Results Math (2020) 75:153

1422-6383/20/040001-9
published online September 25, 2020
https://doi.org/10.1007/s00025-020-01281-6

Results in Mathematics

Counting Finite-Dimensional Algebras Over Finite Field

Nikolaas D. Verhulst

Abstract. In this paper, we describe an elementary method for counting the number of non-isomorphic algebras of a fixed, finite dimension over a given finite field. We show how this method works in the case of 2-dimensional algebras over the field $\mathbb{F}_2$.

Introduction

Classifying finite-dimensional algebras over a given field is usually a very hard problem. The first general result was a classification by Hendersson and Searle of 2-dimensional algebras over the base field $\mathbb{R}$, which appeared in 1992 ([1]). This was generalised in 2000 by Petersson ([3]), who managed to give a full classification of 2-dimensional algebras over an arbitrary base field. The methods employed in these papers are quite involved and rely on a large amount of previous work by many illustrious authors.

Our aim in this paper is to give perhaps not a classification but at least a way to compute the exact number of non-isomorphic n-dimensional algebras over a fixed finite field by elementary means. Indeed, nothing more complicated than linear algebra and some very basic results about group actions will be needed: we describe isomorphism classes of n-dimensional K-algebras as orbits of a certain $\mathrm{GL}_n(K)$-action on $\mathrm{Mat}_n(K)^n$ and use a basic result about group actions to count these orbits. In the first three sections, we give a proof based on concrete calculations, while Sect. 4 is dedicated to a more abstract alternative which avoids all computations. In Sect. 5, we work out the concrete example $n = 2$, $K = \mathbb{F}_2$.

1. Notation and Basics

Fix a field K. In this article, an *algebra* is understood to be a K-vector space A equipped with a multiplication, i.e. a bilinear map $A \times A \to A$. If a, b are in A, we will write ab for the image of (a, b) under this map. We do not assume algebras to have a unit or to be associative. By the *dimension* of an algebra we mean its dimension as a K-vector space. Two algebras A and A' will be called *isomorphic* if there exists a K-linear bijection $f : A \to A'$ with $f(ab) = f(a)f(b)$ for all a, b in A. The isomorphism class of an algebra A will be denoted by $[A]$. For $n \in \mathbb{N}$, we define $\mathrm{Alg}_n(K)$ to be the set of isomorphism classes of n-dimensional algebras.

Given a vector $\mathcal{M} = (M_i)_{i=1,\ldots,n}$ of n $(n \times n)$-matrices over K, we can define an algebra $\mathrm{alg}(\mathcal{M})$ which is K^n as a K-vector space and for which multiplication is defined to be the unique bilinear map $K^n \times K^n \to K^n$ with

$$e_i e_j = \sum_k (M_i)_{kj} e_k$$

where the e_i are the canonical basis vectors of K^n. Intuitively, this means that multiplying an element $a \in \mathrm{alg}(\mathcal{M})$ on the left with e_i is multiplying the coordinate vector of a (with respect to the canonical basis) with M_i and interpreting the result again as a coordinate vector (with respect to the canonical basis). This allows us to define the map

$$[\mathrm{alg}] : \mathrm{Mat}_n(K)^n \to \mathrm{Alg}_n(K), \mathcal{M} \mapsto [\mathrm{alg}(\mathcal{M})]$$

which will play an important role in this paper.

Lemma 1.1. *The map* [alg] *defined above is surjective.*

Proof. Let A be an n-dimensional algebra with basis $a_1, \ldots, a_n$. There are $\alpha_{ij,k}$ in K such that $a_i a_j = \sum_k \alpha_{ik,j} a_k$ for all $1 \leq i, j \leq n$. Define the matrix M_i by putting $(M_i)_{jk} = \alpha_{ij,k}$ and set $\mathcal{M} = (M_i)_{i=1,\ldots,n} \in \mathrm{Mat}_n(K)^n$. There is a unique linear map $\mathrm{alg}(\mathcal{M}) \to A, e_i \mapsto a_i$ which is clearly bijective and which, by construction, preserves multiplication. Hence $[A] = [\mathrm{alg}(\mathcal{M})]$. □

On the other hand, [alg] is clearly not injective, since for any $\mathcal{M} = (M_i)_{i=1,\ldots,n}$ and $\alpha \in K^*$, for example, we have $[\mathrm{alg}(\mathcal{M})] = [\mathrm{alg}(\alpha\mathcal{M})]$.

