Linear Algebra and its Applications 688 (2024) 157–178

Contents lists available at ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

Cyclic algebras, symbol algebras and gradings on matrices

C. Boboc [a], S. Dăscălescu [b], L. van Wyk [c,*]

[a] *University of Bucharest, Faculty of Physics, Department of Theoretical Physics, Mathematics, Optics, Plasma, Lasers, Atomiştilor 405, PO-Box MG-11 RO-077125, Bucharest-Măgurele, Romania*
[b] *University of Bucharest, Faculty of Mathematics and Computer Science, Str. Academiei 14, Bucharest 1, RO-010014, Romania*
[c] *Department of Mathematical Sciences (Mathematics Division), Stellenbosch University, Private Bag X1, Matieland 7602, Stellenbosch, South Africa*

ARTICLE INFO

Article history:
Received 13 November 2023
Received in revised form 14 February 2024
Accepted 15 February 2024
Available online 21 February 2024
Submitted by P. Semrl

MSC:
16W50
16S50

Keywords:
Graded algebra
Cyclic algebra
Symbol algebra
Matrix algebra
Galois extension
Graded division algebra

ABSTRACT

We consider cyclic algebras, Milnor's symbol algebras, and certain graded algebra structures on them. We classify these gradings with respect to both isomorphism and equivalence relations. Some of them induce gradings on matrix algebras, which we also classify. As an application, we obtain the classification of all group gradings on the algebra $\mathrm{M}_p(F)$, where p is a prime number and F is an arbitrary field.

[*] Corresponding author.
E-mail addresses: crinaboboc@yahoo.com (C. Boboc), sdascal@fmi.unibuc.ro (S. Dăscălescu), LvW@sun.ac.za (L. van Wyk).

https://doi.org/10.1016/j.laa.2024.02.016
0024-3795/© 2024 Elsevier Inc. All rights reserved.

1. Introduction and preliminaries

We work over a fixed field F. If G is a group, a G-graded F-algebra is an F-algebra A which has a decomposition $A = \underset{g \in G}{\oplus} A_g$ into a direct sum of F-subspaces such that $A_g A_h \subset A_{gh}$ for any $g, h \in G$. Two G-graded algebras A and B are isomorphic if there is an algebra isomorphism $f : A \to B$ preserving degrees, i.e., $f(A_g) = B_g$ for any $g \in G$. A general problem is to classify up to isomorphism all possible group gradings on a given algebra A.

If $\theta : H \to G$ is a group morphism and $A = \underset{h \in H}{\oplus} A_h$ is an H-graded algebra, then A also has a G-graded algebra structure, denoted by A^θ, defined by $(A^\theta)_g = \sum_{h \in H, \theta(h)=g} A_h$ for any $g \in G$. In particular, if A is a G-graded algebra and $\theta : G \to G$ is a group automorphism of G, we can define a new G-grading A^θ on A. In this way the automorphism group $\mathrm{Aut}(G)$ acts on the set of isomorphism types of G-graded algebras. If A and B are two G-graded algebras, we say that A and B are equivalent, and we write $A \equiv B$, if A and B are in the same orbit of this action, i.e., if there is $\theta \in \mathrm{Aut}(G)$ such that $B \cong A^\theta$ as G-graded algebras. A second problem is to classify up to equivalence the gradings on a given algebra A; this second classification identifies (possibly non-isomorphic) gradings which are obtained one from each other by “mixing” the degrees by an automorphism of the group. It makes sense to identify such gradings, since from the point of view of graded ring theory, if A is a G-graded algebra and $\theta \in \mathrm{Aut}(G)$, then the graded algebras A and A^θ essentially have the same properties.

Of particular interest is the case where $A = \mathrm{M}_s(F)$ is a full matrix algebra. The classification of all group gradings on A is a wide open problem. The case where F is algebraically closed was solved in [1], [2], see also [6]. If F is an arbitrary field, all possible gradings were determined for $s = 2$ in [7], and for $s = 3$ in [3]. Among special classes of gradings that have been investigated we mention gradings for which all usual matrix units in $\mathrm{M}_s(F)$ are homogeneous elements. Such gradings are called good gradings (or elementary gradings in [1], [6]) and they play a key role in the general problem of classification of all gradings on a matrix algebra; good G-gradings on $\mathrm{M}_s(F)$ were classified in [4] by the orbits of a biaction of G and the symmetric group S_s on the set G^s.

Now we recall from [8, Section 14] the definition of cyclic algebras. Let $F \subset K$ be a Galois extension of finite degree $s \geq 2$ such that the Galois group $\mathrm{Gal}(K/F)$ is a cyclic group. Let σ be a generator of $\mathrm{Gal}(K/F)$, and let $a \in F^*$. The associated cyclic algebra $(K/F, \sigma, a)$ is the quotient of the Ore extension $K[X, \sigma]$ by the ideal generated by the polynomial $X^s - a$. Denoting by x the class of the indeterminate X in this quotient, we have

$$(K/F, \sigma, a) = K \oplus Kx \oplus \cdots \oplus Kx^{s-1},$$

subject to the relations $x^s = a$ and $xb = \sigma(b)x$ for any $b \in K$. Let $C_s = \langle\omega\rangle$ be the cyclic group of order s. It is clear that $(K/F, \sigma, a)$ as above has a C_s-grading, whose homogeneous component of degree ω^i is Kx^i for any $0 \le i \le s-1$. We denote this C_s-graded algebra by $D_1(K/F, \sigma, a)$. In Section 2 we classify graded algebras of this kind up to isomorphism and up to equivalence. The cyclic algebra $(K/F, \sigma, a)$ is isomorphic to $\mathrm{M}_s(F)$ if and only if $a \in N_{K/F}(K^*)$, where $N_{K/F}$ is the norm associated with the extension K/F; in this situation the grading of $D_1(K/F, \sigma, a)$ induces one on $\mathrm{M}_s(F)$. A consequence of the results in this section is the following.

Proposition A. *The equivalence classes of all C_s-gradings on $\mathrm{M}_s(F)$ arising from gradings of type $D_1(K/F, \sigma, a)$ are in bijection to the isomorphism types of cyclic Galois extensions of degree s of F.*

Now consider a cyclic algebra $(K/F, \sigma, a)$ and assume that F contains primitive roots of unity of order s. By Hilbert's Theorem 90, K is a splitting field of a polynomial of the form $Y^s - b$ for some $b \in F$, see [9, pages 288-289]. If y is a root of $Y^s - b$ in K, then $K = F(y) = F \oplus Fy \oplus \cdots \oplus Fy^{s-1}$, and there exists a primitive s-th root of unity ε in F such that $\sigma(y) = \varepsilon y$. Then $(K/F, \sigma, a) = \bigoplus_{0 \le i,j \le s-1} Fy^i x^j$, $x^s = a$, $y^s = b$, and $xy = \varepsilon yx$.

This suggests a consideration of a more general construction as follows. Assume that F contains a primitive root of unity ε of order s. Let $C_s \times C_s = \langle\omega\rangle \times \langle\rho\rangle$ be the product of two cyclic groups of order s, and let $a, b \in F^*$. Define the $C_s \times C_s$ - graded algebra $D_2(F, \varepsilon, a, b)$ by generators x, y subject to the relations

$$x^s = a,\ y^s = b,\ xy = \varepsilon yx,$$

with grading given by $D_2(F, \varepsilon, a, b)_{\omega^i \rho^j} = Fy^i x^j$ for any $0 \le i, j \le s-1$. The algebras $D_2(F, \varepsilon, a, b)$, considered just as F-algebras, with no reference to the graded structure, were introduced by Milnor [10] in algebraic K-theory, in his approach to the K_2 functor. More precisely, $D_2(F, \varepsilon, a, b)$ is a central simple F-algebra, and the mapping taking a pair (a, b) to the class of $D_2(F, \varepsilon, a, b)$ in the Brauer group of F defines a Steinberg symbol $\{,\} : F^* \times F^* \to \mathrm{Br}(F)$, and further induces a group morphism from K_2F to $\mathrm{Br}(F)$; for this reason $D_2(F, \varepsilon, a, b)$ is called a symbol algebra.

Note that in other words, the algebra $D_2(F, \varepsilon, a, b)$ is the quotient of the quantum polynomial algebra $F_\varepsilon[X, Y]$ (also known as a quantum plane) by the ideal generated by $X^s - a$ and $Y^s - b$. If $s = 2$, then the algebras $D_2(F, \varepsilon, a, b)$ are just the quaternion algebras, which play a key role in the theory of quadratic forms.

Clearly, $D_2(F, \varepsilon, a, b)$ is a graded division algebra, i.e., any non-zero homogeneous element is invertible. Denote by $K_b \cong F[Y]/(Y^s - b)$ its subalgebra generated by y, and by $N_{K_b/F}$ the associated norm. We collect the main results about these algebras proved in Sections 3 and 4 in:

Theorem B. *$D_2(F, \varepsilon, a, b)$ is isomorphic to $\mathrm{M}_s(F)$ if and only if $a \in N_{K_b/F}(K_b)$. The isomorphism types of $C_s \times C_s$ - graded algebras of type $D_2(F, \varepsilon, a, b)$ are in bijection to the set $U(\mathbb{Z}_s) \times F^*/(F^*)^s \times F^*/(F^*)^s$, while the equivalence classes of such graded algebras are classified by the orbits of a certain action of $\mathrm{SL}_2(\mathbb{Z}_s)$ on $F^*/(F^*)^s \times F^*/(F^*)^s$. As for the $C_s \times C_s$ - graded algebras induced on $\mathrm{M}_s(F)$ from graded algebras of type $D_2(F, \varepsilon, a, b)$, their isomorphism types are in bijection to $U(\mathbb{Z}_s) \times \mathcal{E}(F, s)$, where $\mathcal{E}(F, s)$ is the $\mathrm{SL}_2(\mathbb{Z}_s)$-subset of $F^*/(F^*)^s \times F^*/(F^*)^s$ consisting of all pairs $(\overline{a}, \overline{b})$ with the property that $a \in N_{K_b/F}(K_b)$, while their equivalence classes are classified by the orbits of $\mathcal{E}(F, s)$.*

The result in the first sentence of Theorem B is not new. It was proved in [10, Theorem 15.7]. The if implication was showed by using some properties of the Steinberg symbol, while the only if one used linear algebra arguments, by regarding $\mathrm{M}_s(F)$ as the algebra of endomorphisms of a vector space V, and then by investigating when there are two endomorphisms of V satisfying the same relations as x and y in the symbol algebra. Another proof was given in [5, Corollary 4, page 82] by using considerations involving Brauer groups. Our approach is different. We uncover the ring structure of $D_2(F, \varepsilon, a, b)$, by showing that its basement is a direct sum of isomorphic cyclic Galois extensions of F, and there is an invertible element whose inner action on these extensions permutes them in a cycle, while the compositions of the isomorphisms in this cycle provide generators of the Galois groups. Then we prove the first implication by investigating the dimension of a non-zero left ideal. As for the other implication, we observe that K_b/F is a Hopf-Galois extension over the dual of the group Hopf algebra FC_s.

