Bull. Math. Soc. Sc. Math. Roumanie
Tome 49(97) No. 1, 2006, 5–11

Good gradings of matrix algebras by finite abelian groups of prime index

by
Crina Boboc and S. Dăscălescu*

To Professor Ion D. Ion on the occasion of his 70th Birthday

Abstract

A group grading on a matrix algebra $M_m(k)$ is called good if all the matrix units e_{ij} are homogeneous elements. We present a new way to classify good G-gradings by the orbits of a certain action of the group G on a set of G-tuples of non-negative integers, and we use it to count the isomorphism types of good G-gradings on $M_m(k)$ in the case where $G = \mathbf{Z}_p^n$ is a cyclic group of prime index p.

Key Words: Matrix algebra, group graded algebra, good grading.
2000 Mathematics Subject Classification: Primary: 16W50.

1 Introduction and Preliminaries

Let k be a field, A a k-algebra and G a group. A G-grading on A is a decomposition $A = \oplus_{g\in G} A_g$ as a direct sum of k-subspaces of A such that $A_g A_h \subseteq A_{gh}$ for any $g, h \in G$. The elements of $\cup_{g\in G} A_g$ are called homogeneous elements of A. A general open problem is to describe all group gradings of the matrix algebra $M_m(k)$, see [7]. There have been several papers devoted to this problem during the last few years, see [1], [2], [3], [4] and the references cited there. In these works a special class of gradings on a matrix algebra have proved to be of a major importance, namely the good gradings (also called elementary gradings in [1]). A grading on $M_m(k)$ is called good if any matrix unit e_{ij} (the matrix having 1 on the (i,j)-position, and 0 everywhere else) is a homogeneous element. If G is a cyclic group and k is algebraically closed, it is proved in [1], [3] that any grading is isomorphic to a good grading. For gradings by abelian groups, the good gradings play a central role in the classification of all gradings on the matrix algebra, see [1]. We note that good gradings had appeared in [5], [6], where the algebra $M_m(k)$ is viewed as a quotient of the path algebra of the quiver Γ,

*This work was supported by Kuwait University Research Grant No. SM03/05

where Γ is the complete graph on m points, and good gradings on $M_m(k)$ were constructed from weight functions on Γ. The aim of this paper is to give a new description for the isomorphism types of good G-gradings on $M_m(k)$ for an arbitrary group G, and to count explicitly the isomorphism types for the case where $G = \mathbf{Z}_p^n = \mathbf{Z}_p \times \mathbf{Z}_p \times \ldots \times \mathbf{Z}_p$ is a finite abelian group of prime index p. A classification result for the types of good G-gradings on $M_m(k)$ was done in [3], where these types were proved to be in bijection with the orbits of a certain biaction by the symmetric group S_m from the left and G from the right on the set G^m. We give in Section 2 a more effective description of the types of good gradings as the orbits of a certain action of the group G on a set of G-tuples of non-negative integers. Our description makes more accessible the combinatorial computation to count the orbits. Then in Section 3 we use this description to compute the number of isomorphism types of good gradings on $M_m(k)$ by a finite abelian group of prime index $G = \mathbf{Z}_p^n$. The formula is given by a recurrence relation, and in Section 4 we use it to work out the number for specific values of n.

Throughout the paper k will be an arbitrary field. For facts about graded algebras we refer the reader to [8].

2 Good gradings and algebras of endomorphisms

A grading on the matrix algebra $M_m(k)$ is called good if all the matrix units e_{ij} are homogeneous elements. It is proved in [4, Proposition 1.2] that any good grading on the matrix algebra $M_m(k)$ is isomorphic to a graded algebra of the form $END(V)$ for some graded vector space V of dimension m. If V is such a G-graded vector space, let $B = \{v_1, \ldots, v_m\}$ be a basis consisting of homogeneous elements, say of degrees $g_1, \ldots, g_m$. Then the endomorphism algebra $End(V)$ (with the map composition as a multiplication) has a graded algebra structure $End(V) = \oplus_{\sigma \in G} End(V)_\sigma$, where $End(V)_\sigma = \{f \in End(V) | f(V_g) \subseteq V_{\sigma g}$ for any $g \in G\}$. The resulting graded algebra is denoted by $END(V)$. But $End(V)$ is isomorphic to the matrix algebra $M_m(k)$, and the matrix unit e_{ij} corresponds via the isomorphism $M_m(k) \simeq End(V)$ induced by the basis B, to the endomorphism $E_{ij} \in End(V)$ such that $E_{ij}(v_t) = \delta_{tj} v_i$ for any $1 \leq i, j, t \leq m$. Therefore $M_m(k)$ has a G-graded algebra structure such that e_{ij} has degree $g_i g_j^{-1}$.

