A Computational Approach to Gradings on Matrix Algebras

by

©Samuel A. Bauer

A thesis submitted to the Department of Mathematics and Statistics in partial fulfillment of the requirements for the degree of Bachelor of Science (Honours) in Pure Mathematics.

Memorial University of Newfoundland

St. John's, Newfoundland and Labrador, Canada

May 2021

Contents

Abstract

For a given group G, a G-grading Γ on an algebra $\mathcal{A}$ is a decomposition of $\mathcal{A}$ into the direct sum of subspaces $\mathcal{A}_g$ called homogeneous components, labeled by elements of G, such that $\mathcal{A}_g \mathcal{A}_h \subset \mathcal{A}_{gh}$ for all $g, h \in G$. All G-gradings have been classified up to isomorphism for many important algebras, including the classical simple Lie algebras and matrix algebras (for abelian G) over an algebraically closed field $\mathbb{F}$. In this thesis we review the classification of gradings on matrix algebras, which are parameterized by triples (T, β, κ) where T is a finite subgroup of G, $\beta : T \times T \to \mathbb{F}^\times$ is a nondegenerate alternating bicharacter and $\kappa : G/T \to \mathbb{N}_0$ is a function with finite support. Given a G-grading on a matrix algebra $M_n(\mathbb{F})$ where $\mathbb{F}$ is algebraically closed and of characteristic zero and G is a finitely generated abelian group, we propose an algorithm to compute the corresponding parameters T, β and κ.

Acknowledgments

This thesis was completed under the supervision of Dr. M. Kotchetov; it would not have been possible without his guidance, patience and exacting standards. I would like to thank A.J. Ryan for her excellent edits on such short notice. Dr. C. De Naday Hornhardt's thesis proved invaluable at several points, and my work would have been made significantly more difficult without him sending me a version before his PhD defense. I would also like to thank a number of my fellow students for their help keeping me grounded throughout my undergraduate degree, with Alex Sanger, Angela Dawson, Chickie Who, Sarah Muth and Deirdra Cameron-McKenna deserving special mention. I should also thank my parents, Dr. Larry Bauer and Shelley Bauer, for providing support throughout the difficult months of completing this thesis during the lock down.

And of course, thanks goes out to the countless people who laid the groundwork for my research, provided me with community during the hardest points of the process, or otherwise made this possible. Many I have never spoken to, or I do not know their names; regardless, this would not have been possible without their contributions.

Chapter 1

Introduction

There has been a marked increase in recent years in the study of gradings by arbitrary groups (see definition in Section 1.3 below) on many types of algebras, including finite dimensional simple associative, Lie, and Jordan algebras. Our aim in this thesis is to produce an algorithm to compute the parameters that classify a given G-grading on a matrix algebra $M_n(\mathbb{F})$ where G is a finitely generated abelian group and $\mathbb{F}$ is an algebraically closed field of characteristic zero. We will first recall the origins of Lie theory, make a slight detour through the shallows of algebraic group theory, and finish our introduction by defining various group gradings on matrix algebras and classifying graded modules over graded-division algebras. Then, in Chapter 2, we discuss the duality between abelian group gradings and actions on algebras. We finish, in Chapter 3, by reviewing the classification of abelian group gradings on matrix algebras by triples (T, β, κ) and providing an algorithm to compute the triple for a given G-graded matrix algebra. This algorithm can be applied, for example, to study gradings on the simple Lie algebra of type D_4, which behaves differently from other algebras in series D due to the exceptional automorphisms associated to triality.

1.1 Origins of Lie theory

Group theory, considered broadly in the modern day as the theory of symmetry, began its life by the hand of a young French radical Republican, Evariste Galois. The tale of how those ideas entered the public sphere, spanning from the 1830s to the 1870s is one of high drama and death, [13, p. 1–2] and as such, will not be covered in this thesis. The key point is this: Galois, by focusing on the symmetries of a polynomial equation in one variable, was able to understand properties of this equation[1] through those symmetries. In doing so, he established the basis for group theory [13, p. 13].

We now must move forward several years to around the 1870s [13, p. 22]. Sophus Lie, in the company of Felix Klein and Camille Jordan, was familiar with the work of Galois. In the environment of geometry, Lie was interested in "continuous groups" and their relation to the solutions of differential equations [13, p. 107]. Through this concern with "continuous groups" and the surprising association they have with certain algebras, Lie, together with his student, Wilhelm Killing, was able to prove deep and intriguing results in what eventually became known as "Lie Theory," which studies what has become known as "Lie Groups" and "Lie Algebras."

The modern definition of a Lie group has developed significantly since the days of Lie himself. We now use the definition that a group G is a *Lie group* if

1. G is a finite-dimensional smooth manifold;
2. Group multiplication, $\mu : G \times G \to G$ is a smooth map;
3. The inversion[2] $\iota : G \to G$ is a smooth map.

Furthermore, a group homomorphism $\phi : G \to H$ between two Lie groups is said to be a *Lie group homomorphism* if ϕ is, again, a smooth map.[3]

1.2 Lie groups and algebraic groups

Algebraic group theory is, in many ways, parallel to Lie theory. It is a deep and rich area of study on its own, so we will stay in the shallows here. We give the "naïve" definition of an (affine) algebraic group over an algebraically closed field $\mathbb{F}$. A group G is an *algebraic group over* $\mathbb{F}$ if

1. For some n, G is a subset of $\mathbb{F}^n$ that is defined by polynomial equations;[4]

[1] In particular, solvability in radicals.

[2] That is, sending each element to its inverse.

[3] One may notice that this is the definition of the category of "group objects" in the category of smooth manifolds.

[4] That is, the set of common zeros of a set of polynomials in n variables.

2. The group multiplication $\mu : G \times G \to G$ is given by the restriction of a polynomial map $\mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^n$;

3. The inversion $\iota : G \to G$ is a restriction of a polynomial map $\mathbb{F}^n \to \mathbb{F}^n$.

Furthermore, an algebraic group homomorphism is a group homomorphism between two algebraic groups given by a polynomial map.[5] We will now look at a small selection of algebraic groups. There are the *vector groups* $\mathbb{F}^n$, with the group operation being vector addition. There is also the *multiplicative group*, $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$, which is defined slightly unexpectedly:

$$\mathbb{F}^\times = \{(x, y) \in \mathbb{F}^2 \mid xy = 1\}.$$

Taking the direct product of copies of the multiplicative group gives us the (algebraic) *tori*,[6] $(\mathbb{F}^\times)^n$. Any finite group is also an algebraic group. If H is a finite abelian group, then $H \times (\mathbb{F}^\times)^n$ is an abelian algebraic group called a *quasi-torus*. Quasi-tori are special in the class of algebraic groups for being diagonalizable [7, p. 103]. As a glimpse of nonabelian algebraic groups, one is the *special linear group* $\mathrm{SL}(n, \mathbb{F})$, defined by

$$\mathrm{SL}(n, \mathbb{F}) := \{X \in M_n(\mathbb{F}) \cong \mathbb{F}^{n^2} \mid \det(X) = 1\}.$$

There is also the *general linear group*, $\mathrm{GL}(n, \mathbb{F})$, defined by

$$\mathrm{GL}(n, \mathbb{F}) := \{(X, y) \in M_n(\mathbb{F}) \times \mathbb{F} \mid \det(X)y = 1\}.$$

One should note, as well, that for any $\mathbb{F}$-vector space V of dimension $n \in \mathbb{N}$, we have $\mathrm{GL}(V) \cong \mathrm{GL}(n, \mathbb{F})$ through the identification of linear transformations with matrices that represent them with respect to a fixed basis, so $\mathrm{GL}(V)$ is an algebraic group.

For a finite dimensional algebra $\mathcal{A}$, we furthermore have that $\mathrm{Aut}(\mathcal{A})$, the automorphism group of the algebra, is a subgroup of $\mathrm{GL}(\mathcal{A})$ defined by polynomial equations. As such, it is also an algebraic group.

[5] One may notice that this is the category of "group objects" in the category of (affine) algebraic varieties over $\mathbb{F}$, similarly to the case of Lie groups above.

[6] The topological torus of dimension n is the compact real form of the algebraic torus $(\mathbb{C}^\times)^n$.

1.3 Gradings

From here on, we will be working with $\mathbb{F}$ algebraically closed and of characteristic zero, unless otherwise noted.