We give explicit presentations of the gradings on $\mathrm{M}_s(F)$ obtained in this way.

In Section 5 we classify all gradings on $\mathrm{M}_p(F)$, where p is a prime number and F is an arbitrary field, by any possible group. In brief, the classification is done in the following theorem, showing that any grading is either isomorphic to a good grading, or it arises from a cyclic algebra or from a symbol algebra. The complete and precise statement is in Section 5.

Theorem C. *Let p be a prime number. Then any group grading on the algebra $\mathrm{M}_p(F)$ is isomorphic to one of the following three types:*

- **(I)** *A good grading;*
- **(II)** *A grading induced from $D_1(K/F, \sigma, 1)$ for a Galois extension K/F of degree p and a generator σ of $\mathrm{Gal}(K/F)$. The equivalence classes of such gradings are in bijection to the set of isomorphism types of Galois extensions of degree p of F;*
- **(III)** *A grading induced from $D_2(F, \varepsilon, a, b)$ for a p-th root of unity $\varepsilon \neq 1$, and elements $a, b \in F^*$ satisfying a certain condition. The equivalence classes of such gradings are in bijection to the orbits of the action of $\mathrm{SL}_2(\mathbb{Z}_p)$ on $\mathcal{E}(F, p)$. Gradings of this type do not occur if F does not contain non-trivial p-th roots of unity.*

2. Gradings on cyclic algebras

Let $F \subset K$ be a cyclic Galois extension of degree $s \geq 2$, thus the Galois group $\mathrm{Gal}(K/F)$ is isomorphic to C_s. Let σ be a generator of $\mathrm{Gal}(K/F)$, and let $a \in F^*$. We consider the C_s-graded algebra $D_1(K/F, \sigma, a)$ described in Section 1. Let $N_{K/F}$ denote the norm associated to the extension $F \subset K$. We have $N_{K/F}(b) = b\sigma(b) \cdots \sigma^{s-1}(b)$ for any $b \in K$, in particular, $N_{K/F}(b) = b^s$ for any $b \in F$.

We first classify these C_s-gradings.

Proposition 2.1. *Let $F \subset K$ and $F \subset E$ be cyclic Galois extensions of degree s, with* $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ *and* $\mathrm{Gal}(E/F) = \langle\tau\rangle$, *and let $a, b \in F^*$. Then:*

(1) *$D_1(K/F, \sigma, a) \cong D_1(E/F, \tau, b)$ as C_s-graded algebras if and only if there is an F-isomorphism $\varphi : K \to E$ such that $\tau\varphi = \varphi\sigma$, and $a/b \in N_{E/F}(E^*)$ $(= N_{K/F}(K^*))$.*

(2) *$D_1(K/F, \sigma, a) \equiv D_1(E/F, \tau, b)$ if and only if there is an F-isomorphism $\varphi : K \to E$ such that $a/b^m \in N_{K/F}(K^*)$, where m is an integer (relatively prime to s, and unique modulo s) such that $\varphi\sigma = \tau^m\varphi$.*

Proof. (1) If $f : D_1(K/F, \sigma, a) \to D_1(E/F, \tau, b)$ is an isomorphism of C_s-graded algebras, then restricting f to the homogeneous components of trivial degree, we obtain an F-isomorphism $\varphi : K \to E$. Now $x \in D_1(K/F, \sigma, a)_\omega$, so then $f(x) \in D_1(E/F, \tau, b)_\omega$, showing that $f(x) = \delta x$ for some $\delta \in E^*$. Apply f to $xu = \sigma(u)x$, where $u \in K$, and get $\delta x\varphi(u) = \varphi(\sigma(u))\delta x$, and then $\delta\tau(\varphi(u))x = \varphi(\sigma(u))\delta x$. This shows that $\tau\varphi = \varphi\sigma$.

On the other hand, if we apply f to $x^s = a$ and use the commutation relations in $D_1(E/F, \tau, b)$, we get $\delta\tau(\delta) \cdots \tau^{s-1}(\delta)x^s = a$, which rewrites as $a/b = N_{E/F}(\delta)$.

Note that indeed $N_{E/F}(E^*) = N_{K/F}(K^*)$, since for any $\delta \in E$ we have

$$\begin{aligned} N_{E/F}(\delta) &= \delta\tau(\delta) \cdots \tau^{s-1}(\delta) \\ &= \delta(\varphi\sigma\varphi^{-1})(\delta)(\varphi\sigma^2\varphi^{-1})(\delta) \cdots (\varphi\sigma^{s-1}\varphi^{-1})(\delta) \\ &= \varphi(\varphi^{-1}(\delta)\sigma(\varphi^{-1}(\delta))\sigma^2(\varphi^{-1}(\delta)) \cdots \sigma^{s-1}(\varphi^{-1}(\delta))) \\ &= \varphi(N_{K/F}(\varphi^{-1}(\delta))) \\ &= N_{K/F}(\varphi^{-1}(\delta)), \end{aligned}$$

showing that $N_{E/F}(E^*) = N_{K/F}(K^*)$.

Conversely, if $a/b = N_{E/F}(\delta)$, with $\delta \in E^*$, and there is an F-isomorphism $\varphi : K \to E$ such that $\tau\varphi = \varphi\sigma$, then it is a straightforward check that the linear map $f : D_1(K/F, \sigma, a) \to D_1(E/F, \tau, b)$ defined such that $f(ux^i) = \varphi(u)\left(\prod_{0 \leq j \leq i-1} \tau^j(\delta)\right)x^i$ for any $u \in K$ and $0 \leq i \leq s-1$, is an isomorphism of C_s-graded algebras.

(2) Assume that $D_1(K/F, \sigma, a) \equiv D_1(E/F, \tau, b)$ and let $\theta \in \mathrm{Aut}(C_s)$ be such that there is an isomorphism of C_s-graded algebras $f : D_1(K/F, \sigma, a) \to D_1(E/F, \tau, b)^\theta$. The

restriction of f to the homogeneous components of trivial degree is an F-isomorphism $\varphi : K \to E$. We have $\theta^{-1}(\omega) = \omega^m$ for some m relatively prime to s, and then $f(x) = \delta x^m$ for some $\delta \in E^*$. Apply f to $xu = \sigma(u)x$, where $u \in K$, and see that $\delta x^m \varphi(u) = \varphi(\sigma(u))\delta x^m$, so then $\tau^m(\varphi(u))x^m = \varphi(\sigma(u))x^m$, showing that $\tau^m\varphi = \varphi\sigma$.

Now apply f to $x^s = a$, and get that $(\delta x^m)^s = a$, so then

$$\delta\tau^m(\delta)\tau^{2m}(\delta)\cdots\tau^{(s-1)m}(\delta)x^{sm} = a. \tag{2.1}$$

As τ^m is a generator of $\mathrm{Gal}(E/F)$ and $x^s = b$ in $D_1(E/F, \tau, b)$, the left hand side in (2.1) is $N_{E/F}(\delta)b^m$, showing that $a/b^m = N_{E/F}(\delta) \in N_{E/F}(E^*) = N_{K/F}(K^*)$.

For the converse, let $\delta \in E^*$ with $a/b^m = N_{E/F}(\delta)$. Let $\theta \in \mathrm{Aut}(C_s)$ such that $\theta^{-1}(\omega) = \omega^m$. Then the unique algebra map $f : D_1(K/F, \sigma, a) \to D_1(E/F, \tau, b)^\theta$ whose restriction to the trivial degree component is φ and such that $f(x) = \delta x^m$, is an isomorphism of graded algebras. □

Corollary 2.2.

(1) *The isomorphism classes of C_s-graded algebras of the type $D_1(K/F, \sigma, a)$ are in bijection to the set of triples (K, σ, μ), where K runs through the isomorphism types of cyclic Galois extensions of degree s of F, σ is an arbitrary generator of* $\mathrm{Gal}(K/F)$*, and $\mu \in F^*/N_{K/F}(K^*)$.*

(2) *The equivalence classes of C_s-graded algebras of the type $D_1(K/F, \sigma, a)$ are in bijection to the set of pairs (K, μ), where K runs through the isomorphism types of cyclic Galois extensions of degree s of F, and $\mu \in F^*/N_{K/F}(K^*)$.*

Proof. (1) It is clear that we can choose K in a set of representatives for the isomorphism types of cyclic Galois extensions of degree s of F. Next it suffices to see that $D_1(K/F, \sigma, a) \cong D_1(K/F, \tau, b)$ if and only if $a/b \in N_{K/F}(K^*)$, i.e., a and b lie in the same $N_{K/F}(K^*)$-coset of F^*, and there is $\varphi \in \mathrm{Gal}(K/F)$ such that $\tau\varphi = \varphi\sigma$. As $\mathrm{Gal}(K/F)$ is abelian, the latter implies that $\tau = \sigma$.

(2) Let K/F be a cyclic Galois extension of degree s, and fix some generator σ of the associated Galois group. If τ is any other generator, and $b \in K^*$, then $\sigma = \tau^m$ for some m relatively prime to s, and $D_1(K/F, \tau, b) \equiv D_1(K/F, \sigma, b^m)$ by Proposition 2.1. Thus we can only consider gradings of the type $D_1(K/F, \sigma, a)$, with $a \in K^*$. Now $D_1(K/F, \sigma, a) \equiv D_1(K/F, \sigma, b)$ if and only if there is m (relatively prime to s) such that $\sigma^m = \sigma$, which means that $m = 1$ (modulo s), and $a/b^m \in N_{K/F}(K^*)$, implying that $a/b \in N_{K/F}(K^*)$. □

It is known that $D_1(K/F, \sigma, a)$ is a central simple F-algebra of dimension s^2, and $D_1(K/F, \sigma, a) \cong \mathrm{M}_s(F)$ if and only if $a \in N_{K/F}(K^*)$, see [8, Theorem 14.6 and Theorem 14.7] for details. In fact, if $a \in N_{K/F}(K^*)$, then we have already seen in Proposition 2.1 that $D_1(K/F, \sigma, a) \cong D_1(K/F, \sigma, 1)$ as C_s-graded algebras, and on the other hand, there is an algebra isomorphism $\pi : D_1(K/F, \sigma, 1) \to \mathrm{End}_F(K)$ such that $\pi(\beta)$ is the multiplication by β for any $\beta \in K$, and $\pi(x) = \sigma$. Hence the C_s-grading of $D_1(K/F, \sigma, 1)$ induces a C_s-grading on $\mathrm{End}_F(K)$ via π, and further a C_s-grading on the matrix algebra $\mathrm{M}_s(F)$ via an algebra isomorphism $\mathrm{End}_F(K) \cong \mathrm{M}_s(F)$. An immediate consequence of Corollary 2.2 is the following.

