$ and its parameter set is quantifier-free defined by $\varepsilon(\bar{u})$.

2.1.4. Corollary. For any field F the center of $M_n(F)$ is existentially definable by $\exists \bar{u} \ \Big(\varepsilon_n(\bar{u}) \wedge \delta_n(v, \bar{u}) \Big).$

2.1.5. Corollary.

- (1) For a field F, the theory of $M_n(F)$ is axiomatised by saying the following about a model A with center C:
 - (a) A is a ring whose center C is elementarily equivalent to F.
 - (b) There is some realization $\bar{a} = (a_{ij})_{i,j \in \{1,...,n\}}$ of ε_n in A^{n^2} and for each such realization, $\gamma_n(\bar{x}, y, \bar{a})$ defines an isomorphism $M_n(C) \longrightarrow A$.
- (2) If A, B are rings that are elementarily equivalent to $M_n(F)$, and if A is a subring of B, then the center C_A of A is a subring of C_B . Further, for each realization $\bar{a} = (a_{ij})_{i,j \in \{1,...,n\}}$ of ε_n in A^{n^2} the following diagram commutes:

$$A \hookrightarrow B$$

$$\Theta_{\bar{a}} \cong \cong \Theta_{\bar{a}}$$

$$M_n(C_A) \hookrightarrow M_n(C_B)$$

2.1.6. **Definition.** Let F be a field and let \tilde{F} be an expansion of F in some language \mathscr{L} extending \mathscr{L}_{ri} . Then we define the \mathscr{L} -structure $M_n(\tilde{F})$ as the structure expanding the ring $M_n(F)$ and that interprets new relation symbols and constant symbols only on the center C of $M_n(F)$ as given by \tilde{F} . A new m-ary function symbol f is interpreted on C^m as given by \tilde{F} , and set to be 0 outside of C^m .

For algebraically closed fields, the following may be found in [Ros80, Theorem 5.4].

2.1.7. **Proposition.** If \tilde{F} is a model complete expansion of a field F in some language \mathcal{L} extending \mathcal{L}_{ri} , then the \mathcal{L} -structure $M_n(\tilde{F})$ is also model complete. Hence, for example, the ring $M_n(\mathbb{C})$ is model complete and the ring $M_n(\mathbb{R})$ expanded by the natural order on its center is model complete.

Proof. This is a routine argument using 2.1.5: Let \tilde{A}, \tilde{B} be \mathscr{L} -structures with underlying rings A, B respectively. Suppose \tilde{A}, \tilde{B} are elementarily equivalent to $M_n(\tilde{F})$ with $\tilde{A} \subseteq \tilde{B}$. We need to show that $\tilde{A} \prec \tilde{B}$. Choose a realization $\bar{a} = (a_{ij})_{i,j \in \{1,\ldots,n\}}$ of ε_n in A^{n^2} as in 2.1.5(1) and consider the commutative diagram of 2.1.5(2). We see that the \mathscr{L} -structure \mathscr{M} induced by \tilde{A} on C_A is a substructure of the \mathscr{L} -structure \mathscr{N} induced by \tilde{B} on C_B . By assumption this extension is elementary. Since \tilde{A} is interpretable in \mathscr{M} in the same way \tilde{B} is interpretable in \mathscr{N} , we get $\tilde{A} \prec \tilde{B}$.

2.1.8. Remark. A corresponding version of 2.1.7 for quantifier elimination (instead of model completeness) fails; for instance the ring $M_n(\mathbb{C})$ does not have quantifier elimination in \mathcal{L}_{ri} for any $n \geq 2$. In fact, by [Ros78, proof of Theorem 3.2], for any infinite field F, the center of $M_n(F)$ is not quantifier-free definable with parameters from $F \cdot I_n$ in the ring $M_n(F)$.

A geometric argument goes as follows: Assume $F \cdot I_n$ is quantifier-free $F \cdot I_n$ -definable in $M_n(F)$. Then $F \cdot I_n$ is a finite union of nonempty sets of the form $\{X \in M_n(F) \mid p_1(X) = \ldots = p_r(X) = 0 \text{ and } q_1(X), \ldots, q_s(X) \neq 0\}$, where p_i, q_j are univariate polynomials from F[t]. Since such polynomials have only finitely many roots in F and F is infinite, one of these sets is of the form $\{X \in M_n(F) \mid q_1(X), \ldots, q_s(X) \neq 0\}$. But then $F \cdot I_n$ has nonempty Zariski interior in $M_n(F)$, a contradiction.

If we allow matrix units as parameters, then a corresponding version of 2.1.7 for quantifier elimination does hold.

2.1.9. **Lemma.** If U is a subring of $M_n(F)$, F a field and U contains the standard matrix units E_{ij} , $1 \le i, j \le n$, then

$$R_U = \{a \in F \mid a \text{ is the } (1,1) \text{ entry of some } Y \in U\}$$

is a subring of F and $U = M_n(R_U)$.

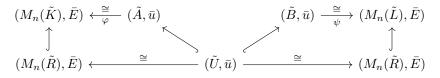
Proof. Let $a, b \in R_U$, say a is the (1,1) entry of $X \in U$, and b is the (1,1) entry of $Y \in U$. Then a + b is the (1,1) entry of $X + Y \in U$, and ab is the (1,1) entry of $XE_{11}YE_{11} \in U$, proving then R_U is a subring of k.

Given $X \in U \subseteq M_n(F)$, $X = (x_{ij})_{i,j}$, we see that x_{ij} is the (1,1) entry of $E_{1i}XE_{j1} \in U$, so $U \subseteq M_n(R_U)$. Conversely, if $X = (x_{ij})_{i,j} \in M_n(R_U)$, then each x_{ij} is the (1,1) entry of some $Y_{ij} \in U$. Hence $X = \sum_{i,j} E_{i1}Y_{ij}E_{1j} \in U$.

- 2.1.10. Recall from [Hod93, Thm. 8.4.1] that an \mathscr{L} -theory T has quantifier elimination if and only if it is model complete and models of T have the amalgamation property over substructures.
- 2.1.11. **Proposition.** Let \tilde{F} be an expansion with quantifier elimination of a field F in some language \mathcal{L} extending \mathcal{L}_{ri} and let $\bar{c} = (c_{ij})_{i,j \in \{1,...,n\}}$ be new constant symbols. Then the $\mathcal{L}(\bar{c})$ -structure $(M_n(\tilde{F}), \bar{e})$, where \bar{c} is interpreted by a tuple \bar{e} of matrix units, also has quantifier elimination.

In particular, the ring $M_n(\mathbb{C})$ expanded by the standard matrix units E_{ij} and the ring $M_n(\mathbb{R})$ expanded by the natural order on its center and the standard matrix units E_{ij} have quantifier elimination.