Let G be a group. An $\mathbb{F}$-vector space V is called *G-graded* if there is a fixed direct sum decomposition,

$$\Gamma : V = \bigoplus_{g\in G} V_g,$$

called a *G-grading* on V. Each V_g is called a *homogeneous component* of V (or of Γ). Furthermore, the *support* of V or Γ is the subset

$$\mathrm{supp}(V) := \{g \in G \mid V_g \neq \{0\}\},$$

We will say any element $v \in V_g \setminus \{0\}$ has *degree* g, written as

$$\deg(v) = g.$$

Thus, any element $v \in V$ can be written uniquely as the sum of homogeneous elements: $v = \sum_{g\in G} v_g$, $v_g \in V_g$ for all $g \in G$, and $v_g = 0$ for all but finitely many $g \in G$.

A subspace $W \subset V$ is a *graded subspace* if

$$W = \bigoplus_{g\in G} W_g \text{ where } W_g := W \cap V_g.$$

If $v = \sum_{g\in G} v_g$ as above, then $v \in W$ if and only if $v_g \in W_g$ for all $g \in G$.

We can assign degree to certain linear maps between graded vector spaces. If we have two G-graded spaces $V = \bigoplus_{g\in G} V_g$ and $W = \bigoplus_{g\in G} W_g$, then a linear map $T : V \to W$ is *homogeneous of degree g* if

$$T(V_h) \subset W_{gh} \quad \forall h \in G.$$

We will denote the subspace of $\mathrm{Hom}(V, W)$ consisting of all such maps by $\mathrm{Hom}(V, W)_g$, and define

$$\mathrm{Hom}^{\mathrm{gr}}(V, W) := \bigoplus_{g\in G} \mathrm{Hom}(V, W)_g.$$

When $V = W$, we denote $\mathrm{Hom}(V, V)_g$ by $\mathrm{End}(V)_g$ and $\mathrm{Hom}^{\mathrm{gr}}(V, V)$ by $\mathrm{End}^{\mathrm{gr}}(V)$.

Note that if V is finite dimensional, then $\mathrm{Hom}(V,W) = \bigoplus_{g_1,g_2\in G}\mathrm{Hom}(V_{g_1},W_{g_2})$, which implies that $\mathrm{Hom}^{\mathrm{gr}}(V,W) = \mathrm{Hom}(V,W)$ and, in particular, $\mathrm{End}^{\mathrm{gr}}(V) = \mathrm{End}(V)$.

The term "degree" is pulled from one of the most natural instances of gradings, those on polynomial algebras. Consider the ring of polynomials over $\mathbb{F}$ in n variables, denoted $\mathbb{F}[x_1,\dots,x_n]$. There are several gradings we can impose on this algebra. There is the most natural $\mathbb{Z}$-grading, given by

$$\deg(x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}) = \alpha_1+\alpha_2+\cdots+\alpha_n.$$

There is also the "multidegree" grading, which is the $\mathbb{Z}^n$-grading given by

$$\deg(x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}) = (\alpha_1,\alpha_2,\dots,\alpha_n).$$

This is a refinement of the natural $\mathbb{Z}$-grading. More generally, let G be an abelian group (written multiplicatively) and $w_1,\dots,w_n\in G$. Then, we have a G-grading given by

$$\deg(x_i) = w_i$$

and the rule that

$$\deg(pq) = \deg(p)\deg(q)$$

for all monomials $p,q\in\mathbb{F}[x_1,\dots,x_n]$.

This rule is taken as the basic idea of the definition of a grading on an algebra. We say that an algebra $\mathcal{A}$ (not necessarily associative) is *G-graded* if $\mathcal{A}$ is G-graded as a vector space,

$$\mathcal{A} = \bigoplus_{g\in G}\mathcal{A}_g,$$

such that

$$\mathcal{A}_g\mathcal{A}_h \subset \mathcal{A}_{gh} \quad \forall g,h\in G, \tag{1.1}$$

where $\mathcal{A}_g\mathcal{A}_h := \mathrm{span}\{xy \mid x\in\mathcal{A}_g, y\in\mathcal{A}_h\}$ and G is written multiplicatively. Note that for $e\in G$ the identity element, the component $\mathcal{A}_e$ is a subalgebra of $\mathcal{A}$. Also, one can easily show that if $\mathcal{A}$ is unital with identity element 1, then $1\in\mathcal{A}_e$.

Note that $\mathrm{End}^{\mathrm{gr}}(V)$ from above is naturally a graded algebra with respect to composition, as if we have two homogeneous maps, say T and S where $\deg(T) = g$ and $\deg(S) = h$, then for all $k\in G$ we have:

$$(T\circ S)(V_k) = T(S(V_k)) \subset T(V_{hk}) \subset V_{ghk}.$$

That is, $T \circ S \in \mathrm{End}(V)_{gh}$.

The rigidity of condition (1.1) provides us the ability to classify gradings on certain types of algebras up to isomorphism. We say that two G-graded algebras $\mathcal{A}$ and $\mathcal{B}$ are *isomorphic as graded algebras* (or just *isomorphic* for short) if there exists an isomorphism of algebras $\phi : \mathcal{A} \to \mathcal{B}$ such that $\phi(\mathcal{A}_g) = \mathcal{B}_g$ for all $g \in G$. Furthermore, we will say that two gradings, Γ and Δ, on the same algebra $\mathcal{A}$ are isomorphic if $(\mathcal{A}, \Gamma)$ and $(\mathcal{A}, \Delta)$ are isomorphic as graded algebras; that is, there exists an automorphism $\phi : \mathcal{A} \to \mathcal{A}$ that sends each homogeneous component of Γ onto the homogeneous component of Δ of the same degree.

There are a couple more concepts related to gradings on algebras that we will need for later. A *graded subalgebra* (resp. *graded ideal*) is a subalgebra (resp. ideal) that is also a graded subspace.

Let $\mathcal{A}$ be a G-graded associative algebra. Then a left $\mathcal{A}$-module V is a *graded left module* if V is a graded $\mathbb{F}$-vector space such that

$$\mathcal{A}_g V_h \subset V_{gh}, \ \forall g, h \in G.$$

The definition of a graded right module is similar.

We can also take the *tensor product* of two graded algebras. Let $\mathcal{A}$ be G-graded and $\mathcal{B}$ be H-graded. Then, there exists a natural $G \times H$-grading on $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$ given by $\mathcal{C}_{(g,h)} = \mathcal{A}_g \otimes \mathcal{B}_h$. If $G = H$ is an abelian group, then we can also view $\mathcal{C}$ as a G-graded algebra:

$$\mathcal{C}_g = \bigoplus_{\substack{g_1, g_2 \in G \\ g_1 g_2 = g}} \mathcal{A}_{g_1} \otimes \mathcal{B}_{g_2}.$$

From now on, all algebras will be assumed to be associative unless noted otherwise.

We should now examine some examples of graded algebras. We have already looked at polynomial algebras, but of more interest to us here are matrix algebras. For example, consider the matrix algebra $M_2(\mathbb{F})$. There is a $\mathbb{Z}$-grading, given by

$$\begin{aligned} \deg \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} &= -1, \ \deg \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = 0, \\ \deg \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} &= 0, \quad \deg \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = 1, \end{aligned} \tag{1.2}$$

and there is also the so-called *Pauli grading*, which is a $\mathbb{Z}_2^2$-grading given by

$$\begin{aligned} \deg \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} &= (\bar{1}, \bar{0}), \quad \deg \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = (\bar{0}, \bar{1}), \\ \deg \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} &= (\bar{0}, \bar{0}), \quad \deg \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = (\bar{1}, \bar{1}). \end{aligned} \tag{1.3}$$

In fact, these are both special cases of more general constructions.

Given any n-tuple $\mathbf{g} = (g_1, g_2, \ldots, g_n) \in G^n$, we can define a G-grading on the matrix algebra $M_n(\mathbb{F})$ by

$$\deg(E_{i,j}) := g_i g_j^{-1}, \tag{1.4}$$

where $E_{i,j}$ denote the matrix units. The proof that this is a grading is rather simple: we have

$$E_{i,j} E_{k,\ell} = \begin{cases} E_{i,\ell} & \text{if } j = k, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\deg(E_{i,k}) = g_i g_k^{-1} = g_i g_j g_j^{-1} g_k^{-1} = \deg(E_{i,j}) \deg(E_{j,k}).$$

We will call a grading Γ on $M_n(\mathbb{F})$ an *elementary grading* if it is isomorphic to a grading of this form.[7]

Thus the grading from (1.2) is an elementary grading where the group is $\mathbb{Z}$ and $\mathbf{g} = (0, 1)$. We can define a similar grading if we set the grading group to $\mathbb{Z}_3$ and $\mathbf{g} = (\bar{0}, \bar{1})$. We can get a coarser grading by setting the grading group to $\mathbb{Z}_2$ and $\mathbf{g} = (\bar{0}, \bar{1})$.

