LATTICES AND PARAMETER REDUCTION IN DIVISION ALGEBRAS

M. LORENZ AND Z. REICHSTEIN

ABSTRACT. Let k be an algebraically closed field of characteristic 0 and let D be a division algebra whose center F contains k. We shall say that D can be reduced to r parameters if we can write $D \simeq D_0 \otimes_{F_0} F$, where D_0 is a division algebra, the center F_0 of D_0 contains k and $\mathrm{trdeg}_k(F_0) = r$.

We show that every division algebra of odd degree $n \geq 5$ can be reduced to $\leq \frac{1}{2}(n-1)(n-2)$ parameters. Moreover, every crossed product division algebra of degree $n \geq 4$ can be reduced to $\leq (\lfloor \log_2(n) \rfloor - 1)n + 1$ parameters. Our proofs of these results rely on lattice-theoretic techniques.

CONTENTS

1991 *Mathematics Subject Classification.* 16K20, 14L30, 20C10, 20J06.

Key words and phrases. division algebra, integral representation, lattice, algebraic transformation group, essential dimension, crossed product, central simple algebra.

M. Lorenz was supported in part by NSF grant DMS-9618521.

Z. Reichstein was supported in part by NSF grant DMS-9801675.

1. Introduction

Throughout this paper k denotes a (fixed) algebraically closed base field of characteristic zero. Let K be a field containing k and let A be a finite-dimensional K-algebra. We would like to write A as $A = A_0 \otimes_{K_0} K$ for some K_0-algebra A_0 over an intermediate field $k \subseteq K_0 \subseteq K$ with $\operatorname{trdeg}_k(K_0)$ as low as possible; the minimal value of $\operatorname{trdeg}_k(K_0)$ will be denoted by $\tau(A)$. Note that if $\operatorname{trdeg}_k(K_0) < \operatorname{trdeg}_k(K)$ then passing from A to A_0 may be viewed as "parameter reduction" in A.

We shall be particularly interested in the case where $A = \mathrm{UD}(n)$ is the universal division algebra of degree n and K is the center of $\mathrm{UD}(n)$ which we shall denote by $Z(n)$. Recall that $\mathrm{UD}(n)$ is the subalgebra of $\mathrm{M}_n(k(x_{ij}, y_{ij}))$ generated (as a division algebra) by two generic $n \times n$-matrices $X = (x_{ij})$ and $Y = (y_{ij})$, where x_{ij} and y_{ij} are $2n^2$ independent variables over k; see, e.g., [Pr, Section II.1] or [Row_1, Section 3.2]. We will denote $\tau(\mathrm{UD}(n))$ by $d(n)$. It is easy to show that $d(n) \geq \tau(A)$ for any central simple algebra A of degree n whose center contains k (see, e.g., [Re_2, Lemma 9.2]); in other words, every central simple algebra of degree n can be "reduced to at most $d(n)$ parameters". In the language of [Re_2], $d(n) = \mathrm{ed}(\mathrm{PGL}_n)$, where ed denotes the essential dimension; see [Re_2, Lemma 9.2].

To the best of our knowledge, the earliest attempt to determine the value of $d(n)$ is due to Procesi, who showed that $d(n) \leq n^2$; see [Pr, Thm. 2.1]. Note that if $\mathrm{UD}(n)$ is cyclic then $d(n) = 2$, because we can take A_0 to be a symbol algebra; cf. [Re_2, Lemma 9.4]. This is known to be the case for $n = 2$, 3 and 6. For other n the exact value of $d(n)$ is not known. However, the following inequalities hold:

$$d(n) \leq n^2 - 2n \quad ([\mathrm{Re}_2, \text{Proposition 4.5}])\,, \tag{1.1}$$

$$d(n) \leq d(nm) \leq d(n) + d(m) \quad \text{if } (n,m) = 1 \quad ([\mathrm{Re}_2, \text{Section 9.4}])\,, \tag{1.2}$$

$$d(n^r) \geq 2r \quad ([\mathrm{Re}_1, \text{Theorem 16.1}])\,, \tag{1.3}$$

$$d(n) \leq \tfrac{1}{2}(n-1)(n-2) + n \quad \text{if } n \text{ is odd} \quad ([\mathrm{Row}_2]; \text{cf. } [\mathrm{Re}_2, \text{Section 9.3}])\,. \tag{1.4}$$

The last inequality is due to Rowen. In this paper we will sharpen it by showing that, in fact, $d(n) \leq \frac{1}{2}(n-1)(n-2)$ for every odd $n \geq 5$. Moreover, in $\mathrm{UD}(n)$, reduction to this number of parameters can be arranged in a particularly nice fashion:

Theorem 1.1. *Let $n \geq 5$ be an odd integer, $\mathrm{UD}(n)$ be the universal division algebra of degree n and $Z(n)$ be its center. Then there exists a subfield F of $Z(n)$ and a division algebra D of degree n with center F such that*

(a) $\mathrm{UD}(n) = D \otimes_F Z(n)$,
(b) $\operatorname{trdeg}_k(F) = \frac{1}{2}(n-1)(n-2)$ *and*
(c) $Z(n)$ *is a rational extension of* F.

In particular, $d(n) = \mathrm{ed}(\mathrm{PGL}_n) \leq \frac{1}{2}(n-1)(n-2)$.

In the course of the proof of Theorem 1.1 we will obtain an explicit description of the center F of D: $F \simeq k(\bigwedge^2 A_{n-1})^{\mathcal{S}_n}$, where $\mathcal{S}_n$ denotes the symmetric group on n symbols and

$$A_{n-1} = \{(a_1, \ldots, a_n) \in \mathbb{Z}^n \mid a_1 + \cdots + a_n = 0\}\,, \tag{1.5}$$

with the natural $\mathcal{S}_n$-action. Our argument relies on the results of [LL], where the symmetric square $\mathsf{Sym}^2 A_{n-1}$ is shown to be stably permutation for n odd; see Proposition 4.5 below.

For our next result, recall that if A is a central simple algebra of degree n with center F and L is a subfield of A then L is called *strictly maximal* if $F \subset L$ and $[L : F] = n$.

Theorem 1.2. *Let A be a finite-dimensional central simple algebra of degree n with center F, L be a strictly maximal subfield of A, L^{norm} be the normal closure of L over F, and $\mathcal{G} = \mathrm{Gal}(L^{norm}/F)$. Suppose $\mathcal{G}$ is generated by r elements together with $\mathcal{H} = \mathrm{Gal}(L^{norm}/L)$. If either $r \geq 2$ or $\mathcal{H} \neq \{1\}$ then $\tau(A) \leq r|\mathcal{G}| - n + 1$.*

If A be a central simple algebra of degree n then the upper bounds we have for $\tau(A)$ (or, equivalently, for $d(n)$), are all quadratic in n; see (1.1), (1.4) and Theorem 1.1. However, if we assume that A is a crossed product, Theorem 1.2 yields an asymptotically better bound:

Corollary 1.3. *Suppose a group $\mathcal{G}$ of order n can be generated by $r \geq 2$ elements. Then $\tau(A) \leq (r-1)n + 1$ for any $\mathcal{G}$-crossed product central simple algebra A. In particular, $\tau(A) \leq (\lfloor \log_2(n) \rfloor - 1)n + 1$, for any crossed product central simple algebra of degree $n \geq 4$. Here, as usual, $\lfloor x \rfloor$ denotes the largest integer $\leq x$.* □

Recall that A is called a *$\mathcal{G}$-crossed product* if it contains a strictly maximal subfield L, such that L/F is a Galois extension and $\mathrm{Gal}(L/F) = \mathcal{G}$; cf. [Row$_1$, Definition 3.1.23]. Thus the first assertion of the corollary is an immediate consequence of Theorem 1.2. The second assertion follows from the first, because any group of order n can be generated by $r \leq \log_2(n)$ elements. (Indeed, $|{<}\mathcal{G}_0, g{>}| \geq 2|\mathcal{G}_0|$ for any subgroup $\mathcal{G}_0$ of $\mathcal{G}$ and any $g \in \mathcal{G} \setminus \mathcal{G}_0$.) Note also that $\lfloor \log_2(n) \rfloor \geq 2$ for any $n \geq 4$.

The case of central simple algebras of degree 4 is of special interest since, by a theorem of Albert, every such algebra is a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$-crossed product; see e.g., [Row$_1$, Theorem 3.2.28]. Thus Corollary 1.3 says that $d(4) = \tau(\mathrm{UD}(4)) \leq 5$. On the other hand, $d(4) \geq 4$ by (1.3). This proves:

Corollary 1.4. $d(4) = \mathrm{ed}(\mathrm{PGL}_4) = 4$ *or* 5. □

The rest of this paper is structured as follows. In Section 2 we discuss preliminary material from invariant theory and the theory of $\mathcal{G}$-lattices. In Section 3 we explain how $\mathcal{G}$-lattices can be used to give an upper bound on essential dimensions of certain groups. We prove Theorem 1.1 in Section 4 and Theorem 1.2 in Section 5. In Section 6 we show that the methods of this paper cannot be used to decide whether the exact value of $d(4)$ equals 4 or 5.

2. Preliminaries

2.1. **G-varieties.** A *G-variety* X is an algebraic variety with a (regular) action of an algebraic group G. If G acts freely (i.e., with trivial stabilizers) on a dense open subset of X, then X is called a *generically free* G-variety.

A dominant rational map $\pi \colon X \dashrightarrow Y$ is called the *rational quotient map* if $k(Y) = k(X)^G$ and $\pi^* \colon k(Y) \hookrightarrow k(X)$ is the natural inclusion $k(X)^G \hookrightarrow k(X)$. We will usually denote the rational quotient Y by X/G; note that X/G is only defined up to birational equivalence. By a theorem of Rosenlicht a rational quotient map separates points in general position in X; see [Ros$_1$, Theorem 2] and [Ros$_2$] (also cf. [PV, Theorem 2.3]). In other words, there exists a dense open subset U of X such that f is regular on U and $x, y \in U$ lie in the same G-orbit iff $f(x) = f(y)$.