Proof. Since $M_n(\tilde{F})$ is model complete by 2.1.7, it suffices to show that the theory of $(M_n(\tilde{F}), \bar{e})$ has the amalgamation property. Let $(\tilde{A}, \bar{a}), (\tilde{B}, \bar{b})$ be $\mathscr{L}(\bar{c})$ -structures with underlying rings A, B respectively. Suppose $(\tilde{A}, \bar{a}), (\tilde{B}, \bar{b})$ are elementarily equivalent to $(M_n(\tilde{F}), \bar{e})$ and suppose \mathscr{U} is a common $\mathscr{L}(\bar{c})$ -substructure. Hence $\mathscr{U} = (\tilde{U}, \bar{u})$, where \tilde{U} is an expansion of a common subring U of A and B, and $\bar{u} = \bar{a} = \bar{b}$. Let K, L be the center of A, B respectively. By 2.1.5 there are ring isomorphisms $\varphi : A \longrightarrow M_n(K), \psi : B \longrightarrow M_n(L)$ that map u_{ij} to the standard matrix unit E_{ij} for all i, j. We expand $M_n(K)$ to the \mathscr{L} -structure $M_n(\tilde{K})$ that makes φ an \mathscr{L} -isomorphism $\tilde{A} \longrightarrow M_n(\tilde{K})$, and similarly for $M_n(L)$. By 2.1.9, there are subrings $R \subseteq K, S \subseteq L$ such that the restriction of φ, ψ to U are isomorphisms onto $M_n(R), M_n(S)$ respectively. We expand $M_n(R), M_n(S)$ to the induced \mathscr{L} -substructures of $M_n(\tilde{K}), M_n(\tilde{L})$ respectively and obtain the following commutative diagram:



Restricting all maps to centers and using that \tilde{F} has quantifier elimination, there is some $\tilde{\Omega}$ elementarily equivalent to \tilde{K} and \tilde{L} together with \mathscr{L} -embeddings $\varepsilon:\tilde{K}\longrightarrow \tilde{\Omega}$, $\delta:\tilde{L}\longrightarrow \tilde{\Omega}$ such that for every v in the center of U we have $\varepsilon(\varphi(v))=\delta(\psi(v))$. Let $\bar{\varepsilon}:M_n(K)\longrightarrow M_n(\Omega)$, $\bar{\delta}:M_n(L)\longrightarrow M_n(\Omega)$ be the unique extensions of ε,δ preserving the standard matrix units. We see that $\bar{\varepsilon},\bar{\delta}$ are $\mathscr{L}(\bar{c})$ -morphisms and thus the desired amalgamation is given by the maps $\bar{\varepsilon}\circ\varphi$ and $\bar{\delta}\circ\psi$.

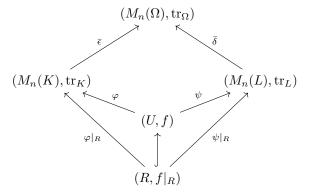
2.2. Quantifier elimination with trace and transposition. We have seen in 2.1.11 that quantifier elimination of a field in a suitable language carries over to its matrix rings if we allow naming of definable parameters (i.e., the set of these parameters is 0-definable). Without parameters the assertion fails, see 2.1.8. We now consider quantifier elimination of expansions of matrix rings by trace and transposition in the case of Pythagorean fields. We will see in 2.2.4 that quantifier elimination is equivalent to a property in invariant theory describing simultaneous orthogonal similarity of matrices. For the real field the characterization entails

quantifier elimination of the ring $M_n(\mathbb{R})$ expanded by the trace, transposition and the order on its center.

- 2.2.1. **Lemma.** Let K, L be fields. Let \mathscr{L} be the extension of \mathscr{L}_{ri} by a unary function symbol F. Consider the \mathscr{L} -structures $(M_n(K), \operatorname{tr}_K)$ and $(M_n(L), \operatorname{tr}_L)$. Let (U, f) be an \mathscr{L} -structure and suppose we are given \mathscr{L} -embeddings $\varphi : (U, f) \hookrightarrow (M_n(K), \operatorname{tr}_K)$ and $\psi : (U, f) \hookrightarrow (M_n(L), \operatorname{tr}_L)$. Then
- (1) The subring R of U generated by the image of f is commutative and $\varphi(R) \subseteq K \cdot I_n$, $\psi(R) \subseteq L \cdot I_n$.
- (2) If $K \cdot I_n$ and $L \cdot I_n$ can be amalgamated over $\varphi|_R$, $\psi|_R$ into some field Ω by maps $\varepsilon : K \cdot I_n \longrightarrow \Omega \cdot I_n$, $\delta : L \cdot I_n \longrightarrow \Omega \cdot I_n$, then for the induced maps $\bar{\varepsilon} : M_n(K) \longrightarrow M_n(\Omega)$, $\bar{\delta} : M_n(L) \longrightarrow M_n(\Omega)$ and every $X \in U$ we have

$$\operatorname{tr}_{\Omega}(\bar{\varepsilon}(\varphi(X))) = \operatorname{tr}_{\Omega}(\bar{\delta}(\psi(X))).$$

Here are the maps in a (not necessarily commutative) diagram.



Proof. (1) Let $X \in U$, then $\varphi(f(X)) = \operatorname{tr}_K(\varphi(X))$ since φ is an \mathscr{L} -homomorphism $(U, f) \longrightarrow (M_n(K), \operatorname{tr}_K)$. Since $\operatorname{tr}_K(\varphi(X)) \in K \cdot I_n$ we get $\varphi(f(X)) \in K \cdot I_n$. Hence $\varphi(f(U)) \subseteq K \cdot I_n$. Since φ is an embedding $U \longrightarrow M_n(K)$, R is commutative and $\varphi(R) \subseteq K \cdot I_n$. Similarly, $\psi(R) \subseteq L \cdot I_n$.

(2) For $X \in U$ we have

$$\begin{split} \operatorname{tr}_{\Omega}(\bar{\varepsilon}(\varphi(X))) &= \varepsilon(\operatorname{tr}_{K}(\varphi(X))) \text{ since } \operatorname{tr}_{\Omega} \circ \bar{\varepsilon} = \varepsilon \circ \operatorname{tr}_{K} \\ &= \varepsilon(\varphi(f(X))) \text{ since } \operatorname{tr}_{K} \circ \varphi = \varphi \circ f \\ &= \delta(\psi(f(X))) \text{ since } \varepsilon \circ \varphi = \delta \circ \psi, \end{split}$$

and similarly $\operatorname{tr}_{\Omega}(\bar{\delta}(\psi(X))) = \delta(\psi(f(X))).$

- 2.2.2. **Theorem.** Let Ω be a real closed field or the algebraic closure of a real closed field. For $X_1, \ldots, X_d, Y_1, \ldots, Y_d \in M_n(\Omega)$ the following are equivalent:
 - (1) There is some unitary $O \in M_n(\Omega)$ with $O \cdot X_i \cdot O^* = Y_i$ for all $i \in \{1, ..., d\}$.
 - (2) For every word w in the letters $x_1, \ldots, x_d, x_1^*, \ldots, x_d^*$ we have

$$\operatorname{tr}_{\Omega}(w(X_1,\ldots,X_d,X_1^*,\ldots,X_d^*)) = \operatorname{tr}_{\Omega}(w(Y_1,\ldots,Y_d,Y_1^*,\ldots,Y_d^*)).$$

(3) For every word w of degree $\leq n^2$ in the letters $X_1, \ldots, X_d, X_1^*, \ldots, X_d^*$,

$$\operatorname{tr}_{\Omega}(w(X_1,\ldots,X_d,X_1^*,\ldots,X_d^*)) = \operatorname{tr}_{\Omega}(w(Y_1,\ldots,Y_d,Y_1^*,\ldots,Y_d^*)).$$

²If Ω is real closed then X^* is the transpose of X. If Ω is the algebraic closure of a real closed field $\Omega_0 \subseteq \Omega$ then X^* is the conjugate transpose of X with respect to Ω_0 .

Proof. The equivalence of (1) and (2) over \mathbb{C} is established in [Wie62, Thm. 4] and in [Sib68, Cor. 1]. The equivalence of (1) and (2) over \mathbb{R} is given by [Sib68, Lemma 2] (see also [Pro76, Thm 7.1, Thm. 15.3]). For degree bounds in (3) (when $\Omega = \mathbb{R}$ or \mathbb{C}), see [Pro76, Thm 7.3] and [Raz74].³ Since (2) is equivalent to (3), all equivalences carry over to all real closed fields and to their algebraic closures.

2.2.3. **Observation.** Let F be a formally real field. Then

$$X = 0 \iff \operatorname{tr}(X^t X) = 0$$

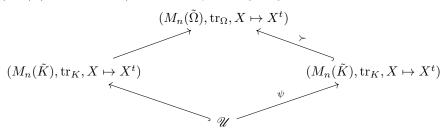
for every matrix $X = (x_{ij}) \in M_n(F)$, because $\operatorname{tr}(X^t X) = \sum_{i,j} x_{ij}^2$.