2. A Group Action on $\mathrm{Mat}_n(K)^n$

Recall that for a given set X and a group G with neutral element e, a (right) *G-action* on X is a map $\phi : X \times G \to X$ such that

(1) $\phi(x, e) = x$ for any $x \in X$,
(2) $\phi(x, gg') = \phi(\phi(x, g), g')$ for all $g, g' \in G$, $x \in X$.

If ϕ is a G-action on X, then the *ϕ-orbit* of an element $x \in X$ is the set $G(x) = \{\phi(x, g) \mid g \in G\}$. The set of ϕ-orbits is denoted by X/G. The *fixpoints* of a $g \in G$ are the elements of $X^g = \{x \in X \mid \phi(x, g) = x\}$.

Lemma 2.1. *The map*

$$\phi : \mathrm{Mat}_n(K)^n \times \mathrm{GL}_n(K) \to \mathrm{Mat}_n(K)^n, \left(\begin{bmatrix} M_1 \\ \vdots \\ M_n \end{bmatrix}, G \right) \mapsto \begin{bmatrix} G^{-1} \sum_i G_{i1} M_i G \\ \vdots \\ G^{-1} \sum_i G_{in} M_i G \end{bmatrix}$$

is a $\mathrm{GL}_n(K)$*-action on* $\mathrm{Mat}_n(K)^n$*.*

Proof. It is clear that $\phi(\mathcal{M}, \mathbb{1}_n) = \mathcal{M}$ for all $\mathcal{M}$ in $\mathrm{Mat}_n(K)^n$. Take $\mathcal{M} = (M_i)_{i=1,\dots,n}$ in $\mathrm{Mat}_n(K)^n$ and G, G' in $\mathrm{GL}_n(K)$. We have to show $\phi(\mathcal{M}, GG') = \phi(\phi(\mathcal{M}, G), G')$. The term on the right is

$$\begin{aligned} \phi \left(\begin{bmatrix} G^{-1} \sum_i G_{i1} M_i G \\ \vdots \\ G^{-1} \sum_i G_{in} M_i G \end{bmatrix}, G' \right) &= \begin{bmatrix} G'^{-1} \sum_j G'_{j1} \left(G^{-1} \sum_i G_{ij} M_i G \right) G' \\ \vdots \\ G'^{-1} \sum_j G'_{jn} \left(G^{-1} \sum_i G_{ij} M_i G \right) G' \end{bmatrix} \\ &= \begin{bmatrix} (GG')^{-1} \sum_i (GG')_{i1} M_i GG' \\ \vdots \\ (GG')^{-1} \sum_i (GG')_{in} M_i GG' \end{bmatrix} \end{aligned}$$

which is the term on the left. □

Lemma 2.2. *Two elements* $\mathcal{M}, \mathcal{M}'$ *of* $\mathrm{Mat}_n(K)^n$ *are in the same* ϕ*-orbit if and only if* $\mathrm{alg}(\mathcal{M})$ *and* $\mathrm{alg}(\mathcal{M}')$ *are isomorphic, i.e. if and only if* $[\mathrm{alg}(\mathcal{M})] = [\mathrm{alg}(\mathcal{M}')]$.