We will not generally assume that X is irreducible; however, we will always require X to be *primitive*. This means that G transitively permutes the irreducible components of X; equivalently, X/G is irreducible, i.e., $k(X)^G$ is a field; cf. [Re$_2$, Section 2.2]. Note that an irreducible G-variety is always primitive, and, if G is connected, a primitive variety is necessarily irreducible. Thus the notion of a primitive variety is only of interest if the group G is disconnected.

If N is a normal subgroup of G then the G-action on X induces a (rational) G/N-action on X/N; moreover, one can choose a model Y of X/N such that the G/N-action on Y is regular; see [PV, Proposition 2.6], [Re$_2$, Remark 2.6].

Lemma 2.1. *Let N be a normal subgroup of G and let X be a G-variety. Then X is generically free as a G-variety if and only if*

(a) *X is generically free as an N-variety and*
(b) *X/N is generically free as a G/N-variety.*

Proof. Assume (a) and (b) hold. Choose x in X in general position and suppose $g \in \mathrm{Stab}(x)$. Then (b) implies that $g \in N$ and (a) says that $g = 1$. This shows that the G-action on X is generically free. The converse in proved in a similar manner. $\square$

2.2. **(G, H)-sections and compressions.** Let X be a G-variety and let $\pi\colon X \dashrightarrow X/G$ be the rational quotient map. Furthermore, let H be a closed subgroup of G. An H-invariant subvariety S of X is called a *(G, H)-section* if the following conditions are satisfied.

(i) $\pi(S)$ contains an open dense subset of X/G and
(ii) if x is a point in general position in S then $gx \in S$ if and only if $g \in H$.

Recall that a *G-compression* $X \dashrightarrow Y$ is a dominant rational map of generically free G-varieties.

Lemma 2.2. *Suppose S is a (G, H)-section of X. Then*

(a) *$k(S)^H = k(X)^G$ and*
(b) *any H-compression $S \dashrightarrow S'$ lifts to a G-compression $X \dashrightarrow X'$, where S' is a (G, H)-section of X'.*

Proof. (a) See [PV, Section 2.8], [Po, 1.7.2] or [Re$_2$, Lemma 2.11].

(b) Note that X and $G *_H S$ are birationally equivalent as G-varieties, where $G *_H S$ is defined as $G \times S/H$ for the H-action given by $h(g, s) = (gh^{-1}, hs)$; see [Po, Theorem 1.7.5] or [Re$_2$, Lemma 2.14]. Now we set $X' = G *_H S'$ and extend f to a rational map $X \dashrightarrow X'$ by $f(g, s) \longrightarrow (g, f(s))$. It is easy to see that this map has the desired properties; cf. the proof of [Re$_2$, Lemma 4.1]. $\square$

2.3. **$\mathcal{G}$-lattices.** Let $\mathcal{G}$ be a finite group. A *$\mathcal{G}$-lattice* is a (left) module over the integral group ring $\mathbb{Z}[\mathcal{G}]$ that is free of finite rank as a $\mathbb{Z}$-module. A $\mathcal{G}$-lattice M is called

- *faithful* if the structure map $\mathcal{G} \longrightarrow \mathrm{Aut}_{\mathbb{Z}}(M)$ is injective, and
- a *permutation lattice* if M has a $\mathbb{Z}$-basis that is permuted by $\mathcal{G}$.

For any $\mathcal{G}$-lattice M, the $\mathcal{G}$-action on M extends canonically to actions of $\mathcal{G}$ on the group algebra $k[M]$ and on the field of fractions $k(M)$ of $k[M]$. The operative fact concerning the $\mathcal{G}$-fields (i.e., fields with $\mathcal{G}$-action) of the form $k(M)$ for our purposes is the following result of Masuda [M]; cf. also [L, proof of Prop. (1.5)].

Proposition 2.3. *Let $0 \longrightarrow M \longrightarrow E \longrightarrow P \longrightarrow 0$ be an exact sequence of $\mathcal{G}$-lattices with M faithful and P permutation. Then, as $\mathcal{G}$-fields, $k(E) \simeq k(M)(t_1, \dots, t_r)$, where the elements t_i are $\mathcal{G}$-invariant and transcendental over $k(M)$ and $r = \operatorname{rank} P$.*

2.4. **The symmetric and exterior squares.** Let M be a $\mathcal{G}$-lattice. By definition, the symmetric square $\mathsf{Sym}^2 M$ is the quotient of $M^{\otimes 2} = M \otimes M$ modulo the subgroup generated by the elements $m \otimes m' - m' \otimes m$ for $m, m' \in M$. Similarly, the exterior square $\bigwedge^2 M$ is the quotient of $M^{\otimes 2}$ modulo the subgroup generated by the elements $m \otimes m$, as m ranges over M. The action of $\mathcal{G}$ on $M^{\otimes 2}$ restricts down to $\mathsf{Sym}^2 M$ and $\bigwedge^2 M$, making each a $\mathcal{G}$-lattice. The $\mathcal{G}$-lattice $\bigwedge^2 M$ can be identified with the sublattice of *antisymmetric tensors* in $M^{\otimes 2}$, that is,

$$\bigwedge^2 M \simeq \mathsf{A}_2'(M) = \{x \in M^{\otimes 2} \mid x^\tau = -x\}$$

where $\tau : M^{\otimes 2} \longrightarrow M^{\otimes 2}$ is the switch $(m \otimes m')^\tau = m' \otimes m$; see [Bou, Exerc. 8 on p. A III.190]. Furthermore, $\mathsf{A}_2'(M)$ is exactly the kernel of the canonical map $M^{\otimes 2} \twoheadrightarrow \mathsf{Sym}^2 M$. Hence, we have an exact sequence of $\mathcal{G}$-lattices

$$0 \longrightarrow \bigwedge^2 M \longrightarrow M^{\otimes 2} \longrightarrow \mathsf{Sym}^2 M \longrightarrow 0\ . \tag{2.1}$$

3. Groups of the form $T_{n-1} \rtimes \mathcal{G}$ and lattices

3.1. **Notations.** In this section we shall focus on the following situation. Let $T_{n-1} = (\mathbb{G}_m)^n/\Delta$ be the (diagonal) maximal torus of PGL_n; here $\Delta \simeq \mathbb{G}_m$ diagonally embedded in $(\mathbb{G}_m)^n$. Recall that $\mathcal{S}_n$ acts on T_{n-1} by permuting the n copies of $\mathbb{G}_m$ and that the normalizer $N(T_{n-1})$ of T_{n-1} in PGL_n is isomorphic to $T_{n-1} \rtimes \mathcal{S}_n$. We shall be interested in subgroups of $N(T_{n-1})$ of the form $T_{n-1} \rtimes \mathcal{G}$, where $\mathcal{G}$ is a subgroup of $\mathcal{S}_n$. These groups have two properties that will be important to us in the sequel: (i) $T_{n-1} \rtimes \mathcal{G}$-varieties and their compressions can be constructed from $\mathcal{G}$-lattices and (ii) certain $(\mathrm{PGL}_n, T_{n-1} \rtimes \mathcal{G})$-sections will naturally come up in the proofs of Theorems 1.1 and 1.2. In this section we will focus on the relationship between $T_{n-1} \rtimes \mathcal{G}$-varieties and $\mathcal{G}$-lattices.

3.2. **$T_{n-1} \rtimes \mathcal{G}$-varieties and $\mathcal{G}$-lattices.** Suppose we are given a morphism

$$f \colon M \longrightarrow A_{n-1}$$

of $\mathcal{G}$-lattices, where A_{n-1} is the root lattice defined in (1.5). Note that $A_{n-1} \simeq X_*(T_{n-1})$ as an $\mathcal{S}_n$-lattice (and hence as $\mathcal{G}$-lattice), where $X_*(T_{n-1})$ is the lattice of characters of T_{n-1}. We will always identify A_{n-1} with $X_*(T_{n-1})$.

We will now associate to f a $T_{n-1} \rtimes \mathcal{G}$-variety X_f as follows. Let $\mathcal{G}$ act on $k[M]$ as usual and define a T_{n-1}-action on $k[M]$ by putting

$$t(m) = f(m)(t) \cdot m \qquad (t \in T_{n-1},\ m \in M)\ .$$

One easily checks that, by k-linear extension of this rule, one obtains a well-defined action of T_{n-1} by automorphism on $k[M]$. Moreover, for $t \in T_{n-1}$, $g \in \mathcal{G}$ and $m \in M$, one calculates

$$t(gm) = f(gm)(t) \cdot gm = [gf(m)](t) \cdot gm = f(m)(t^g) \cdot gm = [gt^g](m)\ ;$$

so the actions of $\mathcal{G}$ and T_{n-1} combine to yield a locally finite action of $T_{n-1} \rtimes \mathcal{G}$ on $k[M]$ and thus an algebraic action on $X_f = \operatorname{Spec} k[M]$.