Recall that a *division algebra* is a unital algebra in which all nonzero elements have a multiplicative inverse. A G-graded unital algebra $\mathcal{D}$ is said to be a *graded-division* algebra if all nonzero homogeneous elements have a multiplicative inverse. One can easily show that if $\deg(d) = g$ then $\deg(d^{-1}) = g^{-1}$. This gives us two important results. First, $\mathcal{D}_e$ is a division algebra over $\mathbb{F}$. In particular, if $\mathcal{D}$ is finite dimensional and $\mathbb{F}$ is algebraically closed then $\mathcal{D}_e = \mathbb{F}1$ where 1 is the identity element of $\mathcal{D}$. Second, $\operatorname{supp}(\mathcal{D})$ will always be a subgroup of G.

---

[7]Some authors reserve the term elementary grading to gradings of the form (1.4) rather than those isomorphic to that form.

Following the notation from [5, p. 2], the *generalized Pauli matrices* on $M_n(\mathbb{F})$ are

$$X = \begin{bmatrix} \varepsilon^{n-1} & 0 & 0 & \dots & 0 & 0 \\ 0 & \varepsilon^{n-2} & 0 & \dots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & \dots & \varepsilon & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix} \text{ and } Y = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \end{bmatrix} \tag{1.5}$$

where ε is a primitive n-th root of unity. Note that $XY = \varepsilon YX$ and $X^n = Y^n = I_n$.

Lemma 1.1. *The set $\{X^kY^\ell \mid 0 \le k, \ell < n\}$ is a basis of $M_n(\mathbb{F})$.*

Proof. Since the size of this set is $n^2 = \dim M_n(\mathbb{F})$, it is sufficient to show that it is linearly independent. Consider a linear relation of the elements:

$$0 = \sum_{k=0}^{n-1} \sum_{\ell=0}^{n-1} \lambda_{k,\ell} X^k Y^\ell. \tag{1.6}$$

We should first consider what powers of Y do to the unit vectors; it simply cyclically permutes them. As well, as X is a diagonal matrix, we furthermore have that multiplication on the left by a power of X will correspond to multiplying the columns of the matrix by a set of constants. Therefore, any linear combination that gives us the zero action on the underlying vector space can be separated by the powers of Y, that is, (1.6) holds if and only if for all $1 \le \ell \le n$ we have

$$0 = \sum_{k=0}^{n-1} \lambda_{k,\ell} X^k Y^\ell$$

we can cancel the Y^ℓ as Y is invertible, giving us

$$0 = \sum_{k=0}^{n-1} \lambda_{k,\ell} X^k.$$

As each X^k is a diagonal matrix, we can consider them as columns of a matrix of the form

$$\begin{bmatrix} 1 & \varepsilon^{n-1} & \varepsilon^{2(n-1)} & \cdots & \varepsilon^{(n-1)(n-1)} \\ 1 & \varepsilon^{n-2} & \varepsilon^{2(n-2)} & \cdots & \varepsilon^{(n-1)(n-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \varepsilon & \varepsilon^{2} & \cdots & \varepsilon^{n-1} \\ 1 & 1 & 1 & \cdots & 1 \end{bmatrix}.$$

This is a so-called *Vandermonde matrix*, see e.g. [10, Thm. 3.2.7]. Thus, the determinant of our matrix is given by the product

$$\prod_{1\leq i<j\leq n} (\varepsilon^{n-j} - \varepsilon^{n-i}).$$

This is clearly nonzero, making our determinant nonzero, and thus our set a basis. $\square$

We can thus define a $\mathbb{Z}_n^2$-grading by setting

$$\deg(X^k Y^\ell) := (\overline{k}, \overline{\ell}).$$

Since X and Y are invertible matrices, this is a *division grading*, that is, it makes $M_n(\mathbb{F})$ a graded-division algebra. Example (1.3) above is an example of such a generalized Pauli grading.

It turns out that all such gradings are made up of an elementary grading and a division grading, combined in a certain way, as we will see in ADD REF

1.4 Graded modules over graded-division algebras

It is well known that any vector space or, more generally, any module over a division algebra has a basis. The following result is the graded version of this fact.

Lemma 1.2. *Every graded module over a graded-division algebra has a basis of homogeneous elements.*

Proof. Let $\mathcal{D}$ be G-graded graded-division algebra and V be a graded right $\mathcal{D}$-module. We will proceed with Zorn's Lemma. Let

$$S := \{X \subset \bigcup_{g\in G} V_g \mid X \text{ is linearly independent over } \mathcal{D}\}.$$

The set S is partially ordered by inclusion, and it contains $\varnothing$. We will now check that it satisfies the hypothesis of Zorn's Lemma. If $C \subset S$ is a chain, then consider $X = \bigcup_{c\in C} c$. We have that $X \subset \bigcup_{g\in G} V_g$. For any finite selection of elements of X, they must all be in some element of $c \in C$, and thus linearly independent over $\mathcal{D}$. As linear independence concerns itself only with finite sums, we have that X, as a whole, is linearly independent, so $X \in S$. Thus, we have some maximal element M in S. We now must show that this M is a basis for the $\mathcal{D}$-module V. Suppose not. That is, the $\mathcal{D}$-span of M is a proper submodule of V. Now, as every element of V is the sum of homogeneous elements, we know there must exist some homogeneous element $v_{g_0} \in V_{g_0}$ such that v_{g_0} is not a linear combination of elements of M with coefficients in $\mathcal{D}$. We claim that the set $M \cup \{v_{g_0}\}$ is linearly independent over $\mathcal{D}$. Consider a linear relation

$$v_{g_0} d + \sum_{v\in M} v\alpha_v = 0, \tag{1.7}$$

where $d, \alpha_v \in \mathcal{D}$, and all but finitely many α_v are 0. If $d = 0$, then all $\alpha_v = 0$ by the linear independence of M, so assume $d \neq 0$. Now, as $\mathcal{D}$ is graded, we can write $d = \sum_{g\in G} d_g$, where $d_g \in \mathcal{D}_g$ and all but finitely many d_g are 0. Choose a $g_1 \in G$ such that $d_{g_1} \neq 0$ and let $h = g_0 g_1$. By the fact that G is a group, we have that $g_0 g \neq h$ for $g \neq g_1$, so the projection of $v_{g_0} d$ onto V_h is $v_{g_0} d_{g_1}$. Taking the projection of both sides of (1.7) onto V_h gives:

$$0 = v_{g_0} d_{g_1} + \sum_{v\in M} v\beta_v$$

Since d_{g_1} is a nonzero homogeneous element, it has an inverse in $\mathcal{D}$, so we obtain

$$v_{g_0} = -\sum_{v\in M} v\beta_v d_{g_1}^{-1}$$

This is a contradiction, so $M \cup \{v_{g_0}\}$ is linearly independent over $\mathcal{D}$, as claimed. Since $M \cup \{v_{g_0}\} \subset \bigcup_{g\in G} V_g$, this is a contradiction with maximality. $\square$

We now introduce a parameter to classify graded right $\mathcal{D}$-modules of finite rank where $\mathcal{D}$ is a graded-division G-graded algebra. Let $T = \mathrm{supp}(\mathcal{D})$ and G/T be the set of left cosets. For V a graded right $\mathcal{D}$-module we define the map $\kappa : G/T \to \mathbb{N}_0$ by $\kappa(gT) := \dim(V_g)$. To show this is well defined, consider $h \in gT$. That is, $g = ht$ for some $t \in T$. Let $d_t \in \mathcal{D}_t$, $d_t \neq 0$. Then, $\phi : V_g \to V_h$ given by $\phi(v) = vd_t$ is an isomorphism of vector spaces; the inverse $\phi^{-1} : V_h \to V_g$ is given by $\phi^{-1}(v) = vd_t^{-1}$ (recall that $d_t^{-1} \in \mathcal{D}_{t^{-1}}$). The fact that the dimension is finite follows from the alternative definition of κ: if we have a graded $\mathcal{D}$-basis $\{v_1, \ldots, v_k\}$ of V with $\deg(v_i) = h_i$ for all i, then $\kappa(x)$ is the number of times x appears in the list of cosets $h_1T, \ldots, h_kT$, as can be seen from the proof of the lemma below, which is derived from [5, p. 33].[8] We will call κ *the multiplicity function associated to* V.