Corollary 2.3.

(1) *The isomorphism types of C_s-gradings on $\mathrm{M}_s(F)$ obtained as above from C_s-gradings of type $D_1(K/F, \sigma, a)$ are in bijection to the pairs (K, σ), where K is an isomorphism type of cyclic Galois extension of degree s of F, and σ is a generator of* $\mathrm{Gal}(K/F)$.

(2) *The equivalence types of C_s-gradings on $\mathrm{M}_s(F)$ obtained from C_s-gradings of type $D_1(K/F, \sigma, a)$ are in bijection to the isomorphism types of cyclic Galois extensions of degree s of F.*

Remark 2.4. We discuss the possibility to obtain an explicit description of the C_s-grading on $\mathrm{M}_s(F)$ induced from cyclic algebras via the isomorphism $\pi : D_1(K/F, \sigma, 1) \to \mathrm{End}_F(K)$ described above. A cyclic Galois extension K/F of degree s, with $\mathrm{Gal}(K/F) = \langle \sigma \rangle$, has a normal basis, this is a basis of the form $\{w, \sigma(w), \sigma^2(w), \dots, \sigma^{s-1}(w)\}$, where w is an element of K. Then the matrix of $\pi(x)$ in this basis is the permutation matrix associated to the cycle $(1\ 2\ \dots\ n)$, but in general we do not have an explicit form for the matrices of the endomorphisms in $\pi(K)$. However, if we assume that F contains a primitive s-th root of unity ε, then K is obtained by adjoining to F an element y such that $y^s = b$, where $b \in F$, and then a normal basis of K/F is $z_0, z_1, \dots, z_{s-1}$, where $z_i = 1 + \varepsilon^i y + \varepsilon^{2i} y^2 + \cdots + \varepsilon^{(s-1)i} y^{s-1}$ for any $0 \leq i \leq s-1$. Now a simple computation produces the matrix Y in this normal basis, and then the homogeneous component of degree ω^i of the C_s-grading induced on $\mathrm{M}_s(F)$ is the subspace spanned by $X^i, YX^i, \dots, Y^{s-1}X^i$ for any $0 \leq i \leq s-1$.

We note that one can also obtain explicitly an associated grading on $\mathrm{M}_s(F)$ by working with the basis $\{1, y, \dots, y^{s-1}\}$ instead of the normal basis $\{z_0, \dots, z_{s-1}\}$. We postpone the details for the end of Remark 3.4, because such a grading will follow as a coarsening of a $C_s \times C_s$ - grading described there.

3. The graded algebras $D_2(F, \varepsilon, a, b)$

If A is a finite dimensional commutative F-algebra, we denote by $N_{A/F}$ the associated norm, defined by $N_{A/F}(a) = \det(m_a) \cdot 1_A$ for any $a \in A$, where $m_a : A \to A$ is the multiplication by a, $\det(m_a)$ is its determinant, and 1_A is the identity of A. If F is identified with its image inside A, we simply regard $N_{A/F}$ as taking values in F.

In this section and in the next one we assume that F contains primitive s-th roots of unity. Consider now a $C_s \times C_s$ - graded algebra of the type $D_2(F, \varepsilon, a, b)$, where ε is a primitive s-th root of unity in F, and $a, b \in F^*$. It is known that $D_2(F, \varepsilon, a, b)$ is a central simple F-algebra, see [10, Theorem 15.1]. The aim of this section is to investigate the ring structure of $D_2(F, \varepsilon, a, b)$, in particular to prove the first part of Theorem B, and to give explicit presentations of the gradings induced on the matrix algebra $\mathrm{M}_s(F)$.

Denote $K_b = F \oplus Fy \oplus \cdots \oplus Fy^{s-1} \cong F[Y]/(Y^s - b)$, an F-subalgebra of dimension s of $D_2(F, \varepsilon, a, b)$. We have that $D_2(F, \varepsilon, a, b) = K_b \oplus K_b x \oplus \cdots \oplus K_b x^{s-1}$. Let $\sigma \in \mathrm{Aut}_F(K_b)$ such that $\sigma(y) = \varepsilon y$. As $xy = \varepsilon yx$, we see that $xu = \sigma(u)x$ for any $u \in K_b$.

Proposition 3.1. *$N_{K_b/F}(u) = u\sigma(u) \cdots \sigma^{s-1}(u)$ for any $u \in K_b$.*

Proof. Let $u = a_0 + a_1 y + \cdots + a_{s-1} y^{s-1}$, with $a_0, \ldots, a_{s-1} \in F$, and let $m_u : K_b \to K_b$, $m_u(v) = vu$ for any $v \in K_b$. The matrix of m_u in the basis $\{1, y, \ldots, y^{s-1}\}$ is

$$U = \begin{bmatrix} a_0 & ba_{s-1} & ba_{s-2} & \ldots & ba_1 \\ a_1 & a_0 & ba_{s-1} & \ldots & ba_2 \\ a_2 & a_1 & a_0 & \ldots & ba_3 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{s-1} & a_{s-2} & a_{s-3} & \ldots & a_0 \end{bmatrix}.$$

If we consider the matrix

$$V = \begin{bmatrix} 1 & y & y^2 & \ldots & y^{s-1} \\ 1 & \varepsilon y & \varepsilon^2 y^2 & \ldots & \varepsilon^{s-1} y^{s-1} \\ 1 & \varepsilon^2 y & \varepsilon^4 y^2 & \ldots & \varepsilon^{2(s-1)} y^{s-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \varepsilon^{s-1} y & \varepsilon^{2(s-1)} y^2 & \ldots & \varepsilon^{(s-1)^2} y^{s-1} \end{bmatrix},$$

a direct computation shows that

$$VU = \begin{bmatrix} u & uy & uy^2 & \ldots & uy^{s-1} \\ \sigma(u) & \varepsilon\sigma(u)y & \varepsilon^2\sigma(u)y^2 & \ldots & \varepsilon^{s-1}\sigma(u)y^{s-1} \\ \sigma^2(u) & \varepsilon^2\sigma^2(u)y & \varepsilon^4\sigma^2(u)y^2 & \ldots & \varepsilon^{2(s-1)}\sigma^2(u)y^{s-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \sigma^{s-1}(u) & \varepsilon^{s-1}\sigma^{s-1}(u)y & \varepsilon^{2(s-1)}\sigma^{s-1}(u)y^2 & \ldots & \varepsilon^{(s-1)^2}\sigma^{s-1}(u)y^{s-1} \end{bmatrix},$$

and equating the determinants, we see that $\det(V)\det(U) = u\sigma(u) \cdots \sigma^{s-1}(u)\det(V)$. As $\det(V) = \prod_{0 \le i < j \le s-1} (\varepsilon^j y - \varepsilon^i y) = y^{s(s-1)/2} \prod_{0 \le i < j \le s-1} (\varepsilon^j - \varepsilon^i)$ (the first equality follows from the Vandermonde determinant) is an invertible element of K_b (since y is invertible and the second factor is a product of nonzero elements of F), we get that $N_{K_b/F}(u) = \det(U) = u\sigma(u) \cdots \sigma^{s-1}(u)$. □

We prove now the if implication in the first sentence of Theorem B.

Proposition 3.2. *If $a \in N_{K_b/F}(K_b)$, then $D_2(F,\varepsilon,a,b) \cong \mathrm{M}_s(F)$.*

Proof. Let $a = N_{K_b/F}(v) = v\sigma(v)\cdots\sigma^{s-1}(v)$ for some $v \in K_b$. Then v is invertible in K_b and $aN_{K_b/F}(v^{-1}) = 1$. Now

$$\begin{aligned}(v^{-1}x)^s &= v^{-1}xv^{-1}x\cdots v^{-1}x\\ &= v^{-1}\sigma(v^{-1})\sigma^2(v^{-1})\cdots\sigma^{s-1}(v^{-1})x^s\\ &= N_{K_b/F}(v^{-1})a\\ &= 1,\end{aligned}$$

and $(v^{-1}x)y = \varepsilon v^{-1}yx = \varepsilon y(v^{-1}x)$, so replacing x by $v^{-1}x$, we find that $D_2(F,\varepsilon,a,b) \cong D_2(F,\varepsilon,1,b)$ as F-algebras (however, this is not an isomorphism of graded algebras).

We will show that $D_2(F,\varepsilon,1,b) \cong \mathrm{M}_s(F)$. Let G be the subgroup of the automorphism group of the F-algebra K_b generated by σ, thus $G = \{\mathrm{Id},\sigma,\ldots,\sigma^{s-1}\}$. Then G acts on K_b, and the subalgebra of invariants is F. Thus K_b is a left module algebra over the group Hopf algebra FG, or equivalently, a right $(FG)^*$-comodule algebra, with coaction given by $z \mapsto \sum_{i=0}^{s-1} \sigma^i(z) \otimes p_i$, where $(p_i)_{i=0,s-1}$ denotes the basis of $(FG)^*$ dual to the basis $(\sigma^i)_{i=0,s-1}$ of FG. Here $(FG)^*$ denotes the dual Hopf algebra of FG. We claim that K_b/F is a right $(FG)^*$-Galois extension, i.e., the map

$$\beta : K_b \otimes_F K_b \to K_b \otimes_F (FG)^*,\ \beta(z \otimes u) = \sum_{i=0}^{s-1} z\sigma^i(u) \otimes p_i,$$

is bijective, see [11, Section 8.1]. As $K_b \otimes_F K_b$ and $K_b \otimes_F (FG)^*$ have the same dimension, it suffices to show that β is injective. Let $\xi = \sum_{j=0}^{s-1} z_j \otimes y^j \in \mathrm{Ker}(\beta)$. As

$$\begin{aligned}\beta(\xi) &= \sum_{i,j=0}^{s-1} z_j\sigma^i(y^j) \otimes p_i\\ &= \sum_{i,j=0}^{s-1} \varepsilon^{ij} y^j z_j \otimes p_i,\end{aligned}$$

we get that $\sum_{j=0}^{s-1} \varepsilon^{ij} y^j z_j = 0$ for any i. Regarding these equations as a system in $z_0,\ldots,z_{s-1}$, the matrix of coefficients is just the matrix V in the proof of Proposition 3.1, which we showed to be invertible. Consequently, $z_0 = \ldots = z_{s-1} = 0$ and $\xi = 0$.