Lemma 3.1. *The $T_{n-1} \rtimes \mathcal{G}$-variety X_f is a generically free if and only if*

(a) *f is surjective and*
(b) *$\operatorname{Ker}(f)$ is a faithful $\mathcal{G}$-lattice.*

Proof. Condition (a) is equivalent to saying that the T_{n-1}-action on X_f is generically free; cf., e.g., [OV, Theorem 3.2.5]. To interpret condition (b) geometrically, note that $k(X_f) = k(M)$ and $k(X_f/T_{n-1}) = k(M)^{T_{n-1}} = k(\operatorname{Ker}(f))$. Thus condition (b) holds iff $\mathcal{G}$ acts faithfully on X_f/T_{n-1} or, equivalently, iff the $\mathcal{G}$-action on X_f/T_{n-1} is and generically free (the two notions coincide for finite groups). The desired conclusion now follows from Lemma 2.1. □

3.3. **Compressions and $\mathcal{G}$-lattices.** In the sequel we will only be interested in generically free $T_{n-1} \rtimes \mathcal{G}$-varieties. In particular, we will assume that f is surjective and expand it into an exact sequence of $\mathcal{G}$-lattices:

$$0 \longrightarrow K = \operatorname{Ker}(f) \longrightarrow M \xrightarrow{f} A_{n-1} \longrightarrow 0\,, \tag{3.1}$$

where K is a faithful $\mathcal{G}$-lattice. For future reference, we extract the following equality from the proof of Lemma 3.1:

$$k(X_f/T_{n-1} \rtimes \mathcal{G}) = k(X_f)^{T_{n-1} \rtimes \mathcal{G}} = [k(M)^{T_{n-1}}]^{\mathcal{G}} = k(K)^{\mathcal{G}}\ . \tag{3.2}$$

We can now obtain information about $T_{n-1} \rtimes \mathcal{G}$-compressions of X_f by studying this sequence more closely.

Lemma 3.2. *Suppose that the exact sequence* (3.1) *extends to a commutative diagram*

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] & M \arrow[r, "f"] & A_{n-1} \arrow[r] & 0 \\
0 \arrow[r] & K_0 \arrow[r] \arrow[u, hook] & M_0 \arrow[r, "f_0"] \arrow[u] & A_{n-1} \arrow[r] \arrow[u, equal] & 0
\end{tikzcd}$$

of $\mathcal{G}$-lattices, where K_0 is faithful, and the vertical map $M_0 \longrightarrow M$ is injective. Then there exists a $T_{n-1} \rtimes \mathcal{G}$-compression $X_f \dashrightarrow X_{f_0}$.

Proof. Since $k(M_0) = k(X_{f_0})$ is an $T_{n-1} \rtimes \mathcal{G}$-invariant subfield of $k(M) = k(X_f)$, it defines a dominant $T_{n-1} \rtimes \mathcal{G}$-equivariant map $X_f \dashrightarrow X_{f_0}$. Furthermore, by Lemma 3.1, the $T_{n-1} \rtimes \mathcal{G}$-action on both X_f and X_{f_0} is generically free. Thus, the rational map $X_f \dashrightarrow X_{f_0}$ we have constructed is a $T_{n-1} \rtimes \mathcal{G}$-compression. □

3.4. **Linearization and essential dimension.** If the $\mathcal{G}$-lattice M in Section 3.2 is a permutation lattice then the $T_{n-1} \rtimes \mathcal{G}$-variety X_f is birationally linearizable. To see this, fix a $\mathbb{Z}$-basis $m_1, \ldots, m_r$ of M that is permuted by $\mathcal{G}$. Clearly, $k(X_f) = k(M) = k(m_1, \ldots, m_r)$. Thus, putting $V_f = \sum_i km_i$ we obtain a $T_{n-1} \rtimes \mathcal{G}$-invariant k-subspace of $k(X_f)$ with $k(X_f) = k(V_f)$.

A similar argument goes through if M to be *permutation projective*, i.e., M is a direct summand of a permutation $\mathcal{G}$-lattice.

Lemma 3.3. *If M is permutation projective in* (3.1) *then there is a $T_{n-1} \rtimes \mathcal{G}$-compression $V \dashrightarrow X_f$ with V a generically free linear $T_{n-1} \rtimes \mathcal{G}$-variety. In particular,* $\mathrm{ed}(T_{n-1} \rtimes \mathcal{G}) \leq \mathrm{rank}\, K$.

Proof. Suppose $M \oplus N = P$, where P is a permutation $\mathcal{G}$-lattice. Then the sequence (3.1) embeds in the obvious fashion in an exact sequence $0 \longrightarrow K \oplus N \longrightarrow P = M \oplus N \longrightarrow A_{n-1} \longrightarrow 0$. In view of the foregoing and Lemma 3.2, this proves the first assertion.

To complete the proof, recall that the essential dimension of an algebraic group G is defined as the smallest possible value $\dim(X/G)$, where X is a generically free G-variety so that there is a G-compression $V \dashrightarrow X$ with V a generically free linear G-variety; see [Re$_2$, Definition 3.5]. For $G = T_{n-1} \rtimes \mathcal{G}$ and $X = X_f$, we have $\dim(X/G) = \mathrm{rank}\, K$ by (3.2). □

4. Proof of Theorem 1.1

4.1. **Reduction to a lattice-theoretic problem.** The universal division algebra $\mathrm{UD}(n)$ is represented by a class $c \in H^1(Z(n), \mathrm{PGL}_n)$. We can write $\mathrm{UD}(n) = D \otimes_{Z(D)} Z(n)$ if and only if c lies in the image of the natural map

$$H^1(Z(D), \mathrm{PGL}_n) \longrightarrow H^1(Z(n), \mathrm{PGL}_n) \tag{4.1}$$

Recall that for any finitely generated field extension L/k, an element of $\alpha \in H^1(L, \mathrm{PGL}_n)$ may also be interpreted as a PGL_n*-torsor*, i.e., a generically free PGL_n-variety X_α such that $k(X_\alpha)^{\mathrm{PGL}_n} = L$. Moreover, X_α is uniquely determined (up to birational isomorphism of PGL_n-varieties), and the central simple algebra corresponding to α can be recovered as the algebra of PGL_n-equivariant rational maps $X_\alpha \dashrightarrow \mathrm{M}_n$. In particular, $X_c = \mathrm{M}_n \times \mathrm{M}_n$, where PGL_n acts on $\mathrm{M}_n \times \mathrm{M}_n$ by simultaneous conjugation; to say that c lies in the image of the map (4.1) is equivalent to saying that there exists a PGL_n-compression $\mathrm{M}_n \times \mathrm{M}_n \dashrightarrow X'$ such that $k(X')^{\mathrm{PGL}_n} = Z(D)$. For a more detailed discussion of these facts and further references, see [RY, Section 3].

Denote the linear subspace of M_n consisting of diagonal matrices by D_n. It is easy to see that $D_n \times \mathrm{M}_n$ is a $(\mathrm{PGL}_n, N(T_{n-1}))$-section of $\mathrm{M}_n \times \mathrm{M}_n$, where $N(T_{n-1}) = T_{n-1} \rtimes \mathcal{S}_n$ is the normalizer of the maximal torus $T_{n-1} = (\mathbb{G}_m)^n/\Delta$ in PGL_n, as in the previous section. (See Lemma 5.2 below for a more general fact.) Thus, in view of Lemma 2.2, we have the following

Reduction 4.1. In order to prove Theorem 1.1 it is enough to show that there exists an $N(T_{n-1})$-compression

$$D_n \times \mathrm{M}_n \longrightarrow X \tag{4.2}$$

such that

(i) $\dim(X) = \frac{1}{2}(n-1)(n-2) + n - 1$ or equivalently, $\dim(X/N(T_{n-1})) = \operatorname{trdeg}_k k(X)^{N(T_{n-1})} = \frac{1}{2}(n-1)(n-2)$.

(ii) $Z(n) = k(\mathrm{M}_n \times \mathrm{M}_n)^{\mathrm{PGL}_n} = k(D_n \times \mathrm{M}_n)^{N(T_{n-1})}$ is purely transcendental over $k(X)^{N(T_{n-1})}$.

Our construction of the compression (4.2) will be based on Lemma 3.2. In order to apply this lemma, we need to write the linear $N(T_{n-1})$-variety $D_n \times \mathrm{M}_n$ birationally in the form X_f, where f is as in (3.1). Let x_i and y_{rs} be the standard coordinates on D_n and M_n respectively. In this coordinate system, the $\mathcal{S}_n$-action on $D_n \times \mathrm{M}_n$ is given by

$$\sigma(x_i) = x_{\sigma(i)} \quad \text{and} \quad \sigma(y_{rs}) = y_{\sigma(r)\sigma(s)}\ .$$

Thus, monomials in these coordinates and their inverses form an $\mathcal{S}_n$-lattice isomorphic to $M = U_n \oplus U_n^{\otimes 2}$, where $U_n = \mathbb{Z}^n$ be the standard permutation $\mathcal{S}_n$-lattice. Moreover, an element $t = (t_1, \ldots, t_n)$ of $T_{n-1} = (\mathbb{G}_m)^n/\Delta$ acts on monomials in x_i, y_{rs} by characters determined (multiplicatively) by

$$t(x_i) = x_i \text{ and } t(y_{rs}) = t_r t_s^{-1} y_{rs}\ .$$

Denoting the standard basis of U_n by $b_1, \ldots, b_n$ and defining $f\colon M = U_n \oplus U_n^{\otimes 2} \longrightarrow A_{n-1}$ by $f(b_i, b_r \otimes b_s) = b_r - b_s$, the above formulas give exactly the action of $N(T_{n-1}) = T_{n-1} \rtimes \mathcal{S}_n$ on X_f as described in (3.2). The exact sequence (3.1) for this f is the Formanek – Procesi exact sequence

$$0 \longrightarrow K = \operatorname{Ker}(f) \longrightarrow U_n \oplus U_n^{\otimes 2} \xrightarrow{f} A_{n-1} \longrightarrow 0\,; \tag{4.3}$$

see [F]. Note that

$$K \simeq U_n \oplus U_n \oplus A_{n-1}^{\otimes 2}\ .$$

Here, the first copy of U_n is mapped identically onto the first summand of $U_n \oplus U_n^{\otimes 2}$, the second U_n corresponds to the sublattice of $U_n^{\otimes 2}$ consisting of the monomials in $y_{ii} \in K$, and $A_{n-1}^{\otimes 2}$ describes the kernel of f, restricted to the sublattice $\langle y_{rs} \mid r \neq s\rangle \simeq U_n \otimes A_{n-1} \subset U_n^{\otimes 2}$; cf. [B, p. 3573].