Lemma 1.3. *Two graded right $\mathcal{D}$-modules of finite rank, V and V', are isomorphic if and only if $\kappa = \kappa'$.*

Proof. Suppose that $V \cong V'$ as graded $\mathcal{D}$-modules. This implies, for each element $g \in G$, $V_g \cong V'_g$ as vector spaces, which gives

$$\kappa'(gT) = \dim(V'_g) = \dim(V_g) = \kappa(gT).$$

Now, to prove the converse, suppose $\kappa = \kappa'$. That is, for all $x \in G/T$, $\kappa(x) = \kappa'(x)$. As left cosets of G with respect to any subgroup form a partition of G, let Ξ be a set of representatives of the cosets. That is, $|\Xi \cap x| = 1$ for every $x \in G/T$.

Let $B = \{v_1, \ldots, v_k\}$ be a graded $\mathcal{D}$-basis of V. We will be modifying this basis B to obtain that $\deg(v_i) \in \Xi$ for all i. For each v_i there is a unique coset $x_i \in G/T$ such that $\deg(v_i) \in x_i$. Let g_i be the representative of x_i in Ξ. Then $\deg(v_i)t_i = g_i$ for a unique $t_i \in T$. As "rescaling" a basis element by a nonzero homogeneous element of $\mathcal{D}$ gives rise to a new graded basis, we can replace v_i with $v_i d_{t_i}$, where $d_{t_i} \in \mathcal{D}_{t_i}$, $d_{t_i} \neq 0$. After these replacements, V_g for $g \in \Xi$ is spanned by the basis elements v_i with $g_i = g$, hence we have $\kappa(gT) = \dim(V_g) = |B \cap V_g|$.

Once we have done this for V, we can do the same thing for V', giving us the bases B and B' respectively. Since $\kappa = \kappa'$, we may order basis elements so that $\deg(v_i) = \deg(v'_i)$. Then the mapping $v_i \mapsto v'_i$ extends to an isomorphism and thus $V \cong V'$ as graded $\mathcal{D}$-modules. □

[8] We differ from the notation in [5] in that what we denote by κ is the multiplicity function associated to the multiset $\Xi(\kappa, \gamma)$ in [5, Def. 2.25].

We need the concept of a *shift* of a graded vector space. Let G be a group and V a G-graded vector space. For each element $g \in G$, we can define the *right shift* $V^{[g]}$ by setting $V^{[g]}_{hg} := V_h$ for all $h \in G$. That is, the underlying vector space is the same, but the elements that are homogeneous of degree h in V become homogeneous of degree hg in $V^{[g]}$. Similarly, the *left shift* ${}^{[g]}V$ is defined by ${}^{[g]}V_{gh} := V_h$. If $\mathcal{D}$ is a graded algebra, then ${}^{[g^{-1}]}\mathcal{D}^{[g]}$ is also a graded algebra. As well, if V is a graded right $\mathcal{D}$-module then $V^{[g]}$ is a graded right ${}^{[g^{-1}]}\mathcal{D}^{[g]}$-module (rather than a graded right $\mathcal{D}$-module).

We will now see how to handle isomorphism up to a shift. Say we have a graded right $\mathcal{D}$-module, V, with multiplicity function κ. Let the multiplicity function associated with $V^{[g]}$ be denoted $\kappa^{[g]} : G/g^{-1}Tg \to \mathbb{N}_0$. Writing it explicitly:

$$\kappa^{[g]}(h(g^{-1}Tg)) = \dim(V^{[g]}_h) = \dim(V_{hg^{-1}}) = \kappa(hg^{-1}T).$$

Note that if G is abelian, then this becomes the usual action on functions, namely,

$$\kappa^{[g]}(x) = \kappa(g^{-1}x) \quad \forall x \in G/T.$$

Chapter 2

Gradings and Actions

2.1 Actions of a character group $\widehat{G}$ associated to G-gradings

Let G be a group. We will denote by $\widehat{G}$ the *character group* of G over the field $\mathbb{F}$:

$$\widehat{G} := \{\chi : G \to \mathbb{F}^{\times} \mid \chi(xy) = \chi(x)\chi(y), \forall x, y \in G\}$$

with group operation defined by pointwise multiplication. It should be noted that the character group is of principal interest to us when G is abelian, as the group $\widehat{G}$ is always abelian.[1]

Lemma 2.1. *Let G be an abelian group and $\mathbb{F}$ an algebraically closed field of characteristic zero. If $K \leqslant G$, then any character ξ of K can be extended to a character of G, that is, there exists $\chi \in \widehat{G}$ such that $\chi|_K = \xi$.*

Proof. We are going to apply Zorn's Lemma. Consider the set S of pairs (H, ψ) where H is a subgroup of G containing K and $\psi : H \to \mathbb{F}^{\times}$ is a character such that $\psi|_K = \xi$. In particular, $(K, \xi) \in S$. Consider the partial order on this set of pairs given by

$$(H_1, \psi_1) \preceq (H_2, \psi_2) \;\Leftrightarrow\; H_1 \subset H_2 \text{ and } \psi_2|_{H_1} = \psi_1.$$

[1] Some authors denote by $\widehat{G}$ the set of irreducible characters of G. Our $\widehat{G}$ consists of one-dimensional characters. If G is abelian and $\mathbb{F}$ is algebraically closed, then all irreducible characters are one-dimensional.

We now need to check the hypothesis of Zorn's Lemma for S. Let $C = \{(H_j, \psi_j)\}_{j\in J}$ be a chain in S. Our upper bound of C will be (H, ψ) where $H = \bigcup_{j\in J} H_j$ and $\psi|_{H_j} = \psi_j$. It is easy to check that H is a subgroup of G and ψ is a character on H, so this is an upper bound of C in S. By Zorn's Lemma, S has a maximal element, say (M, χ). We will now prove that $M = G$.

Suppose not, that is $M \neq G$. Then there would be an element, say $x \in G$ such that $x \notin M$. Let $M' = \langle M, x\rangle$. We will construct an extension of χ to a character $\chi' : M' \to \mathbb{F}^\times$.

Case 1. If $x^n = y \in M$ for some natural number n, we take the least such n and we extend χ to χ' by defining $\chi'(x)$ to be an n-th root of $\chi(y)$. It is left as an exercise that there exists such a homomorphism χ'.

Case 2. If $x^n \notin M$ for all $n > 0$, then we can extend χ by setting $\chi'(x) = 1$. Again, it is left as an exercise that there exists such a homomorphism χ'.

In either case, we now have $(M, \chi) \prec (M', \chi')$, a contradiction with maximality. Therefore, $M = G$, and we have a character on the entire group. $\square$

We will find these two additional corollaries useful.

Corollary 2.2. *In the setting of Lemma 2.1, $\widehat{G}$ separates points, that is, for any $g, h \in G$, $g \neq h$, there exists $\chi \in \widehat{G}$ such that $\chi(g) \neq \chi(h)$.*

Proof. Let $k = gh^{-1}$. We define a homomorphism, $\xi : \langle k\rangle \to \mathbb{F}^\times$, where $\xi(k)$ is a primitive n-th root of unity if k is of order $n < \infty$, and $\xi(k) = 2$ if k is of infinite order. Both of these elements exist in $\mathbb{F}^\times$ since $\mathbb{F}$ is algebraically closed and of characteristic zero. By Lemma 2.1 we can extend this into a character of G, say χ such that $\chi|_{\langle k\rangle} = \xi$. Therefore, $\chi(k) \neq 1$, so $\chi(g) \neq \chi(h)$. $\square$

This corollary is in fact a special case of another corollary.

Corollary 2.3. *In the setting of Lemma 2.1, if $K \leqslant G$ is a subgroup of G and $x \notin K$ is an element of G, then there exists a character $\chi \in \widehat{G}$ such that $\chi(k) = 1$ for all $k \in K$ and $\chi(x) \neq 1$.*

Proof. Note that as $x \notin K$, $x \neq e$. We have two cases.

Case 1. $\langle x\rangle \cap K = \{e\}$. That is, $\langle K, x\rangle = K \times \langle x\rangle$, and we can define $\xi : K \times \langle x\rangle \to \mathbb{F}^\times$ such that $\xi(x) \neq 1$ and $\xi(k) = 1$ for all $k \in K$. By Lemma 2.1 this can be extended to $\chi \in \widehat{G}$.