We consider the set

$$\mathcal{Y}(m, G) = \{(a_g)_{g \in G} | a_g \in \mathbf{Z}, a_g \geq 0 \text{ for any } g \in G, \text{ and } \sum_{g \in G} a_g = m\}$$

The group G acts from the right on the set $\mathcal{Y}(m, G)$ by

$$(a_g)_{g \in G} \cdot h = (a_{gh})_{g \in G}$$

The next results classifies the good G-gradings on $M_m(k)$ in terms of the orbits of this action.

Proposition 2.1. *The isomorphism types of good G-gradings on $M_m(k)$ are in bijective correspondence to the orbits of the right G-set $\mathcal{Y}(m,G)$.*

Proof: A good G-grading on $M_m(k)$ is isomorphic to $END(V)$ for some G-graded vector space V of dimension m. Clearly $\mathcal{Y}(m,G)$ is in bijective correspondence to the set of isomorphism types of G-graded vector spaces $V=\oplus_{g\in G}V_g$ of dimension m, where the correspondence associates to such a V the G-tuple $(\dim(V_g))_{g\in G}$. By [3, Theorem 2.1], if V and W are G-graded vector spaces of dimension m, then the graded algebras $END(V)$ and $END(W)$ are isomorphic if and only if $W\simeq V(\sigma)$ for some $\sigma\in G$. Hence $END(V)$ and $END(W)$ are isomorphic if and only if $\dim(W_g)=\dim(V_{g\sigma})$ for any $g\in G$, i.e. $(\dim(W_g))_{g\in G}=(\dim(V_g))_{g\in G}\cdot\sigma$, and the result follows. □

Remark 2.2. *We can construct explicitly the good grading corresponding to an orbit via the bijective correspondence from Proposition 2.1. Let $(a_g)_{g\in G}\in\mathcal{Y}(m,G)$. For any $g\in G$ let V_g be a vector space of dimension a_g, and consider $V=\oplus_{g\in G}V_g$. Then V is a graded vector space of dimension m, and a basis of V consisting of homogeneous elements has a_g elements of degree g for any $g\in G$. Thus the degrees of the basis elements are $g_1,\ldots,g_m$, where in this sequence we put a_g of g for any $g\in G$ (the order of the arrangement is not important). Then $END(V)$ is isomorphic to $M_m(k)$ with the good grading given by assigning to e_{ij} degree $g_ig_j^{-1}$.*

In [3] the isomorphism types of good G-gradings on $M_m(k)$ are classified by the orbits of the biaction of the symmetric group S_m (by permutation from the left) and G (by translation from the right) on the set G^m. We can describe the bijective correspondence between the orbits of the right G-set $\mathcal{Y}(m,G)$ and the orbits of this biaction. If $z=(g_1,\ldots,g_m)\in G^m$, define $a_g(z)=|\{i|1\le i\le m \text{ and } g_i=g\}|$, which is the number of appearances of g in the G-tuple z. Now define the map $\phi:G^m\to\mathcal{Y}(m,G)$ by $\phi(z)=(a_g(z))_{g\in G}$. Then clearly ϕ induces a bijection between the orbits of the biaction of S_m and G on G^m and the orbits of the right action of G on $\mathcal{Y}(m,G)$.

3 Gradings over finite abelian groups of prime index

In this section $G=\mathbf{Z}_p^n=\mathbf{Z}_p\times\mathbf{Z}_p\times\ldots\times\mathbf{Z}_p$, a finite abelian group of prime index p. The operation on G is additive, so the right action of G on $\mathcal{Y}(m,G)$ is $(a_g)_{g\in G}\cdot h=(a_{g+h})_{g\in G}$. Our aim is to count the orbits of this action.

For any $t\le n$ we denote by $s_{n,t}$ the number of subgroups of order p^t of G.