Now by [11, Theorem 8.3.3] there is an algebra isomorphism $\pi : K_b * G \to \mathrm{End}_F(K_b)$, given by $\pi(u\sigma^i)(v) = u\sigma^i(v)$ for any $u, v \in K_b$ and $0 \le i \le s-1$. Here $K_b * G$ is the skew group ring associated with the action of G on K_b. On the other hand, it is clear that $D_2(F, \varepsilon, 1, b) \cong K_b * G$, with x corresponding to σ. We conclude that $D_2(F, \varepsilon, 1, b) \cong \mathrm{M}_s(F)$. □

Remark 3.3. The isomorphism between $D_2(F, \varepsilon, 1, b)$ and $\mathrm{End}_F(K_b)$ in the proof of the previous Proposition could have been proved directly by considering the linear map $\tilde{\pi} : D_2(F, \varepsilon, 1, b) \to \mathrm{End}_F(K_b)$ defined by $\tilde{\pi}(ux^i)(v) = u\sigma^i(v)$ for any $u, v \in K_b$ and any $0 \le i \le s-1$, and showing that this is an algebra morphism. Then $\tilde{\pi}$ is injective since $D_2(F, \varepsilon, 1, b)$ is a simple algebra, hence it is an isomorphism, since $D_2(F, \varepsilon, 1, b)$ and $\mathrm{End}_F(K_b)$ have the same dimension. We preferred the approach using Hopf-Galois extensions since it shows that the algebra $D_2(F, \varepsilon, 1, b)$ is constructed over a Hopf-Galois extension in a similar fashion to the way a cyclic algebra is constructed over a Galois extension.

Remark 3.4. We can give an explicit description of the $C_s \times C_s$ - gradings induced on the matrix algebra $\mathrm{M}_s(F)$ from gradings of the type $D_2(F, \varepsilon, a, b)$ with $a, b \in F^*$ and $a \in N_{K_b/F}(K_b)$. Indeed, let $a = N_{K_b/F}(v)$ for some $v = a_0 + a_1 y + \cdots + a_{s-1}y^{s-1} \in K_b$, where $a_0, \ldots, a_{s-1} \in F$. By the proof of Proposition 3.2, there is an isomorphism of algebras (not of graded algebras) $\pi' : D_2(F, \varepsilon, a, b) \to D_2(F, \varepsilon, 1, b)$ such that $\pi'(y) = y$ and $\pi'(x) = vx$. On the other hand, we have seen in Remark 3.3 that there is an algebra isomorphism $\tilde{\pi} : D_2(F, \varepsilon, 1, b) \to \mathrm{End}_F(K_b)$, $\tilde{\pi}(ux^i)(w) = u\sigma^i(w)$ for any $u, w \in K_b$. Transfer by $\tilde{\pi}\pi'$ the $C_s \times C_s$ - grading of $D_2(F, \varepsilon, a, b)$ to a grading on $\mathrm{End}_F(K_b)$, and then to a $C_s \times C_s$ - grading on $\mathrm{M}_s(F)$ by associating to an endomorphism of K_b its matrix in the basis $\{1, y, \ldots, y^{s-1}\}$. As $(\tilde{\pi}\pi')(y)(y^j) = y^{j+1}$ for any $0 \le j \le s-1$, we get that the homogeneous component of degree ω in this grading of $\mathrm{M}_s(F)$ is the 1-dimensional space spanned by the matrix

$$Y = \begin{bmatrix} 0 & 0 & \ldots & 0 & b \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 0 \end{bmatrix}.$$

On the other hand,

$$\begin{aligned}
(\tilde{\pi}\pi')(x)(y^j) &= \tilde{\pi}(vx)(y^j) \\
&= v\sigma(y^j) \\
&= \varepsilon^j v y^j \\
&= \varepsilon^j a_0 y^j + \cdots + \varepsilon^j a_{s-1-j} y^{s-1} + \varepsilon^j a_{s-j} b + \cdots + \varepsilon^j a_{s-1} b y^{j-1}
\end{aligned}$$

for any $1 \le j \le s-1$, and $(\tilde{\pi}\pi')(x)(1) = v$, so the homogeneous component of degree ρ of the same grading is the subspace spanned by the matrix

$$X = \begin{bmatrix} a_0 & \varepsilon b a_{s-1} & \varepsilon^2 b a_{s-2} & \dots & \varepsilon^{s-1} b a_1 \\ a_1 & \varepsilon a_0 & \varepsilon^2 b a_{s-1} & \dots & \varepsilon^{s-1} b a_2 \\ a_2 & \varepsilon a_1 & \varepsilon^2 a_0 & \dots & \varepsilon^{s-1} b a_3 \\ \dots & \dots & \dots & \dots & \dots \\ a_{s-1} & \varepsilon a_{s-2} & \varepsilon^2 a_{s-3} & \dots & \varepsilon^{s-1} a_0 \end{bmatrix}.$$

We conclude that the homogeneous component of degree $\omega^i \rho^j$ in the induced $C_s \times C_s$ - grading on $\mathrm{M}_s(F)$ is FY^iX^j.

In the case where $a = 1$, we can take $v = 1$, so $a_0 = 1,\ a_1 = \ldots = a_{s-1} = 0$, and so we have the matrices

$$Y = \begin{bmatrix} 0 & 0 & \dots & 0 & b \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}, \quad X = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & \varepsilon & 0 & \dots & 0 \\ 0 & 0 & \varepsilon^2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \varepsilon^{s-1} \end{bmatrix}. \tag{3.1}$$

Therefore we obtain a family of $C_s \times C_s$ - gradings on $\mathrm{M}_s(F)$ parametrized by $b \in F^*$. For $b = 1$, the corresponding grading is the ε-grading considered in [1, Section 4].

We end the remark by going back to Remark 2.4, and showing that in the case where F contains a primitive s-th root of unity ε, an explicit form of the C_s-grading on $\mathrm{M}_s(F)$ induced from $D_1(K/F, \sigma, 1)$ can be obtained as a coarsening of the $C_s \times C_s$ - grading described above. Indeed, there is $b \in F$ such that $K \cong K_b$, there is an algebra isomorphism $D_1(K_b/F, \sigma, 1) \cong D_2(F, \varepsilon, 1, b)$, and the algebra isomorphism $\pi : D_1(K/F, \sigma, 1) \to \mathrm{End}_F(K)$ in Remark 2.4 is just the isomorphism $\tilde{\pi} : D_2(F, \varepsilon, 1, b) \to \mathrm{End}_F(K_b)$ discussed above. The C_s-grading induced on $\mathrm{M}_s(F)$ has the subspace spanned by $X^i, YX^i, \ldots, Y^{s-1}X^i$ as homogeneous component of degree ω^i for any $0 \le i \le s-1$, where X and Y are the matrices in equation (3.1).

Now we consider the converse of Proposition 3.2. In the case where the polynomial $g = Y^s - b$ is irreducible over F, the converse holds, since $K_b \cong F[Y]/(Y^s - b)$ is a field which is a cyclic Galois extension of F. In the general case, by [9, Theorem 6.2, page 289], there exist $c \in F^*$ and a divisor d of s, say $s = dr$ for a positive integer r, such that $Y^d - c$ is irreducible and $b = c^r$. Let $\lambda = \varepsilon^{-d}$, which is a primitive r-th root of unity, and $g_i = Y^d - \lambda^{i-1}c$ for any $1 \le i \le r$. Since $\lambda^r = 1$, there is no harm if we take i modulo r; we will regard i in this way in the rest of this section. Then $g = g_1 \cdots g_r$ is the irreducible decomposition of g, and $F[Y]/(g_i)$, $1 \le i \le r$, are all isomorphic cyclic Galois extensions of degree d of F. Let $\pi_i : F[Y] \to F[Y]/(g_i)$ be the natural projection. By the Chinese remainder lemma, there is an isomorphism of F-algebras $\varphi : F[Y]/(Y^s - b) \to F[Y]/(g_1) \times \cdots \times F[Y]/(g_r)$, $\varphi(\hat{f}) = (\pi_1(f), \ldots, \pi_r(f))$, where $\hat{f}$ denotes the class of $f \in F[Y]$ in $F[Y]/(Y^s - b)$.

Denote $K_b' = F[Y]/(g_1) \times \cdots \times F[Y]/(g_r)$, and for any i let K_i be the natural image of $F[Y]/(g_i)$ and y_i be the image of $\pi_i(Y)$ in K_b'. Thus $K_b' = K_1 \oplus \cdots \oplus K_r$, and K_i has the basis $y_i, \dots, y_i^d$, with relation $y_i^{d+1} = \lambda^{i-1} c y_i$; K_i is a field with identity $1_{K_i} = \frac{1}{\lambda^{i-1}c} y_i^d$, and it is a cyclic Galois extension of F of degree d. The family $1_{K_1} = \frac{1}{c} y_1^d, 1_{K_2} = \frac{1}{\lambda c} y_2^d, \dots, 1_{K_r} = \frac{1}{\lambda^{r-1}c} y_r^d$ is a complete system of orthogonal idempotents of K_b'.

Denote by $\overline{\sigma}$ the algebra automorphism of $F[Y]$ such that $\overline{\sigma}(Y) = \varepsilon Y$, which induces the automorphism σ of $K_b = F[Y]/(Y^s - b)$; thus $\sigma(\hat{f}) = \widehat{\overline{\sigma}(f)}$ for any $f \in F[Y]$. We see that $\overline{\sigma}(g_i) = \lambda^{-1} g_{i+1}$ for any i.

Lemma 3.5. *For each $1 \leq i \leq r$ let $h_i = \frac{1}{c^{r-1}} \prod_{\substack{1 \leq j \leq r \\ j \neq i}} (\frac{1}{\lambda^{i-1} - \lambda^{j-1}} g_j)$. Then $\pi_i(h_i) = 1$ and $\pi_j(h_i) = 0$ for any $j \neq i$.*

Proof. Let $P(Z) = \prod_{\substack{0 \leq j \leq r-1 \\ j \neq i-1}} (Z - \lambda^j c) \in F[Z]$. Then $P(\lambda^{i-1}c) = c^{r-1} \prod_{\substack{0 \leq j \leq r-1 \\ j \neq i-1}} (\lambda^{i-1} - \lambda^j)$, so $P(Z) = (Z - \lambda^{i-1}c)Q(Z) + c^{r-1} \prod_{\substack{0 \leq j \leq r-1 \\ j \neq i-1}} (\lambda^{i-1} - \lambda^j)$ for some $Q \in F[Z]$. For $Z = Y^d$ and after dividing by $c^{r-1} \prod_{\substack{0 \leq j \leq r-1 \\ j \neq i-1}} (\lambda^{i-1} - \lambda^j)$ we obtain $h_i = g_i H(Y) + 1$ for some $H \in F[Y]$, which shows that $\pi_i(h_i) = 1$. It is clear that $\pi_j(h_i) = 0$ for any $j \neq i$. □