Case 2. $\langle x\rangle \cap K \neq \{e\}$. That is, there is some least $n \in \mathbb{N}$, $n > 0$ such that $x^n \in K$. Let ω be an n-th root of unity, and define $\xi : \langle x, K\rangle \to \mathbb{F}^\times$ by $\xi(x) = \omega$ and $\xi(k) = 1$ for all $k \in K$. By Lemma 2.1 this can be extended to $\chi \in \widehat{G}$. □

Given a subset $H \subset G$ of an abelian group G, we define

$$H^\perp := \{\chi \in \widehat{G} \mid \chi(h) = 1,\ \forall h \in H\}.$$

Similarly and by an abuse of notation, for a subset $K \subset \widehat{G}$ we define

$$K^\perp := \{g \in G \mid \chi(g) = 1,\ \forall \chi \in K\}.$$

This is in fact a form of duality.

Lemma 2.4. *Let G be an abelian group and $\mathbb{F}$ an algebraically closed field of characteristic zero. For any subgroup $H \leqslant G$ we have $H = (H^\perp)^\perp$.*

Proof. First, it is clear that $H \subset (H^\perp)^\perp$. It only remains to prove that $(H^\perp)^\perp \subset H$. Suppose not, that there is some $x \in (H^\perp)^\perp$ such that $x \notin H$. By Corollary 2.3, there exists some $\chi \in \widehat{G}$ such that $\chi(x) \neq 1$ and $\chi(h) = 1$ for all $h \in H$. Note that this implies that $\chi \in H^\perp$. By $x \in (H^\perp)^\perp$ we know $\chi(x) = 1$ a contradiction. □

Given a G-grading Γ on V, where G is abelian, we have a group homomorphism, $\eta_\Gamma : \widehat{G} \to \mathrm{GL}(V)$, defined by

$$\eta_\Gamma(\chi)(v) = \chi(g)v,\ \forall v \in V_g, g \in G$$

and by linearity. Thus, a G-grading on V gives rise to $\widehat{G}$-action on V. These operators $\eta_\Gamma(\chi)$, $\chi \in \widehat{G}$, commute with each other and are diagonalizable.

Lemma 2.5. *Let G be an abelian group, $\mathbb{F}$ an algebraically closed field of characteristic zero and V a vector space. Furthermore let $\varrho : \widehat{G} \to \mathrm{GL}(V)$ be a group action. If ϱ is associated with a G-grading Γ on V, then Γ is determined by*

$$V_g := \{v \in V \mid \varrho(\chi)(v) = \chi(g)(v), \forall \chi \in \widehat{G}\}.$$

Proof. We know that all operators $\varrho(\chi)$ for $\chi \in \widehat{G}$ are simultaneously diagonalizable. Let $W \subset V$ be a simultaneous eigenspace, that is

$$W = \{v \in V \mid \varrho(\chi)(v) = \lambda_\chi v\}.$$

We claim that $W = V_g$ for some $g \in G$. Pick a nonzero $w \in W$. Then we can write $w = \sum_{i=1}^k w_i$ where each $w_i \in V_{g_i}$ and $w_i \neq 0$. Then, for all characters $\chi \in \widehat{G}$, we get:

$$\begin{aligned} \varrho(\chi)(w) &= \varrho(\chi)\left(\sum_{i=1}^k w_i\right) \\ \lambda_\chi w &= \sum_{i=1}^k \varrho(\chi)(w_i) \\ \sum_{i=1}^k \lambda_\chi w_i &= \sum_{i=1}^k \chi(g_i) w_i \\ \Rightarrow \lambda_\chi w_i &= \chi(g_i) w_i \\ \Rightarrow \lambda_\chi &= \chi(g_i). \end{aligned}$$

By the fact that $\widehat{G}$ separates points, this gives us that $k = 1$ hence $w \in V_{g_1}$ and $\lambda_\chi = \chi(g_1)$ for all $\chi \in \widehat{G}$. Therefore, $W = V_{g_1}$, proving the claim. □

We will limit ourselves to finite dimensional vector spaces. Since we can replace G with the subgroup generated by the support of the grading, we can assume without loss of generality that G is finitely generated.

2.2 Finitely generated abelian groups

2.2.1 The fundamental theorem

The classification of finitely generated abelian groups is well-known, however we will briefly recall it here.

Theorem 2.6 (The Fundamental Theorem of Finitely Generated Abelian Groups)**.** *If G is a finitely generated abelian group, then*

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_k^{\alpha_k}} \times \mathbb{Z}^n,$$

where p_i are primes, not necessarily distinct. This decomposition is unique up to order of factors.[2] *We also have*

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \ldots \times \mathbb{Z}_{d_m} \times \mathbb{Z}^n,$$

where $d_i \geq 2$ and $d_i \mid d_{i+1}$. This decomposition is unique.[3]

We will call a generating set, say $\{g_1, \ldots, g_n\}$, of a group G a *reduced generating set* if for all i we have $g_i \neq e$ and

$$G = \langle g_1 \rangle \times \cdots \times \langle g_n \rangle.$$

We will prove this using Smith Normal Form of an integer matrix, which we will also need in Chapter 3.

Theorem 2.7 (Smith Normal Form)**.** *Let $k, \ell \in \mathbb{N}$ and $A \in M_{k\times\ell}(\mathbb{Z})$. Then, we can write $A = CDB$ where $B \in \mathrm{GL}_\ell(\mathbb{Z})$, $C \in \mathrm{GL}_k(\mathbb{Z})$, and $D \in M_{k\times\ell}(\mathbb{Z})$ has the form $D = \mathrm{diag}_{k\times\ell}(a_1, a_2, \ldots, a_r, 0, \ldots, 0)$, where $r \leq \min\{k, \ell\}$ is the rank of A and $a_i > 0$, $a_i \mid a_{i+1}$. The matrix D is uniquely determined and is called the Smith Normal Form of A.*

Proof. Consider the elementary $k \times k$ matrices over $\mathbb{Z}$. Left multiplication by these matrices performs elementary row operations: swapping rows, adding an integer multiple of a row to another row, and multiplying a row by -1. Similarly, right multiplication by elementary $\ell \times \ell$ matrices over $\mathbb{Z}$ performs the same operations on columns. We will show these operations are sufficient to carry A to Smith Normal Form. Then we can write

$$C_q \ldots C_1 A B_1 \ldots B_p = D,$$

where each C_i is a $k \times k$ elementary matrix and each B_j is an $\ell \times \ell$ elementary matrix. Then clearly $C = (C_q \ldots C_1)^{-1}$ and $B = (B_1 \ldots B_p)^{-1}$ satisfy the conditions of the theorem. (Observe that elementary matrices as above are invertible over the integers.) This will give us existence.

If A is the zero matrix, then there is nothing to prove. Otherwise, take a non-zero entry in A with the smallest absolute value, and by switching rows and columns place it in position $(1, 1)$. Let this entry be denoted a_1, so

---

[2] This is sometimes called the *primary decomposition* of G.

[3] This is called the *invariant factor decomposition* of G.

$a_{1,1} = a_1$. If $a_1 < 0$ then multiply the first row by -1 to make $a_1 > 0$. We now have two cases:

Case 1. All entries in A are divisible by a_1. By adding multiples of the first row or column to other rows or columns, we can carry A into block-diagonal form, with a 1×1 block consisting of a_1 and a $(k-1) \times (\ell - 1)$ block. By induction, we can write this second block in Smith Normal Form by row and column operations, so we get that we can reduce A to a diagonal matrix, $D = \mathrm{diag}_{k \times \ell}(a_1, a_2, \ldots, a_r, 0, \ldots, 0)$, with each $a_i > 0$ and $a_2 \mid a_3 \mid \ldots \mid a_r$. It remains to show that $a_1 \mid a_2$. As every entry of A was divisible by a_1, and elementary row and column operations do not change that divisibility, we get that $a_1 \mid a_2$.

Case 2. There is $a_{i,j}$ such that $a_1 \nmid a_{i,j}$. We now have two subcases:

Subcase 1. $i = 1$ or $j = 1$. As the argument is the same for both cases, say without loss of generality that $i = 1$. That is, $a_1 \nmid a_{1,j}$ for some j. Then, using division with remainder, we have $a_{1,j} = q_1 a_1 + r_1$ with $0 < r_1 < a_1$. Subtracting column 1 times q_1 from column j, we get r_1 in position $(1, j)$. We now have a new smallest element, and start the procedure over. This cannot continue forever, as the decrease is strict.

