A basis for the graded identities of the matrix algebra of order two over a finite field of characteristic $p \neq 2$

Plamen Koshlukov[*]and Sérgio S. Azevedo[†]
IMECC, UNICAMP, Cx. P. 6065
13083-970 Campinas, SP, Brazil
e-mail addresses
plamen@ime.unicamp.br and sergios@ime.unicamp.br

Abstract

Let K be a finite field of characteristic $p > 2$, and let $M_2(K)$ be the matrix algebra of order two over K. We describe up to a graded isomorphism the 2-gradings of $M_2(K)$. It turns out there are only two nonisomorphic nontrivial such gradings. Furthermore we exhibit bases of the graded polynomial identities for each one of these two gradings. One can distinguish these two gradings by means of the graded polynomial identities they satisfy.

Introduction

The description of the polynomial identities satisfied by an algebra is an important task and it may yield a lot of information about the algebra. One distinguishes three quite different cases depending on the base field K. The first is when K is of characteristic 0; the second when K is infinite, and the third when K is finite. The methods that work in each one of these cases are rather different. In the case char $K = 0$ one may consider multilinear polynomial identities since they determine all identities of a given algebra. In this case one applies the theory of representations of the symmetric group and other refinements, see, for example [3, 5, 12]. When

[*]Partially supported by CNPq
[†]Supported by PhD Grant # 98/16449-5, FAPESP

$|K| = \infty$ it is sufficient to consider multihomogeneous identities. The methods one uses in this case are based on the invariant theory [1]. Finally if K is finite field then neither of the above identities are sufficient. And in general, neither of the methods described can function properly. Instead one uses the structure theory of rings [8, 9] and combinatorics based on the properties of the finite fields.

Let $M_2(K)$ be the matrix algebra of order two over the field K. Its identities have been extensively studied, see for example [12] for the case $\operatorname{char} K = 0$, [6] for $|K| = \infty$, and [10] for finite fields. The graded polynomial identities play an important role in the study of PI algebras, see for example [5]. We fix the non-trivial grading Ω on $M_2(K)$

$$\Omega_0 = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in K \right\}, \qquad \Omega_1 = \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \mid b, c \in K \right\}.$$

When the characteristic of the field K equals zero, $\operatorname{char} K = 0$, O. M. Di Vincenzo [2] showed that the graded identities of Ω follow from two identities namely from $y_1 y_2 = y_2 y_1$ and $z_1 z_2 z_3 = z_3 z_2 z_1$ for y_i being even and z_i odd variables. When K is infinite, the authors [7] proved that the result of O. M. Di Vincenzo holds. In this paper, we prove that if K is a finite field with q elements and $\operatorname{char} K = p \neq 2$ that is $K = GF(q)$ and $q = p^n$, then the graded identities of Ω are consequences of the identities $y_1^q = y_1$ and

$$(y_1 + z_1 - (y_1 + z_1)^q)(y_2 + z_2 - (y_2 + z_2)^{q^2})(1 - [y_1 + z_1, y_2 + z_2]^{q-1}) = 0$$

where $[x_1, x_2] = x_1 x_2 - x_2 x_1$ is the commutator of z_1 and z_2.

Let $0 \neq \alpha \in K$, and define a nontrivial grading Ω^α on $M_2(K)$:

$$\Omega_0^\alpha = \left\{ \begin{pmatrix} a & d \\ \alpha d & a \end{pmatrix} \mid a, d \in K \right\}, \qquad \Omega_1^\alpha = \left\{ \begin{pmatrix} b & c \\ -\alpha c & -b \end{pmatrix} \mid b, c \in K \right\}.$$

We describe, up to a graded isomorphism, the non-trivial gradings for $M_2(K)$. Namely, one grading is Ω^α where α is a perfect square in K. This grading is isomorphic to Ω. The other is Ω^α where α is not a perfect square in K. In the latter case the basis for the graded identities consists of the following three identities $y_1^{q^2} = y_1$, $z_1^{2q-1} = z_1$ and

$$(y_1 + z_1 - (y_1 + z_1)^q)(y_2 + z_2 - (y_2 + z_2)^{q^2})(1 - [y_1 + z_1, y_2 + z_2]^{q-1}) = 0.$$

Our method is similar to the one used in [10] to prove that the ordinary polynomial identities of $M_2(K)$, where K is finite field with q elements, follow from the identities

$$\begin{aligned} (x_1 - x_1^q)(x_2 - x_2^{q^2})(1 - [x_1, x_2]^{q-1}) &= 0, \\ (x_1 - x_1^q) \cdot (x_2 - x_2^q) - ((x_1 - x_1^q) \cdot (x_2 - x_2^q))^q &= 0. \end{aligned}$$

Here we denote $x_1 \cdot x_2 = x_1x_2 + x_2x_1$. We also use ideas and methods from [8] and [9].