- 2.2.4. **Theorem.** Let F be a formally real Pythagorean field (hence sums of squares are squares) and let \tilde{F} be an expansion of F in a language \mathcal{L} extending the language \mathcal{L}_{ri} . Suppose \tilde{F} has quantifier elimination in \mathcal{L} . Let $\mathcal{L}(tr, invo)$ be the extension of \mathcal{L} by two new unary function symbols. The following are equivalent.
 - (1) The structure $(M_n(\tilde{F}), \operatorname{tr}_F, X \mapsto X^t)$ has quantifier elimination in $\mathcal{L}(\operatorname{tr}, \operatorname{invo})$.
 - (2) F has the Specht property for the transpose, i.e., there is some D = D(n) such that for all d and any two d-tuples of $n \times n$ matrices $X, Y \in M_n(F)^d$ with

$$\operatorname{tr}(w(X, X^t)) = \operatorname{tr}(w(Y, Y^t))$$

for all words w in x, x^t of length $\leq D$, there is some $O \in M_n(F)$ with $OO^t = I_n$ and $O^t X_i O = Y_i$ for all i.

(3) If $\tilde{K} \equiv \tilde{F}$ and \mathscr{U} is a substructure of $(M_n(\tilde{K}), \operatorname{tr}_K, X \mapsto X^t)$ and $\psi : \mathscr{U} \longrightarrow (M_n(\tilde{K}), \operatorname{tr}_K, X \mapsto X^t)$ is an embedding, then there is an elementary extension $\tilde{\Omega} \succ \tilde{K}$ and an extension of ψ to an embedding $(M_n(\tilde{K}), \operatorname{tr}_K, X \mapsto X^t) \longrightarrow (M_n(\tilde{\Omega}), \operatorname{tr}_{\Omega}, X \mapsto X^t)$. Hence the following diagram commutes:



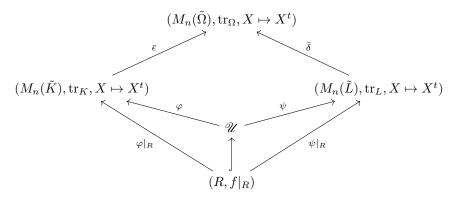
Proof. (2) \Rightarrow (1) Since \tilde{F} is model complete we know from 2.1.7 that $M_n(\tilde{F})$ is model complete and so is its definable expansion $(M_n(\tilde{F}), \operatorname{tr}_F, X \mapsto X^t)$. Hence by 2.1.10 it suffices to show that the theory T of $(M_n(\tilde{F}), \operatorname{tr}_F, X \mapsto X^t)$ has the amalgamation property over finitely generated substructures. So let $\mathscr{M}, \mathscr{N} \models T$ and let \mathscr{U} be a common finitely generated $\mathscr{L}(\operatorname{tr}, \operatorname{invo})$ -substructure of \mathscr{M}, \mathscr{N} . Using 2.1.1, 2.1.3 and as $\mathscr{M} \models T$ we see that there is an isomorphism $\bar{\varphi} : \mathscr{M} \longrightarrow (M_n(\tilde{K}), \operatorname{tr}_K, X \mapsto X^t)$ where $\tilde{K} \equiv \tilde{F}$: In the language $\mathscr{L}(\operatorname{tr}, \operatorname{invo})$ we can say that there are matrix units a_{ij} over the center K of \mathscr{M} such that the ring homomorphism $M_n(K) \longrightarrow \mathscr{M}$ that maps E_{ij} to a_{ij} , is an isomorphism mapping transposition to the action of invo \mathscr{M} .

We write φ for the restriction of $\bar{\varphi}$ to \mathscr{U} . Similarly, we see that there is an isomorphism $\bar{\psi}: \mathscr{N} \longrightarrow (M_n(\tilde{L}), \operatorname{tr}_L, X \mapsto X^t)$, with $\tilde{L} \equiv \tilde{F}$ and we write ψ

 $^{^3}$ For d=1, this result is classical. The equivalence between (1) and (2) over C is due to [Spe40, Satz 1]. The degree bounds and the real case for d=1 are due to [Pea62, Thm. 1 and Cor. to Thm. 2].

for the restriction of $\bar{\psi}$ to \mathscr{U} . We now replace \mathscr{M} by $(M_n(\tilde{K}), \operatorname{tr}_K, X \mapsto X^t)$ and \mathscr{N} by $(M_n(\tilde{L}), \operatorname{tr}_L, X \mapsto X^t)$ and we need to amalgamate these $\mathscr{L}(\operatorname{tr}, \operatorname{invo})$ structures over \mathscr{U} via the $\mathscr{L}(\operatorname{tr}, \operatorname{invo})$ -embeddings φ, ψ . We write $\mathscr{U} = (\tilde{U}, f, h)$, where $f: U \longrightarrow U$ and $h: U \longrightarrow U$ are the maps induced by the trace functions and the transpositions, respectively on U.

Let R be the subring of U generated by the image of f. By 2.2.1(1), R is commutative, $\varphi(R) \subseteq K \cdot I_n$ and $\psi(R) \subseteq L \cdot I_n$. For better readability we now identify K with $K \cdot I_n$ and L with $L \cdot I_n$. Since φ is an \mathscr{L} -embedding, $M_n(\tilde{K})$ and $M_n(\tilde{L})$ induce the same \mathscr{L} -structure \tilde{R} on R and $\varphi|_R : \tilde{R} \longrightarrow \tilde{K}$, $\psi|_R : \tilde{R} \longrightarrow \tilde{L}$ are embeddings of \mathscr{L} -structures. Since \tilde{F} has quantifier elimination there are $\tilde{\Omega} \equiv \tilde{F}$ and \mathscr{L} -embeddings $\varepsilon : \tilde{K} \longrightarrow \tilde{\Omega}$, $\delta : \tilde{L} \longrightarrow \tilde{\Omega}$ such that $\varepsilon \circ \varphi|_R = \delta \circ \psi|_R$. We write $\bar{\varepsilon}, \bar{\delta}$ for the induced \mathscr{L} (tr, invo)-embeddings as in 2.2.1 and consider the diagram



Notice that in general only the outer square in this diagram commutes. Since \mathscr{U} is a finitely generated \mathscr{L} -structure, there are $X_1, \ldots, X_d \in U$ such that U is the ring generated by X_1, \ldots, X_d .

Claim. There is some orthogonal matrix $O \in M_n(\Omega)$ such that for all $i \in \{1, \ldots, d\}$ we have

$$O \cdot \bar{\varepsilon}(\varphi(X_i)) \cdot O^t = \bar{\delta}(\psi(X_i)).$$

Proof. We write $Y_i = \bar{\varepsilon}(\varphi(X_i))$ and $Z_i = \bar{\delta}(\psi(X_i))$. To see the claim we use (2), by which it suffices to show that for every word w in $x_1, \ldots, x_d, x_1^t, \ldots, x_d^t$ we have

$$\operatorname{tr}_{\Omega}(w(Y_1,\ldots,Y_d,Y_1^t,\ldots,Y_d^t)) = \operatorname{tr}_{\Omega}(w(Z_1,\ldots,Z_d,Z_1^t,\ldots,Z_d^t)).$$

Let $X = w(X_1, \ldots, X_d, h(X_1), \ldots, h(X_d)) \in U$ (the degree bound D is used to transfer (2) from \tilde{F} to $\tilde{\Omega}$). By 2.2.1(2) we know that

$$\operatorname{tr}_{\Omega}(\bar{\varepsilon}(\varphi(X))) = \operatorname{tr}_{\Omega}(\bar{\delta}(\psi(X))).$$

Since $\bar{\varepsilon}$ and φ respect the function symbol for the adjoint we see that

$$\bar{\varepsilon}(\varphi(X)) = \bar{\varepsilon}(\varphi(w(X_1, \dots, X_d, h(X_1), \dots, h(X_d))))
= w(\bar{\varepsilon}(\varphi(X_1)), \dots, \bar{\varepsilon}(\varphi(X_d)), \bar{\varepsilon}(\varphi(X_1))^t, \dots, \bar{\varepsilon}(\varphi(X_d))^t)
= w(Y_1, \dots, Y_d, Y_1^t, \dots, Y_d^t).$$

Similarly, $\bar{\delta}(\psi(X)) = w(Z_1, \dots, Z_d, Z_1^t, \dots, Z_d^t)$, establishing the claim.