We now want to apply Lemma 3.2 to the above sequence, with $K_0 = \bigwedge^2 A_{n-1}$. Recall that $\bigwedge^2 A_{n-1}$ may be viewed as a sublattice $A_{n-1}^{\otimes 2}$; see (2.1). Let

$$\varphi\colon \bigwedge^2 A_{n-1} \hookrightarrow U_n \oplus U_n \oplus A_{n-1}^{\otimes 2} \tag{4.4}$$

be the natural embedding of $\bigwedge^2 A_{n-1}$ into the third component of $U_n \oplus U_n \oplus A_{n-1}^{\otimes 2}$. We remark that for $n > 3$, $\mathcal{S}_n$ acts faithfully on $\bigwedge^2 A_{n-1}$; in fact, $\bigwedge^2 A_{n-1} \otimes_{\mathbb{Z}} \mathbb{Q}$ is the irreducible S_n-representation corresponding to the partition $(n-2, 1^2)$ of n; see, e.g., [FH, Exerc. 4.6].

Combining Reduction 4.1 with Lemma 3.2, we obtain:

Reduction 4.2. Theorem 1.1 follows from Propositions 4.3 and 4.4 stated below.

Proposition 4.3. *For odd $n \geq 5$, $k(U_n \oplus U_n \oplus A_{n-1}^{\otimes 2}) \simeq k(\bigwedge^2 A_{n-1})(y_1, \dots, y_r)$ as $\mathcal{S}_n$-fields, where the elements y_i are $\mathcal{S}_n$-invariant and transcendental over $k(\bigwedge^2 A_{n-1})$. In particular, $k(U_n \oplus U_n \oplus A_{n-1}^{\otimes 2})^{\mathcal{S}_n}$ is rational over $k(\bigwedge^2 A_{n-1})^{\mathcal{S}_n}$.*

Proposition 4.4. *For odd n, there exists a commutative diagram of $\mathcal{S}_n$-lattices:*

$$\begin{tikzcd}
0 \arrow[r] & U_n \oplus U_n \oplus A_{n-1}^{\otimes 2} \arrow[r] & U_n \oplus U_n^{\otimes 2} \arrow[r, "f"] & A_{n-1} \arrow[r] & 0 \\
0 \arrow[r] & \bigwedge^2 A_{n-1} \arrow[r] \arrow[u, hook, "\varphi"] & L \arrow[r, "f_0"] \arrow[u] & A_{n-1} \arrow[r] \arrow[u, equal] & 0
\end{tikzcd}$$

Here the first row is the Formanek – Procesi sequence (4.3).

Indeed, Proposition 4.4 in conjunction with Lemma 3.2 yields an $N(T_{n-1})$-compression

$$D_n \times \mathrm{M}_n \xrightarrow{\simeq} X_f \longrightarrow X = X_{f_0} ,$$

and formula (3.2) further implies that $k(D_n \times M_n)^{N(T_{n-1})} = k(X_f)^{N(T_{n-1})} = k(U_n \oplus U_n \oplus A_{n-1}^{\otimes 2})^{\mathcal{S}_n}$ and $k(X)^{N(T_{n-1})} = k(\bigwedge^2 A_{n-1})^{\mathcal{S}_n}$. Thus, condition (i) in Reduction 4.1 is clearly satisfied and Proposition 4.3 ensures that (ii) holds as well.

4.2. **Solution of the lattice-theoretic problem.** Our proofs of Propositions 4.3 and 4.4 will be based on the following result from [LL, Section 3.5]. If $\mathcal{G}$ is a finite group, $\mathcal{H}$ is a subgroup of $\mathcal{G}$ and M a $\mathbb{Z}[\mathcal{H}]$-module then $M\!\uparrow_{\mathcal{H}}^{\mathcal{G}} = \mathbb{Z}[\mathcal{G}] \otimes_{\mathbb{Z}[\mathcal{H}]} M$ will denote the induced $\mathbb{Z}[\mathcal{G}]$-module.

Proposition 4.5. *For odd n, there is an isomorphism of $\mathcal{S}_n$-lattices*

$$\mathsf{Sym}^2 A_{n-1} \oplus U_n \oplus \mathbb{Z} \simeq \mathbb{Z}\!\uparrow_{\mathcal{S}_{n-2} \times \mathcal{S}_2}^{\mathcal{S}_n} \oplus U_n \oplus \mathbb{Z} ,$$

where $\mathbb{Z}$ has the trivial $\mathcal{S}_n$-action. In particular, $\mathsf{Sym}^2 A_{n-1} \oplus U_n \oplus \mathbb{Z}$ is a permutation lattice.

Proof of Proposition 4.3. First, applying Proposition 2.3 to the obvious sequence $0 \longrightarrow U_n \oplus A_{n-1}^{\otimes 2} \longrightarrow U_n \oplus U_n \oplus A_{n-1}^{\otimes 2} \longrightarrow U_n \longrightarrow 0$, we see that

$$k(U_n \oplus U_n \oplus A_{n-1}^{\otimes 2}) \simeq k(U_n \oplus A_{n-1}^{\otimes 2})(t_1, \dots, t_n)$$

as $\mathcal{S}_n$-fields.

Next, sequence (2.1) for $M = A_{n-1}$ combined with Proposition 4.5 gives rise to an exact sequence of $\mathcal{S}_n$-lattices

$$0 \longrightarrow \bigwedge^2 A_{n-1} \longrightarrow A_{n-1}^{\otimes 2} \oplus U_n \oplus \mathbb{Z} \longrightarrow P \longrightarrow 0 ,$$

where $P = \mathsf{Sym}^2 A_{n-1} \oplus U_n \oplus \mathbb{Z}$ is permutation. Applying Proposition 2.3 to this sequence, we deduce that

$$k(A_{n-1}^{\otimes 2} \oplus U_n \oplus \mathbb{Z}) \simeq k(\bigwedge^2 A_{n-1})(x_1, \dots, x_m)$$

as $\mathcal{S}_n$-fields.

Finally,

$$\begin{aligned} k(U_n \oplus U_n \oplus A_{n-1}^{\otimes 2}) &\simeq k(U_n \oplus A_{n-1}^{\otimes 2})(t_1, \dots , t_n) \\ &= k(A_{n-1}^{\otimes 2} \oplus U_n \oplus \mathbb{Z})(t_1, \dots , t_{n-1}) \\ &\simeq k(\bigwedge^2 A_{n-1})(x_1, \dots , x_m, t_1, \dots , t_{n-1}) \end{aligned}$$

as $\mathcal{S}_n$-fields, which proves the first assertion of Proposition 4.3. The second assertion is an immediate consequence of the first. $\square$

Proof of Proposition 4.4. Recall that the embedding φ of (4.4) is defined as the composition

$$\varphi\colon \bigwedge^2 A_{n-1} \overset{\psi}{\hookrightarrow} A_{n-1}^{\otimes 2} \hookrightarrow U_n \oplus U_n \oplus A_{n-1}^{\otimes 2} ,$$

where ψ is the injection from (2.1) (with $M = A_{n-1}$) and the second map identifies $A_{n-1}^{\otimes 2}$ with the third component of $U_n \oplus U_n \oplus A_{n-1}^{\otimes 2}$. We aim to show that φ together with sequence (4.3) will give rise to a commutative diagram as in the statement of Proposition 4.4. In other words, our goal is to show that the class in $\mathrm{Ext}_{\mathbb{Z}[\mathcal{S}_n]}(A_{n-1}, U_n \oplus U_n \oplus A_{n-1}^{\otimes 2})$ corresponding to the extension (4.3) belongs to the image of the map

$$\varphi_*\colon \mathrm{Ext}_{\mathbb{Z}[\mathcal{S}_n]}(A_{n-1}, \bigwedge^2 A_{n-1}) \longrightarrow \mathrm{Ext}_{\mathbb{Z}[\mathcal{S}_n]}(A_{n-1}, U_n \oplus U_n \oplus A_{n-1}^{\otimes 2}) .$$

In fact, we will prove:

Lemma 4.6. *For odd n, the map φ_* is surjective.*

Proof. We will tacitly use the following standard facts from homological algebra, valid for any finite group $\mathcal{G}$:

- If V is a $\mathcal{G}$-module and M an $\mathcal{H}$-module for some subgroup $\mathcal{H} \leq \mathcal{G}$ then $\mathrm{Ext}^*_{\mathbb{Z}[\mathcal{G}]}(V, M\uparrow_{\mathcal{H}}^{\mathcal{G}}) \simeq \mathrm{Ext}^*_{\mathbb{Z}[\mathcal{H}]}(V\big|_{\mathcal{H}}, M)$; see [HS, Prop. IV.12.3] and [Br, Prop. III.5.9]. For $V = \mathbb{Z}$, the trivial $\mathcal{G}$-module, this isomorphism is the "Shapiro isomorphism" $H^*(\mathcal{G}, M\uparrow_{\mathcal{H}}^{\mathcal{G}}) \simeq H^*(\mathcal{H}, M)$. In case, M is actually a $\mathcal{G}$-module, the restriction map $\mathrm{Res}^{\mathcal{G}}_{\mathcal{H}}\colon H^*(\mathcal{G}, M) \longrightarrow H^*(\mathcal{H}, M)$ factors through the Shapiro isomorphism:
$$\mathrm{Res}^{\mathcal{G}}_{\mathcal{H}} : H^*(\mathcal{G}, M) \xrightarrow{\mu_*} H^*(\mathcal{G}, M\uparrow_{\mathcal{H}}^{\mathcal{G}}) \xrightarrow{\sim} H^*(\mathcal{H}, M) ,$$
where $\mu\colon M \longrightarrow M\uparrow_{\mathcal{H}}^{\mathcal{G}}$ sends $m \mapsto \sum_{g \in \mathcal{G}/\mathcal{H}} g \otimes g^{-1}m$; see [Br, p. 81].
- For any $\mathcal{G}$-lattices V and W, $\mathrm{Ext}^*_{\mathbb{Z}[\mathcal{G}]}(V, W) \simeq H^*(\mathcal{G}, V^* \otimes W)$, where $\otimes = \otimes_{\mathbb{Z}}$ and $V^* = \mathrm{Hom}_{\mathbb{Z}}(V, \mathbb{Z})$ is the dual $\mathcal{G}$-lattice; see [Br, Prop. III.2.2].
- If V and W are both permutation $\mathcal{G}$-lattices then $\mathrm{Ext}_{\mathbb{Z}[\mathcal{G}]}(V, W) = 0$; cf. [L, Propositions 1.1, 1.2].