1 Gradings for the matrix algebra of order two

A graded algebra A is an associative algebra that can be expressed as the direct sum of two subspaces A_0 and A_1 such that $A_iA_j \subseteq A_{i+j}$ where the sum $i+j$ is taken modulo 2. One defines naturally graded subalgebras, ideals, homomorphisms, isomorphisms etc.

Let $X = \{x_1, x_2, \ldots\}$, $Y = \{y_1, y_2, \ldots\}$ and $Z = \{z_1, z_2, \ldots\}$ be three sets of symbols such that $Y \cup Z = X$ and $Y \cap Z = \emptyset$. Denote by $K\langle X\rangle$ the free associative algebra that is freely generated over K by the set X. Let f be a monomial in the algebra $K\langle X\rangle$. We say that f is even if it contains an even number of entries from Z, i.e., if its degree with respect to the symbols in Z is even. Otherwise f is called odd. The span of all even (odd) monomials is denoted by $K\langle X\rangle_0$ (respectively $K\langle X\rangle_1$). Therefore $K\langle X\rangle = K\langle X\rangle_0 \oplus K\langle X\rangle_1$ becomes a graded algebra. If $A = A_0 \oplus A_1$ is a graded algebra and $f(y_1, \ldots, y_m, z_1, \ldots, z_n) \in K\langle X\rangle$ then f is a graded identity for A if $f(a_1, \ldots, a_m, b_1, \ldots, b_n) = 0$ for all $a_1, \ldots, a_m \in A_0$ and $b_1, \ldots, b_n \in A_1$. A graded ideal $I = I_0 \oplus I_1$ of A is called T_2-ideal of A if it is closed under all graded endomorphisms of A. In other words if $\phi\colon A \to A$ is a graded homomorphism then $\phi(I) \subseteq I$. The set $T_2(A)$ of all graded identities of A is a T_2-ideal of $K\langle X\rangle$. If $g \in K\langle X\rangle$ we say that g is T_2-consequence of f (or that g follows from f as graded identity) if g belongs to the T_2-ideal generated in $K\langle X\rangle$ by f.

Let K be a finite field with q elements and characteristic $p \neq 2$, $K = GF(q)$ and $q = p^n$. For convenience we shall identify the field K with the centre of the matrix algebra $M_2(K)$

Lemma 1 *Let $A = A_0 \oplus A_1$ be a grading for $M_2(K)$. Then:*

(i) There exists an invertible element u_A in $M_2(K)$ such that $u_A^2 \neq 0 \in K$ and $A_0 = \{a \in A \mid au_A = u_Aa\}$ and $A_1 = \{a \in A \mid au_A = -u_Aa\}$;

(ii) $u_A^q = u_A$ or $u_A^q = -u_A$;

(iii) If $B = B_0 \oplus B_1$ is a grading of $M_2(K)$ and there exists an invertible matrix P in $M_2(K)$ such that $P^{-1}u_AP = u_B$ then the map $\phi\colon A \to B$ defined by $\phi(x) = P^{-1}xP$ is a graded isomorphism.

Proof: As $M_2(K)$ is a central simple (ungraded) algebra and A is a central simple graded algebra, by Lemma 6 of [13], we know that there exists $u_A \in A$ such that $0 \neq u_A^2 \in K$ and $A_0 = \{a \in A \mid au_A = u_Aa\}$, $A_1 = \{a \in A \mid au_A = -u_Aa\}$.

Furthermore, $u_A^q = u_A$ or $u_A^q = -u_A$; for $u_A^q = (u_A^2)^{(q-1)/2}u_A = (\alpha I)^{(q-1)/2}u_A = \pm u_A$ where I stands for the identity matrix.

The third assertion follows easily from the fact that $B_0 = \{b \in B \mid b\phi(u_A) = \phi(u_A)b\}$, and $B_1 = \{b \in B \mid b\phi(u_A) = -\phi(u_A)b\}$. Then observe that if $a \in A_0$ then $\phi(a)\phi(u_A) = \phi(au_A) = \phi(u_Aa) = \phi(u_A)\phi(a)$ hence $\phi(a) \in B_0$. Similarly, if $a \in A_1$ then $\phi(a)\phi(u_A) = \phi(au_A) = -\phi(u_Aa) = -\phi(u_A)\phi(a)$, therefore $\phi(a) \in B_1$. ■

For example, for the gradings Ω and Ω^α one can choose the elements

$$u_\Omega = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } u_{\Omega^\alpha} = \begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix},$$

respectively. For the trivial grading T, the element u_T can be chosen as the identity matrix.

Now we are ready to show that there exist only two non-trivial gradings for $M_2(K)$. More precisely, when $A = A_0 \oplus A_1$ is a grading for $M_2(K)$, if $u_A^q = u_A$, then A is isomorphic to Ω^α for any perfect square $0 \neq \alpha \in K$, else A is isomorphic to Ω^α for any not square $\alpha \in K$. Besides, when $\alpha \neq 0$ is a square in K then the gradings Ω and Ω^α are isomorphic. We shall prove these facts in the next lemmas.