Now take an orthogonal $O \in M_n(\Omega)$ as in the claim and observe that the map $\gamma: M_n(\Omega) \longrightarrow M_n(\Omega), X \mapsto O \cdot X \cdot O^t$ preserves traces, adjoints of matrices and

the \mathscr{L} -structure of $M_n(\tilde{\Omega})$. Hence γ is an $\mathscr{L}(\operatorname{tr}, \operatorname{invo})$ -automorphism of $(M_n(\tilde{\Omega}), \operatorname{tr}_{\Omega}, X \mapsto X^t)$.

Consequently, by the claim, $\gamma \circ \bar{\varepsilon} \circ \varphi = \bar{\delta} \circ \psi$. This shows that the maps $\gamma \circ \bar{\varepsilon} \circ \varphi$ and $\bar{\delta} \circ \psi$ form an amalgamation of the $\mathcal{L}(\mathrm{tr,invo})$ -structures \mathcal{M} and \mathcal{N} over the $\mathcal{L}(\mathrm{tr,invo})$ -embeddings φ and ψ .

 $(1)\Rightarrow(3)$ is a weakening, see 2.1.10.

(3) \Rightarrow (2) By a standard compactness argument it suffices to show that (2) holds without the degree bound for all $\tilde{K} \equiv \tilde{F}$.

Let \mathscr{U} be the $\mathscr{L}(\operatorname{tr},\operatorname{invo})$ -substructure of $M_n(\tilde{K})$ generated by $K\cdot I_n$ and the X_i . Let U be the ring underlying \mathscr{U} . Hence U is generated as a K-algebra by all words in the X_i, X_i^t . Let $\varphi: U \to M_n(K)$ be the identity mapping and let $\psi: U \to M_n(K)$ be the K-algebra homomorphism that maps X_i to Y_i and X_i^t to Y_i^t .

We claim that ψ is an $\mathcal{L}(\mathrm{tr,invo})$ -homomorphism. Firstly, ψ is well defined: It suffices to show that for every noncommutative polynomial $p(x,x^t)$ with coefficients in K and $p(X,X^t)=0$, we have $p(Y,Y^t)=0$. By 2.2.3 we know $\mathrm{tr}(p(X,X^t)^tp(X,X^t))=0$. But the left-hand side of this equation is simply a linear combination of traces of words in the X,X^t . Hence by the assumption on traces, $\mathrm{tr}(p(Y,Y^t)^tp(Y,Y^t))=0$. Thus $p(Y,Y^t)=0$ by 2.2.3 again. It is clear that ψ is an $\mathcal{L}(\mathrm{tr,invo})$ -embedding.

Now we amalgamate as asserted in (3). There are an elementary extension $\tilde{\Omega}$ of \tilde{K} and an \mathscr{L} -embedding $\bar{\epsilon}: M_n(\tilde{K}) \to M_n(\tilde{\Omega})$, preserving tr and invo such that $\psi(u) = \bar{\epsilon}(u)$ for all $u \in \mathscr{U}$. Since $\bar{\epsilon}$ is compatible with the traces it is a K-algebra homomorphisms. Hence by the Skolem-Noether theorem (see [Bre14, Thm 4.46]), there is some invertible $Z \in M_n(\Omega)$ with

$$\bar{\epsilon}(X) = Z^{-1}XZ$$
 for all $X \in M_n(K)$.

Now,

$$Z^{-1}X^tZ = \bar{\epsilon}(X^t) = (\bar{\epsilon}(X))^t = (Z^{-1}XZ)^t = Z^tX^t(Z^{-1})^t = Z^tX^t(Z^t)^{-1},$$

whence $ZZ^tX^t = X^tZZ^t$ for all X. Hence ZZ^t is central and there is some $\lambda \in \sum \Omega^2$ with $ZZ^t = Z^tZ = \lambda I_n$.

By the commutativity in the amalgamation diagram we know

$$Z^{-1}X_iZ = Y_i$$

for all i. Since Ω is Pythagorean we also know that λ is a square and so we may replace Z by $\frac{Z}{\sqrt{\lambda}}$ and assume $\lambda=1$. Hence $O=Z^{-1}$ is an orthogonal matrix with coefficients in Ω satisfying $O^tX_iO=Y_i$ for all i. Since Ω is an elementary extension of K we may find such an O with coefficients in K as well.

We next identify a large class of fields with the Specht property, namely fields that can be written as intersections of real closed fields. We refer to [Cra80] for a systematic study of such fields. In [MSV93] the authors say such fields satisfy the principal axis property: every symmetric matrix over F is orthogonally similar to a diagonal matrix over F. Notice that all fields that can be written as intersections of real closed fields are Pythagorean and by [Bec78, III, §1, Thm. 1], every hereditarily Pythagorean field is the intersection of real closed fields.

2.2.5. **Proposition.** Suppose the field F is an intersection of real closed fields. Then F has the Specht property for transposition.

More precisely, given two d-tuples of $n \times n$ matrices $X, Y \in M_n(F)^d$ with

$$\operatorname{tr}(w(X,X^t)) = \operatorname{tr}(w(Y,Y^t))$$

for all words w in x, x^t of length $\leq n^2$, there is some $O \in M_n(F)$ with $OO^t = I_n$ and $O^t X_i O = Y_i$ for all i.

Proof. By 2.2.2, for every real closed field $R \supseteq F$ there is an orthogonal matrix $U \in M_n(R)$ with $U^t X_i U = Y_i$.

Consider the system of linear equations $PX_i = Y_iP$ and $PX_i^t = Y_i^tP$ for $i = 1, \ldots, d$. It has solutions P with nonzero determinant in every real closed field extension of F by the above, so it must have a solution $P \in M_d(F)$ that is invertible. Hence $P^{-1}X_iP = Y_i$ and $P^{-1}X_i^tP = Y_i^t$ for all i. In particular,

$$P^{-1}X_i^t P = Y_i^t = (P^{-1}X_i P)^t = P^t X_i^t (P^t)^{-1},$$

whence PP^t commutes with all X_i and X_i^t .

Since F has the principal axis property, we can diagonalize PP^t . There is an orthogonal matrix $V \in M_n(F)$ and a diagonal matrix $D \in M_n(F)$ with $V^tPP^tV = D$. By construction, each entry of D is a (sum of) square(s). We thus find a diagonal matrix $\sqrt{D} \in M_n(F)$ with $\sqrt{D}^2 = D$. Let $H := V\sqrt{D}V^t \in M_n(F)$. Then

$$H^2 = V\sqrt{D}V^tV\sqrt{D}V^t = V\sqrt{D}^2V^t = VDV^t = PP^t,$$

i.e., H is the symmetric square root of PP^t . Thus by standard linear algebra, it commutes with all elements that commute with PP^t .

Set $O = H^{-1}P$. Then

$$O^t O = P^t H^{-1} H^{-1} P = P^t H^{-2} P = P^t (PP^t)^{-1} P = P^t P^{-t} P^{-1} P = I,$$

so $O \in M_n(F)$ is an orthogonal matrix. Further,

$$O^{t}X_{i}O = O^{-1}X_{i}O = P^{-1}HX_{i}H^{-1}P = P^{-1}X_{i}P = Y_{i}$$

as desired. \Box

2.2.6. Corollary. Let F be an intersection of real closed fields and let \tilde{F} be an expansion of F in a language \mathcal{L} extending the language of rings. Suppose \tilde{F} has quantifier elimination in \mathcal{L} . Let $\mathcal{L}(\operatorname{tr}, \operatorname{invo})$ be the extension of \mathcal{L} by two new unary function symbols. Then the structure $(M_n(\tilde{F}), \operatorname{tr}_F, X \mapsto X^t)$ has quantifier elimination in $\mathcal{L}(\operatorname{tr}, \operatorname{invo})$.

