HIGHER TRACE FORMS AND ESSENTIAL DIMENSION IN CENTRAL SIMPLE ALGEBRAS

Z. REICHSTEIN

Abstract. We show that the essential dimension of a finite-dimensional central simple algebra coincides with the essential dimension of its r-linear trace form, $(a_1, \dots, a_r) \mapsto \mathrm{tr}(a_1 \dots a_r)$, for any $r \geq 3$.

1. Introduction

Throughout this paper A will be a central simple algebra of degree n, K will be the center of A and k will be a subfield of K. I will denote the (reduced) trace function $A \longrightarrow K$ by tr. Let F_r be the r-linear trace form of A, given by

$$F_r(a_1, \dots, a_r) = \mathrm{tr}(a_1 \dots a_r)\,.$$

The main question motivating this paper is to determine how much information about A is carried by the trace form F_r.

The bilinear form F_2 has been studied by many authors. Suppose $\mathrm{char}(K) \neq 2$. If the degree n of A is odd then after an odd degree splitting extension L/K, F_2 becomes isomorphic to the trace form of the matrix algebra $\mathrm{M}_n(L)$. Using Springer's theorem (cf. e.g., [3, Theorem 7.2.3]), one readily deduces that the quadratic form associated to F_2 is isomorphic to

$$n < 1 > \oplus \frac{(n^2 - n)}{2} < 1, -1 > \tag{1}$$

over K. In particular, in this case F_2 carries no information about A.

The situation is different if n is even. It is well known that for $n = 2$ the algebra A is completely determined by its bilinear trace form F_2; cf. e.g., [3, Proposition III.2.5]. Recently Rost, Serre and Tignol [8] gave a description of F_2 for algebras A of degree 4, assuming K contains a 4th root of unity. They showed that in this case F_2 also encodes many of the algebra properties of A. In particular, one can tell whether or not A is cyclic or biquaternion by looking only at F_2. (For related results in characteristic two, see [9].)

On the other hand, the bilinear trace form F_2 does not, in general, capture the *essential dimension* of A for any $n \geq 3$; cf. Remark 6. The purpose of this paper is to show that the essential dimension of A is captured by the r-linear trace form F_r for any $r \geq 3$. Before stating this formally I will briefly recall the definition of essential dimension.

2000 *Mathematics Subject Classification.* 11E76, 16K20.
Partially supported by an NSERC research grant.

Let $\mathcal{F}$ be a functor from the category of field extensions of k to the category of sets. I will say that $\alpha \in \mathcal{F}(K)$ descends to a subfield $K_0 \subset K$ if α lies in the image of the natural map $\mathcal{F}(K_0) \to \mathcal{F}(K)$. The essential dimension $\operatorname{ed}(\alpha)$ is defined as the minimal value of $\operatorname{trdeg}_k(K_0)$, where α descends to K_0; cf. [1, 5]. In this paper we will be particularly interested in the functors CSA_n and $\mathrm{Forms}_{r,m}$, where

$\mathrm{CSA}_n(K)$ = set of central simple algebras A/K of degree n, up to K-isomorphism

and

$\mathrm{Forms}_{r,m}(K)$ = set of pairs (V, F), where V is an m-dimensional K-vector space and F is an r-linear form on V, up to equivalence. Here (V, F) and (V', F') are considered equivalent if there is an isomorphism $V \to V'$ of K-vector spaces, which takes F to F'.

I will view A as an element of $\mathrm{CSA}_n(K)$ and F_r as an element of $\mathrm{Forms}_{r,n^2}(K)$. With these notations, the main result of this paper is the following theorem.

Theorem 1. *Let A/K be a central simple algebra of degree n and F_r be the r-linear trace form in A. Suppose* $\operatorname{char}(K)$ *does not divide n. Then* $\operatorname{ed}(F_r) = \operatorname{ed}(A)$ *for any $r \geq 3$.*

Note that the inequality $\operatorname{ed}(F_r) \leq \operatorname{ed}(A)$ is obvious. Indeed, if A descends to a subfield K_0 of K then clearly F_r also descends to K_0. The proof of the opposite inequality given below does not show that if F_r descends to K_0 then so does A. I don't know whether or not this is true. Instead, I will show that if F_r descends to a subfield $K_0 \subset K$ then A descends to a subfield K_1 such that $K_0 \subset K_1 \subset K$ and $[K_1 : K_0] < \infty$ (in fact, $K_1 = K_0(c)$, where $c^r \in K_0$).