Lemma 2 *Every non-trivial grading $A = A_0 \oplus A_1$ of $M_2(K)$ such that $u_A^q = u_A$ is isomorphic to Ω.*

Proof: If $u_A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $u_A^2 = \begin{pmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{pmatrix}$. Therefore, since $u_A^2 \in K$, we have $b = c = 0$ or $a = -d$. In the first case $A_0 = M_2(K)$ and $A_1 = 0$, which is a contradiction. So $a = -d$. The characteristic polynomial of u_A is $f(x) = x^2 - (a^2+bc)$ whose roots are $\pm\lambda$ where $\lambda = \sqrt{a^2+bc}$. But $u_A^2 \neq 0$ implies $a^2 + bc \neq 0$. Hence there exists an invertible matrix $P \in M_2(GF(q^2))$ such that $P^{-1}u_AP = \begin{pmatrix} \lambda & 0 \\ 0 & -\lambda \end{pmatrix}$. Thus

$$\begin{pmatrix} \lambda^q & 0 \\ 0 & (-\lambda)^q \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & -\lambda \end{pmatrix}^q = (P^{-1}u_AP)^q = P^{-1}u_A^qP = P^{-1}u_AP = \begin{pmatrix} \lambda & 0 \\ 0 & -\lambda \end{pmatrix}.$$

Therefore $\lambda \in GF(q)$, $P \in M_2(K)$ and the map ϕ: $A \to \Omega$ defined by $\phi(x) = P^{-1}xP$ is a graded isomorphism. ■

Remark 3 *If $\alpha \neq 0$ is a square in K then $u_{\Omega^\alpha}^q = u_{\Omega^\alpha}$. For instance when $\alpha = 1$ we have the grading Ω^1 where $u_{\Omega^1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Its eigenvalues are -1 and 1. Therefore there exists an invertible matrix $P \in M_2(GF(q))$ such that*

$$P^{-1}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}P = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Hence

$$P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad P^{-1} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix}.$$

The graded isomorphism $\phi\colon \Omega^1 \to \Omega$ such that $\phi(x) = P^{-1}xP$ is the following:

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \frac{1}{2}\begin{pmatrix} a+b+c+d & a-b+c-d \\ a+b-c-d & a-b-c+d \end{pmatrix}.$$

Corollary 4 *Every grading of $M_2(K)$ satisfying the identity $y_1^q = y_1$ is isomorphic to Ω.*

Lemma 5 *Every non-trivial grading $A = A_0 \oplus A_1$ of $M_2(K)$ such that $u_A^q = -u_A$ is isomorphic to Ω^α, for any $\alpha \in K$ that is not perfect square.*

Proof: If $u_A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $u_A^2 = \begin{pmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{pmatrix}$. Therefore, $b = c = 0$ or $a = -d$. If $b = c = 0$ we obtain the trivial grading, so $a = -d$. The characteristic polynomial of u_A is $f(x) = x^2 - (a^2+bc)$ whose roots are $\pm\lambda$ where $\lambda = \sqrt{a^2+bc}$. Since $u \neq 0$ we get that $a^2+bc \neq 0$. Furthermore $\lambda \notin K$, for $u_A^q \neq u_A$; i.e. a^2+bc is not a square in K. As α and a^2+bc are not squares in K then $\alpha(a^2+bc)$ is a square in K. Choose $\beta \in K$ such that $\beta^2 = \alpha(a^2+bc)$, and consider the matrix $u'_A = \frac{\alpha}{\beta}\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$. Its characteristic polynomial is $f(x) = x^2 - \alpha$ whose roots are $\sqrt{\alpha}$ and $-\sqrt{\alpha}$, and there exists an invertible $P \in M_2(K(\sqrt{\alpha}))$ such that

$$P^{-1}u'_AP = \begin{pmatrix} \sqrt{\alpha} & 0 \\ 0 & -\sqrt{\alpha} \end{pmatrix}.$$

The characteristic polynomial of u_{Ω^α} is $f(x) = x^2 - \alpha$ as well, and for some invertible $Q \in M_2(K(\sqrt{\alpha}))$ we have

$$Q^{-1}u_{\Omega^\alpha}Q = \begin{pmatrix} \sqrt{\alpha} & 0 \\ 0 & -\sqrt{\alpha} \end{pmatrix}.$$

Thus $(PQ^{-1})^{-1}u'_APQ^{-1} = u_{\Omega^\alpha}$ and the map $\phi\colon A \to \Omega^\alpha$, $\phi(x) = P^{-1}xP$, is a graded isomorphism. ■

Remark 6 *If α is not a square in K then $u_{\Omega^\alpha}^q = -u_{\Omega^\alpha}$. Thus for $K = \mathbb{Z}_3$ and $\alpha = -1$, we obtain the grading*

$$\Omega_0^{-1} = \left\{\begin{pmatrix} a & d \\ -d & a \end{pmatrix} \mid a, d \in K\right\}, \quad \Omega_1^{-1} = \left\{\begin{pmatrix} b & c \\ c & -b \end{pmatrix} \mid b, c \in K\right\}$$

where $u_{\Omega^{-1}} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and $u_{\Omega^{-1}}^3 = -u_{\Omega^{-1}}$, because -1 is not a square in K.