Proof. Assume $\mathrm{alg}(\mathcal{M})$ and $\mathrm{alg}(\mathcal{M}')$ to be isomorphic for some $\mathcal{M} = (M_i)_{i=1,\dots,n}$ and $\mathcal{M}' = (M'_i)_{i=1,\dots,n}$ in $\mathrm{Mat}_n(K)^n$. Take an isomorphism $f : \mathrm{alg}(\mathcal{M}) \to \mathrm{alg}(\mathcal{M}')$. Since $\mathrm{alg}(\mathcal{M})$ and $\mathrm{alg}(\mathcal{M}')$, considered as K-vector spaces, are just K^n, there must be a $G \in \mathrm{GL}_n(K)$ such that $f(x)$ is just Gx for all $x \in \mathrm{alg}(\mathcal{M}')$. As f is an isomorphism, we find

$$G \sum_i x_i M_i y = f(xy) = f(x) f(y) = Gx \cdot Gy = \sum_i \left(\sum_j G_{ij} x_j M'_i \right) Gy$$

for arbitrary $x, y \in \mathrm{alg}(\mathcal{M})$. In particular, if $x = e_l$, we find $GM_l y = \sum_i G_{il} M'_i G y$ for all y, so $M_l = G^{-1} \sum_i G_{il} M'_i G$ showing $\phi(\mathcal{M}', G) = \mathcal{M}$.

Suppose now that, for given $\mathcal{M}$ and $\mathcal{M}'$ in $\mathrm{Mat}_n(K)^n$, there is some $G \in \mathrm{GL}_n(K)$ with $\phi(\mathcal{M}', G) = \mathcal{M}$. G induces a function $f : K^n \to K^n, x \mapsto Gx$ which is bijective as G is invertible. To prove that f is an isomorphism between $\mathrm{alg}(\mathcal{M})$ and $\mathrm{alg}(\mathcal{M}')$, it suffices to show $f(e_i e_j) = f(e_i) f(e_j)$ for all i, j since f is linear. We find

$$\begin{aligned} f(e_i) f(e_j) = (Ge_i)(Ge_j) = \left(\sum_k G_{ki} M'_k \right) (Ge_j) &= \left(\sum_k G_{ki} M'_k G \right) e_j \\ &= GG^{-1} \left(\sum_k G_{ki} M'_k G \right) e_j = GM_i e_j = f(e_i e_j), \end{aligned}$$

the penultimate equality following from $\phi(\mathcal{M}', G) = \mathcal{M}$. □

3. Counting Orbits

From now on, we assume K to be a finite field with q elements. As a consequence of Lemma 2.2, we find that alg induces a well-defined, injective map

$$\overline{\text{alg}} : \text{Mat}_n(K)^n/\text{GL}_n(K) \to \text{Alg}_n(K), (\text{GL}_n(K))(\mathcal{M}) \mapsto [\text{alg}(\mathcal{M})]$$

which is also surjective by Lemma 1.1. The number of isomorphism classes of n-dimensional K-algebras therefore equals the number of ϕ-orbits of $\text{Mat}_n(K)^n$. The following well-known result from the theory of group actions will help us count the latter:

Proposition 3.1 (Burnside's lemma). *Suppose ϕ is an action of a finite group G on a finite set X. Then*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Proof. Cf. e.g. [5], p.58. □

To use this lemma, we need to know the number of fixpoints of a given invertible matrix M. For that, we need the following definition:

Definition 3.2. For a matrix $M \in \text{Mat}_{k\times l}(K)$, the *vectorisation* of M is the vector $\text{vec}(M) \in K^{kl}$ obtained by stacking the columns of M, the first column being on top. For an element $\mathcal{M} = (M_i)_{i=1,\dots,n} \in \text{Mat}_n(K)^n$, we write $\text{Vec}(\mathcal{M})$ for the single vector consisting of the vectorisations of all the M_i. For more on the vectorisation operation, we refer to [2].

Lemma 3.3. *For an invertible matrix M, we have*

$$\left|(\text{Mat}_n(K)^n)^M\right| = q^{\dim \text{Eig}_1(M^T \otimes M^T \otimes M^{-1})}$$

where $\text{Eig}_1(A)$ denotes the eigenspace of the matrix A with eigenvalue 1.