Proof. Immediate from Theorem 2.2.4 and Proposition 2.2.5. \Box

2.2.7. An application: Sylvester's equation A famous matrix equation from control theory is Sylvester's equation [BR97], AX - XB = C for some $n \in \mathbb{N}$ and $n \times n$ real (or complex) matrices A, B, C. By the Sylvester-Rosenblum theorem, given A, B there is a unique solution X for every C iff the spectra of A and B are disjoint, and by the quantifier elimination proved in Corollary 2.2.6 (or 2.4.2 below, for the complex case), this can be expressed quantifier free in A, B purely in terms of the trace and (conjugate) transpose.

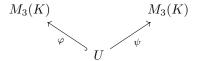
- 2.3. Trace and transposition are needed. We present three examples establishing the optimality of 2.2.4. The first example shows that we cannot omit the trace.
- 2.3.1. Example. Let K be a field of characteristic zero. Let

$$X_1 = \begin{pmatrix} 1 & & \\ & 2 & \\ & & 2 \end{pmatrix}, \qquad X_2 = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 2 \end{pmatrix} \in M_3(K).$$

Let U be the unital subring of $M_3(\mathbb{Z})$ generated by X_1 . Consider the ring homomorphism $\psi: U \to M_3(K)$ defined by

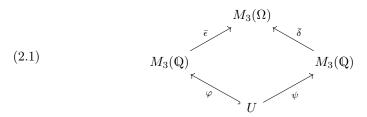
$$X_1 \mapsto X_2$$

and let $\varphi:U\to M_3(K)$ be the inclusion mapping. Then the following diagram cannot be amalgamated:



(Notice that φ and ψ also respect the transposition, since all $X \in U$ are symmetric.)

Proof. Notice that it suffices to verify the claim for $K = L = \mathbb{Q}$. Firstly, the map ψ is well-defined, since the minimal polynomial of X_1 is (t-1)(t-2) and is equal to the minimal polynomial of X_2 . Now assume $M_3(\Omega)$ is an amalgamation of ψ and ϕ over U, and the following diagram commutes:



Then $\bar{\epsilon}, \bar{\delta}: M_3(\mathbb{Q}) \to M_3(\Omega)$ are ring homomorphisms. By the Skolem-Noether theorem (see, e.g. [Bre14, Theorem 4.46]), there are invertible matrices $W, V \in M_3(\Omega)$ such that

$$\bar{\epsilon}(Y) = W^{-1}YW, \quad \bar{\delta}(Y) = V^{-1}YV$$

for all $Y \in M_3(\mathbb{Q})$. Then

$$V^{-1}X_2V = \bar{\delta}(X_2) = \bar{\delta}(\psi(X_1)) = \bar{\epsilon}(\phi(X_1)) = \bar{\epsilon}(X_1) = W^{-1}X_1V,$$

vielding

$$X_2 = (VW^{-1}) X_1 (VW^{-1})^{-1}.$$

However, this is not possible because X_1 and X_2 are not similar; for example they have different characteristic polynomials.

The second example shows that we cannot omit transposition in 2.2.4.

2.3.2. Example. Let K be a field of characteristic zero. Consider

Let U be the unital subring of $M_4(\mathbb{Z})$ generated by X_1 . Consider the ring homomorphism $\psi: U \to M_4(K)$ defined by

$$X_1 \mapsto X_2$$

and let $\varphi: U \to M_4(K)$ be the identity mapping. Then ψ and φ cannot be amalgamated over U. (Notice that φ and ψ also respect the trace functions.)

Proof. Again, it suffices to verify the claim for $K = L = \mathbb{Q}$. Note that ψ is well-defined since the minimal polynomial of X_1 and of X_2 is t^2 . Now assume $M_4(\Omega)$ amalgamates φ and ψ over U. As in 2.3.1 this leads to X_1 being conjugate to X_2 (over Ω and thus over \mathbb{Q}). However, this is impossible since X_1 and X_2 are not similar; for example dim $\ker(X_1) = 2 \neq 3 = \dim \ker(X_2)$.

By 2.2.6, the structure $(M_n(\mathbb{R}, \leq), \operatorname{tr}_{\mathbb{R}}, X \mapsto X^t)$ has quantifier elimination in $\mathcal{L}_{ri}(\leq, \operatorname{tr}, \operatorname{invo})$. The third example shows that $(M_n(\mathbb{C}), \operatorname{tr}_{\mathbb{C}}, X \mapsto X^t)$ does not have quantifier elimination in $\mathcal{L}_{ri}(\operatorname{tr}, \operatorname{invo})$.

2.3.3. Example. Complex matrices with the trace and transpose do not admit quantifier elimination. For the same reasons as above it suffices to show there exist symmetric order two nilpotents with different rank. For this we take N_1 to be the rank one outer product $N_1 = uu^t$ with $u = \begin{pmatrix} 1 & i & 0 & 0 \end{pmatrix}^t$ and we let N_2 be the symmetric order two nilpotent

$$N_2 = \left(\begin{array}{cccc} 0 & 1 & 0 & -i \\ 1 & 0 & -i & 0 \\ 0 & -i & 0 & -1 \\ -i & 0 & -1 & 0. \end{array} \right).$$

2.4. The simultaneous conjugacy problem.

2.4.1. As in the proof of $2.2.4(2) \Rightarrow (1)$, using the complex Specht property (see 2.2.2), one can establish that the theory of $(M_n(\mathbb{C}), \leq, \operatorname{tr}_{\mathbb{C}}, X \mapsto X^*)$ has quantifier elimination; here \leq is the order on the symmetric center $\mathbb{R} \cdot I_n$. The underlying expansion of the field \mathbb{C} is $\tilde{\mathbb{C}} := (\mathbb{C}, z \mapsto \overline{z}, \leq)$, where \leq is the order on \mathbb{R} and \overline{z} is complex conjugation. Since \mathbb{R} is not definable in the field \mathbb{C} , the structure $\tilde{\mathbb{C}}$ is a proper expansion of \mathbb{C} . Conversely, the field \mathbb{R} obviously defines the structure $\tilde{\mathbb{C}}$; hence the complex version of 2.2.4 is a statement about the real field.

2.4.2. The question on whether a natural definable expansion of the ring $M_n(\mathbb{C})$ has quantifier elimination is tightly related to a "hopeless" open problem in invariant theory [LB95, LBP87, GfP69]. Namely the classification of d-tuples of $n \times n$ matrices under simultaneous conjugation by $GL_n(\mathbb{C})$, i.e., understanding the quotient $M_n(\mathbb{C})^d/GL_n(\mathbb{C})$. Alternately, in algebraic language, one is interested in a canonical form for tuples of matrices under simultaneous conjugation, a role played by the Jordan canonical form in the case d=1. A relaxation of the problem asks for a set of invariants that separate the orbits.

In model theoretic terms this can be phrased as follows. Let M be the ring $M_n(\mathbb{C})$ and fix $d \in \mathbb{N}$. We write \sim_d for the simultaneous similarity relation on M^d . Then

 \sim_d is a 0-definable equivalence relation and by elimination of imaginaries of the field \mathbb{C} (cf. [Hod93, Thm. 4.4.6]), there is a 0-definable function $f_d: M^d \longrightarrow M^k$ for some k such that $\bar{X} \sim \bar{Y} \iff f_d(\bar{X}) = f_d(\bar{Y})$. If we add names for all the f_d to the language of rings, one can prove quantifier elimination of the resulting expansion of M just like in the proof of 2.2.4(2) \Rightarrow (1); the sequence of the f_d substitutes the role of the transposition and the trace.