2. Preliminaries

The remainder of this paper will be devoted to proving Theorem 1. In particular, I will always assume that $\operatorname{char}(K)$ does not divide n and set $m = n^2 = \dim_K(A)$. As usual, $[\ ,\ ]$ will denote the natural Lie bracket in A, defined by $[a, b] = ab - ba$.

The following simple lemma will be used in the proof of Theorem 1.

Lemma 2. *Let A/K be a central simple algebra of degree n and let $b_1, \dots, b_m$ be a K-basis of A. Then*

(a) for every $d \geq 1$, monomials of degree d in $b_1, \dots, b_m$ span A as a K-vector space.

(b) Let $A_0 = \{a \in A \mid \operatorname{tr}(a) = 0\}$. Then for any $d \geq 2$, elements of the form $[b_{i_1}, [b_{i_2}, \dots [b_{i_{d-1}}, b_{i_d}] \dots]]$ span A_0 as a K-vector space.

Note that part (a) and its proof below remain valid for any K-algebra A.

Proof. (a) Use induction on d. The base case, $d = 1$, is obvious. For the induction step suppose that $d \geq 2$ and that the lemma holds for monomials of degree $d-1$. In particular, the identity element of A can be written as

$$1_A = c_1X_1 + \cdots + c_mX_m$$

where $X_1, \dots, X_m$ are monomials of degree $d-1$ and $c_1, \dots, c_m \in K$. Then for each $i = 1, \dots, m$,

$$b_i = b_i \cdot 1_A = c_1(b_iX_1) + \cdots + c_m(b_iX_m)$$

is a linear combination of monomials of degree d in $b_1, \dots, b_m$. Since $b_1, \dots, b_m$ form a K-basis of A, this shows that monomials of degree d span A over K.

(b) The assertion of part (b) is equivalent to $[A, [A, \dots [A, A]] \dots] = A_0$ (where the Lie bracket is applied $d \geq 2$ times). Thus it suffices to show that

$$[A, A] = [A, A_0] = [A_0, A_0] = A_0\,.$$

The first two of these identities are obvious and the third one is a consequence of the fact that A_0 is a simple Lie algebra (it is a form of sl_n). In concrete terms, in order to prove the identity $[A_0, A_0] = A_0$, one may pass to the separable closure K^{sep} of K, i.e., replace K by K^{sep} and A by $\mathrm{M}_n(K^{sep})$. In the case where A is the matrix algebra, it is easy to see that elements of the form $[e_{ab}, e_{cd}]$ span A_0, as a, b, c and d range from 1 to m. (Here e_{ij} are the matrix units.) □

Before we proceed with the proof of Theorem 1, we record the following special cases of the definitions in the previous section.

A central simple algebra A/K descends to $K_0 \subset K$ if there is a K-basis $b_1, \dots, b_m$ of A such that the structure constants of A relative to this basis lie in K_0.

The r-linear trace form F_r descends to $K_0 \subset K$ if there is a K-basis $b_1, \dots, b_m$ of A such that $\mathrm{tr}(b_{i_1} \dots b_{i_r})$ lies in K_0 for every $i_1, \dots, i_r = 1, \dots, m$.

3. Proof of Theorem 1

Since the inequality $\mathrm{ed}(F_r) \leq \mathrm{ed}(A)$ is obvious (see the paragraph after the statement of Theorem 1), I will focus on proving the opposite inequality, $\mathrm{ed}(A) \leq \mathrm{ed}(F_r)$. The following lemma was motivated by [2].

Lemma 3. *Suppose for some $r \geq 3$ there exists a K-basis $b_1, \dots, b_m$ of A and a subfield $K_0 \subset K$ such that $\mathrm{tr}(M) \in K_0$ for every monomial M in $b_1, \dots, b_m$ of degree r or $r-1$. Then A descends to K_0.*

Note that Lemma 3 (and its proof below) remain valid for any semisimple K-algebra A.