Lemma 3.1. *For any $1\le t\le n$ we have that*

$$s_{n,t}=\frac{(p^n-1)(p^n-p)\ldots(p^n-p^{t-1})}{(p^t-1)(p^t-p)\ldots(p^t-p^{t-1})}$$

Proof: Regard G as a $\mathbf{Z}_p$-vector space of dimension n. Then a subgroup of order p^t of G is a vector subspace of dimension t. The number of linear independent subsets $\{g_1, g_2, \dots, g_t\}$ with t elements of G is $\frac{1}{t!}(p^n - 1)(p^n - p)\dots(p^n - p^{t-1})$. Indeed, g_1 can be any non-zero element, so there are $p^n - 1$ choices for it. Then g_2 can be anything which is not a scalar multiple of g_1, so it can be selected in $p^n - p$ ways, and so on. In this way any linear independent set with t elements is counted $t!$ times (all the possible permutations of its elements). The same argument shows that a $\mathbf{Z}_p$-vector space of dimension t has $\frac{1}{t!}(p^t - 1)(p^t - p)\dots(p^t - p^{t-1})$ bases, so the same subgroup of order p^t of G is spanned by any of this number of linear independent subsets with t elements of G, and the desired formula follows. □

Lemma 3.2. *The elements of an orbit of $\mathcal{Y}(m, G)$ have the same stabilizer.*

Proof: Let $y, z \in \mathcal{Y}(m, G)$ belong to the same orbit. Then the stabilizers of y and z are conjugate subgroups, and since G is abelian, they must be equal. □

Lemma 3.3. *Let H be a subgroup of order p^{n-t} of G. Then the number of elements of the set $\{z \in \mathcal{Y}(m, G) | z \cdot h = z$ for any $h \in H\}$ is*
(i) $\binom{\frac{m}{p^{n-t}}+p^t-1}{p^t-1}$, if p^{n-t} divides m.
(ii) 0, if p^{n-t} does not divide m.

Proof: Let $z = (a_g)_{g\in G} \in \mathcal{Y}(m, G)$. Then $z \cdot h = z$ for any $h \in H$ if and only if $a_{g+h} = a_g$ for any $g \in G$ and any $h \in H$. This is equivalent to a_g taking the same value for all g's in the same H-coset of G. Since any such coset has p^{n-t} elements, we must have $p^{n-t}|m$ (otherwise such z does not exist). Moreover, defining such a z is equivalent to defining a G/H-tuple of non-negative integers with sum $\frac{m}{p^{n-t}}$, and this can be done in $\binom{\frac{m}{p^{n-t}}+p^t-1}{p^t-1}$ ways. □

If H is a subgroup of G, let $\mathcal{Y}(m, G)_H = \{z \in \mathcal{Y}(m, G) | Stab_G(z) = H\}$. We will need the following.

Lemma 3.4. *Let H and K subgroups of G with $|H| = |K|$. Then $|\mathcal{Y}(m, G)_H| = |\mathcal{Y}(m, G)_K|$.*

Proof: Regarding again G as a $\mathbf{Z}_p$-vector space, we have that H and K are subspaces of the same dimension. Then there exists an automorphism ϕ of G such that $\phi(H) = K$. This induces a bijection $\tilde{\phi} : \mathcal{Y}(m, G) \to \mathcal{Y}(m, G)$ defined by $\tilde{\phi}((a_g)_{g\in G}) = (a_{\phi(g)})_{g\in G}$. Moreover, we have that

$$\begin{aligned}\tilde{\phi}((a_g)_{g\in G}\cdot u) &= \tilde{\phi}((a_{g+u})_{g\in G})\\ &= (a_{\phi(g+u)})_{g\in G}\\ &= (a_{\phi(g)+\phi(u)})_{g\in G}\\ &= \tilde{\phi}((a_g)_{g\in G})\cdot\phi(u)\end{aligned}$$