In [Fri83] functions f_d as above are explicitly constructed, up to a finite number of exceptions. Alternatively one can use techniques from Gröbner bases to construct them explicitly (without exceptions). This is work in progress and will be published in another paper.

3. Undecidability of dimension-free matrices

We now turn to model theoretic properties of dimension-free matrices. We present six natural algebraic structures capturing the set of all matrices of all sizes over a given field and prove that all of them are undecidable. This is based on undecidability of finite groups, which is reviewed first (suitably for our purpose). As a general reference for elementary properties of classes of finite groups in relation to decidability questions, we refer to [BM04, Section 6.3].

3.1. The universal Horn theory of finite groups. Throughout, \mathcal{L}_{gr} denotes the language $\{\cdot, ^{-1}, e\}$ of groups and T_{fin} denotes the \mathcal{L}_{gr} -theory of finite groups. Hence

$$T_{\text{fin}} = \{ \varphi \mid \varphi \text{ an } \mathscr{L}_{\text{gr}}\text{-sentence with } G \models \varphi \text{ for every finite group } G \}.$$

Further, $T_{\text{fin},\forall}$ denotes the **universal theory of finite groups**, hence all sentences in T_{fin} of the form

$$\forall x_1, \dots, x_n \bigwedge_{\lambda=1}^r \left(\bigwedge_{j=1}^m s_{\lambda j} = e \longrightarrow \bigvee_{i=1}^k t_{\lambda i} = e \right),$$

where $r, m, k \in \mathbb{N}_0$, $r \geq 1$ and $s_{\lambda j}, t_{\lambda i}$ are \mathcal{L}_{gr} -terms in the free variables x_1, \ldots, x_n (aka "words in the x_i and x_i^{-1} "). A **universal Horn sentence** of \mathcal{L}_{gr} is a sentence of the form

$$\forall x_1, \dots, x_n \left(\bigwedge_{j=1}^m s_j = e \longrightarrow t = e \right),$$

where $m \in \mathbb{N}_0$ and s_j, t are \mathcal{L}_{gr} -terms. We write $T_{fin,H-\forall}$ for the set of all universal Horn sentences in $T_{fin,\forall}$ and call it the universal Horn theory of finite groups.

Notice that by the shape of the sentences in $T_{\text{fin},\forall}$ and in $T_{\text{fin},H-\forall}$, every subgroup of a model of $T_{\text{fin},\forall}$, $T_{\text{fin},H-\forall}$ is again a model of $T_{\text{fin},\forall}$, $T_{\text{fin},H-\forall}$ respectively.

3.1.1. **Fact.** (cf. [Slo81])

The universal Horn theory of finite groups is undecidable. More precisely: $T_{\mathrm{fin},H-\forall}$ is not a recursive subset of the set of $\mathcal{L}_{\mathrm{gr}}$ -sentences. The same is then obviously true for $T_{\mathrm{fin},\forall}$.

- 3.1.2. **Definition.** We call a class K of groups satiated if
 - (a) Every finite group embeds into some member of \mathcal{K} , and,
- (b) Every member of \mathcal{K} is a model of the universal Horn theory of finite groups.

Let \mathcal{R} be any first order structure in an arbitrary language \mathscr{L} . We call \mathcal{R} satiated if \mathcal{R} has a uniform interpretation of a satiated set of groups. This means that there are $k, n \in \mathbb{N}$ and an \mathscr{L} -formula $\mu(\bar{x}_1, \bar{x}_2, \bar{y}, \bar{z})$, where $\bar{x}_1, \bar{x}_2, \bar{y}$ are n-tuples and \bar{z} is a k-tuple such that

- (a) for every $\bar{a} \in \mathcal{R}^k$, the subset defined by $\mu(\bar{x}_1, \bar{x}_2, \bar{y}, \bar{a})$ in \mathcal{R}^{3n} is the graph of multiplication of a group $G_{\bar{a}}$ with universe contained in \mathcal{R}^n , and,
- (b) the set of groups $\{G_{\bar{a}} \mid \bar{a} \in \mathcal{R}^k\}$ is satiated.
- 3.1.3. **Proposition.** Any satiated structure is undecidable.

Proof. The definition readily implies that the universal Horn theory of every satiated class \mathcal{K} (thus, all universal Horn \mathcal{L}_{gr} -sentences that are true in all $G \in \mathcal{K}$) is the universal Horn theory of finite groups. Now suppose that \mathcal{R} is a decidable satiated structure. Take a formula μ as in 3.1.2. It is then clear that there is a map $\varphi \mapsto \tilde{\varphi}$ from universal Horn sentences in \mathcal{L}_{gr} to the set of \mathcal{L} -sentences with recursive image such that $\varphi \in T_{\text{fin},H-\forall}$ if and only if $\tilde{\varphi}$ is true in \mathcal{R} . But then $T_{\text{fin},H-\forall}$ is recursive, in contradiction to 3.1.1.

Recall that a **linear group** is a group that can be embedded into some $GL_n(F)$ for some field F.

3.1.4. **Proposition.** Every linear group is a model of the universal theory of finite groups.

Proof. It suffices to show the claim for the group $G = \mathrm{GL}_n(F)$ when F is an algebraically closed field. If F has characteristic p > 0, then by completeness of the theory of algebraically closed fields of fixed characteristic we may assume that F is the algebraic closure $\overline{\mathbb{F}_p}$ of \mathbb{F}_p . But then G is the union of all the $\mathrm{GL}_n(K)$, where K runs through the finite fields of characteristic p. Since universal sentences are preserved by unions we get the assertion. When F is of characteristic 0, then using Loś's theorem, G is elementarily equivalent to any non-principal ultraproduct of the $\mathrm{GL}_n(\overline{\mathbb{F}_p})$, p prime. Hence the result follows.

3.1.5. Corollary. Let K be any class of linear groups such that every finite group embeds into some member of K. Then K is satisfied. This, for example, is the case for any class of linear groups containing all the $GL_n(F)$ for some fixed field F.

Proof.	Immediate from	3.1.4.		L
--------	----------------	--------	--	---

- 3.2. Applications to dimension-free matrices. There are various ways how the collection of all square matrices of arbitrary (finite) size over a field can be given an algebraic structure. We present six such constructions and show that each of them is undecidable. In the realm of infinite matrix theory in the sense of Poincaré (cf. [Ber68] and [Coo50]), one can find many constructions containing all finite square matrices. But then either one does not have a handle on the finitely sized matrices, or one of the constructions below will be interpretable.
- 3.2.1. Dimension-free matrices with partial operations. Let F be a field and let $\mathcal{R}_1, \mathcal{R}_2$ be the following structures (the languages are defined implicitly and en route). The universe of \mathcal{R}_1 is the disjoint union of all the $\mathrm{GL}_n(F)$. Further, \mathcal{R}_1 has a partial function \cdot with domain $\bigcup_n (\mathrm{GL}_n(F) \times \mathrm{GL}_n(F))$ and interpreted as multiplication. The universe of \mathcal{R}_2 is the disjoint union of all the $M_n(F)$. Further, \mathcal{R}_2 has two partial functions + and \cdot defined on $\bigcup_n (M_n(F) \times M_n(F))$ and interpreted as addition and multiplication respectively.

Then $\mathcal{R}_1, \mathcal{R}_2$ are satiated, hence undecidable by 3.1.3. The formula μ that uniformly interprets the satiated set $\{GL_n(F) \mid n \in \mathbb{N}\}$ in \mathcal{R}_1 is the formula

$$x_1 \cdot z, x_2 \cdot z, y \cdot z$$
 are defined and $x_1 \cdot x_2 = y$.

For \mathcal{R}_2 we take the formula $\mu(x_1, x_2, y, z)$ & " x_1, x_2 are invertible", where "x invertible" stands for the formula expressing that x is invertible in the group of all u for which $u \cdot x$ is defined.