Subcase 2. All entries in the first column and the first row are divisible by a_1. Then we can reduce A to a block-diagonal matrix in the same way as in Case 1. The entry $a_{i,j}$ is still not divisible by a_1, so adding row i to row 1 puts us into Subcase 1.

This completes the proof of existence. Now, we must show that D is unique.

Consider the set $\mathcal{I}_n(A)$ of all $n \times n$ submatrices of A, and let

$$m_n(A) := \gcd\{\det(X) \mid X \in \mathcal{I}_n(A)\}.$$

It is left as an exercise for the reader to verify that these numbers are preserved by elementary row and column operations. Therefore $m_n(A) = m_n(D)$. Due to the condition $a_i \mid a_{i+1}$, calculating $m_n(D)$ is trivial:

$$m_n(D) = \prod_{i=1}^{n} a_i.$$

This implies uniqueness: $a_n = \frac{m_n(D)}{m_{n-1}(D)} = \frac{m_n(A)}{m_{n-1}(A)}$ where $m_0(A) := 1$. $\square$

Now let us prove Theorem 2.6.

Proof. Note that any abelian group can be regarded as a $\mathbb{Z}$-module in a natural way. In particular, a finitely generated abelian group can be presented as a quotient of a free $\mathbb{Z}$-module of finite rank. Let G be an abelian group (written multiplicatively) generated by a set $S = \{g_j\}_{j=1}^{\ell}$. Then, we have a surjective homomorphism $\psi : \mathbb{Z}^\ell \to G$, defined by

$$\psi : (x_1, \ldots, x_\ell) \mapsto \prod_{j=1}^{\ell} g_j^{x_j}.$$

As $\mathbb{Z}$ is a Noetherian ring, the kernel of ψ is finitely generated, say by $R = \{r_i\}_{i=1}^{k}$. We can arrange the r_i's into a $k \times \ell$ matrix with entries in $\mathbb{Z}$, say A. Note that the row space[4] of A is the kernel of ψ. Now $A = CDB$ as in Theorem 2.7. Since row operations do not change the row space of A, we can replace A with $A' = C^{-1}A$, whose rows form a new generating set R' of $\ker\psi$. The rows of B form a basis of $\mathbb{Z}^\ell$, say $\mathbf{b}_1, \ldots, \mathbf{b}_\ell$. The k rows of $A' = DB$ are $a_1\mathbf{b}_1, \ldots, a_r\mathbf{b}_r, 0, \ldots, 0$, hence

$$\begin{aligned} G &\cong \mathbb{Z}^\ell / \ker\psi \cong (\mathbb{Z}\mathbf{b}_1 \oplus \cdots \oplus \mathbb{Z}\mathbf{b}_\ell) / (\mathbb{Z}a_1\mathbf{b}_1 \oplus \cdots \oplus \mathbb{Z}a_r\mathbf{b}_r) \\ &\cong \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_r} \times \mathbb{Z}^{\ell - r}. \end{aligned}$$

Explicitly, G is the direct product of cyclic subgroups generated by the elements

$$\psi(\mathbf{b}_i) = \prod_{j=1}^{\ell} g_j^{b_{i,j}}.$$

Dropping any $a_i = 1$, this proves the existence of the invariant factor decomposition.

We should now derive the primary factor decomposition. This makes use of the Chinese Remainder Theorem, stating that

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm} \iff \gcd(n, m) = 1.$$

Let

$$G \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_m} \times \mathbb{Z}^n$$

be an invariant factor decomposition of G. Suppose the distinct prime factors of d_m are $p_1, p_2, \ldots, p_t$. Then, for each i, let

$$d_i = p_1^{\alpha_1^{(i)}} \cdots p_t^{\alpha_t^{(i)}}$$

[4] In this setting, by row space we mean the submodule of $\mathbb{Z}^\ell$ generated by the rows.

be the prime factor decomposition of d_i where $\alpha_j^{(i)} \geq 0$. We can now make the substitution

$$\mathbb{Z}_{d_i} \rightsquigarrow \mathbb{Z}_{p_1^{\alpha_1^{(i)}}} \times \cdots \times \mathbb{Z}_{p_t^{\alpha_t^{(i)}}}.$$

After cleaning out any factors $\mathbb{Z}_1$, we get our primary factor decomposition of G. Conversely, a primary factor decomposition gives rise uniquely to an invariant factor decomposition. To do this, for each distinct prime in the decomposition, take the factor with the highest exponent and multiply them together. This is the highest factor in the invariant factor decomposition. Then, we repeat with the remaining prime factors until we get the invariant factor decomposition.

Now, we must prove uniqueness. Let

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}} \times \mathbb{Z}^n \tag{2.1}$$

be a primary factor decomposition of G. Consider the set

$$\mathrm{t}(G) := \{x \in G \mid o(x) < \infty\}.$$

Since G is abelian, $\mathrm{t}(G)$ is a subgroup, called the *torsion subgroup*. The isomorphism (2.1) induces the isomorphisms

$$\mathrm{t}(G) \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}} \quad \text{and} \quad {}^{G}\!/_{\mathrm{t}(G)} \cong \mathbb{Z}^n. \tag{2.2}$$

Therefore, n is the rank of the free group $G/\mathrm{t}(G)$, which is determined by G. Then, for any prime p, consider the p-subgroups of G, defined by

$$\mathrm{t}_p(G) := \{x \in G \mid o(x) = p^\ell, \ell \in \mathbb{N}_0\}.$$

First, note that $\mathrm{t}_p(G) \leq \mathrm{t}(G)$ for all primes p. Furthermore, looking at the first isomorphism in (2.2), we see that

$$\mathrm{t}_p(G) \cong \mathbb{Z}_{p^{\beta_1}} \times \cdots \times \mathbb{Z}_{p^{\beta_t}}$$

where the β_j are the α_i with $p_i = p$. Furthermore, we can order the factors so that $\beta_i \leq \beta_{i+1}$ without loss of generality. By the isomorphism, we can find generators $g_1, \ldots, g_t$ of $\mathrm{t}_p(G)$ such that

$$\mathrm{t}_p(G) = \langle g_1 \rangle \times \cdots \times \langle g_t \rangle.$$

We now consider the group homomorphism $\phi_p : \mathrm{t}_p(G) \to \mathrm{t}_p(G)$ defined by $x \mapsto x^p$. This homomorphism gives rise to a sequence of subgroups:

$$\begin{aligned} H_0 &= \mathrm{t}_p(G) \\ H_{j+1} &= \phi_p(H_j). \end{aligned}$$

Writing this in terms of the generators of $\mathrm{t}_p(G)$, we see that

$$\begin{aligned} H_j &= \langle g_1^{p^j} \rangle \times \cdots \times \langle g_t^{p^j} \rangle \\ \Rightarrow H_j &\cong \mathbb{Z}_{p^{\beta_{r_j}-j}} \times \cdots \times \mathbb{Z}_{p^{\beta_t - j}} \end{aligned}$$

where β_{r_j} is the least β_i such that $\beta_i > j$. Hence,

$$H_j / H_{j+1} = \langle g_1^{p^j} \rangle \times \cdots \times \langle g_t^{p^j} \rangle \Big/ \langle g_1^{p^{j+1}} \rangle \times \cdots \times \langle g_t^{p^{j+1}} \rangle$$

and, by the definition of β_{r_j}, we get that

$$H_j / H_{j+1} \cong \mathbb{Z}_p^{t+1-r_j}.$$

Therefore, the number $t+1-r_j$ is recoverable from G by

$$\log_p \left| H_j / H_{j+1} \right| = t + 1 - r_j.$$

Thus we are able to obtain the r_j's as the recursive sequence:

$$\begin{aligned} r_0 &:= 1, \\ r_j &:= r_{j-1} + \log_p \frac{\left| H_{j-1} / H_j \right|}{\left| H_j / H_{j+1} \right|}. \end{aligned}$$

Furthermore, we can recover the primary factor decomposition of $\mathrm{t}_p(G)$ from this sequence, as the factor $\mathbb{Z}_{p^j}$ will occur exactly $r_j - r_{j-1}$ times. □

2.2.2 Character groups

We should now prove a few useful facts about character groups.