Proof. Let c_{ij}^h be the structure constants of A with respect to the basis $b_1, \dots, b_m$. That is,

$$b_ib_j = \sum_{h=1}^{m} c_{ij}^h b_h\,, \tag{2}$$

for $i, j = 1, \ldots, m$. Our goal is to show that each c_{ij}^h lies in K_0. In order to do this, I will fix i and j and try to solve (2) for the m coefficients $c_{ij}^1, c_{ij}^2, \ldots, c_{ij}^m$.

By Lemma 2(a), with $d = r - 2$, there exists a K-basis $Z_1, \ldots, Z_m$ of A where each Z_i is a monomial in $b_1, \ldots, b_m$ of degree $r-2$. Since the (bilinear) trace form on A is nonsingular, (2) is equivalent to the system

$$\begin{cases} \mathrm{tr}(b_i b_j Z_1) = \sum_{h=1}^m \mathrm{tr}(b_h Z_1) c_{ij}^h \\ \mathrm{tr}(b_i b_j Z_2) = \sum_{h=1}^m \mathrm{tr}(b_h Z_2) c_{ij}^h \\ \vdots \qquad \vdots \\ \mathrm{tr}(b_i b_j Z_m) = \sum_{h=1}^m \mathrm{tr}(b_h Z_m) c_{ij}^h \end{cases} \tag{3}$$

of m linear equations in m unknowns, $c_{ij}^1, c_{ij}^2, \ldots, c_{ij}^m$. Since $b_1, \ldots, b_m$ and $Z_1, \ldots, Z_m$ are both K-bases of A, and the (bilinear) trace form on A is nonsingular, an easy exercise in linear algebra shows that the matrix of this system,

$$\begin{pmatrix} \mathrm{tr}(b_1 Z_1) & \mathrm{tr}(b_2 Z_1) & \ldots & \mathrm{tr}(b_m Z_1) \\ \mathrm{tr}(b_1 Z_2) & \mathrm{tr}(b_2 Z_2) & \ldots & \mathrm{tr}(b_m Z_2) \\ \vdots & & \vdots & \\ \mathrm{tr}(b_1 Z_m) & \mathrm{tr}(b_2 Z_m) & \ldots & \mathrm{tr}(b_m Z_m) \end{pmatrix},$$

is nonsingular. Note the $b_h Z_l$ and $b_i b_j Z_l$ are monomials in $b_1, \ldots, b_m$ of degree $r - 1$ and r respectively. Thus, by our assumption, every coefficient of the system (3) lies in K_0. Solving this system by Cramer's rule, we conclude that every c_{ij}^h lies in K_0. □

The inequality $\mathrm{ed}(A) \leq \mathrm{ed}(F_r)$ (and thus Theorem 1) is now an immediate consequence of Proposition 4(b) below.

Proposition 4. *Suppose $b_1, \ldots, b_m$ is a K-basis of A and K_0 is a subfield of K such that $\mathrm{tr}(M) \in K_0$ for every monomial M in $b_1, \ldots, b_m$ of degree $r \geq 3$.*

(a) There exist $\alpha_1, \ldots, \alpha_r \in K_0$ such that $\sum_{i=1}^m \alpha_i b_i = c \cdot 1_A$ for some $0 \neq c \in K$.

(b) There exists a finite extension K_1 of K_0 such $K_0 \subset K_1 \subset K$ and $\mathrm{tr}(N) \in K_1$ for any monomial N in $b_1, \ldots, b_m$ of degree $\leq r$.

Proof. By Lemma 2(b), with $d = r - 1$, there exists a K-basis $Y_1, \ldots, Y_{m-1}$ of A_0 such that each Y_i has the form

$$Y_i = [b_{i_1}, [b_{i_2}, \ldots [b_{i_{r-2}}, b_{i_{r-1}}] \ldots]]$$

for some $i_1, \ldots, i_{r-1} \in \{1, \ldots, m\}$.