2 The graded identities of Ω

The next theorem supplies a basis for the graded identities of Ω.

Theorem 7 *The graded identities for Ω follow from the identities*

$$\begin{aligned} f_1(y_1) &= y_1^q - y_1, \\ f_2(y_1, y_2, z_1, z_2) &= (X_1 - X_1^q)(X_2 - X_2^{q^2})(1 - [X_1, X_2]^{q-1}), \end{aligned}$$

where $X_1 = y_1 + z_1$, $X_2 = y_2 + z_2$.

The proof of this theorem is modelled on the paper of Maltsev and Kuzmin [10] for ungraded identities.

A variety of graded algebras $\mathfrak{V}$ is the class of all graded algebras satisfying a given collection of graded polynomial identities. Clearly $\mathfrak{V}$ is closed under the operations of taking graded subalgebras, graded homomorphic images, and direct products. The variety $\mathfrak{V}$ is generated by a class $\mathfrak{A}$ of graded algebras, if every graded algebra in $\mathfrak{V}$ can be obtained from algebras in $\mathfrak{A}$ by a finite number of applications of these operations. We write $\mathfrak{V} = Var\mathfrak{A}$ and if $\mathfrak{A}$ contains only one graded algebra A we use the notation $\mathfrak{V} = VarA$.

Lemma 8 *If A is a finite graded K-algebra, then there exists a class $\mathfrak{A}$ of subdirectly irreducible finite graded K-algebras such that $VarA = Var\mathfrak{A}$.*

Proof: For $0 \neq a \in A$, let I_a be a graded ideal of A maximal with respect to the exclusion of a. (According to Zorn's Lemma such I_a does exist.) The projections $\pi_a \colon A \to A/I_a$ are graded epimorphisms and $\cap_{0 \neq a \in A} \ker \pi_a = \cap_{a \in A} I_a = 0$. Hence A is a subdirect product of the algebras A/I_a. As $a + I_a$ is not zero and belongs to all nonzero ideal of A/I_a, then A/I_a is subdirectly irreducible. Let $\mathfrak{A}$ be the class of the graded algebras A/I_a.

Suppose that $a \in A$; then obviously $T_2(A) \subseteq T_2(A/I_a)$.

If $f(y_1, \ldots, y_m, z_1, \ldots, z_n) \in T_2(A/I_a)$, then $f(a_1, \ldots, a_m, b_1, \ldots, b_n) \in \ker \pi_a$ for all a_1, ..., $a_m \in A_0$ and b_1, ..., $b_n \in A_1$, and $a \in A$. Hence $f \in \cap_{a \in \Omega} T_2(A/I_a)$. ■

The next lemma is analogous to the result 2.2 of [8].

Lemma 9 *Every variety of graded algebras is generated by its finitely generated algebras.*

The *exponent* of a variety of graded algebras $\mathfrak{V}$ is the greatest lower bound of the set of all positive integers r such that $ra = 0$ for every element a belonging to every algebra of $\mathfrak{V}$. The *index* of $\mathfrak{V}$ is the least upper bound of the set of all nilpotent indices of its nilpotent algebras, see [8], [9] for details. The next lemma is analogous to [9], Corollary 2.9.

Lemma 10 *A variety of graded algebras having finite index and exponent is locally finite.*

Theorem 11 *A variety $\mathfrak{V}$ of graded algebras having finite index and exponent is generated by a class of subdirectly irreducible finite graded algebras.*

Proof: According to the previous two lemmas, $\mathfrak{V}$ is generated by a class of finite graded algebras. Hence $\mathfrak{V}$ is generated by a class of subdirectly irreducible finite graded algebras. ■

We denote by $\mathfrak{V}$ the variety of 2-graded algebras defined by the identities $f_1 = 0$ and $f_2 = 0$.

Lemma 12 $Var\Omega \subseteq \mathfrak{V}$.

Proof: Since $a^q = a$ for every $a \in K$ then f_1 is a graded identity of Ω. By [10], f_2 is an identity of $M_2(K)$ and hence of Ω. ■

Lemma 13 $\mathfrak{V} \subseteq Var\Omega$.