Lemma 3.6. $\overline{\sigma}(h_i) = h_{i+1}$ *for any i.*

Proof. We have that

$$\begin{aligned}
\overline{\sigma}(h_i) &= \frac{1}{c^{r-1} \prod_{\substack{1 \leq j \leq r \\ j \neq i}} (\lambda^{i-1} - \lambda^{j-1})} \prod_{\substack{1 \leq j \leq r \\ j \neq i}} \overline{\sigma}(g_j) \\
&= \frac{1}{c^{r-1} \prod_{\substack{1 \leq j \leq r \\ j \neq i}} (\lambda^{i-1} - \lambda^{j-1})} \cdot \lambda^{-(r-1)} \prod_{\substack{1 \leq j \leq r \\ j \neq i+1}} g_j \\
&= \frac{1}{c^{r-1} \prod_{\substack{1 \leq j \leq r \\ j \neq i}} (\lambda^{i} - \lambda^{j})} \prod_{\substack{1 \leq j \leq r \\ j \neq i+1}} g_j \\
&= \frac{1}{c^{r-1} \prod_{\substack{1 \leq j \leq r \\ j \neq i+1}} (\lambda^{i} - \lambda^{j-1})} \prod_{\substack{1 \leq j \leq r \\ j \neq i+1}} g_j \\
&= h_{i+1}. \quad \square
\end{aligned}$$

The automorphism σ of K_b induces an automorphism $\tilde{\sigma} = \varphi \sigma \varphi^{-1}$ of K_b'. Taking into account Lemma 3.5 and Lemma 3.6, we see that

$$\tilde{\sigma}(y_i) = \tilde{\sigma}(\pi_1(Y h_i), \dots, \pi_r(Y h_{i+1}))$$

$$\begin{aligned}
&= \varphi\sigma(\widehat{Yh_i})\\
&= \varphi(\widehat{\overline{\sigma}(Yh_i)})\\
&= \varphi(\widehat{\varepsilon Yh_{i+1}})\\
&= \varepsilon(\pi_1(Yh_{i+1}),\dots,\pi_r(Yh_{i+1}))\\
&= \varepsilon y_{i+1}.
\end{aligned}$$

Then $\tilde{\sigma}(\frac{1}{\lambda^{i-1}c}y_i^d) = \frac{1}{\lambda^i c}y_{i+1}^d$, and $\tilde{\sigma}$ induces an F-isomorphism between K_i and K_{i+1}. We conclude that we have algebra isomorphisms $D_2(F,\varepsilon,a,b) \cong K_b[X,\sigma]/(X^s - a) \cong K_b'[X,\tilde{\sigma}]/(X^s - a)$, and the latter one has a presentation with generators $y_1,\dots,y_r,x$, subject to the relations

$$\begin{gathered}
y_iy_j = 0 \text{ for } i \neq j,\ y_i^{d+1} = \lambda^{i-1}cy_i,\\
\frac{1}{c}y_1^d + \frac{1}{\lambda c}y_2^d + \cdots + \frac{1}{\lambda^{r-1}c}y_r^d = 1,\\
xy_i = \varepsilon y_{i+1}x,\ x^s = a.
\end{gathered}$$

Let us note that $\tilde{\sigma}^r(y_i) = \varepsilon^r y_i$ for any i, so the restriction of $\tilde{\sigma}^r$ to K_i is an F-automorphism of order d, thus a generator of the Galois group $\mathrm{Gal}(K_i/F)$.

At this point, since F embeds differently into $K_1,\dots,K_r$ and K_b', we will regard $N_{K_1/F},\dots,N_{K_r/F}$ and $N_{K_b'/F}$ as taking values in $K_1,\dots,K_r$ and K_b', respectively, rather than in F.

Lemma 3.7. *Let $v = v_1 + \cdots + v_r \in K_b'$, where $v_1 \in K_1,\dots,v_r \in K_r$. Then*

$$\begin{aligned}
N_{K_b'/F}(v) = N_{K_1/F}(v_1\tilde{\sigma}(v_r)\cdots\tilde{\sigma}^{r-1}(v_2)) + \tilde{\sigma}(N_{K_1/F}(v_1\tilde{\sigma}(v_r)\cdots\tilde{\sigma}^{r-1}(v_2)))\\
+\cdots+\tilde{\sigma}^{r-1}(N_{K_1/F}(v_1\tilde{\sigma}(v_r)\cdots\tilde{\sigma}^{r-1}(v_2))).
\end{aligned}$$

Proof. For each i we have $\tilde{\sigma}^i(v) = \tilde{\sigma}^i(v_1) + \cdots + \tilde{\sigma}^i(v_r)$, and $\tilde{\sigma}^i(v_1) \in K_{i+1},\dots,\tilde{\sigma}^i(v_r) \in K_{i+r}$ (remember that we look at the indices i modulo r). As $K_iK_j = 0$ for $i \neq j$, a product of elements in K_b' is the sum of the products of the components in K_1, respectively $K_2,\dots,K_r$, of those elements. Thus the component in K_1 of $v\tilde{\sigma}(v)\cdots\tilde{\sigma}^{s-1}(v)$, denote it by L, is

$$\begin{aligned}
L &= (v_1\tilde{\sigma}^r(v_1)\cdots\tilde{\sigma}^{r(d-1)}(v_1)) \cdot (\tilde{\sigma}(v_r)\tilde{\sigma}^{r+1}(v_r)\cdots\tilde{\sigma}^{r(d-1)+1}(v_r)) \cdot\\
&\quad \cdots \cdot (\tilde{\sigma}^{r-1}(v_2)\tilde{\sigma}^{2r-1}(v_2)\cdots\tilde{\sigma}^{r(d-1)+r-1}(v_2))\\
&= N_{K_1/F}(v_1\tilde{\sigma}(v_r)\cdots\tilde{\sigma}^{r-1}(v_2)).
\end{aligned}$$

On the other hand, $N_{K_b'/F}(v) = \alpha \cdot 1_{K_b'} = \alpha \cdot 1_{K_1} + \cdots + \alpha \cdot 1_{K_r}$ for some $\alpha \in F$, so $L = \alpha \cdot 1_{K_1}$, and then $\alpha \cdot 1_{K_2} = \alpha \cdot \tilde{\sigma}(1_{K_1}) = \tilde{\sigma}(L)$, and so on, which shows that $N_{K_b'/F}(v) = L + \tilde{\sigma}(L) + \cdots + \tilde{\sigma}^{r-1}(L)$. □

Corollary 3.8. *Let $\alpha \in F^*$. Then there exists $v \in K_b'$ such that $N_{K_b'/F}(v) = \alpha \cdot 1_{K_b'}$ if and only if there exists $u \in K_1$ such that $N_{K_1/F}(u) = \alpha \cdot 1_{K_1}$.*

Proof. If $N_{K_b'/F}(v) = \alpha \cdot 1_{K_b'}$ for some $v = v_1 + \cdots + v_r$, with $v_i \in K_i$, then by Lemma 3.7 we have $N_{K_1/F}(u) = \alpha \cdot 1_{K_1}$, where $u = v_1\tilde{\sigma}(v_r)\cdots\tilde{\sigma}^{r-1}(v_2) \in K_1$.

Conversely, if $N_{K_1/F}(u) = \alpha \cdot 1_{K_1}$ for some $u \in K_1$, let $v = u + 1_{K_2} + \cdots + 1_{K_r} \in K_b'$. The same lemma shows that $N_{K_b'/F}(v) = L + \tilde{\sigma}(L) + \cdots + \tilde{\sigma}^{r-1}(L)$, where $L = N_{K_1/F}(u) = \alpha \cdot 1_{K_1}$. Now we get that $N_{K_b'/F}(v) = \alpha \cdot 1_{K_b'}$. □

Lemma 3.9. *Let $z = u_0 + u_1 x + \cdots + u_{s-1}x^{s-1}$ be a non-zero element of $K_b'[X, \tilde{\sigma}]/(X^s - a)$ such that $u_0, u_1, \ldots, u_{s-1} \in K_1$. Then the set $\mathcal{B}(z) = \{y_i^j x^{i-1} z \mid 1 \le i \le r,\ 0 \le j \le d-1\}$ is linearly independent over F.*

Proof. Let $\sum_{\substack{1\le i\le r\\ 0\le j\le d-1}} \alpha_{ij} y_i^j x^{i-1} z = 0$ for some $\alpha_{ij} \in F$. Then $\sum_{1\le i\le r}\left(\sum_{0\le j\le d-1}\alpha_{ij}y_i^j\right)x^{i-1}z = 0$, $\sum_{0\le j\le d-1}\alpha_{ij}y_i^j \in K_i$ and $x^{i-1}z = \tilde{\sigma}^{i-1}(u_0)x^{i-1} + \tilde{\sigma}^{i-1}(u_1)x^i + \cdots + \tilde{\sigma}^{i-1}(u_{s-1})x^{s+i-2}$ is a linear combination of $1, x, \ldots, x^{s-1}$ with all coefficients in K_i. As $K_1, \ldots, K_r$ are in a direct sum, we must have $\left(\sum_{0\le j\le d-1}\alpha_{ij}y_i^j\right)x^{i-1}z = 0$ for any i, which means that $\left(\sum_{0\le j\le d-1}\alpha_{ij}y_i^j\right)\tilde{\sigma}^{i-1}(u_k) = 0$ for any i and k. Fix some i. Since not all $\tilde{\sigma}^{i-1}(u_k)$ are zero and K_i is a field, $\sum_{0\le j\le d-1}\alpha_{ij}y_i^j$ must be zero, and so $\alpha_{ij} = 0$ for any j. □

Proposition 3.10. *If $K_b'[X, \tilde{\sigma}]/(X^s - a)$ has a left ideal of dimension s, then there exists $u \in K_1$ such that $N_{K_1/F}(u) = a \cdot 1_{K_1}$.*

Proof. Let I be a left ideal of dimension s in $K_b'[X, \tilde{\sigma}]/(X^s - a)$, and let $w \in I$, $w \ne 0$. Since $w = 1_{K_1} \cdot w + \cdots + 1_{K_r} \cdot w$, there is $1 \le m \le r$ such that $1_{K_m} \cdot w \ne 0$. Since x is invertible, we also have $x^{r-m+1}1_{K_m} \cdot w \in I \setminus \{0\}$. Since $x^{r-m+1}1_{K_m} = \tilde{\sigma}^{r-m+1}(1_{K_m})x^{r-m+1} = 1_{K_1}x^{r-m+1}$ it follows that $z = 1_{K_1} \cdot (x^{r-m+1}w) \in I \setminus \{0\}$, which shows that $z = u_0 + u_1 x + \cdots + u_{s-1}x^{s-1}$ for some $u_0, u_1, \ldots, u_{s-1} \in K_1$, not all zero. By Lemma 3.9, $\mathcal{B}(z)$ is a linear independent set with s elements, thus it is a basis of I. Hence $x^r z$ is a linear combination over F of the elements of $\mathcal{B}(z)$. As

$$\begin{aligned} x^r z &= \tilde{\sigma}^r(u_0)x^r + \tilde{\sigma}^r(u_1)x^{r+1} + \cdots + \tilde{\sigma}^r(u_{s-1})x^{r+s-1} \\ &= a\tilde{\sigma}^r(u_{s-r}) + \cdots + a\tilde{\sigma}^r(u_{s-1})x^{r-1} + \tilde{\sigma}^r(u_0)x^r + \cdots + \tilde{\sigma}^r(u_{s-1-r})x^{s-1}, \end{aligned}$$

we see that the coefficient of each x^t in $x^r z$ lies in K_1, so then $x^r z$ is a linear combination over F of only the elements $z, y_1 z, \ldots, y_1^{d-1}z$ of $\mathcal{B}(z)$. This means that $x^r z = uz$ for some $u \in K_1$. Obviously, $u \ne 0$, since $z \ne 0$ and x is invertible.