Now observe that the orthogonal complement to A_0 in A, with respect to the trace form, is precisely $K \cdot 1_A$. Thus, $J \in A$ lies in $K \cdot 1_A$ if and only if

$$\begin{cases} \operatorname{tr}(Y_1 J) = 0\,, \\ \operatorname{tr}(Y_2 J) = 0\,, \\ \dots \\ \operatorname{tr}(Y_{m-1} J) = 0\,. \end{cases} \tag{4}$$

Writing $J = \alpha_1 b_1 + \cdots + \alpha_m b_m$, with indeterminate coefficients $\alpha_1, \dots, \alpha_m$ and expanding (4), we obtain the homogeneous linear system

$$\begin{cases} \operatorname{tr}(Y_1 b_1)\alpha_1 + \cdots + \operatorname{tr}(Y_1 b_m)\alpha_m = 0\,, \\ \operatorname{tr}(Y_2 b_1)\alpha_1 + \cdots + \operatorname{tr}(Y_2 b_m)\alpha_m = 0\,, \\ \dots \\ \operatorname{tr}(Y_{m-1} b_1)\alpha_1 + \cdots + \operatorname{tr}(Y_{m-1} b_m)\alpha_m = 0\,. \end{cases}$$

of $m-1$ equations in m variables. By our choice of $Y_1, \dots, Y_{m-1}$ every coefficient $\operatorname{tr}(Y_i b_j)$ lies in K_0. Thus this system has a nontrivial solution $(\alpha_1, \dots, \alpha_m) \in K_0^m$. For these $\alpha_1, \dots, \alpha_m$,

$$J = \alpha_1 b_1 + \cdots + \alpha_m b_m \neq 0$$

satisfies (4) and hence is of the form $c \cdot 1_A$ for some $0 \neq c \in K$.

(b) Let $J = \alpha_1 b_1 + \cdots + \alpha_m b_m = c \cdot 1_A$ be as in part (a). We do not know that $c \in K_0$; however, I claim that $K_1 = K_0(c)$ is a finite extension of K_0. Indeed, since $\alpha_1, \dots \alpha_m$ lie in K_0, $nc^r = \operatorname{tr}(J^r)$ is a K_0-linear combination of elements of the form $\operatorname{tr}(b_{i_1} \dots b_{i_r})$, which, by our assumption, lie in K_0. Thus $nc^r \in K_0$, and since $\operatorname{char}(K)$ does not divide n, we conclude that $c^r \in K_0$. This shows that c is algebraic over K_0 and thus proves the claim.

It remains to show that $\operatorname{tr}(b_{i_1} \dots b_{i_s})$ lies in K_1 for any $1 \le s \le r$ and any $i_1, \dots, i_s = 1, \dots, m$. Since $c \neq 0$, we have

$$\operatorname{tr}(b_{i_1} \dots b_{i_s}) = \frac{1}{c^{r-s}} \operatorname{tr}(b_{i_1} \dots b_{i_s} J^{r-s})\,. \tag{5}$$

Expanding $\operatorname{tr}(b_{i_1} \dots b_{i_s} J^{r-s})$ and remembering that $\alpha_1, \dots, \alpha_m$ lie in K_0, we see that $\operatorname{tr}(b_{i_1} \dots b_{i_s} J^{r-s})$ lies in K_0. Equation (5) now tells us that $\operatorname{tr}(b_{i_1} \dots b_{i_s})$ lies in K_1, as claimed. □

4. Concluding remarks

Remark 5. The conclusion of Proposition 4(b) can be strengthened as follows: $\operatorname{tr}(N) \in K_1$ for every monomial N in $b_1, \dots, b_m$. To prove this, we argue by induction on $\deg(N)$. The base case, where $\deg(N) \le r$, is given by Proposition 4(b), and the induction step is carried out by using the relations (2) to lower the degree of N. (Recall from the proof of Lemma 3 that the structure constants c_{ij}^h lie in K_1.)

Remark 6. If $r = 2$, Theorem 1 fails for every $n \ge 3$. That is, for every $n \ge 3$ there exists a central simple algebra of degree n such that $\operatorname{ed}(F_2) < \operatorname{ed}(A)$.

Proof. For the purpose of constructing A, I will take the base field k to be the field $\mathbb{C}$ of complex numbers. As usual, K will denote a field extension of $k = \mathbb{C}$. If A/K is non-split then clearly A cannot descend to $\mathbb{C}$, i.e., $\mathrm{ed}(A) \geq 1$ (in fact, we even have $\mathrm{ed}(A) \geq 2$ by Tsen's theorem; cf. e.g., [6, Corollary 19.4a]). Thus it suffices to construct an algebra A/K of degree $n \geq 3$ whose bilinear trace form F_2 descends to $\mathbb{C}$. In this case we will have $0 = \mathrm{ed}(F_2) < \mathrm{ed}(A)$, as desired.