Armed with these facts, we proceed as follows. First, $\mathrm{Ext}_{\mathbb{Z}[\mathcal{S}_n]}(A_{n-1}, U_n) = 0$, because $U_n \simeq \mathbb{Z}{\uparrow}_{\mathcal{S}_{n-1}}^{\mathcal{S}_n}$ and $A_{n-1}\big|_{\mathcal{S}_{n-1}} \simeq U_{n-1}$. Therefore, it suffices to show that the map

$$\psi_*\colon\ \mathrm{Ext}_{\mathbb{Z}[\mathcal{S}_n]}(A_{n-1}, \bigwedge^2 A_{n-1}) \longrightarrow \mathrm{Ext}_{\mathbb{Z}[\mathcal{S}_n]}(A_{n-1}, A_{n-1}^{\otimes 2})$$

is surjective. But the extension (2.1) (for $M = A_{n-1}$) gives rise to an exact sequence

$$\mathrm{Ext}_{\mathbb{Z}[\mathcal{S}_n]}(A_{n-1}, \bigwedge^2 A_{n-1}) \xrightarrow{\psi_*} \mathrm{Ext}_{\mathbb{Z}[\mathcal{S}_n]}(A_{n-1}, A_{n-1}^{\otimes 2}) \longrightarrow \mathrm{Ext}_{\mathbb{Z}[\mathcal{S}_n]}(A_{n-1}, \mathsf{Sym}^2 A_{n-1})\ .$$

Therefore, it suffices to prove:

$$\mathrm{Ext}_{\mathbb{Z}[\mathcal{S}_n]}(A_{n-1}, \mathsf{Sym}^2 A_{n-1}) = 0 \quad \text{for odd } n.$$

For this, we use the isomorphism $\mathsf{Sym}^2 A_{n-1} \oplus U_n \oplus \mathbb{Z} \simeq \mathbb{Z}{\uparrow}_{\mathcal{G}}^{\mathcal{S}_n} \oplus U_n \oplus \mathbb{Z}$ of Proposition 4.5, where we have put $\mathcal{G} = \mathcal{S}_{n-2} \times \mathcal{S}_2$ for simplicity. This isomorphism entails

$$\begin{aligned}
\mathrm{Ext}_{\mathbb{Z}[\mathcal{S}_n]}(A_{n-1}, \mathsf{Sym}^2 A_{n-1}) &\simeq \mathrm{Ext}_{\mathbb{Z}[\mathcal{S}_n]}(A_{n-1}, \mathbb{Z}{\uparrow}_{\mathcal{G}}^{\mathcal{S}_n}) \\
&\simeq \mathrm{Ext}_{\mathbb{Z}[\mathcal{G}]}(A_{n-1}\big|_{\mathcal{G}}, \mathbb{Z}) \\
&\simeq H^1(\mathcal{G}, A_{n-1}^*)\ .
\end{aligned}$$

Dualizing the augmentation sequence $0 \longrightarrow A_{n-1} \longrightarrow U_n \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$ we obtain an exact sequence $0 \longrightarrow \mathbb{Z} \xrightarrow{\epsilon^*} U_n \longrightarrow A_{n-1}^* \longrightarrow 0$, where $\epsilon^*(1) = \sum_i e_i$, the sum of the natural basis elements of U_n. This sequence, viewed as exact sequence of $\mathcal{G}$-lattices, in turn yields an exact sequence

$$H^1(\mathcal{G}, U_n) = 0 \longrightarrow H^1(\mathcal{G}, A_{n-1}^*) \longrightarrow H^2(\mathcal{G}, \mathbb{Z}) \longrightarrow H^2(\mathcal{G}, U_n)\ .$$

Thus, it suffices to show that $H^2(\mathcal{G}, \mathbb{Z}) \longrightarrow H^2(\mathcal{G}, U_n)$ is injective. As a $\mathcal{G}$-module, $U_n = V \oplus W$, where $V = \bigoplus_{i=1}^{n-2} \mathbb{Z}e_i \simeq \mathbb{Z}{\uparrow}_{\mathcal{S}_{n-3}\times\mathcal{S}_2}^{\mathcal{G}}$ and $W = \mathbb{Z}e_{n-1} \oplus \mathbb{Z}e_n \simeq \mathbb{Z}{\uparrow}_{\mathcal{S}_{n-2}}^{\mathcal{G}}$. Therefore, the Shapiro isomorphism gives

$$H^2(\mathcal{G}, U_n) \simeq H^2(\mathcal{S}_{n-3} \times \mathcal{S}_2, \mathbb{Z}) \oplus H^2(\mathcal{S}_{n-2}, \mathbb{Z})$$

and the map $H^2(\mathcal{G}, \mathbb{Z}) \longrightarrow H^2(\mathcal{G}, U_n)$ becomes the restriction map

$$\mathrm{Res}_{\mathcal{S}_{n-3}\times\mathcal{S}_2}^{\mathcal{G}} \times \mathrm{Res}_{\mathcal{S}_{n-2}}^{\mathcal{G}}\colon H^2(\mathcal{G}, \mathbb{Z}) \longrightarrow H^2(\mathcal{S}_{n-3} \times \mathcal{S}_2, \mathbb{Z}) \oplus H^2(\mathcal{S}_{n-2}, \mathbb{Z})\ .$$

This map is indeed injective, as is easily seen by identifying $H^2(\mathcal{G}, \mathbb{Z})$ in the usual fashion with $\mathrm{Hom}(\mathcal{G}, \mathbb{Q}/\mathbb{Z})$, and similarly for the subgroups $\mathcal{S}_{n-3} \times \mathcal{S}_2$ and $\mathcal{S}_{n-2}$. This finishes the proof of the Lemma, and hence, of Proposition 4.4 and of Theorem 1.1. $\square$

5. Proof of Theorem 1.2

5.1. **General observations.** The following notations will be used throughout this section:

F	will be a field containing k;
A	will be a finite-dimensional central simple algebra with center F;
L	will be a strictly maximal commutative subfield of A;
n	denotes the degree of A, so $\dim_F A = n^2$ and $[L : F] = n$;
$\mathcal{G}$	is the Galois group of the normal closure L^{norm} of L over F;
T_{n-1}	denotes the diagonal maximal torus of PGL_n.

Reduction 5.1. In the course of proving Theorem 1.2 we may assume without loss of generality that F is a finitely generated field extension of k.

Proof. Indeed, choose a primitive element x for the extension L/F and complete $1, x, \dots, x^{n-1}$ to an F-basis $e_1, \dots, e_{n^2}$ of A, where $e_i = x^{i-1}$ for $i = 1, \dots, n$. Let c_{rs}^t be the structure constants for A in this basis, i.e.,

$$e_r e_s = \sum_{t=1}^{n^2} c_{rs}^t e_t \tag{5.1}$$

for every $r, s = 1, \dots, n^2$. Then $A = A_0 \otimes_{F_0} F$, where $F_0 = k(c_{rs}^t)$ and A_0 is the n^2-dimensional F_0-algebra spanned by $e_1, \dots, e_{n^2}$ with multiplication given by (5.1). Moreover, A_0 is a central simple algebra of degree n with center F_0 and A_0 contains the strictly maximal subfield $L_0 = F_0(x)$ whose normal closure L_0^{norm} has Galois group $\mathcal{G}$ over F_0. Clearly, $\tau(A) \le \tau(A_0)$. Thus, after replacing A by A_0 we may assume that F is finitely generated extension of k. $\square$

Next we pass from central simple algebras to generically free PGL_n-varieties, as we did at the beginning of Section 4. Recall that a central simple algebra A of degree n with center F defines a class $H^1(F, \mathrm{PGL}_n)$. This class, in turn, gives rise to a PGL_n-torsor X_A over F. Since we are assuming F is a finitely generated extension of k, X_A is a generically free PGL_n-variety; moreover, $F = k(X_A/\mathrm{PGL}_n)$ and A can be recovered from X_A as the algebra of PGL_n-equivariant rational maps $X_A \dashrightarrow \mathrm{M}_n$; cf. [RY, Section 3].

The algebras A we are concerned with in the context Theorem 1.2 are of a special form: they have a maximal subfield L/F such that $\mathrm{Gal}(L^{norm}/F)$ is the given group $\mathcal{G}$. We would like to know how this extra structure is reflected in the geometry of the PGL_n-variety X_A. The following lemma gives a partial answer. We continue to let T_{n-1} denote the diagonal maximal torus of PGL_n, as in Section 3.1.