Hence we have that $\tilde{\phi}((a_g)_{g\in G})\cdot u = \tilde{\phi}((a_g)_{g\in G})$ if and only if $\tilde{\phi}((a_g)_{g\in G}\cdot\phi^{-1}(u)) = \tilde{\phi}((a_g)_{g\in G})$, and this is equivalent to $(a_g)_{g\in G}\cdot\phi^{-1}(u) = (a_g)_{g\in G}$. Thus $Stab_G(\tilde{\phi}(z)) = \phi(Stab_G(z))$ for any $z\in\mathcal{Y}(m,G)$. In particular we see that $Stab_G(z) = H$ if and only if $Stab_G(\tilde{\phi}(z)) = K$, showing that $\tilde{\phi}$ induces a bijection between $\mathcal{Y}(m,G)_H$ and $\mathcal{Y}(m,G)_K$. □

The previous lemma shows that for any $0\le t\le n$ we may define the integer γ_t by $\gamma_t = |\mathcal{Y}(m,G)_H|$, where H is a subgroup of G of order p^{n-t} (i.e. the definition does not depend on the choice of H). By Lemma 3.3 we have that $\gamma_0 = 1$ if p^n divides m, and $\gamma_0 = 0$ if p^n does not divide m. Then the numbers γ_t can be computed recurrently by using the following.

Lemma 3.5. *For any $1\le t\le n$ we have the following.*
(1) $\gamma_t = 0$ if p^{n-t} does not divide m.
(2) $\gamma_t = \binom{\frac{m}{p^{n-t}}+p^t-1}{p^t-1} - s_{t,1}\gamma_{t-1} - s_{t,2}\gamma_{t-2} - \ldots - s_{t,t}\gamma_0$ if p^{n-t} divides m.

Proof: Let H be a subgroup of order p^{n-t} of G. If p^{n-t} does not divide m, then by Lemma 3.3 we have that $\gamma_t = 0$, proving (1). Assume now that p^{n-t} divides m. Then

$$\mathcal{Y}(m,G)_H = \{z\in\mathcal{Y}(m,G) | z\cdot h = z \text{ for any } h\in H\} - \bigcup_{H<K\le G}\mathcal{Y}(m,G)_K \qquad (1)$$

Indeed, this is true since for any $z\in\mathcal{Y}(m,G)$ with the property that $z\cdot h = z$ for any $h\in H$, the stabilizer of z is a subgroup K of G with $H\le K$. Moreover, if K_1 and K_2 are different subgroups of G that contain H, then $\mathcal{Y}(m,G)_{K_1}\cap\mathcal{Y}(m,G)_{K_2} = \emptyset$. For any $1\le i\le t$ there exist precisely $s_{t,i}$ subgroups K of order p^{n-t+i} of G with $H<K$ (this is true since $|G/H| = p^t$ and $|K/H| = p^i$), and for any such K we have that $|\mathcal{Y}(m,G)_K| = \gamma_{t-i}$. Then (2) follows by counting the sets in equation (1). □

We are now in the position to count the G-good gradings on the matrix algebra.

Theorem 3.6. *Let p be a prime number and $G = \mathbf{Z}_p^n$. Then the number of isomorphism types of good G-gradings on the matrix algebra $M_m(k)$ is*

$$\sum_{t=0,n}\frac{1}{p^t}\gamma_t s_{n,n-t}.$$

Proof: The number of isomorphism types of good G-gradings on $M_m(k)$ is the number of orbits of the right G-set $\mathcal{Y}(m,G)$. Let $0 \leq t \leq n$. Then an element z of $\mathcal{Y}(m,G)$ has orbit of length p^t if and only if its stabilizer is a subgroup H of G of order p^{n-t}, and in this case H is the stabilizer of any other element in the orbit of z. Since there are γ_t elements with stabilizer H, and there exist $s_{n,n-t}$ subgroups of G of order p^{n-t}, the number of elements having orbit of length p^t is $\gamma_t s_{n,n-t}$. Hence the number of orbits of length p^t is $\frac{1}{p^t}\gamma_t s_{n,n-t}$, and the result follows by summing over all possible values of t. □

4 Examples

We first consider the case where $n = 1$, i.e. $G = C_p$. We have that $\gamma_0 = 1$ if p divides m, and $\gamma_0 = 0$ otherwise. The recurrence relation in Lemma 3.5 shows that $\gamma_1 = \binom{m+p-1}{p-1} - \gamma_0$. This shows that the number of isomorphism types of good gradings by the cyclic group C_p on the matrix algebra $M_m(k)$ is $1 + \frac{1}{p}(\binom{m+p-1}{p-1} - 1)$ in the case where p divides m, and $\frac{1}{p}\binom{m+p-1}{p-1}$ in the case where p does not divide m. This was proved in [2, Proposition 3.3] in the case where k contains a primitive p-th root of unity, and in [3, Example 2.7] for an arbitrary field k.