Proof: Let $N = N_0 \oplus N_1$ be a nilpotent algebra in $\mathfrak{V}$. Then N_0 is also a nilpotent algebra of $\mathfrak{V}$. The nilpotency index s of N_0 is 2; for if $s > 2$, we can take elements $a_1, \ldots, a_{s-1} \in N_0$ such that $a_1 \ldots a_{s-1} \neq 0$. By f_1, we know that

$$0 = (a_1 \ldots a_{s-1})^q - a_1 \ldots a_{s-1} = a_1 \ldots a_{s-1},$$

which is a contradiction. Thus if $a \in N_0$ then $a = a^q = 0$. Therefore $N_0 = 0$ and $N = N_1$. Moreover, as $N_1 N_1 \subseteq N_0 = 0$, we have that $N^2 = 0$.

The variety $\mathfrak{V}$ has finite index and exponent. By Theorem 11, $\mathfrak{V}$ is generated by a class of subdirectly irreducible finite graded algebras. To prove the lemma, it suffices to show that each of these algebras belongs to $Var\Omega$. We shall prove even more: each of them is isomorphically embedded in Ω. Till the end of the proof, we assume that A is a finite subdirectly irreducible algebra in $\mathfrak{V}$.

If A is nilpotent then $A_0 = 0$, $A_1 = A$, $A^2 = 0$ and $\dim_K A = 1$; for if $a_1, a_2 \in A$ were linearly independent, the subspaces spanned by a_1 and a_2 would have been ideals with intersection zero. Thus the map $\phi\colon A \to \Omega$ defined by $\phi(\alpha g) = \alpha e_{12}$ is a graded monomorphism, where g is a generator of A.

Suppose A is a simple ungraded algebra i.e., $A = M_k(GF(p^t))$ and $p^t \geq q$. If $k \geq 3$ then $f_2(a_0, b_0, a_1, b_1) = e_{13} \neq 0$ where a_0, $b_0 \in A_0$ and a_1, $b_1 \in A_1$ are such that $e_{12} = a_0 + a_1$ and $e_{23} = b_0 + b_1$.

Hence $k \leq 2$. Let $k = 2$. If a_0, $b_0 \in A_0$ and a_1, $b_1 \in A_1$ are such that $\alpha e_{11} = a_0 + a_1$ and $e_{12} = b_0 + b_1$, then $f_2(a_0, b_0, a_1, b_1) = (\alpha^q - \alpha)e_{12} = 0$. Hence $\alpha - \alpha^q = 0$, $q \geq p^t$, and $A = M_2(GF(q))$. By Corollary 4, Ω and A are isomorphic.

Now let us consider $k = 1$, i.e., $A = GF(p^t)$. If $0 \neq a \in A_1$ then

$$a^{q^2} = (a^2)^{(q+1)(q-1)/2}a = (a^2a^2)^{(q-1)/2}a = (a^2)^{q-1}a = a^{2q}a^{-2}a = a^2a^{-2}a = a.$$

If $a_0 \in A_0$ and $a_1 \in A_1$, then $(a_0 + a_1)^{q^2} = a_0^{q^2} + a_1^{q^2} = a_0 + a_1$. Therefore $\alpha^{q^2} - \alpha = 0$ for any $\alpha \in A$, whereby $q^2 \geq p^t$, $A = GF(q)$ or $A = GF(q^2)$. If $A = GF(q)$ then there exists an injective graded homomorphism from A into Ω. If $A = GF(q^2)$ then the unique possible grading is $A_0 \cong GF(q)$ and $A_1 \cong GF(q)$ and, by Lemma 5 of [13], there exists $u \in A_1$ such that $A_1 = A_0u$ and $u^2 = a \neq 0$ belongs to $GF(q)$. Hence $A = GF(q)\mathbf{1} + GF(q)u$, where $\mathbf{1}$ is the multiplicative unit of A. Thus the map $\phi\colon A \to \Omega$ defined as

$$\phi(\alpha\mathbf{1} + \beta u) = \begin{pmatrix} \alpha & \beta a \\ \beta & \alpha \end{pmatrix}$$

is an injective graded homomorphism.

Now suppose $A = B \oplus N$ as a direct sum of vector spaces where B is a semisimple ungraded subalgebra of A and N is the Jacobson radical of A. The Jacobson radical is graded [5] and, since N is nilpotent, $N^2 = 0$. If $x \in A_0 \cap N$ then f_1 implies that $x = x^q = 0$ thus $N \subseteq A_1$. Hence $A_1 = A_1 \cap B \oplus N$. If $x \in A_1 \cap B$ and $u \in N$, then ux, $xu \in A_0 \cap N$, i.e., $ux = xu = 0$. Therefore $x = 0$, for the ideal of A generated by x has zero intersection with N. Hence $A_1 = N$. As $A/N \cong B$ and $A/N \cong A_0$, we have $A_0 \cong B$. Thus A_0 is a semisimple ungraded subalgebra of A.