3.2.2. **Lemma.** Let F be a field and let S be a subsemigroup of $M_n(F)$. If S is a group, then S is isomorphic to a subgroup of $GL_m(F)$ for some $m \leq n$. In particular, S is a linear group.

Proof. Let I be the neutral element of S. Then I is idempotent and there is some $P \in GL_n(F)$ such that $P^{-1} \cdot I \cdot P$ is of the form

$$E' = \begin{pmatrix} E & 0 \\ 0 & 0 \end{pmatrix},$$

where E is the identity matrix of $M_m(F)$ for some $m \leq n$. Let $\sigma: M_n(F) \longrightarrow M_n(F)$; $\sigma(X) = P^{-1} \cdot X \cdot P$. Then σ is an automorphism of $M_n(F)$ and as $I \cdot X \cdot I = X$ we get $E' \cdot \sigma(X) \cdot E' = \sigma(X)$ for all $X \in S$. However, matrices with this property are all of the form

$$Y' = \begin{pmatrix} Y & 0 \\ 0 & 0 \end{pmatrix},$$

for some $Y \in M_m(F)$. If we embed $M_m(F)$ into $M_n(F)$ by mapping Y to Y', we see that σ maps S into $M_m(F)$. Hence S is isomorphic to a subgroup of $GL_m(F)$. \square

3.2.3. Finite rank infinite matrices. Let F be a field and let \mathcal{R} be the semigroup of all $\mathbb{N} \times \mathbb{N}$ -matrices with finite support and multiplication as operation. Then \mathcal{R} is a satiated structure and is thus undecidable by 3.1.3.

Proof. We consider $M_n(F)$ as the subsemigroup of \mathcal{R} consisting of all $n \times n$ -matrices sitting in the corner of \mathcal{R} . We give a uniform definition of a satiated class of linear groups in \mathcal{R} using a formula μ in the language $\{\cdot\}$ of semigroups, as explained in 3.1.2. For $X \in \mathcal{R}$, consider the set

$$\mathcal{C}(X) = \{ Y \in \mathcal{R} \mid \forall Z \in \mathcal{R} \left((X \cdot Z = 0 \to Y \cdot Z = 0) \& (Z \cdot X = 0 \to Z \cdot Y = 0) \right) \}.$$

It is easy to see that $C(X) \subseteq M_n(F)$ for $X \in M_n(F)$ and that $C(X) = M_n(F)$ for $X \in GL_n(F)$.

Let $\psi(z_1, z_2)$ be an $\{\cdot\}$ -formula such that ψ holds at $(X, I) \in \mathbb{R}^2$ in \mathbb{R} just if the set

$$\mathcal{G}(X,I) = \{ Y \in \mathcal{C}(X) \mid \exists Z \in \mathcal{C}(X) \ Y \cdot Z = Z \cdot Y = I \}$$

is a group with neutral element I. Then the formula $\varphi(x, z_1, z_2)$ defined as

$$(\psi(z_1, z_2) \to x \in \mathcal{G}(z_1, z_2)) \& (\neg \psi(z_1, z_2) \to x = 0)$$

has the following properties for all $(X, I) \in \mathbb{R}^2$:

- (a) The set of all $Y \in \mathcal{R}$ with $\mathcal{R} \models \varphi(Y, X, I)$ is a linear group (use 3.2.2).
- (b) If $X \in GL_n(F)$ and $I = I_n$, then set of all $Y \in \mathcal{R}$ with $\mathcal{R} \models \varphi(Y, X, I)$ is $GL_n(F)$.

It is now standard to write down a $\{\cdot\}$ -formula $\mu(x_1, x_2, y, z_1, z_2)$ that uniformly defines a satiated class of groups (also invoke 3.1.5).

3.2.4. **Products.** If $(G_i \mid i \in I)$ is a satiated family of groups, then $\prod_{i \in I} G_i$ is undecidable, in fact the universal Horn theory of that product is undecidable. Hence by 3.1.5, for any field F, the group $\prod_{n \in \mathbb{N}} \operatorname{GL}_n(F)$ is undecidable, and consequently so is the semigroup $\prod_{n \in \mathbb{N}} M_n(F)$ (observe that $\prod_{n \in \mathbb{N}} \operatorname{GL}_n(F)$ is the set of invertible elements of $\prod_{n \in \mathbb{N}} M_n(F)$).

Proof. We write $P = \prod_{i \in I} G_i$ and show that P satisfies exactly the same universal Horn sentences as the those satisfied by all finite groups. Then 3.1.1 gives the assertion.

As a product, P satisfies all universal Horn sentences that are true in all G_i and so P satisfies all universal Horn sentences that are true in all finite groups.

Conversely, let φ be a quantifier-free Horn formula

$$\bigwedge_{j} s_{j} = e \to t = e$$

in l free variables and assume $P \models \forall \varphi$. Let H be a finite group and suppose $H \models \bigwedge_j s_j(h_1, \ldots, h_l) = e$. Fix some $i_0 \in I$ and an embedding $\iota : H \hookrightarrow G_{i_0}$. We define $X_1, \ldots, X_l \in P$ by

$$X_{j,i} = \begin{cases} \iota(h_j) & \text{if } i = i_0, \\ e & \text{if } i \neq i_0. \end{cases}$$

It is clear that $G_i \models \bigwedge_j s_j(X_{1,i},\ldots,X_{l,i}) = e$ for all $i \in I$. Hence

$$P \models \bigwedge_{j} s_{j}(X_{1}, \dots, X_{l}) = e$$

and so $P \models t(X_1, ..., X_l) = e$. Looking at the i_0^{th} component we see that $H \models t(h_1, ..., h_l) = e$ as required.

3.2.5. Ultraproducts. For any field F and any non-principal ultrafilter $\mathfrak U$ on $\mathbb N$, the universal Horn theory of the ultraproduct $\prod_{n\in\mathbb N}\operatorname{GL}_n(F)/\mathfrak U$ is the universal Horn theory of finite groups, and is thus undecidable. Since the natural map

$$\prod_{n} \operatorname{GL}_{n}(F)/\mathfrak{U} \longrightarrow (\prod_{n} M_{n}(F)/\mathfrak{U})^{\times}$$

is an isomorphism, the semigroup $\prod_n M_n(F)/\mathfrak{U}$ is undecidable as well.

Proof. Let $G_{\infty} = \prod_n \operatorname{GL}_n(F)/\mathfrak{U}$, for some non-principal ultrafilter \mathfrak{U} . If φ is a universal sentence, true in all finite groups, then by 3.1.4 it is true in all $\operatorname{GL}_n(F)$ and so it is also true in G_{∞} .

Conversely if $G_{\infty} \models \varphi$, then φ is true in all finite groups: Let H be a finite group and let $N \in \mathbb{N}$ be such that $\mathrm{GL}_n(F)$ contains an isomorphic copy H_n of H for all $n \geq N$. Since $\mathrm{GL}_n(F) \models \varphi$ for arbitrarily large n and φ is universal, φ is also true in H_n .

Hence the universal theory of the ultraproduct is $T_{\text{fin},\forall}$. Now use 3.1.1.

3.2.6. Direct Limits. Let F be a field. For $n \in \mathbb{N}$ let $f_n : M_{2^n}(F) \longrightarrow M_{2^{n+1}}(F)$ be the ring homomorphism that sends X to $\begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix}$. We consider the direct limit $\lim_{n \to \infty} M_{2^n}(F)$ induced by the f_n .

Then for every infinite field F, the ring $\varinjlim M_{2^n}(F)$ is undecidable. In fact, it interprets the weak monadic second order logic of F.

Proof. By the weak monadic second order logic of the field F we mean the following first order structure W expanding the poset P of finite subsets of F: We identify F with the subset $\{\{a\} \mid a \in F\}$ of P and expand P by the graph of addition and multiplication of F; for details see, for example, [Bau85] or [Tre17, Section 2].