Note that if the quadratic trace form $q_A \colon a \mapsto \mathrm{tr}(a^2)$ descends to $\mathbb{C}$ then so does the bilinear trace form $F_2 \colon (a, b) \mapsto \mathrm{tr}(ab)$, since F_2 can be recovered from q_A by polarization. Thus we only need to construct examples of non-split algebras A/K of degree $n \geq 3$ such that the quadratic trace form q_A descends to $\mathbb{C}$.

If n is odd, the argument in the introduction shows that q_A descends to $\mathbb{C}$ for every A; cf. (1). If $n = 2s \geq 4$ is even, consider algebras A of degree n and index s, i.e., algebras of the form $A = \mathrm{M}_2(D) = \mathrm{M}_2(K) \otimes_K D$, where D/K is a division algebra of degree $s \geq 2$. The quadratic form q_A is easily seen to be the tensor product of $q_{\mathrm{M}_2(K)}$ and q_D. Since $\mathbb{C} \subset K$, the form

$$q_{\mathrm{M}_2(K)} \equiv \langle 1, 1, 1, -1 \rangle$$

is split over K and hence, so is $q_A = q_{\mathrm{M}_2(K)} \otimes q_D$. In particular, q_A descends to $\mathbb{C}$. □

Remark 7. A more interesting example, where the equality $\mathrm{ed}(F_2) = \mathrm{ed}(A)$ fails, is given by a generic division algebra A/K of degree 4. In this case $\mathrm{ed}(F_2) = 4$ (see [4, Theorem 1.5]), while an unpublished theorem of Rost [7] asserts that $\mathrm{ed}(A) = 5$.

Remark 8. To see where the proof of Theorem 1 breaks down for $r = 2$, note that it relies on Lemma 2(a) with $d = r - 2$ (used in the proof of Lemma 3) and Lemma 2(b) with $d = r - 1$ (used in the proof of Proposition 4). Clearly Lemma 2(a) fails for $d = 0$ and Lemma 2(b) fails for $d = 1$.

I will conclude this paper with an open question.

Question 9. Does Theorem 1 remain valid if the central simple algebra A/K is replaced by a finite field extension L/K (and F_r is the r-linear trace form in L/K)? The proof of Theorem 1 presented in this paper does not carry over to this context, because it relies on Lemma 2(b), which clearly fails in the commutative setting.

Acknowledgements

I am grateful to V. Chernousov and R. Parimala for stimulating discussions and to J.-P. Serre and the referee for helpful comments on earlier versions of this paper.

References

[1] G. Berhuy, G. Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*, Doc. Math. 8 (2003), 279–330.

[2] A. Freedman, R. N. Gupta, R. M. Guralnick, *Shirshov's theorem and representations of semigroups*, Olga Taussky-Todd: in memoriam, Pacific J. Math. 1997, Special Issue, 159–176.

[3] T. Y. Lam, The algebraic theory of quadratic forms. Mathematics Lecture Note Series, W. A. Benjamin, Inc., 1973.

[4] M. Lorenz , Z. Reichstein, L.H. Rowen, D. J. Saltman, *Fields of definition for division algebras*, Journal of the London Mathematical Society, **68**, 03 (2003), 651–670.

[5] A. Merkurjev, *Essential dimension*, preprint (2000).

[6] R. S. Pierce, Associative algebras, Graduate Texts in Mathematics, 88, Springer-Verlag, 1982.

[7] M. Rost, *Computation of some essential dimensions*, preprint, 2000. Available at http://www.mathematik.uni-bielefeld.de/˜rost/ed.html

[8] M. Rost, J.-P. Serre, J.-P. Tignol, *La forme trace d'une algèbre simple centrale de degré 4*, C. R. Acad. Sci. Paris, Ser. I 342 (2006), 83–87.

[9] J.-P. Tignol, *La forme seconde trace d'une algèbre simple centrale de degré 4 de caractéristique* 2, C. R. Acad. Sci. Paris, Ser. I 342 (2006), 89–92.

Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada

E-mail address: reichst@math.ubc.ca