Let $A_0 = B_1 \oplus \ldots \oplus B_s$ be the (ungraded) decomposition of A_0 in simple algebras. The identity f_1 implies that $B_i = GF(q)$ for every i. Let e_i be the unit of the subalgebra B_i. Since A is subdirectly irreducible then $AN \neq 0$ or $NA \neq 0$. Suppose that $AN \neq 0$. Since the ideals e_iN intersect in zero, only one of them is nonzero, say e_1N. Since N decomposes into a direct sum of ideals $N = e_1N \oplus (1 - e_1)N$, we have $(1 - e_1)N = 0$ and $N = e_1N$. Similarly the ideals Ne_i have intersection zero, therefore at most one of them can be different from 0. There are three possible cases.

Case 1: $NA = 0$. Then $A_0 = B_1 = GF(q)$ and N is one-dimensional vector space over $GF(q)$. The map $\phi\colon A \to M_2(GF(q))$ defined as

$$\phi(\alpha + \beta u) = \begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix}$$

where α, $\beta \in GF(q)$ and $0 \neq u \in N$ is fixed, is an injective graded homomorphism.

Case 2: $Ne_1 \neq 0$, $N = e_1Ne_1$. Again $A_0 = B_1 = GF(q)$ and we consider N as $(GF(q), GF(q))$-bimodule. Since A is subdirectly irreducible, N cannot have nonzero subbimodules with intersection zero. Therefore there exists an automorphism σ of $GF(q)$ such that $x\alpha = \sigma(\alpha)x$ for all $x \in N$ and all $\alpha \in GF(q)$ (see [11], p. 315). Thus each subspace of N is a subbimodule and therefore N is one-dimensional vector space over $GF(q)$. The map $\phi\colon A \to M_2(GF(q))$ defined as

$$\phi(\alpha + \beta u) = \begin{pmatrix} \alpha & \beta \\ 0 & \sigma(\alpha) \end{pmatrix},$$

where α, $\beta \in GF(q)$ and $0 \neq u \in N$, is an injective graded homomorphism.

Case 3: $Ne_2 \neq 0$, $N = e_1Ne_2$. In this case $A_0 = B_1 \oplus B_2 = GF(q) \oplus GF(q)$, $NB_1 = B_2N = 0$ and N is a $(GF(q), GF(q))$-bimodule. Repeating the argument of case 2, we know that there exists an automorphism σ of $GF(q)$ such that $x\alpha = \sigma(\alpha)x$, for all $x \in N$ and all $\alpha \in GF(q)$, and N is one-dimensional vector space over $GF(q)$. The map $\phi\colon A \to M_2(GF(q))$ defined as

$$\phi(\alpha + \beta + \gamma u) = \begin{pmatrix} \alpha & \gamma \\ 0 & \sigma(\beta) \end{pmatrix},$$

where α, $\gamma \in B_1$, $\beta \in B_2$ and $0 \neq u \in N$ is some fixed element, is an injective graded homomorphism. ■

Remark 14 *We list some other identities for Ω:*

$$\begin{aligned}
f_3(y_1, y_2) &= y_1y_2 - y_2y_1, \\
f_4(z_1, z_2, z_3) &= z_1z_2z_3 - z_3z_2z_1, \\
f_5(y_1, z_1) &= (y_1 \cdot z_1)^q - z_1^{q-1}(y_1 \cdot z_1), \\
f_6(z_1, z_2) &= (z_1^{2(q-1)} - 1)z_1z_2(1 - [z_1, z_2]^{q-1}), \\
f_7(z_1, z_2) &= (z_1^{2(q-1)} - 1)z_2z_1(1 - [z_1, z_2]^{q-1}), \\
f_8(y_1, y_2, z_1, z_2) &= (X_1 - X_1^{q^2})(1 - [X_1, X_2]^{q-1})(X_2 - X_2^q), \\
f_9(y_1, y_2, z_1, z_2) &= (X_1 - X_1^q) \cdot (X_2 - X_2^q) - ((X_1 - X_1^q) \cdot (X_2 - X_2^q))^q
\end{aligned}$$

where $X_i = y_i + z_i$, $i = 1$, 2. The identity f_3 follows from the identity f_1 (see for example [4], p. 73). The identities f_8 and f_9 are known by [10], and we can change the identity f_2 in Theorem 7 by any one of these.

3 The graded identities of Ω^α for α not a square

The next theorem supplies a basis for the graded identities of Ω^α.

Theorem 15 *The graded identities for Ω^α follow from the identities*

$$\begin{aligned} g_1(y_1) &= y_1^{q^2} - y_1, \\ g_2(z_1) &= z_1^{2q-1} - z_1, \\ g_3(y_1, y_2, z_1, z_2) &= (X_1 - X_1^q)(X_2 - X_2^{q^2})(1 - [X_1, X_2]^{q-1}), \end{aligned}$$

where $X_1 = y_1 + z_1$, $X_2 = y_2 + z_2$.