Now we consider the case where $n = 2$, i.e. $G = C_p \times C_p$. Since $s_{2,0} = s_{2,2} = 1$ and $s_{2,1} = p+1$, the number of isomorphism types of good G-gradings on $M_m(k)$ is $\gamma_0 + \frac{p+1}{p}\gamma_1 + \frac{1}{p^2}\gamma_2$. We distinguish three cases.

If p^2 divides m, then $\gamma_0 = 1$, $\gamma_1 = \binom{\frac{m}{p}+p-1}{p-1} - 1$, and $\gamma_2 = \binom{m+p^2-1}{p^2-1} - (p+1)(\binom{\frac{m}{p}+p-1}{p-1} - 1) - 1$. Therefore the number of isomorphism types of good $C_p \times C_p$-gradings on $M_m(k)$ is

$$1 + \frac{p+1}{p}(\binom{\frac{m}{p}+p-1}{p-1} - 1) + \frac{1}{p^2}(\binom{m+p^2-1}{p^2-1} - (p+1)\binom{\frac{m}{p}+p-1}{p-1} + p)$$

If p divides m, but p^2 does not divide m, then $\gamma_0 = 0$, $\gamma_1 = \binom{\frac{m}{p}+p-1}{p-1}$, and $\gamma_2 = \binom{m+p^2-1}{p^2-1} - (p+1)\binom{\frac{m}{p}+p-1}{p-1}$, so we have

$$\frac{p+1}{p}\binom{\frac{m}{p}+p-1}{p-1} + \frac{1}{p^2}(\binom{m+p^2-1}{p^2-1} - (p+1)\binom{\frac{m}{p}+p-1}{p-1})$$

isomorphism types of good $C_p \times C_p$-gradings on $M_m(k)$.

Finally, if p does not divide m, then $\gamma_0 = \gamma_1 = 0$ and $\gamma_2 = \binom{m+p^2-1}{p^2-1}$, so there exist

$$\frac{1}{p^2}\binom{m+p^2-1}{p^2-1}$$

isomorphism types of good $C_p \times C_p$-gradings on $M_m(k)$.

References

[1] Yu. A. Bahturin, S. K. Sehgal and M. V. Zaicev, Group gradings on associative algebras, J. Algebra **241** (2001), No. 2, 677-698.

[2] C. Boboc and S. Dăscălescu, Gradings of matrix algebras by cyclic groups, Comm. Algebra **29** (2001), No. 11, 5013-5021.

[3] S. Caenepeel, S. Dăscălescu and C. Năstăsescu, On Gradings of Matrix Algebras and Descent Theory, Comm. Algebra **30** (2002), No. 12, 5901-5920.

[4] S. Dăscălescu, B. Ion, C. Năstăsescu and J. Rios Montes, Group Gradings on Full Matrix Rings, J. Algebra **220** (1999), No. 2, 709-728.

[5] E. L. Green, Graphs with relations, coverings and group-graded algebras, Trans. Amer. Math. Soc. **279** (1983), 297-310.

[6] E. L. Green and E. N. Marcos, Graded quotients of path algebras: A local theory, J. Pure Appl. Alg. **93**(1994), 195-226.

[7] A. V. Kelarev, Applications of epigroups to graded ring theory, Semigroup Forum **50** (1995), 327-350.

[8] C. Năstăsescu and F. Van Oystaeyen, *Graded Ring Theory*, North Holland (1982).

Received: 7.12.2005

University of Bucharest, Faculty of Physics,
P.O.Box MG 11, Măgurele,
Bucharest, Romania
E-mail: `crina@al.math.unibuc.ro`

Kuwait University, Faculty of Science,
Dept. Mathematics,
PO BOX 5969, Safat 13060, Kuwait
University of Bucharest, Faculty of Mathematics,
Str. Academiei 14, RO-010014,
Bucharest 1, Romania
E-mail: `sdascal@mcs.sci.kuniv.edu.kw`
E-mail: `sdascal@al.math.unibuc.ro`