Proof. Suppose $\mathcal{N} = (N_i)_{i=1,\dots,n}$ is a fixpoint of M, i.e.

$$N_l = M^{-1} \sum_i M_{il} N_i M \quad \text{for all } l. \tag{†}$$

It is known (see e.g. [2]) that, for arbitrary A, B, C in $\text{Mat}_n(K)$, we have $(B^T \otimes A)\text{vec}(C) = \text{vec}(ACB)$. From this, we conclude:

$$\text{Vec}\left((M^{-1}N_iM)_{i=1,\dots,n}\right) = (\mathbb{1}_n \otimes M^T \otimes M^{-1})\text{Vec}(\mathcal{N}).$$

We have furthermore that $\text{Vec}((\sum_i M_{il}O_i)_{l=1,\dots,n}) = (M^T \otimes \mathbb{1}_n \otimes \mathbb{1}_n)\text{Vec}(\mathcal{O})$ for any $\mathcal{O} = (O_i)_{i=1,\dots,n} \in \text{Mat}_n(K)^n$. Consequently, (†) is equivalent to

$$\text{Vec}(\mathcal{N}) = (M^T \otimes \mathbb{1}_n \otimes \mathbb{1}_n)(\mathbb{1}_n \otimes M^T \otimes M^{-1})\text{Vec}(\mathcal{N})$$

$$= (M^T \otimes M^T \otimes M^{-1})\mathrm{Vec}(\mathcal{N}),$$

so $\mathcal{N}$ is a fixpoint of M if and only if $\mathrm{Vec}(\mathcal{N})$ is an eigenvector of $M^T \otimes M^T \otimes M^{-1}$ with eigenvalue 1. □

Theorem 3.4. *The number of non-isomorphic n-dimensional K-algebras is*

$$|\mathrm{Alg}_n(K)| = \frac{1}{|\mathrm{GL}_n(K)|} \sum_{M \in \mathrm{GL}_n(K)} q^{\dim \mathrm{Eig}_1(M^T \otimes M^T \otimes M^{-1})}.$$

Proof. By Lemma 2.2, the number of non-isomorphic n-dimensional k-algebras is the number of ϕ-orbits. By 3.1 and 3.3, this is equal to the given formula. □

4. A Computation-Free Road to Rome

In this section, we will outline a version of the proof which avoids all concrete computations. Grateful use has been made of an anonymous referee's report.

Suppose A is a K-algebra. We can express a choice of basis for A as a K-vector space isomorphism $b : K^n \to A$. An algebra with basis can then be seen as a pair (A, b). We call two such pairs (A, b), (A', b') *isomorphic* if there is a K-algebra isomorphism $f : A \to A'$ with $f \circ b = b'$. We denote the isomorphism class of (A, b) as $\widetilde{(A, b)}$ and the set of isomorphism classes of n-dimensional K-algebras with basis as $\mathrm{AlgBas}_n(K)$.

For a K-algebra A, we write $\mu_A : A \otimes A \to A, x \otimes y \mapsto xy$. Similarly, if M is an element of $\mathrm{Hom}(K^n \otimes K^n, K^n)$, we write $\mathrm{alg}(M)$ for the algebra which is K^n as a K-vector space and with multiplication given by $xy = M(x \otimes y)$ for all x, y in K^n. We can identify the set $\mathrm{AlgBas}_n(K)$ with $\mathrm{Hom}(K^n \otimes K^n, K^n)$ by the following maps

$$\mathrm{AlgBas}_n(K) \to \mathrm{Hom}(K^n \otimes K^n, K^n), \quad \widetilde{(A, b)} \mapsto b^{-1} \circ \mu_A \circ (b \otimes b)$$

$$\mathrm{Hom}(K^n \otimes K^n, K^n) \to \mathrm{AlgBas}_n(K), \quad M \mapsto \widetilde{(\mathrm{alg}(M), \mathrm{Id})}$$

which can be checked to be well-defined and inverse to each other.