Lemma 5.2. *X_A has a $(\mathrm{PGL}_n, T_{n-1} \rtimes \mathcal{G})$-section.*

Note that the group $\mathcal{G}$ comes with a natural permutation representation of $\mathcal{G}$ on the n embeddings $L \hookrightarrow L^{norm}$ over F. This permutation representation gives an embedding $\alpha\colon \mathcal{G} \hookrightarrow \mathcal{S}_n$ that we use to define the semidirect product $T_{n-1} \rtimes \mathcal{G}$. Note that α is only defined up to an inner automorphism of $\mathcal{S}_n$, since the n embedding $L \hookrightarrow L^{norm}$ are not naturally in a 1-1 correspondence with $\{1, \dots, n\}$. Relabeling these embeddings (or, equivalently, reordering the roots of a defining polynomial for L/F) will cause $T_{n-1} \rtimes \mathcal{G}$ to be replaced by a conjugate subgroup of PGL_n; the corresponding section will be translates of each other by elements of $\mathcal{S}_n \subset \mathrm{PGL}_n$.

Thus it is sufficient to verify that such a section exists for a particular numbering of the embeddings $L \hookrightarrow L^{norm}$.

Proof. Suppose $L = F(r)$ for some $r \in L$ and $r = r_1, r_2, \ldots, r_n$ are the conjugates of r in L^{norm}. As we remarked above, the order of the roots is not intrinsic; however, we choose it at this point, and it will not be changed in the sequel. The group $\mathcal{G}$ permutes $r_1, \ldots, r_n$ transitively via a permutation representation $\alpha \colon \mathcal{G} \hookrightarrow \mathcal{S}_n$.

Now let $x_1, \ldots, x_n$ be commuting independent variables over k. The symmetric group acts on the polynomial ring $k[x_1, \ldots, x_n]$ by permuting these variables; composing this action with α, we obtain a (permutation) action of $\mathcal{G}$ on $k[x_1, \ldots, x_n]$. Note that for every $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]^{\mathcal{G}}$, we have $f(r_1, \ldots, r_n) \in F$; we shall write this element of F as f_r.

Recall that A is the algebra of PGL_n-equivariant rational maps $X_A \dashrightarrow \mathrm{M}_n$. We claim that

$$S = \left\{ x \in X_A \quad : \quad \begin{array}{rl} r(x) = \mathrm{diag}(\lambda_1, \ldots, \lambda_n) & \text{is a diagonal matrix} \\ & \text{and} \\ f(\lambda_1, \ldots, \lambda_n) = f_r(x) & \text{for every } f \in k[x_1, \ldots, x_n]^{\mathcal{G}} \end{array} \right\}$$

is an $(\mathrm{PGL}_n, T_{n-1} \rtimes \mathcal{G})$-section S of X_A. Note that S is a $T_{n-1} \rtimes \mathcal{G}$-invariant subvariety of X_A: indeed, T_{n-1} acts trivially on the set of diagonal matrices, and $f_r \in F$ is a PGL_n-invariant rational function on X_A. Thus we need to show that

(i) $\mathrm{PGL}_n x$ intersects S for x in general position in X_A and

(ii) $gs \in S \quad \Longrightarrow \quad g \in T_{n-1} \rtimes \mathcal{G}$ for s in general position in S;

cf. Section 2.2.

Let $\pi \colon X_A \dashrightarrow X_A/\mathrm{PGL}_n$ be the rational quotient map. Recall that $k(X_A/\mathrm{PGL}_n) = k(X_A)^{\mathrm{PGL}_n} = F$. Suppose $p(t) = t^n + a_1 t^{n-1} + \cdots + a_n$ is the minimal polynomial of $r \in L$ over F. Note $a_1, \ldots, a_n \in F$ are PGL_n-invariant rational functions on X_A; in particular, for $x \in X_A$ in general position, the matrix $r(x) \in \mathrm{M}_n$ satisfies the polynomial $p_x(t) = t^n + a_1(x)t^{n-1} + \cdots + a_n(x) \in k[t]$. Since $p(t)$ is an irreducible polynomial over F, its discriminant δ is a non-zero element of F, i.e., a non-zero PGL_n-invariant rational function X_A. This means that for $x \in X_A$ in general position (i.e., away from the zero locus of δ and the indeterminacy locus of r), the $n \times n$-matrix $r(x)$ has distinct eigenvalues. We conclude that in this case $p_x(t)$ is the characteristic polynomial for $r(x)$; in particular, the eigenvalues of $r(x)$ are precisely the roots of $p_x(t)$.

To see what these eigenvalues are more explicitly, let $Y \dashrightarrow X_A/\mathrm{PGL}_n$ be a rational map of varieties induced by the field extension L^{norm}/F. Then $r_1, \ldots, r_n \in L^{norm}$ are rational functions on Y. Thus we have the following diagram of rational maps

$$\begin{tikzcd}
X_A \arrow[r, dashed, "r"] \arrow[dd, dashed, "\pi"'] & \mathrm{M}_n & \\
& Y \arrow[r, dashed, "r_i"] \arrow[dl, dashed] & k \\
X_A/\mathrm{PGL}_n & &
\end{tikzcd}$$

Suppose x be a point of X_A in general position and y is a point of Y lying above $\pi(x)$. Since $r_1, \dots, r_n$ are distinct elements of $L^{norm} = k(Y)$, $\lambda_1 = r_1(y), \dots, \lambda_n = r_n(y)$ are the n distinct roots of $p_x(t)$, i.e., the n distinct eigenvalues of the $n \times n$-matrix $r(x)$.

Proof of (i): In view of the above discussion, we may assume without loss of generality that $r(x)$ is diagonalizable. In other words, the PGL_n-orbit of $r(x)$ in M_n contains the diagonal matrix $\mathrm{diag}(\lambda_1, \dots, \lambda_n)$ or equivalently, $r(x') = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ for some $x' \in \mathrm{PGL}_n x$. It remains to show that $x' \in S$. Indeed, for any $f \in k[x_1, \dots, x_n]^{\mathcal{G}}$, we have

$$f_r(x') = f(r_1(y), \dots, r_n(y)) = f(\lambda_1, \dots, \lambda_n)\,,$$

as desired. This completes the proof of (i).

Proof of (ii): Let x be a point of S in general position. We may assume without loss of generality that the eigenvalues λ_i of the diagonal matrix $r(x) = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ are distinct. Suppose $gx \in S$ for some $g \in \mathrm{PGL}_n$. Then $gr(x)g^{-1}$ is again diagonal; hence, $g \in T_{n-1} \rtimes \mathcal{S}_n$. In other words, $g = t\sigma$, where t is a diagonal matrix and σ is a permutation matrix; our goal is to show that $\sigma \in \mathcal{G}$. Indeed, by the definition of S, σ has the property that $f(\lambda_{\sigma(1)}, \dots, \lambda_{\sigma(n)}) = f(\lambda_1, \dots, \lambda_n)$ for every $f \in k[x_1, \dots, x_n]^{\mathcal{G}}$. Since $\mathcal{G}$-invariant regular functions separate the orbits of the permutation $\mathcal{G}$-action on affine n-space (this is true for any finite group action on an affine variety; see, e.g., [PV, Section 0.4]), the points $(\lambda_{\sigma(1)}, \dots, \lambda_{\sigma(n)})$ and $(\lambda_1, \dots, \lambda_n)$ are in the same $\mathcal{G}$-orbit for this action. On the other hand, since $\lambda_1, \dots, \lambda_n$ are distinct, this is only possible if $\sigma \in \mathcal{G}$. This completes the proof of (ii) and thus of Lemma 5.2. $\square$

Remark 5.3. One can show that the converse of Lemma 5.2 is also true: if X_A has a $(\mathrm{PGL}_n, T_{n-1} \rtimes \mathcal{G})$-section then A contains a strictly maximal subfield L such that $\mathrm{Gal}(L^{norm}/F) = \mathcal{G}$. Since this result is not needed in the sequel, we omit the proof.

5.2. **Conclusion of the proof.** We are now ready to finish the proof of Theorem 1.2. Let A be a central simple algebra of degree n and let X_A denote the PGL_n-variety associated to A. Recall that $\tau(A) = \mathrm{ed}(X_A, \mathrm{PGL}_n)$; see [Re$_2$, Theorem 8.8 and Lemma 9.1]. Moreover, if X has a (PGL_n, H)-section S then $\mathrm{ed}(X, \mathrm{PGL}_n) \le \mathrm{ed}(S, H) \le \mathrm{ed}(H)$; see [Re$_2$, Lemma 4.1 and Definition 3.5]. Applying these inequalities to the situation described by Lemma 5.2, with $H = T_{n-1} \rtimes \mathcal{G}$, we see that

$$\tau(A) \le \mathrm{ed}(T_{n-1} \rtimes \mathcal{G})\,. \tag{5.2}$$

Thus Theorem 1.2 is a consequence of the following:

Lemma 5.4. *Suppose $\mathcal{G}$ is a transitive subgroup of $\mathcal{S}_n$ generated by the subgroup $\mathcal{H} = \mathcal{G} \cap \mathcal{S}_{n-1}$ together with elements $g_1, \ldots, g_r$. Assume that either $r \ge 2$ or $\mathcal{H} \ne \{1\}$. Then* $\mathrm{ed}(T_{n-1} \rtimes \mathcal{G}) \le r|\mathcal{G}| - n + 1$.