Let $\mathfrak{V}$ be the variety of graded algebras defined by the identities $g_1 = g_2 = g_3 = 0$.

Lemma 16 *$Var\Omega^\alpha \subseteq \mathfrak{V}$.*

Proof: Let $y_1 = \begin{pmatrix} a & d \\ \alpha d & a \end{pmatrix}$ be a matrix in Ω_0^α. Its characteristic polynomial is $f(x) = x^2 - (a^2 + \alpha d^2)$ with eigenvalues $\pm\lambda$ where $\lambda = \sqrt{a^2 + \alpha d^2}$. First we observe that

$$\lambda^{q^2} = (\sqrt{a^2 + \alpha d^2})^{q^2} = (a^2 + \alpha d^2)^{(q+1)(q-1)/2}\lambda = (a^2 + \alpha d^2)^{(q-1)}\lambda = \lambda.$$

Similarly we obtain $(-\lambda)^{q^2} = -\lambda$. So, since there exists an invertible matrix $P \in M_2(GF(q^2))$ such that

$$P^{-1} y_1 P = \begin{pmatrix} \lambda & 0 \\ 0 & -\lambda \end{pmatrix},$$

we have $y_1^{q^2} = y_1$.

Now let

$$z_1 = \begin{pmatrix} b & c \\ -\alpha c & -b \end{pmatrix} \in \Omega_1^\alpha.$$

Since

$$z_1^2 = \begin{pmatrix} b^2 - \alpha c^2 & 0 \\ 0 & b^2 - \alpha c^2 \end{pmatrix}$$

and $b^2 - \alpha c^2 \neq 0$ for α is not a square in K, we have $(z_1^2)^{q-1} = 1$. Then $z_1^{2q-1} = z_1$. Finally, by [10], we know that g_3 is a graded identity of Ω^α. ■

Lemma 17 *$\mathfrak{V} \subseteq Var\Omega^\alpha$.*

Proof: Let $N = N_0 \oplus N_1$ be a nilpotent algebra in $\mathfrak{V}$. Hence N_0 is also a nilpotent algebra in $\mathfrak{V}$. The nilpotency index s of N_0 is 2; for if $s > 2$, we can take elements $a_1, \ldots, a_{s-1} \in N_0$ such that $a_1 \ldots a_{s-1} \neq 0$ and, by g_1, we get

$$0 = (a_1 \ldots a_{s-1})^{q^2} - a_1 \ldots a_{s-1} = a_1 \ldots a_{s-1},$$

which is a contradiction. Thus if $a \in N_0$ then $a = a^{q^2} = 0$ and therefore $N_0 = 0$. Moreover, as $N_1N_1 \subseteq N_0 = 0$, we have $N_1^2 = 0$. If $a \in N_1$ then $a = a^{2q-1} = 0$, $N_1 = 0$ and $N = 0$.

The variety $\mathfrak{V}$ has finite index and exponent. By Theorem 11, $\mathfrak{V}$ is generated by a class of subdirectly irreducible finite graded algebras. To prove the lemma it suffices to show that each of these algebras belongs to $Var\Omega^\alpha$. We shall prove even more: each of them is isomorphically embedded in Ω^α. Till the end of the proof we consider A as a finite subdirectly irreducible algebra in $\mathfrak{V}$.

Suppose $A = B \oplus N$ as a direct sum of vector spaces where B is a semisimple (ungraded) subalgebra of A and N is the Jacobson radical of A. Since N is graded ideal and it is nilpotent, $N = 0$. Thus considering $A = B_1 \oplus \ldots \oplus B_s$, the decomposition of A in simple ungraded algebras, we see, due to the subdirect irreducibility of A, that $s = 1$ i.e., A is a simple algebra.

Now suppose A is simple ungraded algebra i.e., $A = M_k(GF(p^t))$ and $p^t \geq q$. Observe that $k \leq 2$, for if $k \geq 3$ then $g_3(a_0, b_0, a_1, b_1) = e_{13} \neq 0$ where a_0, $b_0 \in A_0$ and a_1, $b_1 \in A_1$ are such that $e_{12} = a_0 + a_1$ and $e_{23} = b_0 + b_1$.

Let us consider $k = 2$. If a_0, $b_0 \in A_0$ and a_1, $b_1 \in A_1$ are such that $\alpha e_{11} = a_0 + a_1$ and $e_{12} = b_0 + b_1$ then

$$g_3(a_0, b_0, a_1, b_1) = (\alpha^q - \alpha)e_{12} = 0;$$

hence $\alpha - \alpha^q = 0$, $q \geq p^t$, $A = M_2(GF(q))$. By Lemma 1 we have two possibilities: $u_A^q = u_A$ or $u_A^q = -u_A$. If $u_A^q = u_A$ then A is isomorphic to Ω, and it is a contradiction because Ω does not satisfy g_2. Hence we have $u_A^q = -u_A$. By Lemma 5 there exists a graded isomorphism between Ω^α and A.