Lemma 2.8. *Let G_1, G_2 be abelian groups. Then, $\widehat{G_1 \times G_2} \cong \widehat{G}_1 \times \widehat{G}_2$.*

Proof. Define $\iota_1 : G_1 \to G_1 \times G_2$ by $\iota_1(g) = (g, e)$ and $\iota_2 : G_2 \to G_1 \times G_2$ by $\iota_2(g) = (e, g)$. These are clearly homomorphisms of groups. For $\chi \in \widehat{G_1 \times G_2}$, define $\chi_1 = \chi \circ \iota_1$ and $\chi_2 = \chi \circ \iota_2$. Then, $\chi_1 : G_1 \to \mathbb{F}^\times$ and $\chi_2 : G_2 \to \mathbb{F}^\times$ are compositions of homomorphisms of groups, and thus $\chi_1 \in \widehat{G}_1$ and $\chi_2 \in \widehat{G}_2$. It is clear that the mapping $\chi \mapsto (\chi_1, \chi_2)$ a group homomorphism $\widehat{G_1 \times G_2} \to \widehat{G}_1 \times \widehat{G}_2$.

For the inverse of this mapping, consider two characters $\xi_1 \in \widehat{G_1}$ and $\xi_2 \in \widehat{G_2}$. Then define $\xi : G_1 \times G_2 \to \mathbb{F}^\times$ by $\xi((g_1, g_2)) = \xi_1(g_1)\xi_2(g_2)$. It is trivial to check that ξ is a character and that this construction gives the mapping $\widehat{G_1} \times \widehat{G_2} \to \widehat{G_1 \times G_2}$ which is the inverse of the mapping in the previous paragraph. $\square$

Theorem 2.6 and Lemma 2.8 allow us to describe the character group of any finitely generated abelian group. Let G be a cyclic group. A character is completely defined by its value on a generator. If $G \cong \mathbb{Z}$, then there are no restrictions on the value that the character can take, provided it is not zero. Therefore $\widehat{\mathbb{Z}} \cong \mathbb{F}^\times$. If $G \cong \mathbb{Z}_n$, then the order of the image of the generator must divide n. These are exactly the n-th roots of unity. As $\mathbb{F}$ is algebraically closed and of characteristic zero, we have n such distinct roots of unity. In fact, they form a cyclic subgroup of $\mathbb{F}^\times$. Therefore, $\widehat{\mathbb{Z}_n} \cong \mathbb{Z}_n$. Applying this and repeatedly using Lemma 2.8, we get the following result.

If

$$G \cong \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_m} \times \mathbb{Z}^n$$

then

$$\widehat{G} \cong \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_m} \times (\mathbb{F}^\times)^n s.$$

One should note here that if G is finite, then $|G| = |\widehat{G}|$. In fact, in this case we have that $G \cong \widehat{G}$, though there is no natural isomorphism.

The following result shows that the character group of a finite abelian group behaves similarly to the dual space of a finite dimensional vector space.

Lemma 2.9. *If G is a finite abelian group, $\mathbb{F}$ is algebraically closed and of characteristic zero, and $H = \widehat{G}$, then there exists a natural isomorphism $\phi : G \to \widehat{H}$ defined by*

$$\phi(g)(\chi) = \chi(g) \quad \forall g \in G, \chi \in H.$$

Proof. It is routine to verify that ϕ is a homomorphism. Furthermore, $|G| = |H| = |\widehat{H}|$, and so if ϕ is injective then it is a group isomorphism. To prove injectivity, suppose $x, y \in G$ such that $\phi(x) = \phi(y)$. That is, for all $\chi \in H$, we have $\chi(x) = \phi(x)(\chi) = \phi(y)(\chi) = \chi(y)$. By Corollary 2.2, we know that this implies $x = y$. $\square$

This provides us with a highly useful corollary.

Corollary 2.10. *Let G be a finite abelian group and $H = \widehat{G}$ the character group. For any subgroup $K \leqslant H$ we have $(K^\perp)^\perp = K$.*

Proof. First, it is clear that $K \subset (K^\perp)^\perp$. It only remains to prove that $(K^\perp)^\perp \subset K$. Suppose not. Then there is some $\chi \in (K^\perp)^\perp$ such that $\chi \notin K$. By Corollary 2.3 we know there exists some $f \in \widehat{H}$ such that $f(k) = 1$ for all $k \in K$ and $f(\chi) \neq 1$. By Lemma 2.9 there exists some $g \in G$ such that $\phi(g) = f$, so $1 = f(k) = \phi(g)(k) = k(g)$ for all $k \in K$. By definition we have $g \in K^\perp$. Now, $1 \neq f(\chi) = \phi(g)(\chi) = \chi(g)$, a contradiction as $\chi \in (K^\perp)^\perp$. $\square$

2.3 Gradings and algebraic actions

Recall from Section 2.1 that a G-grading Γ on a vector space V gives rise to a $\widehat{G}$-action on V which we denoted by $\eta_\Gamma : \widehat{G} \to \mathrm{GL}(V)$. From Section 2.2 we also have that for a finitely generated abelian group G, the character group $\widehat{G}$ has the form $K \times (\mathbb{F}^\times)^n$ where K is a finite abelian group. Recall from Chapter 1 that these are known in algebraic group theory as *quasitori*, which are characterized in the category of algebraic groups by being diagonalizable.

This gives us the conditions under which we can go from an action to a grading. If a homomorphism $\varrho : \widehat{G} \to \mathrm{GL}(V)$ is an algebraic group homomorphism[5] – that is, given by a polynomial map – then ϱ will give rise to a grading. See e.g. [5, p. 20].

Lemma 2.11. *Suppose that G is a finitely generated abelian group, V is a finite dimensional[6] vector space over a field $\mathbb{F}$, with $\mathbb{F}$ algebraically closed and of characteristic zero. For any G-grading Γ on V, $\eta_\Gamma : \widehat{G} \to \mathrm{GL}(V)$ is a homomorphism of algebraic groups. Conversely, if $\varrho : \widehat{G} \to \mathrm{GL}(V)$ is a*

[5] Note that both $\widehat{G}$ and $\mathrm{GL}(V)$ are (affine) algebraic groups

[6] This can be generalized to infinite dimensions if we use the definition that an action is algebraic if it is locally finite dimensional and if W is an invariant finite dimensional subspace of V, then $\mathrm{GL}(W)$ is an algebraic group.

homomorphism of algebraic groups, then there exists a unique G-grading Γ on V such that $\eta_\Gamma = \varrho$.

Here we can prove the following special case. (Compare with Lemma 2.5.)

Lemma 2.12. *Let G be a finite abelian group, and let V be a vector space as in Lemma 2.11. Then, for any group action $\varrho : \widehat{G} \to \mathrm{GL}(V)$, there exists a group grading Γ on V such that $\eta_\Gamma = \varrho$.*

Proof. Let $H = \widehat{G}$. As G is finite, H is also finite of the same order. Denote $|G| = |H| = N$. Then, for every operator $\varrho(\chi)$, we have $\varrho(\chi)^N - I = 0$. Thus, we know that the characteristic polynomial of $\varrho(\chi)$ divides $x^N - 1$, which splits over our field $\mathbb{F}$. Therefore, for all $\chi \in H$, we have that $\varrho(\chi)$ is diagonalizable. Furthermore, as H is abelian, we know that the operators commute, and are thus simultaneously diagonalizable. Let the simultaneous eigenspaces be $V_1, \ldots, V_k$. Consider one of these eigenspaces, say V_i. Now, for every $\chi \in H$, we have that $\varrho(\chi)$ acts as a scalar on V_i. Denote this scalar $\lambda_\chi^{(i)}$. The map $\eta_i : H \to \mathbb{F}^\times$ given by $\eta_i(\chi) = \lambda_\chi^{(i)}$ is a character of H. As G is finite and abelian, we know that $\widehat{H} \cong G$ in a natural way by Lemma 2.9. Therefore, there exists $g_i \in G$ such that $\chi(g_i) = \lambda_\chi^{(i)}$ for all $\chi \in H$. By assigning $\deg(V_i) = g_i$, we get the grading Γ that we were looking for. □

Moving now to gradings on algebras, we can determine if a grading on the underlying vector space is a grading on the algebra through the canonical action associated to the grading. See e.g. [3, Prop. 1.24].