Proof. By Lemma 3.3, it suffices to construct an exact sequence (3.1) with M permutation projective and K faithful having $\operatorname{rank} K = r|\mathcal{G}| - n + 1$. To this end, note that $U_n \simeq \mathbb{Z}[\mathcal{G}/\mathcal{H}]$ as $\mathcal{G}$-lattices. Let $\overline{} : \mathbb{Z}[\mathcal{G}] \twoheadrightarrow \mathbb{Z}[\mathcal{G}/\mathcal{H}] = U_n$ denote the canonical epimorphism; the kernel of $\overline{}$ is $\mathbb{Z}[\mathcal{G}]\omega\mathcal{H}$, where $\omega\mathcal{H}$ denotes the augmentation ideal of $\mathbb{Z}[\mathcal{G}]$; cf. [Pa]. Then $\sum_i \mathbb{Z}[\mathcal{G}]\overline{(g_i - 1)} = A_{n-1}$; see [Pa, Lemma 3.1.1]. Therefore, we obtain an epimorphism of $\mathcal{G}$-lattices

$$f\colon M = \mathbb{Z}[\mathcal{G}]^r \twoheadrightarrow A_{n-1}\,, \qquad (\alpha_1, \ldots, \alpha_r) \mapsto \sum_i^r \alpha_i \overline{(g_i - 1)}\,.$$

Put $K = \operatorname{Ker} f$; so K certainly has the required rank. For faithfulness, we may consider $K \otimes \mathbb{Q}$ instead of K and work over the semisimple algebra $\mathbb{Q}[\mathcal{G}]$. Since $f \otimes \mathbb{Q}$ and $\overline{} \otimes \mathbb{Q}$ are split, we have $\mathbb{Q}[\mathcal{G}]$-isomorphisms $(A_{n-1} \otimes \mathbb{Q}) \oplus (K \otimes \mathbb{Q}) \simeq \mathbb{Q}[\mathcal{G}]^r$ and $(A_{n-1} \otimes \mathbb{Q}) \oplus \mathbb{Q} \oplus \mathbb{Q}[\mathcal{G}]\omega\mathcal{H} \simeq \mathbb{Q}[\mathcal{G}]$. Therefore,

$$K \otimes \mathbb{Q} \simeq \mathbb{Q}[\mathcal{G}]^{r-1} \oplus \mathbb{Q} \oplus \mathbb{Q}[\mathcal{G}]\omega\mathcal{H}\,.$$

If $r \ge 2$ then $\mathbb{Q}[\mathcal{G}]^{r-1}$ is $\mathcal{G}$-faithful, and if $\mathcal{H} \ne \{1\}$ then $\omega\mathcal{H} \otimes \mathbb{Q}$ is $\mathcal{H}$-faithful and so $\mathbb{Q}[\mathcal{G}]\omega\mathcal{H} \simeq (\omega\mathcal{H} \otimes \mathbb{Q})\!\uparrow_{\mathcal{H}}^{\mathcal{G}}$ is $\mathcal{G}$-faithful. In either case, $K \otimes \mathbb{Q}$ is faithful, and hence so is K, as desired. ☐

6. Algebras of degree four

Recall that Corollary 1.4 asserts that $d(4)$ equals 4 or 5. Whether the true value of $d(4)$ is four or five is an open question. The purpose of this section is to show that this question cannot be resolved by the methods of this paper.

For the rest of this section we will identify the Klein 4-group $\mathcal{V} = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ with the subgroup of $\mathcal{S}_4$ generated by (12)(34) and (13)(24). Let A_3 be the augmentation (or root) lattice of $\mathcal{S}_4$, restricted to $\mathcal{V}$; see (1.5). In other words,

$$A_3 \simeq \omega\mathcal{V}\,, \tag{6.1}$$

where $\omega\mathcal{V}$ is the augmentation ideal of the group ring $\mathbb{Z}[\mathcal{V}]$.

We now briefly recall how we arrived at the bound $d(4) \le 5$. First of all, since $\mathrm{UD}(4)$ is a $\mathcal{V}$-crossed product, $d(4) = \tau(\mathrm{UD}(4)) \le \mathrm{ed}(T_3 \rtimes \mathcal{V})$; see (5.2). Secondly, Lemma 3.2 tells us that $\mathrm{ed}(T_3 \rtimes \mathcal{V}) \le \operatorname{rank}(K_0)$, for any commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & M & \xrightarrow{f} & A_3 & \longrightarrow & 0 \\ & & \Big\uparrow{\scriptstyle\varphi} & & \Big\uparrow & & \Big\| & & \\ 0 & \longrightarrow & K_0 & \longrightarrow & M_0 & \xrightarrow{f_0} & A_3 & \longrightarrow & 0 \end{array} \tag{6.2}$$

of $\mathcal{V}$-lattices with M permutation projective, K_0 faithful, and φ is injective. Finally, in the course of the proof of Lemma 5.4 (with $\mathcal{G} = \mathcal{V}$ and $r = 2$) we constructed a particular diagram (6.2) with $M = M_0 = \mathbb{Z}[\mathcal{V}]^2$ and $\operatorname{rank}(K_0) = 5$. This gave us the bound $d(4) \le 5$. The question we will now address is whether or not one can sharpen this bound by choosing a different diagram (6.2). The following proposition shows that the answer is "no".

Proposition 6.1. *Let* (6.2) *be a commutative diagram of* $\mathcal{V} = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$*-lattices with* M *permutation projective. Then* K_0 *is faithful and* $\operatorname{rank} K_0 \ge 5$.

Note that in the setting of Lemma 3.2 we assumed that (i) K_0 is faithful and (ii) φ is injective. Here we see that (i) is automatic and (ii) is irrelevant for the rank estimate.

Proof. Since M is permutation projective, we have $H^1(\mathcal{H}, M) = 0 = H^{-1}(\mathcal{H}, M)$ for every subgroup $\mathcal{H}$ of $\mathcal{V}$. (This condition is actually equivalent to M being permutation projective; see [C-TS, Proposition 4].) Consequently, (6.2) yields a commutative diagram

$$\begin{tikzcd} 0 = H^1(\mathcal{H}, M) \arrow[r] & H^1(\mathcal{H}, A_3) \arrow[r, "\delta"] \arrow[d, equal] & H^2(\mathcal{H}, K) \\ & H^1(\mathcal{H}, A_3) \arrow[r, "\delta_0"] & H^2(\mathcal{H}, K_0) \arrow[u, "\varphi_*"'] \end{tikzcd}$$

Thus, δ_0 is mono. Since $H^1(\mathcal{V}, A_3) \simeq \mathbb{Z}/4\mathbb{Z}$ and $H^1(\mathcal{H}, A_3) \simeq \mathbb{Z}/2\mathbb{Z}$ for any nonidentity cyclic subgroup $\mathcal{H}$ of $\mathcal{V}$ (see [LL, Lemma 4.3]), we obtain

$$\mathbb{Z}/4\mathbb{Z} \hookrightarrow H^2(\mathcal{V}, K_0) \qquad \text{and} \qquad H^2(\mathcal{H}, K_0) \ne 0 \text{ for all } 1 \ne \mathcal{H} \le \mathcal{V}. \tag{6.3}$$

Similarly, $0 = H^{-1}(\mathcal{H}, M)$ implies $H^{-1}(\mathcal{H}, A_3) \hookrightarrow \widehat{H}^0(\mathcal{H}, K_0)$. Using the identification (6.1), we have $H^{-1}(\mathcal{V}, A_3) \simeq \omega\mathcal{V}/(\omega\mathcal{V})^2 \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Thus:

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \hookrightarrow \widehat{H}^0(\mathcal{H}, K_0)\ . \tag{6.4}$$

We will show that (6.3) forces K_0 to be faithful, and (6.3) and (6.4) together imply that $\operatorname{rank} K_0 \ge 5$. The discussion below could be shortened somewhat by a reference to [N]; however, for the sake of completeness, we will give a self-contained argument.

Lemma 6.2. *Let* L *be a* $\mathcal{V}$*-lattice,* $1 \ne x \in \mathcal{V}$ *and* $L_\pm = \{l \in L \mid xl = \pm l\}$*. If* $L\big|_{\langle x\rangle} = L_+ \oplus L_-$ *then* $2 \cdot H^2(\mathcal{V}, L) = 0$.

Proof. Since L_+ and L_- are $\mathcal{V}$-sublattices of L, we may assume $L = L_+$ or $L = L_-$. Write $\mathcal{V} = \langle x, y\rangle$. Then $\langle y\rangle$-sublattices of L are stable under $\mathcal{V}$. Therefore, we may assume that L is indecomposable as a $\langle y\rangle$-lattice. This leaves the following possibilities for L: $\mathbb{Z}_\pm\!\uparrow_{\langle x\rangle}^{\mathcal{V}}$ or $\mathbb{Z}_\lambda$ for some $\lambda \in \operatorname{Hom}(\mathcal{V}, \mathbb{Z})$. In each case, $2 \cdot H^2(\mathcal{V}, L) = 0$ is easy to verify. ∎

Lemma 6.2, in combination with the first condition in (6.3), implies that K_0 is faithful. Consequently, $\overline{K_0} = K_0/K_0^{\mathcal{V}}$ is faithful as well, and so $\operatorname{rank} \overline{K_0} \ge 2$. In addition, we know by (6.4) that $\widehat{H}^0(\mathcal{V}, K_0) = K_0^{\mathcal{V}}/(\sum_{\mathcal{V}} v)K_0$ is not cyclic. Hence, neither is $K_0^{\mathcal{V}}$, which forces $\operatorname{rank} K_0^{\mathcal{V}} \ge 2$ and thus $\operatorname{rank} K_0 \ge 4$. Suppose, by way of contradiction, that equality holds here, i.e., $\overline{K_0} = K_0/K_0^{\mathcal{V}}$ and $K_0^{\mathcal{V}}$ both have rank 2. By the well-known classification of finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$, the action of $\mathcal{V}$ on $\overline{K_0}$ is given by either

diag: the matrices $\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$ and $\begin{pmatrix} -1 & \\ & 1 \end{pmatrix}$; so $\overline{K_0} \simeq \mathbb{Z}_{+,-} \oplus \mathbb{Z}_{-,+}$, or

non-diag: the matrices $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$ and $\begin{pmatrix} & -1 \\ -1 & \end{pmatrix}$; so $\overline{K_0} \simeq \mathbb{Z}_- \uparrow_{\mathcal{H}}^{\mathcal{V}}$ for some cyclic $\mathcal{H} \leq \mathcal{V}$.