Pick some $0 \leq i_0 \leq s-1$ such that $u_{i_0} \neq 0$, and let $0 \leq i \leq r-1$ which is congruent to i_0 modulo r. Since

$$uz = uu_0 + \cdots + uu_{r-1}x^{r-1} + uu_r x^r + \cdots + uu_{s-1}x^{s-1},$$

if we equate the coefficients of $x^i, x^{i+r}, \ldots, x^{i+(d-1)r}$ in the equality $x^r z = uz$ (by taking into account the standard representation as a linear combination of $1, x, \ldots, x^{s-1}$ with coefficients in K_1), we obtain

$$\begin{aligned} uu_i &= a\tilde{\sigma}^r(u_{i+(d-1)r}) \\ uu_{i+r} &= \tilde{\sigma}^r(u_i) \\ uu_{i+2r} &= \tilde{\sigma}^r(u_{i+r}) \\ &\cdots\cdots\cdots \\ uu_{i+(d-2)r} &= \tilde{\sigma}^r(u_{i+(d-3)r}) \\ uu_{i+(d-1)r} &= \tilde{\sigma}^r(u_{i+(d-2)r}). \end{aligned}$$

Since $u \in K_1 \setminus \{0\}$, it is invertible, and as $u_{i_0} \neq 0$ and $i_0 = i + tr$ for some t, we get that all $u_i, u_{i+r}, \ldots, u_{i+(d-1)r}$ are non-zero. Now in the sequence of equalities above keep the last equation as it is, apply $\tilde{\sigma}^r$ to the penultimate equation, and so on, up to $\tilde{\sigma}^{(d-2)r}$ to the second equation and $\tilde{\sigma}^{(d-1)r}$ to the first one, and obtain

$$\begin{aligned} uu_{i+(d-1)r} &= \tilde{\sigma}^r(u_{i+(d-2)r}) \\ \tilde{\sigma}^r(u)\tilde{\sigma}^r(u_{i+(d-2)r}) &= \tilde{\sigma}^{2r}(u_{i+(d-3)r}) \\ &\cdots\cdots\cdots \\ \tilde{\sigma}^{(d-3)r}(u)\tilde{\sigma}^{(d-3)r}(u_{i+2r}) &= \tilde{\sigma}^{(d-2)r}(u_{i+r}) \\ \tilde{\sigma}^{(d-2)r}(u)\tilde{\sigma}^{(d-2)r}(u_{i+r}) &= \tilde{\sigma}^{(d-1)r}(u_i) \\ \tilde{\sigma}^{(d-1)r}(u)\tilde{\sigma}^{(d-1)r}(u_i) &= a\tilde{\sigma}^{dr}(u_{i+(d-1)r}). \end{aligned}$$

If we multiply these equations, take into account that $\tilde{\sigma}^{dr}$ is the identity map, and cancel the matching factors, we find that $u\tilde{\sigma}^r(u)\tilde{\sigma}^{2r}(u)\cdots\tilde{\sigma}^{(d-1)r}(u) = a \cdot 1_{K_1}$, i.e., $N_{K_1/F}(u) = a \cdot 1_{K_1}$. □

Now an immediate consequence of Corollary 3.8 and Proposition 3.10 is the converse of Proposition 3.2.

Proposition 3.11. *If $D_2(F, \varepsilon, a, b) \cong \mathrm{M}_s(F)$, then $a \in N_{K_b/F}(K_b)$.*

Note that by reversing the roles of x and y in the generating relations of $D_2(F, \varepsilon, a, b)$, we get that $D_2(F, \varepsilon, a, b) \cong D_2(F, \varepsilon^{-1}, b, a)$ (as algebras). Then an immediate consequence of Proposition 3.11 is that for $a, b \in F^*$, we have $a \in N_{K_b/F}(K_b)$ if and only if $b \in N_{K_a/F}(K_a)$.

4. Classification of the graded algebras $D_2(F, \varepsilon, a, b)$

In this section we classify the $C_s \times C_s$ - graded algebras of type $D_2(F, \varepsilon, a, b)$. We look first at isomorphism types.

Proposition 4.1. *Let ε and μ be primitive s-th roots of unity in F, and let $a, b, c, d \in F^*$. Then $D_2(F, \varepsilon, a, b) \cong D_2(F, \mu, c, d)$ as $C_s \times C_s$ - graded algebras if and only if $\mu = \varepsilon$ and $a/c,\ b/d \in (F^*)^s$.*

Proof. Let $f : D_2(F, \varepsilon, a, b) \to D_2(F, \mu, c, d)$ be an isomorphism of graded algebras. As $x \in D_2(F, \varepsilon, a, b)_\rho$, we get that $f(x) \in D_2(F, \mu, c, d)_\rho$, so $f(x) = \alpha x$ for some $\alpha \in F^*$. Similarly, $f(y) = \beta y$ for some $\beta \in F^*$. Apply f to the relation $xy = \varepsilon yx$ in $D_2(F, \varepsilon, a, b)$, and get that $\alpha\beta xy = \alpha\beta\varepsilon yx$ in $D_2(F, \mu, c, d)$. This shows that $\varepsilon = \mu$. Next apply f to $x^s = a$, and get that $\alpha^s x^s = a$, or $\alpha^s c = a$, which shows that $a/c \in (F^*)^s$. Similarly, $b/d \in (F^*)^s$.

For the converse, we see that if $a/c = \alpha^s$ and $b/d = \beta^s$ with $\alpha, \beta \in F^*$, then the algebra map $f : D_2(F, \varepsilon, a, b) \to D_2(F, \mu, c, d)$ such that $f(x) = \alpha x$ and $f(y) = \beta y$ is an isomorphism of graded algebras. □

Corollary 4.2. *The isomorphism types of $C_s \times C_s$ - graded algebras of type $D_2(F, \varepsilon, a, b)$ are in bijection to the set $U(\mathbb{Z}_s) \times F^*/(F^*)^s \times F^*/(F^*)^s$.*

Next we classify the considered class of algebras up to equivalence. Let us first introduce a group action • whose orbits will classify the equivalence classes. We denote by $\overline{z}$ the class of an element $z \in F^*$ modulo $(F^*)^s$. Also, we denote by $\hat{i}$ the class of an integer i modulo s.

Lemma 4.3. *The group $\mathrm{SL}_2(\mathbb{Z}_s)$ acts on the set $F^*/(F^*)^s \times F^*/(F^*)^s$ by*

$$\begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} \bullet (\overline{a}, \overline{b}) = (\overline{(-1)^{(s-1)ij} a^i b^j}, \overline{(-1)^{(s-1)k\ell} a^k b^\ell}).$$

Proof. We first show that the action is well defined. It is clear by the definition that the definition depends only on the classes of a and b modulo $(F^*)^s$, so it suffices to show that for integers i and j, $(-1)^{(s-1)ij}$ depends only on the classes of i and j modulo s. For this, we see that if $p, q \in \mathbb{Z}$, then $(-1)^{(s-1)(i+ps)(j+qs)} = (-1)^{(s-1)ij} \cdot (-1)^{(s-1)s(pj+iq+pqs)} = (-1)^{(s-1)ij}$ since $s(s-1)$ is even.

Now if $\begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix}, \begin{bmatrix} \hat{i'} & \hat{j'} \\ \hat{k'} & \hat{\ell'} \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}_s)$, then

$$\begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} \bullet \left(\begin{bmatrix} \hat{i'} & \hat{j'} \\ \hat{k'} & \hat{\ell'} \end{bmatrix} \bullet (\overline{a}, \overline{b}) \right) = \begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} \bullet \big(\overline{(-1)^{(s-1)i'j'} a^{i'} b^{j'}}, \overline{(-1)^{(s-1)k'\ell'} a^{k'} b^{\ell'}}\big)$$

$$= \big(\overline{(-1)^{(s-1)(ij+i'j'i+k'\ell'j)} a^{ii'+jk'} b^{ij'+j\ell'}}, \overline{(-1)^{(s-1)(k\ell+i'j'k+k'\ell'\ell)} a^{ki'+\ell k'} b^{kj'+\ell\ell'}}\big),$$

while

$$\left(\begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} \cdot \begin{bmatrix} \hat{i'} & \hat{j'} \\ \hat{k'} & \hat{\ell'} \end{bmatrix} \right) \bullet (\overline{a}, \overline{b}) = \begin{bmatrix} \widehat{ii' + jk'} & \widehat{ij' + j\ell'} \\ \widehat{ki' + \ell k'} & \widehat{kj' + \ell\ell'} \end{bmatrix} \bullet (\overline{a}, \overline{b})$$

$$= \big(\overline{(-1)^{(s-1)(ii'+jk')(ij'+j\ell')} a^{ii'+jk'} b^{ij'+j\ell'}}, \overline{(-1)^{(s-1)(ki'+\ell k')(kj'+\ell\ell')} a^{ki'+\ell k'} b^{kj'+\ell\ell'}}\big).$$

We have that

$$\begin{aligned} &(s-1)(ii'+jk')(ij'+j\ell') - (s-1)(ij+i'j'i+k'\ell'j) \\ &= (s-1)(i^2i'j' + j^2k'\ell' + ijk'j' + iji'\ell' - ij - i'j'i - k'\ell'j) \\ &= (s-1)i'j'(i^2-i) + (s-1)k'\ell'(j^2-j) + 2(s-1)ijk'j' + (s-1)ij(i'\ell' - k'j' - 1), \end{aligned}$$

which is even, as so are $i^2 - i$ and $j^2 - j$, and the last term is also even, since $i'\ell' - k'j' = Ns + 1$ for some integer N, and then $(s-1)ij(i'\ell' - k'j' - 1) = s(s-1)ijN$. Thus the first components of the two elements in $F^*/(F^*)^s \times F^*/(F^*)^s$ are equal, and similarly their second components coincide. We conclude that the action is indeed associative. □

Proposition 4.4. *Let ε and μ be primitive s-th roots of unity in F, and let $a, b, c, d \in F^*$. Then $D_2(F, \varepsilon, a, b) \equiv D_2(F, \mu, c, d)$ as $C_s \times C_s$ - graded algebras if and only if there is $\begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}_s)$ such that*

$$\mu = \varepsilon^{i\ell - jk},\ (-1)^{(s-1)ij} a^i b^j c^{-1} \in (F^*)^s,\ (-1)^{(s-1)k\ell} a^k b^\ell d^{-1} \in (F^*)^s. \tag{4.1}$$

Proof. Suppose that $D_2(F, \varepsilon, a, b) \equiv D_2(F, \mu, c, d)$. Therefore there is an automorphism θ of $C_s \times C_s$ such that $D_2(F, \mu, c, d) \cong D_2(F, \varepsilon, a, b)^\theta$. The automorphism θ is such that θ^{-1} is of the form $\theta^{-1}(\rho) = \rho^i \omega^j$ and $\theta^{-1}(\omega) = \rho^k \omega^\ell$ for some integers i, j, k, ℓ such that $\begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}_s)$.