We can define a $\mathrm{GL}_n(K)$-action ϕ on $\mathrm{AlgBas}_n(K)$ by $\phi((A, b), g) = (A, b \circ g^{-1})$. The $\mathrm{GL}_n(K)$-orbits correspond to the fibers of the forgetful functor

$$\mathrm{AlgBas}_n(K) \to \mathrm{Alg}_n(K), (A, b) \mapsto A,$$

so we can count the number of non-isomorphic n-dimensional K-algebras by counting the $\mathrm{GL}_n(K)$-orbits of ϕ. By the above correspondence, we get a $\mathrm{GL}_n(K)$-action on $\mathrm{Hom}(K^n \otimes K^n, K^n)$ as well and we can count the orbits of that action instead. In order to apply Burnside's lemma, we need to find the $M \in \mathrm{Hom}(K^n \otimes K^n, K^n)$ fixed by a given element $g \in \mathrm{GL}_n(K)$. These are precisely those M which satisfy $g^{-1}M(g \otimes g) = M$.

Let us recall a few results from basic linear algebra. For any two finite-dimensional K-vector spaces V, W we have, if we write V^* for the dual space of V, $\mathrm{Hom}_K(V,W) \simeq V^* \otimes W$ via the isomorphism

$$\Phi : V^* \otimes W \to \mathrm{Hom}_K(V,W), \phi \otimes w \mapsto (\Phi(\phi \otimes w) : V \to W, v \mapsto \phi(v)w).$$

Similarly, a map

$$\mathrm{Hom}_K(V,W) \to \mathrm{Hom}_K(V,W), f \mapsto a \circ f \circ b$$

for some $a \in \mathrm{End}_K(W), b \in \mathrm{End}_K(V)$ corresponds to the map

$$b^* \otimes a : V^* \otimes W \to V^* \otimes W$$

where we have written b^* for the dual of b.

In particular, we can apply this with $V = K^n \otimes K^n$ and $W = K^n$. Writing vec for the isomorphism $\mathrm{Hom}_K(K^n \otimes K^n, K^n) \to (K^n \otimes K^n)^* \otimes K^n$, we find that $g^{-1}M(g \otimes g) = M$ is equivalent to

$$((g \otimes g)^T \otimes g^{-1})\mathrm{vec}(M) = \mathrm{vec}(M).$$

We conclude that vec induces an isomorphism between the subvector space of $\mathrm{Hom}_K(K^n \otimes K^n, K^n)$ consisting of elements fixed under g on the one hand and $\mathrm{Eig}_1((g \otimes g)^T \otimes g^{-1})$ on the other hand.

5. Example: the Case $n = 2$, $q = 2$

Any element of $\mathrm{GL}_2(K)$ has, counting (algebraic) multiplicities, two eigenvalues in the algebraic closure $\overline{K}$ of K. Clearly, either both or none are elements of K which makes counting invertible matrices with eigenvalues in K considerably easier. Indeed, the only possible Jordan normal forms for a 2×2 matrix are[1]

$$J_1 = \begin{bmatrix} \alpha & \\ & \beta \end{bmatrix} \quad \text{and} \quad J_2 = \begin{bmatrix} \alpha & 1 \\ & \alpha \end{bmatrix}$$

for some α, β in the algebraic closure of K. Since $M = SJS^{-1}$, $M' = S'J'S'^{-1}$ implies $M \otimes M' = (S \otimes S')(J \otimes J')(S^{-1} \otimes S'^{-1})$ and since the Jordan normal form of M is also the Jordan normal form of M^T, it follows that every $M^T \otimes M^T \otimes M^{-1}$ must be conjugate either to

$$M_{\alpha,\beta} = \begin{bmatrix} \alpha & & & & & & & \\ & \alpha & & & & & & \\ & & \alpha & & & & & \\ & & & \alpha^2\beta^{-1} & & & & \\ & & & & \alpha^{-1}\beta^2 & & & \\ & & & & & \beta & & \\ & & & & & & \beta & \\ & & & & & & & \beta \end{bmatrix}$$

[1]Here and later we only write the non-zero entries in our matrices, as is usual.