We now show that W is interpretable in $\varinjlim M_{2^n}(F)$. Firstly, we identify F with the center of $\varinjlim M_{2^n}(F)$, which is 0-definable therein. If $X \in \varinjlim M_{2^n}(F)$, then let $\sigma(X)$ be the set of all central elements $\Lambda \in \varinjlim M_{2^n}(F)$ such that there is no $Y \in \varinjlim M_{2^n}(F)$ with $(X - \Lambda) \cdot Y = I$. Hence $\sigma(X)$ is the finite set of eigenvalues of X. The map σ is obviously 0-definable in $\varinjlim M_{2^n}(F)$. Further, if $X, Y \in \varinjlim M_{2^n}(F)$, then the property $\sigma(X) \subseteq \sigma(Y)$ is 0-definable in $\varinjlim M_{2^n}(F)$.

The universe of W then is the image of σ , i.e., the set P of finite subsets of F and the partial order on P is interpretable in $\varinjlim M_{2^n}(F)$. On central elements, the map σ is injective, hence the graph of addition and multiplication on the atoms of W is interpretable in $\varinjlim M_{2^n}(F)$ as well.

Hence $\varinjlim M_{2^n}(F)$ interprets W and W is well known to be undecidable, see for example $[\overline{\text{Tre}}17, 2.5]$ for char(F) = 0 and $[\overline{\text{Tre}}17, 2.6]$ for char(F) > 0.

3.2.7. Row and column finite matrices. Let F be an infinite field and let I be an infinite index set. Let $M_I(F)$ be the set of all $I \times I$ matrices X such that all but a finite number of entries in each row and each column of X are 0. One checks that $M_I(F)$ is a ring under the ordinary definition of addition and multiplication. Then the ring $M_I(F)$ is undecidable.

Proof. The interpretation used in the proof of 3.2.6 now gives the monadic second order theory of F, where second order quantifiers range over subsets of F of size at most the cardinality of I. This is undecidable as well, see the proofs of [Tre17, 2.5, 2.6].

References

- [AM16] J. Agler and J. E. McCarthy. The implicit function theorem and free algebraic sets. Trans. Amer. Math. Soc., 368(5):3157–3175, 2016. 1
- [Bau85] A. Bauval. Polynomial rings and weak second-order logic. J. Symbolic Logic, 50(4):953–972 (1986), 1985. 18
- [Bec78] E. Becker. Hereditarily-Pythagorean fields and orderings of higher level, volume 29 of Monografías de Matemática [Mathematical Monographs]. Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 1978. 10
- [Ber68] M. Bernkopf. A history of infinite matrices. Arch. History Exact Sci., 4(4):308–358, 1968. A study of denumerably infinite linear systems as the first step in the history of operators defined on function spaces. 15
- [BM04] E. I. Bunina and A. V. Mikhalev. Elementary properties of linear groups and related problems. J. Math. Sci. (N. Y.), 123(2):3921–3985, 2004. Algebra. 14
- [BR97] Rajendra Bhatia and Peter Rosenthal. How and why to solve the operator equation AX-XB=Y. Bull. London Math. Soc., 29(1):1–21, 1997. 11
- [Bre14] M. Brešar. Introduction to noncommutative algebra. Universitext. Springer, Cham, 2014. 10, 12
- [Coo50] R. G. Cooke. Infinite Matrices and Sequence Spaces. Macmillan & Co., Ltd., London, 1950. 15
- [Cra80] T. C. Craven. Intersections of real closed fields. Canad. J. Math., 32(2):431–440, 1980.
- [DNT17] T. Drescher, T. Netzer, and A. Thom. On projections of free semialgebraic sets. arXiv preprint arXiv:1709.08424, 2017. 2
- [FHS14] I. Farah, B. Hart, and D. Sherman. Model theory of operator algebras II: model theory. Israel J. Math., 201(1):477–505, 2014. 3
- [Fri83] S. Friedland. Simultaneous similarity of matrices. Adv. Math., 50(3):189–265, 1983. 14

- [GfP69] I. M. Gel' fand and V. A. Ponomarev. Remarks on the classification of a pair of commuting linear transformations in a finite-dimensional space. Funkcional. Anal. i Priložen., 3(4):81–82, 1969. 13
- [HKM11] J. W. Helton, I. Klep, and S. McCullough. Proper analytic free maps. J. Funct. Anal., 260(5):1476–1490, 2011. 1
- [Hod93] W. Hodges. Model theory, volume 42 of Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1993. 3, 6, 14
- [KVV14] D. S. Kaliuzhnyi-Verbovetskyi and V. Vinnikov. Foundations of free noncommutative function theory, volume 199 of Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, 2014. 1
- [LB95] L. Le Bruyn. Orbits of matrix tuples. Universitaire Instelling Antwerpen. Department of Mathematics, 1995. 13
- [LBP87] L. Le Bruyn and C. Procesi. Étale local structure of matrix invariants and concomitants. In Algebraic groups Utrecht 1986, pages 143–175. Springer, 1987. 13
- [MSV93] D. Mornhinweg, B. Shapiro, and K. G. Valente. The principal axis theorem over arbitrary fields. Amer. Math. Monthly, 100(8):749–754, 1993. 10
- [Pea62] C. Pearcy. A complete set of unitary invariants for operators generating finite W*-algebras of type I. Pacific J. Math, 12:1405–1416, 1962. 8
- [Pro76] C. Procesi. The invariant theory of $n \times n$ matrices. Adv. Math., 19(3):306–381, 1976. 8
- [Put07] M. Putinar. Undecidability in a free *-algebra. preprint, 2007. 2
- [Rau10] W. Rautenberg. A concise introduction to mathematical logic. Universitext. Springer, New York, third edition, 2010. With a foreword by Lev Beklemishev. 3
- [Raz74] Ju. P. Razmyslov. Identities with trace in full matrix algebras over a field of characteristic zero. Izv. Akad. Nauk SSSR Ser. Mat., 38:723-756, 1974. 8
- [Ros78] B. I. Rose. Rings which admit elimination of quantifiers. J. Symbolic Logic, 43(1):92– 112, 1978. 5
- [Ros80] B. I. Rose. On the model theory of finite-dimensional algebras. Proc. London Math. Soc. (3), 40(1):21–39, 1980. 5
- [Sib68] K. S. Sibirskiĭ. Algebraic invariants of a system of matrices. Sibirsk. Mat. Ž., 9:152–164, 1968. 8
- [Slo81] A. M. Slobodskoĭ. Undecidability of the universal theory of finite groups. Algebra i Logika, 20(2):207–230, 251, 1981. 14
- [Spe40] W. Specht. Zur Theorie der Matrizen. II. Jber. Deutsch. Math. Verein., 50:19–23, 1940.
- [Tre17] M. Tressl. On the strength of some topological lattices. In Ordered algebraic structures and related topics, volume 697 of Contemp. Math., pages 325–347. Amer. Math. Soc., Providence, RI, 2017. 2, 18
- [Voi10] D.-V. Voiculescu. Free analysis questions II: the Grassmannian completion and the series expansions at the origin. J. Reine Angew. Math., 645:155–236, 2010. 1
- [Wie62] N. A. Wiegmann. Necessary and sufficient conditions for unitary similarity. J. Austral. Math. Soc., 2:122–126, 1961/1962. 8

University of Ljubljana, Faculty of Mathematics and Physics, Department of Mathematics, Jadranska 21, 1000 Ljubljana, Slovenia

HOMEPAGE: https://www.fmf.uni-lj.si/~klep/

Email address: igor.klep@fmf.uni-lj.si

The University of Manchester, Department of Mathematics, Oxford Road, Manchester M13 9PL, UK

HOMEPAGE: http://personalpages.manchester.ac.uk/staff/Marcus.Tressl/

 $Email\ address: {\tt marcus.tressl@manchester.ac.uk}$