Let $f : D_2(F, \mu, c, d) \to D_2(F, \varepsilon, a, b)^\theta$ be an isomorphism of graded algebras. Then $f(x) = \alpha x^i y^j$ and $f(y) = \beta x^k y^\ell$ for some $\alpha, \beta \in F^*$. Apply f to $xy = \mu yx$ and get $\alpha\beta x^i y^j x^k y^\ell = \alpha\beta\mu x^k y^\ell x^i y^j$ in $D_2(F, \varepsilon, a, b)$, which implies that $\varepsilon^{ij+\ell(i+k)} = \mu\varepsilon^{k\ell+j(i+k)}$, or $\mu = \varepsilon^{i\ell - jk}$.

Next, if we apply f to $x^s = c$, we see that $\alpha^s(x^i y^j)^s = c$. Using $xy = \varepsilon yx$ to move all the y's at the beginning, we find $\alpha^s \varepsilon^{ij+2ij+\cdots+sij} y^{sj} x^{si} = c$, or $\alpha^s \varepsilon^{ijs(s+1)/2} a^i b^j = c$.

We have that $\varepsilon^{s(s+1)/2} = (-1)^{s-1}$. Indeed, if s is odd, then $\varepsilon^{s(s+1)/2} = (\varepsilon^s)^{(s+1)/2} = 1 = (-1)^{s-1}$, while if s is even (in this case the characteristic of F cannot be 2), say $s = 2t$ for some integer t, then $\varepsilon^{s(s+1)/2} = \varepsilon^{t(2t+1)} = \varepsilon^t$. As $(\varepsilon^t)^2 = \varepsilon^s = 1$ and $\varepsilon^t \neq 1$, we get that $\varepsilon^t = -1 = (-1)^{s-1}$. Thus we have $(-1)^{(s-1)ij} a^i b^j c^{-1} = \alpha^{-s} \in (F^*)^s$.

In a similar way, applying f to $y^s = b$ we obtain $(-1)^{(s-1)k\ell} a^k b^\ell d^{-1} = \beta^{-s} \in (F^*)^s$.

Conversely, if the relations (4.1) are satisfied for some $\begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}_s)$, say that $(-1)^{(s-1)ij} a^i b^j c^{-1} = \alpha^{-s}$ and $(-1)^{(s-1)k\ell} a^k b^\ell d^{-1} = \beta^{-s}$, where $\alpha, \beta \in F$, then it is straightforward to check that $f : D_2(F, \mu, c, d) \cong D_2(F, \varepsilon, a, b)^\theta$ given by $f(x) = \alpha x^i y^j$ and $f(y) = \beta x^k y^\ell$ is an isomorphism of graded algebras, where θ is the automorphism of $C_s \times C_s$ associated with $\begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix}$ as above. □

Corollary 4.5. *Fix some primitive s-th root of unity, ε, in F. The following assertions hold.*

(i) *For any primitive s-th root of unity μ, and any $c, d \in F^*$, there exist $a, b \in F^*$ such that $D_2(F, \mu, c, d) \equiv D_2(F, \varepsilon, a, b)$.*

(ii) *If $a, b, c, d \in F^*$, then $D_2(F, \varepsilon, a, b) \equiv D_2(F, \varepsilon, c, d)$ if and only if there exists $\begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}_s)$ such that $(\overline{c}, \overline{d}) = \begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} \bullet (\overline{a}, \overline{b})$.*

Proof. (i) We have $\mu = \varepsilon^r$ for some $\hat{r} \in U(\mathbb{Z}_s)$. Let $\hat{t}$ be the inverse of $\hat{r}$ in $\mathbb{Z}_s$. If $a = c^t$ and $b = d$, then $a^r c^{-1} = c^{tr-1} \in (F^*)^s$ and $bd^{-1} = 1 \in (F^*)^s$, and so the relations in (4.1) are satisfied for the matrix $\begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} = \begin{bmatrix} \hat{r} & \hat{0} \\ \hat{0} & \hat{1} \end{bmatrix}$.

(ii) By Proposition 4.4 we have that $D_2(F, \varepsilon, a, b) \equiv D_2(F, \varepsilon, c, d)$ if and only if there exists $\begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}_s)$ such that $\varepsilon = \varepsilon^{i\ell - jk}$, which means that $\begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}_s)$, and $(-1)^{(s-1)ij} a^i b^j c^{-1}, (-1)^{(s-1)k\ell} a^k b^\ell d^{-1} \in (F^*)^s$. Hence, $(\overline{c}, \overline{d}) = \begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} \bullet (\overline{a}, \overline{b})$. □

Corollary 4.6. *The equivalence classes of $C_s \times C_s$ - graded algebras of the type $D_2(F, \varepsilon, a, b)$, where ε is an arbitrary s-th root of unity in F, and $a, b \in F^*$, are in bijection to the orbits of the action $\bullet$ of the group $\mathrm{SL}_2(\mathbb{Z}_s)$ on the set $F^*/(F^*)^s \times F^*/(F^*)^s$.*

Now we look at all possible $C_s \times C_s$ - gradings induced on the algebra $M_s(F)$ from graded algebras of type $D_2(F, \varepsilon, a, b)$.

Let $\mathcal{E}(F,s)$ be the subset of $F^*/(F^*)^s \times F^*/(F^*)^s$ consisting of all pairs $(\overline{a},\overline{b})$ with the property that $a \in N_{K_b/F}(K_b)$, or equivalently, that $b \in N_{K_a/F}(K_a)$; we have seen in Section 3 that this is the same as $D_2(F,\varepsilon,a,b) \cong \mathrm{M}_s(F)$, where ε is any primitive s-th root of unity. Clearly this property depends only on the classes $\overline{a},\overline{b}$ of a,b modulo $(F^*)^s$, and it does not depend on the choice of ε.

Also, we see that $\mathcal{E}(F,s)$ is an $\mathrm{SL}_2(\mathbb{Z}_p)$-subset of $F^*/(F^*)^s \times F^*/(F^*)^s$. Indeed, let $(\overline{a},\overline{b}) \in \mathcal{E}(F,s)$, thus $D_2(F,\varepsilon,a,b) \cong \mathrm{M}_s(F)$ if ε is a primitive s-th root of unity. Then if $(\overline{c},\overline{d}) = \begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} \bullet (\overline{a},\overline{b})$ for some $\begin{bmatrix} \hat{i} & \hat{j} \\ \hat{k} & \hat{\ell} \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}_s)$, then $D_2(F,\varepsilon,a,b) \equiv D_2(F,\varepsilon,c,d)$, in particular $D_2(F,\varepsilon,c,d) \cong \mathrm{M}_s(F)$, so $(\overline{c},\overline{d}) \in \mathcal{E}(F,s)$. Now an immediate consequence of Corollaries 4.2 and 4.6 is

Corollary 4.7.

(1) *The isomorphism types of $C_s \times C_s$ - graded algebras induced on $\mathrm{M}_s(F)$ from graded algebras of type $D_2(F,\varepsilon,a,b)$ are in bijection to the set $U(\mathbb{Z}_s) \times \mathcal{E}(F,s)$.*

(2) *The equivalence classes of $C_s \times C_s$ - graded algebras induced on $\mathrm{M}_s(F)$ from graded algebras of type $D_2(F,\varepsilon,a,b)$ are in bijection to the orbits of the action $\bullet$ of the group $\mathrm{SL}_2(\mathbb{Z}_s)$ on the set $\mathcal{E}(F,s)$.*

5. Gradings on matrices of prime size

The aim of this section is to classify all gradings on the algebra $\mathrm{M}_p(F)$ by all possible groups, where F is an arbitrary field and p is a prime number. We first recall a general construction.

If $A = \bigoplus_{g\in G} A_g$ is a G-graded algebra, n is a positive integer and $\sigma_1,\dots,\sigma_n \in G$, then there is a G-grading on the matrix algebra $\mathrm{M}_n(A)$ whose homogeneous component of degree g is

$$\begin{bmatrix} A_{\sigma_1 g\sigma_1^{-1}} & A_{\sigma_1 g\sigma_2^{-1}} & \dots & A_{\sigma_1 g\sigma_n^{-1}} \\ A_{\sigma_2 g\sigma_1^{-1}} & A_{\sigma_2 g\sigma_2^{-1}} & \dots & A_{\sigma_2 g\sigma_n^{-1}} \\ \dots & \dots & \dots & \dots \\ A_{\sigma_n g\sigma_1^{-1}} & A_{\sigma_n g\sigma_2^{-1}} & \dots & A_{\sigma_n g\sigma_n^{-1}} \end{bmatrix}.$$

We denote this G-graded algebra by $\mathrm{M}_n(A)(\sigma_1,\dots,\sigma_n)$.

We also recall that a grading on the matrix algebra $\mathrm{M}_n(F)$ is called a good grading if all matrix units e_{ij}, with $1 \le i,j \le n$, are homogeneous elements. A G-grading on $\mathrm{M}_n(F)$ is good if and only if it is isomorphic to $\mathrm{M}_n(F)(\sigma_1,\dots,\sigma_n)$ for some $\sigma_1,\dots,\sigma_n \in G$, where F is regarded as a G-graded algebra with the trivial grading, see [12, Propositions 2.10.5 and 9.2.5]. The isomorphism types of good G-gradings on $\mathrm{M}_n(F)$ are determined in [4].