Now let us consider $k = 1$ i.e., $A = GF(p^t)$. If $0 \neq a \in A_1$ then

$$a^{q^2} = (a^2)^{(q+1)(q-1)/2}a = (a^{2q}a^2)^{(q-1)/2}a = (a^2)^{q-1}a = a^{2q-1} = a.$$

If $a_0 \in A_0$ and $a_1 \in A_1$, then

$$(a_0 + a_1)^{q^2} = a_0^{q^2} + a_1^{q^2} = a_0 + a_1.$$

Therefore $\alpha^{q^2} - \alpha = 0$ for any $\alpha \in A$, whereby $q^2 \geq p^t$, $A = GF(q)$ or $A = GF(q^2)$. If $A = GF(q)$ then there exists an injective graded homomorphism from A into Ω^α. If $A = GF(q^2)$ then the unique possible grading is $A_0 \cong K$ and $A_1 \cong K$ and, by Lemma 5 of [13], there exists an element $u \in A_1$ such that $A_1 = A_0u$ and $0 \neq u^2 = a \in K$. Hence $A = Ka + Ku$, and the map $\phi\colon A \to \Omega^\alpha$ defined as

$$\phi(\beta a + \gamma u) = \begin{pmatrix} \beta a + \gamma u & 0 \\ 0 & \beta a - \gamma u \end{pmatrix}$$

is an injective graded homomorphism. ■

Remark 18 *We list some other identities for Ω^α:*

$$\begin{aligned}
g_4(y_1, y_2) &= y_1y_2 - y_2y_1,\\
g_5(z_1, z_2, z_3) &= z_1z_2z_3 - z_3z_2z_1,\\
g_6(y_1, z_1) &= z_1^{2q-2}y_1 - y_1,\\
g_7(y_1, z_1) &= (y_1 \cdot z_1)^q - z_1^{q-1}(y_1 \cdot z_1),\\
g_8(y_1, y_2, z_1, z_2) &= (X_1 - X_1^{q^2})(1 - [X_1, X_2]^{q-1})(X_2 - X_2^q),\\
g_9(y_1, y_2, z_1, z_2) &= (X_1 - (X_1)^q) \cdot (X_2 - X_2^q) - ((X_1 - X_1^q) \cdot (X_2 - X_2^q))^q,
\end{aligned}$$

where X_i stands for $y_i + z_i$, $i = 1$, 2. The identity g_4 follows from g_1. The identities g_8 and g_9 are known by [10], and we can change the identity g_3 in Theorem 15 by any of these.

Corollary 19 *The nonisomorphic gradings of the matrix algebra of order two over a finite field are distinguished by their polynomial identities.*

In fact it is sufficient to consider the graded identity $y_1^q - y_1$. It is satisfied if and only if the grading is isomorphic to Ω.

References

[1] C. de Concini, C. Procesi, *A characteristic free approach to invariant theory*, Adv. Math. **21**, no. 3, 330–354 (1976).

[2] O. M. Di Vincenzo, *On the graded identities of $M_{1,1}(E)$*, Israel J. Math. **80**, 323–335 (1992).

[3] E. Formanek, *The polynomial identities and invariants of $n \times n$ matrices*, CBMS Regional Conference Series in Mathematics, **78**, Amer. Math. Soc., 1991.

[4] I. N. Herstein, *Noncommutative rings*, Math. Assoc. Amer., New York, 1968.

[5] A. R. Kemer, *Ideals of identities of associative algebras*, Transl. Math. Monographs **87**, Amer. Math. Soc., 1991.

[6] P. Koshlukov, *Basis of the identities of the matrix algebra of order two over a field of characteristic $p \neq 2$*, J. Algebra, to appear, 2001.

[7] P. Koshlukov, S. S. Azevedo, *Graded identities for T-prime algebras over fields of positive characteristic*, submitted.

[8] R. L. Kruse, *Identities satisfied by a finite ring*, J. Algebra **26**, 298–318 (1973).

[9] I. V. Lvov, Varieties of associative rings, Algebra Logic **12**, 150–167 (1973).

[10] Yu. N. Maltsev, E. N. Kuzmin, *A basis for identities of the algebra of second order matrices over a finite field*, Algebra Logic **17**, 17–21 (1978).

[11] B. R. McDonald, *Finite rings with identities*, Marcel Dekker, New York, 1974.

[12] Yu. P. Razmyslov, *Identities of algebras and their representations*, Transl. Math. Monographs **138**, Amer. Math. Soc., 1994.

[13] C. T. C. Wall, *Graded Brauer groups*, J. Reine Angew. Math. **213**, 187–199 (1963).