In case **non-diag**, $H^2(\mathcal{V}, \overline{K_0}) \simeq H^2(\mathcal{H}, \mathbb{Z}_-) \simeq \widehat{H}^0(\mathcal{H}, \mathbb{Z}_-) = 0$, and hence $H^2(\mathcal{V}, K_0^{\mathcal{V}})$ maps onto $H^2(\mathcal{V}, K_0)$. But $H^2(\mathcal{V}, K_0^{\mathcal{V}}) \simeq H^2(\mathcal{V}, \mathbb{Z})^2 \simeq \mathrm{Hom}(\mathcal{V}, \mathbb{Q}/\mathbb{Z})^2 \simeq (\mathbb{Z}/2\mathbb{Z})^4$. Thus $H^2(\mathcal{V}, K_0^{\mathcal{V}})$ is annihilated by 2, and hence so is $H^2(\mathcal{V}, K_0)$, contradicting (6.3). Therefore, **diag** must hold:

$$\overline{K_0} = K_0/K_0^{\mathcal{V}} \simeq \mathbb{Z}_{+,-} \oplus \mathbb{Z}_{-,+} \ .$$

The action of $\mathcal{V}$ on K_0 is given by matrices

$$c = \left(\begin{array}{c|cc} \mathbf{1}_{2\times 2} & \mathbf{0} & \boldsymbol{\gamma} \\ \hline & 1 & \\ & & -1 \end{array}\right) \qquad \text{and} \qquad d = \left(\begin{array}{c|cc} \mathbf{1}_{2\times 2} & \boldsymbol{\delta} & \mathbf{0} \\ \hline & -1 & \\ & & 1 \end{array}\right)$$

with $\boldsymbol{\gamma}, \boldsymbol{\delta} \in M_{2\times 1}(\mathbb{Z})$ and $\mathbf{0} = \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)$. By Lemma 6.2, $\boldsymbol{\gamma} \neq \mathbf{0}$ and $\boldsymbol{\delta} \neq \mathbf{0}$. Conjugating by a suitable matrix of the form $\left(\begin{smallmatrix} \mathbf{1}_{2\times 2} & \mathbf{0}\ \boldsymbol{\rho} \\ & \mathbf{1}_{2\times 2} \end{smallmatrix}\right)$ we can ensure that the entries of $\boldsymbol{\gamma}$ are 0 or 1, and similarly for $\boldsymbol{\delta}$. If $\boldsymbol{\gamma} = \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ then conjugating, respectively, by $\left(\begin{smallmatrix} 1 & 1 & \\ & 1 & \\ & & \mathbf{1}_{2\times 2} \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} & 1 & \\ 1 & & \\ & & \mathbf{1}_{2\times 2} \end{smallmatrix}\right)$, we can replace $\boldsymbol{\gamma}$ by $\boldsymbol{\gamma} = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$. Thus we may assume that $\boldsymbol{\gamma} = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$. If $\boldsymbol{\delta} = \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$, then conjugating by $\left(\begin{smallmatrix} 1 & & \\ 1 & 1 & \\ & & \mathbf{1}_{2\times 2} \end{smallmatrix}\right)$, we replace $\boldsymbol{\delta}$ by $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ without changing c. This leaves us with two cases to consider:

$\underline{\boldsymbol{\delta} = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)}$: Then $c = \left(\begin{smallmatrix} 1 & \\ & c' \end{smallmatrix}\right)$ and $d = \left(\begin{smallmatrix} 1 & \\ & d' \end{smallmatrix}\right)$ with $c' = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right)$ and $d' = \left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. Therefore, $K_0 \simeq \mathbb{Z} \oplus (A_3 \otimes_{\mathbb{Z}} \mathbb{Z}_\lambda)$, where $\lambda\colon \mathcal{V} \longrightarrow \mathbb{Z}$ is the map sending the elements of $\mathcal{V}$ acting via c and d both to -1. Tensoring the augmentation sequence $0 \longrightarrow A_3 = \omega\mathcal{V} \longrightarrow \mathbb{Z}[\mathcal{V}] \longrightarrow \mathbb{Z} \longrightarrow 0$ with $\mathbb{Z}_\lambda$ we obtain an exact sequence $0 \longrightarrow A_3 \otimes \mathbb{Z}_\lambda \longrightarrow \mathbb{Z}[\mathcal{V}] \otimes \mathbb{Z}_\lambda = \mathbb{Z}[\mathcal{V}] \longrightarrow \mathbb{Z}_\lambda \longrightarrow 0$. This sequence in turn implies that $H^2(\mathcal{V}, A_3 \otimes \mathbb{Z}_\lambda) \simeq H^1(\mathcal{V}, \mathbb{Z}_\lambda)$, and the inflation-restriction sequence easily gives $H^1(\mathcal{V}, \mathbb{Z}_\lambda) = \mathbb{Z}/2\mathbb{Z}$. Thus, $H^2(\mathcal{V}, K_0) = H^2(\mathcal{V}, \mathbb{Z}) \oplus H^2(\mathcal{V}, A_3 \otimes \mathbb{Z}_\lambda) \simeq (\mathbb{Z}/2\mathbb{Z})^3$, contradicting (6.3).

$\underline{\boldsymbol{\delta} = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)}$: In this case, $cd = \left(\begin{smallmatrix} \mathbf{1}_{2\times 2} & \mathbf{1}_{2\times 2} \\ & -\mathbf{1}_{2\times 2} \end{smallmatrix}\right)$. Letting $\mathcal{H}$ denote the cyclic subgroup of $\mathcal{V}$ acting via cd, we have $K_0\big|_{\mathcal{H}} \simeq \mathbb{Z}[\mathcal{H}]^2$. Thus, $H^2(\mathcal{H}, K_0) = 0$, contradicting (6.3).

This completes the proof of the proposition. $\square$

Acknowledgment. The work on this article was started while the authors were attending the Noncommutative Algebra program at MSRI in the Fall of 1999. The authors would like to thank the organizers of this program and MSRI staff for their hospitality and support.

References

[B] E. Beneish, *Induction theorems on the stable rationality of the center of the ring of generic matrices*, Trans. Amer. Math. Soc. **350** (1998), 3571 – 3585.

[Bou] N. Bourbaki, *Algèbre, chap. 1–3*, Hermann, Paris, 1970.

[Br] K. S. Brown, *Cohomology of Groups*, Springer-Verlag, New York, 1982.

[C-TS] J.-L. Colliot-Thélène and J.-J. Sansuc, *La R-équivalence sur les tores*, Ann. scient. Éc. Norm. Sup. **10** (1977), 175–230.

[F] E. Formanek, *The center of the ring of* 3×3 *generic matrices*, Linear and Multilinear Algebra **7** (1979), 203–212.

[FH] W. Fulton and J. Harris, *Representation Theory, A First Course*, Springer-Verlag, New York, 1991.

[HS] P. J. Hilton and U. Stammbach, *A Course in Homological Algebra*, 2nd ed., Springer-Verlag, New York, 1997.

[LL] N. Lemire, M. Lorenz, *On certain lattices associated with generic division algebras*, preprint, 1999. Available at http://www.math.temple.edu/~lorenz/papers/lattices.html

[L] H. W. Lenstra, *Rational functions invariant under a finite abelian group*, Invent. math. **25** (1974), 299–325.

[M] K. Masuda, *On a problem of Chevalley*, Nagoya Math. J. **8** (1955), 59–63.

[N] L. A. Nazarova, *Integral representations of Klein's four-group*, Soviet Math. Dokl. **2** (1961), 1304–1307.

[OV] A. L. Onishchik, E. B. Vinberg, *Lie Groups and Algebraic Groups*, Springer-Verlag, 1990.

[Pa] D. S. Passman, *The Algebraic Structure of Group Rings*, John Wiley & Sons, New York, 1977.

[Po] V. V. Popov, *Sections in Invariant Theory*, Proceedings of the Sophus Lie Memorial Conference, Scandinavian University Press, 1994, 315–362.

[PV] V. L. Popov, E. B. Vinberg, *Invariant Theory*, in Encyclopedia of Math. Sciences **55**, Algebraic Geometry IV, edited by A. N. Parshin and I. R. Shafarevich, Springer-Verlag, 1994.

[Pr] C. Procesi, *Non-commutative affine rings*, Atti Acc. Naz. Lincei, S. VIII, v. VIII, fo. 6 (1967), 239–255.

[Re_1] Z. Reichstein, *On a theorem of Hermite and Joubert*, Canadian Journal of Math., **51** (1) (1999), 69–95.

[Re_2] Z. Reichstein, *On the notion of essential dimension for algebraic groups*, Transformation groups, to appear. Available at http://ucs.orst.edu/~reichstz/pub.html.

[RY] Z. Reichstein, B. Youssin, *Splitting fields of G-varieties*, preprint.
Available at http://ucs.orst.edu/~reichstz/pub.html.

[Ros_1] M. Rosenlicht, *Some basic theorems on algebraic groups*, American Journal of Math., **78** (1956), 401–443.

[Ros_2] M. Rosenlicht, *A remark on quotient spaces*, Anais da Academia Brasileira de Ciências **35** (1963), 487–489.

[Row_1] L. H. Rowen, Polynomial Identities in Ring Theory, Academic Press, 1980.

[Row_2] L. H. Rowen, *Brauer factor sets and simple algebras*, Trans. Amer. Math. Soc., **282**, no. 2 (1984), 765–772.

Department of Mathematics, Temple University, Philadelphia, PA 19122-6094
E-mail address: lorenz@math.temple.edu

Department of Mathematics, Oregon State University, Corvallis, OR 97331
E-mail address: zinovy@math.orst.edu