Theorem 5.1. *Let F be a field and let p be a prime number. If G is a group, then any G-grading on the algebra $\mathrm{M}_p(F)$ is isomorphic to one of the following three types:*

- **(I)** *A good G-grading.*
- **(II)** *$D_1(K/F,\sigma,1)^\theta$ for a Galois extension K/F of degree p, a generator σ of $\mathrm{Gal}(K/F)$, and a group embedding $\theta : C_p \to G$. The support of such a grading is $\theta(C_p) \cong C_p$. For a fixed embedding θ, the equivalence classes of such gradings are in bijection to the set of isomorphism types of Galois extensions of degree p of F.*
- **(III)** *$D_2(F,\varepsilon,a,b)^\theta$ for a p-th root of unity $\varepsilon \neq 1$, elements $a,b \in F^*$ such that $(\overline{a},\overline{b}) \in \mathcal{E}(F,p)$, and a group embedding $\theta : C_p \times C_p \to G$. The support of such a grading is $\theta(C_p \times C_p) \cong C_p \times C_p$. For a fixed embedding θ, the equivalence classes of such gradings $D_2(F,\varepsilon,a,b)^\theta$ are in bijection to the orbits of the $\mathrm{SL}_2(\mathbb{Z}_p)$-action on the set $\mathcal{E}(F,p)$. Gradings of this type do not occur if F does not contain non-trivial p-th roots of unity.*

Proof. Let $R = \mathrm{M}_p(F)$ with a G-grading, where G is an arbitrary group with neutral element e. R is a graded simple and graded artinian algebra. Let V be a simple object in the category of graded left R-modules. Then $\Delta = \mathrm{End}_R(V)$ is a G-graded algebra, whose homogeneous component of degree d is

$$\Delta_d = \{\delta \in \mathrm{End}_R(V) \mid \delta(V_g) \subset V_{gd} \text{ for any } g \in G\}$$

for any $d \in G$. As V is graded simple, Δ is a graded division algebra. Now V is a G-graded right Δ-module with the usual right action $v \cdot \delta = \delta(v)$ for any $v \in V$, $\delta \in \Delta$, and $\mathrm{End}(V_\Delta)$ has a G-grading in a similar way; the homogeneous component of degree d is $\{u \in \mathrm{End}(V_\Delta) \mid u(V_g) \subset V_{dg} \text{ for any } g \in G\}$. By [12, Corollary 4.6.6] or [6, Theorem 2.6] the map $\varphi : R \to \mathrm{End}_\Delta(V)$, $\varphi(r)(v) = rv$ for any $r \in R$ and $v \in V$, is an isomorphism of G-graded algebras. As Δ is a graded division algebra, V has a finite basis over Δ. Denoting by n the number of basis elements and by $\sigma_1,\ldots,\sigma_n$ their degrees, we obtain that $R \cong \mathrm{End}(V_\Delta) \cong \mathrm{M}_n(\Delta)(\sigma_1,\ldots,\sigma_n)$, where the second isomorphism follows from [12, Proposition 2.10.5].

If we equate the dimensions, we get $p^2 = n^2\dim(\Delta)$, so either $n = p$ and $\dim(\Delta) = 1$, or $n = 1$ and $\dim(\Delta) = p^2$.

In the first case we have $\Delta = F$, and then $R \cong \mathrm{M}_p(F)(\sigma_1,\ldots,\sigma_p)$, which is a good grading on $\mathrm{M}_p(F)$.

In the latter case, $R \cong \Delta$, so we have to describe all possible graded division algebra structures on the matrix algebra $\mathrm{M}_p(F)$. We note that for a G-graded division algebra $\Delta = \underset{g\in G}{\oplus} \Delta_g$ the following hold:

- **(i)** Δ_e is a division algebra over F.
- **(ii)** $\mathrm{supp}(\Delta)$ is a subgroup of G.
- **(iii)** If $x \in \Delta_g \setminus \{0\}$, then $\Delta_g = x\Delta_e = \Delta_e x$; in particular, $\dim \Delta_g = \dim \Delta_e$.

As a consequence, $p^2 = \dim(\Delta) = |\mathrm{supp}(\Delta)| \cdot \dim(\Delta_e)$, and we have three possible cases.

Case 1. $|\mathrm{supp}(\Delta)| = 1$ and $\dim(\Delta_e) = p^2$. Then $\Delta = \Delta_e$ is a division algebra, a contradiction with $\Delta = \mathrm{M}_p(F)$.

Case 2. $\mathrm{supp}(\Delta) = p$ and $\dim(\Delta_e) = p$. Pick $z \in \Delta_e \backslash F$. Since Δ_e has prime dimension p, it must be equal to the field obtained by adjoining z to F. Thus Δ_e is a field. Let $\mathrm{supp}(\Delta) = \langle g \rangle$, and pick a non-zero x in Δ_g. Then $\Delta_{g^i} = \Delta_e x^i$ for any $0 \le i \le p-1$, so $\Delta = \Delta_e \oplus \Delta_e x \oplus \cdots \oplus \Delta_e x^{p-1}$.

Let $\sigma : \Delta_e \to \Delta_e$, $\sigma(z) = xzx^{-1}$ for any $z \in \Delta_e$, which is clearly an F-automorphism of Δ_e. Then $\sigma \neq \mathrm{Id}$, since otherwise $xz = zx$ for any $z \in \Delta_e$, and Δ would be commutative; a contradiction. On the other hand, the fixed subfield $\Delta_e^\sigma = \{z \in \Delta_e | zx = xz\} \subset \mathrm{Cen}(\Delta) = F$, showing that $\Delta_e^{\langle \sigma \rangle} = F$, where $\langle \sigma \rangle$ is the subgroup of the finite group $\mathrm{Gal}(\Delta_e/F)$ generated by σ. By Artin's Theorem ([9, Theorem 1.8, page 264]) we get that Δ_e/F is a Galois extension and its Galois group is $\langle \sigma \rangle$. Thus Δ_e/F is a cyclic Galois extension of degree p and σ has order p.

Since $\sigma^p = \mathrm{Id}$, x^p commutes with any element in Δ_e. As it also commutes with x, we must have $x^p \in \mathrm{Cen}(\Delta) = F$. Now if we denote $a = x^p$, and $\Delta_e = K$, a Galois extension of degree p of F, we have that Δ is isomorphic as an algebra to the cyclic algebra $(K/F, \sigma, a)$. As $\Delta \cong \mathrm{M}_p(F)$, a must lie in $N_{K/F}(K^*)$, and then by Proposition 2.1, $D_1(K/F, \sigma, a) \cong D_1(K/F, \sigma, 1)$ as C_s-graded algebras. Hence we have an isomorphism of G-graded algebras $\Delta \cong D_1(K/F, \sigma, 1)^\theta$, where $\theta : C_p \to G$ is the group embedding defined by $\theta(\omega) = g$.

The equivalence classes of such gradings follow from Corollary 2.3.

Case 3. $\mathrm{supp}(\Delta) = p^2$ and $\dim(\Delta_e) = 1$, so $\Delta_e = F$. It is not possible that $\mathrm{supp}(\Delta)$ is cyclic. Indeed, if $\mathrm{supp}(\Delta) = \langle g \rangle \cong C_{p^2}$, pick $x \in \Delta_g \setminus \{0\}$, and then $\Delta_{g^i} = Fx^i$ for any $0 \le i \le p^2 - 1$, showing that Δ is commutative; a contradiction. Thus $\mathrm{supp}(\Delta) \cong C_p \times C_p$. Let $G = \langle g \rangle \times \langle h \rangle$ with g and h of order p. Pick some nonzero $y \in \Delta_g$ and $x \in \Delta_h$. As each nonzero homogeneous component of Δ has dimension 1, we have $\Delta_{g^i h^j} = Fy^i x^j$ for any $0 \le i, j \le p-1$. Now $xy \in \Delta_{gh}$, so $xy = \varepsilon yx$ for some $\varepsilon \in F^*$. If $\varepsilon = 1$, it follows that Δ is commutative; a contradiction. Thus $\varepsilon \neq 1$. Since $x^p \in \Delta_{g^p} = \Delta_e = F$, we have $x^p y = yx^p$. As $xy = \varepsilon yx$, we get $x^p y = \varepsilon^p y x^p$, showing that $\varepsilon^p = 1$, so ε is a primitive p-th root of unity in F. In the case F does not contain such roots, we get that gradings of this type do not exist. Now $x^p,\ y^p \in \Delta_e = F$, and denote $x^p = a,\ y^p = b$, where $a, b \in F^*$. These show that $\Delta \cong D_2(F, \varepsilon, a, b)^\theta$, where $\theta : C_p \times C_p \to G$ is the group embedding defined by $\theta(\omega) = g$ and $\theta_1(\rho) = h$. Moreover, $(\overline{a}, \overline{b}) \in \mathcal{E}(F, p)$, since $D_2(F, \varepsilon, a, b) \cong \mathrm{M}_p(F)$.

If $H \cong C_p \times C_p$ is a subgroup of G, $\theta_1, \theta_2 : C_p \times C_p \to H$ are group isomorphisms (i.e., embeddings of $C_p \times C_p$ into the same subgroup H of G), and $(\overline{a}, \overline{b}), (\overline{c}, \overline{d}) \in \mathcal{E}(F, p)$, then by Corollary 4.5 we know that $D_2(F, \varepsilon, a, b)^{\theta_1} \equiv D_2(F, \varepsilon, c, d)^{\theta_2}$ if and only if $(\overline{a}, \overline{b})$ and $(\overline{c}, \overline{d})$ lie in the same orbit with respect to the action $\bullet$ of $\mathrm{SL}_2(\mathbb{Z}_p)$, which concludes the proof. □

Declaration of competing interest

There is no competing interest.

Data availability

No data was used for the research described in the article.

Acknowledgements

The second author was supported by a grant of UEFISCDI, project number PN-III-P4-PCE-2021-0282, contract PCE 47/2022.

The authors thank the referee for suggestions which improved the exposition of the paper.

References

[1] Yu.A. Bahturin, S.K. Sehgal, M.V. Zaicev, Group gradings on associative algebra, J. Algebra 241 (2001) 677–698.

[2] Yu.A. Bahturin, M.V. Zaicev, Group gradings on matrix algebras, Can. Math. Bull. 45 (2002) 499–508.

[3] C. Boboc, S. Dăscălescu, Group gradings on $M_3(k)$, Commun. Algebra 35 (2007) 2654–2670.

[4] S. Caenepeel, S. Dăscălescu, C. Năstăsescu, On gradings of matrix algebras and descent theory, Commun. Algebra 30 (2002) 5901–5920.

[5] P.K. Draxl, Skew Fields, London Math. Soc. Lecture Note Series, vol. 81, Cambridge Univ. Press, 1983.

[6] A. Elduque, M. Kochetov, Gradings on Simple Lie Algebras, Math. Surveys and Monographs, vol. 189, AMS, 2013.

[7] R. Khazal, C. Boboc, S. Dăscălescu, Group gradings on $M_2(k)$, Bull. Aust. Math. Soc. 68 (2003) 285–293.

[8] T.Y. Lam, A First Course in Noncommutative Rings, second edition, GTM, vol. 131, Springer Verlag, 2001.

[9] S. Lang, Algebra, revised third edition, GTM, vol. 211, Springer, 2002.

[10] J. Milnor, Introduction to Algebraic K-Theory, Annals of Mathematics Studies, vol. 72, Princeton Univ. Press, 1971.

[11] S. Montgomery, Hopf Algebras and Their Actions on Rings, CBMS Regional Conf. Series in Math., vol. 82, AMS, Providence, RI, 1993.

[12] C. Năstăsescu, F. van Oystaeyen, Methods of Graded Rings, Lecture Notes in Math., vol. 1836, Springer Verlag, 2004.