or to

$$N_\alpha = \begin{bmatrix} \alpha & -1 & 1 & -\alpha^{-1} & 1 & -\alpha^{-1} & \alpha^{-1} & -\alpha^{-2} \\ & \alpha & & 1 & & 1 & & \alpha^{-1} \\ & & \alpha & -1 & & & 1 & -\alpha^{-1} \\ & & & \alpha & & & & 1 \\ & & & & \alpha & -1 & 1 & -\alpha^{-1} \\ & & & & & \alpha & & 1 \\ & & & & & & \alpha & -1 \\ & & & & & & & \alpha \end{bmatrix}.$$

for some $\alpha, \beta \in \overline{K}$. Note that $\dim \mathrm{Eig}_1(N_1) = 3$ unless the characteristic of K is 2, in which case $\dim \mathrm{Eig}_1(N_1) = 4$. If $\alpha \neq 1$, we obviously have $\dim \mathrm{Eig}_1(N_\alpha) = 0$. For $M_{\alpha,\beta}$, the dimension of the eigenspace associated to 1 depends heavily on α and β, ranging from 8 if $\alpha = \beta = 1$ to 0 if $1 \notin \{\alpha, \beta, \alpha^2\beta^{-1}, \alpha^{-1}\beta^2\}$.

We will do the computations explicitly for the concrete example of $K = \mathbb{F}_2$. There are 6 invertible matrices, namely

$$\mathbb{1}_2, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

The identity obviously yields a contribution of 2^8. The next three are conjugate to J_2 with $\alpha = 1$, therefore yielding a contribution of 2^4 each. The last two have no eigenvalues over K. Their eigenvalues are the roots t_1, t_2 of the polynomial x^2+x+1. As these roots satisfy $t_1^2 = t_2, t_2^2 = t_1$, both matrices give a contribution of 2^2. This gives a total of $2^8 + 3 \cdot 2^4 + 2 \cdot 2^2 = 312$ which divided by the total number of invertible matrices gives $312/6 = 52$. This number fits the formulae which were obtained, using completely different methods, by Petersson and Scherer in [4].

6. Outlook

Theorem 3.4 suggests the following question: how many invertible $n \times n$-matrices M have

$$\dim \mathrm{Eig}_1(M^T \otimes M^T \otimes M^{-1}) = k$$

for a given $k \in \mathbb{N}$? If q and n are fixed, this is a finite problem and can therefore be calculated, but this is rather tedious and time-consuming. Having a closed formula in q and n would be nice.

On the algebraic side, it would be interesting to see whether the method described in this paper can also be used to count certain subclasses of algebras, like alternating algebras, associative algebras, or division algebras.

Acknowledgements

With the exception of Sect. 4, almost all of this work was carried out during the author's stay at the TU Dresden. The author is grateful to an anonymous referee for a very detailed and helpful report which was the basis for Sect. 4.

References

[1] Althoen, S.C., Hansen, K.D.: Two-dimensional real algebras with zero divisors. Acta Sci. Math (Szeged) **56**, 23–42 (1992)

[2] Henderson, H.V., Searle, S.R.: The vec-permutation matrix, the vec operator and Kronecker products: a review. Linear Multilinear Algebra **9**(4), 271–288 (1981)

[3] Petersson, H.P.: The classification of two-dimensional nonassociative algebras. Results Math. **37**(1–2), 120–154 (2000)

[4] Petersson, H.P., Scherer, M.: The number of nonisomorphic two-dimensional algebras over a finite field. Results Math. **42**(1–2), 137–152 (2004)

[5] Rotman, J.J.: An Introduction to the Theory of Groups. Grad. Texts in Math., vol. 148. Springer, Berlin (2012). ISBN: 9781461241768

Nikolaas D. Verhulst
Delft Institute of Applied Mathematics
TU Delft
Mourik Broekmanweg 6
2628 XE Delft
The Netherlands

and

Technische Universität Dresden
Institut für Algebra
01062 Dresden
Germany
e-mail: n.d.verhulst@tudelft.nl

Received: November 27, 2019.
Accepted: September 11, 2020.