Lemma 2.13. *Let $\mathcal{A}$ be an algebra over an algebraically closed field of characteristic zero and let G be an abelian group. Suppose Γ is a G-grading on the underlying vector space of $\mathcal{A}$. Then Γ is a grading on the algebra $\mathcal{A}$ if and only if $\mathrm{im}(\eta_\Gamma) \subset \mathrm{Aut}(\mathcal{A})$.*

Proof. Let $a_1, a_2 \in \mathcal{A}$ be homogeneous elements of degrees $g_1, g_2 \in G$ respectively. By Lemma 2.5 the element $a_1 a_2$ has degree $g_1 g_2$ if and only if, for all $\chi \in \widehat{G}$,

$$\eta_\Gamma(\chi)(a_1 a_2) = \chi(g_1 g_2) a_1 a_2. \tag{2.3}$$

Since

$$\chi(g_1 g_2) a_1 a_2 = \chi(g_1)\chi(g_2) a_1 a_2 = \chi(g_1) a_1 \chi(g_2) a_2 = \eta_\Gamma(\chi)(a_1)\eta_\Gamma(\chi)(a_2),$$

Equation (2.3) holds for all homogeneous elements a_1, a_2 if and only if $\eta_\Gamma(\chi) \in \mathrm{Aut}(\mathcal{A})$. □

Chapter 3

Group Gradings on Matrix Algebras

3.1 Preliminaries on matrix algebras

For computations involving matrix algebras, there are several results that will be extremely useful. First, we need this well-known result, see e.g. [8, Corollary 17.8].

Lemma 3.1. *For an algebra $\mathcal{A}$, the only ideals of $M_n(\mathcal{A})$ are of the form $M_n(\mathcal{I})$ where $\mathcal{I} \subset \mathcal{A}$ is a ideal of $\mathcal{A}$.*

This means that in particular, an algebra $\mathcal{A}$ is *simple* (that is, $\mathcal{A}^2 \neq 0$ and the only ideals of $\mathcal{A}$ are $\{0\}$ and $\mathcal{A}$) if and only if $M_n(\mathcal{A})$ is simple.

Another well known result that is going to be useful concerns the structure of the center of a matrix algebra.[1]

Lemma 3.2. *For an algebra $\mathcal{A}$, we have*

$$\mathcal{Z}(M_n(\mathcal{A})) = \{aI_n \mid a \in \mathcal{Z}(\mathcal{A})\}.$$

Proof. Consider $\iota : \mathcal{Z}(\mathcal{A}) \to M_n(\mathcal{A})$ defined by $\iota : a \mapsto aI_n$. As $\ker(\iota) = \{0\}$, ι is injective. It thus remains to show that $\operatorname{im}(\iota) = \mathcal{Z}(M_n(\mathcal{A}))$. Let $X \in \mathcal{Z}(M_n(\mathcal{A}))$. Note that $X = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,j} E_{i,j}$ for $a_{i,j} \in \mathcal{A}$. Therefore, we

[1] This can also be proven quickly from [8, Proposition 17.4].

have for all zI_n with $z \in \mathcal{A}$ that

$$XzI_n = zI_nX$$
$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{i,j}zE_{i,j} = \sum_{i=1}^{n}\sum_{j=1}^{n} za_{i,j}E_{i,j}$$

which give us that $a_{i,j} \in \mathcal{Z}(\mathcal{A})$ for all i, j.

$$XE_{k,\ell} = E_{k,\ell}X$$
$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{i,j}E_{i,j}E_{k,\ell} = \sum_{i=1}^{n}\sum_{j=1}^{n} E_{k,\ell}a_{i,j}E_{i,j}$$
$$\sum_{i=1}^{n} a_{i,k}E_{i,\ell} = \sum_{j=1}^{n} a_{\ell,j}E_{k,j}$$

This implies that $a_{i,k} = 0$ for all $i \neq k$. Therefore, we can write $X = \operatorname{diag}(a_1, a_2, \ldots, a_n)$ where $a_i \in \mathcal{Z}(\mathcal{A})$.

We can now consider the set of block-diagonal matrices

$$S_i := \operatorname{diag}_{n-1}\left(1, 1, \ldots, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \ldots, 1, 1\right)$$

where the 2×2 block is at the i-th position on the list.

$$S_iX = XS_i$$
$$\operatorname{diag}\left(a_1, \ldots, \begin{bmatrix} 0 & a_{i+1} \\ a_i & 0 \end{bmatrix}, \ldots, a_n\right) = \operatorname{diag}\left(a_1, \ldots, \begin{bmatrix} 0 & a_i \\ a_{i+1} & 0 \end{bmatrix}, \ldots, a_n\right).$$

Therefore, $a_i = a_{i+1}$ for all $1 \leq i < n$, and so all a_i are equal. That gives us that $X = aI_n$ for some $a \in \mathcal{Z}(\mathcal{A})$, or $\mathcal{Z}(M_n(\mathcal{A})) = \operatorname{im}(\iota)$. $\square$

These two lemmas together prove that matrix algebras are so-called *central simple* algebras. That is, they are simple, unital and their center is of the form $\mathbb{F}1$ where 1 is the unit element of the algebra.

As matrix algebras are central-simple, they satisfy the hypothesis of the Noether-Skolem theorem:

Theorem 3.3 (Noether-Skolem). *Let $\mathcal{A}$ be a central simple algebra. Then, any automorphism $\phi \in \operatorname{Aut}(\mathcal{A})$ is inner, that is, there exists some invertible element $a \in \mathcal{A}$ such that $\phi(x) = axa^{-1}$ for all $x \in \mathcal{A}$.*

In the case of matrix algebras, Szigeti and van Wyk in [12] provide an efficient construction of such a matrix A for a given automorphism ϕ as follows.

1. Consider the matrices $E_{n,1}$ and $S = E_{1,2} + E_{2,3} + \cdots + E_{n-1,n}$.
2. Let $P = \phi(E_{n,1})$ and $Q = \phi(S)$, and let $\mathbf{a} \in \ker(I_n - Q^{n-1}P)$ with $\mathbf{a} \neq 0$.
3. Then A is constructed of the columns $Q^{n-i}P\mathbf{a}$ as follows:

$$A = [\ Q^{n-1}P\mathbf{a} \mid Q^{n-2}P\mathbf{a} \mid \cdots \mid QP\mathbf{a} \mid P\mathbf{a}\ ]. \tag{3.1}$$

Proof. Note that $S^{n-1} = E_{1,n}$, so

$$I_n - \phi(S^{n-1}E_{n,1}) = I_n - \phi(E_{1,1}) = \phi(I_n - E_{1,1}) = \phi(E_{2,2} + E_{3,3} + \cdots + E_{n,n})$$

is not invertible, as that would imply that $E_{2,2} + E_{3,3} + \cdots + E_{n,n}$ is invertible. Since it is not invertible, there exists an $\mathbf{a} \in \mathbb{F}^n, \mathbf{a} \neq 0$ such that $(I_n - \phi(E_{1,1}))\,\mathbf{a} = 0$. As $S^{n-1} = E_{1,n}$ and $S^{n-1}E_{n,1} = E_{1,1}$, we have that $Q^{n-1}P = \phi(E_{1,1})$ and thus $Q^{n-1}P\mathbf{a} = \mathbf{a}$. Furthermore, as $S^iE_{j,1} = E_{j-i,1}$ for $1 \leq i < j \leq n$, and so $S^n = E_{n,1}S^{n-2}E_{n,1} = \cdots = E_{n,1}SE_{n,1} = E_{n,1}^2 = 0$, we have that $Q^n = PQ^{n-2}P = \cdots = PQP = P^2 = 0$.

Claim: $AE_{n,1} = PA$ and $AS = QA$, where A is defined by equation (3.1).

Since

$$AE_{n,1} = [\ P\mathbf{a} \mid 0 \mid \cdots \mid 0 \mid 0\ ]$$

and

$$PA = [\ PQ^{n-1}P\mathbf{a} \mid PQ^{n-2}P\mathbf{a} \mid \cdots \mid PQP\mathbf{a} \mid P^2\mathbf{a}\ ],$$

we get by the observations above that $AE_{n,1} = PA$. Now, since

$$AS = AE_{1,2} + AE_{2,3} + \cdots + AE_{n-1,n} = [\ 0 \mid Q^{n-1}P\mathbf{a} \mid \cdots \mid Q^2P\mathbf{a} \mid QP\mathbf{a}\ ]$$

and

$$QA = [\ Q^nP\mathbf{a} \mid Q^{n-1}P\mathbf{a} \mid \cdots \mid Q^2P\mathbf{a} \mid QP\mathbf{a}\ ],$$

then $Q^n = 0$ gives that $AS = QA$. To show that A is invertible, consider a linear combination of the column vectors of A that sums to zero:

$$\lambda_{n-1}Q^{n-1}P\mathbf{a} + \lambda_{n-2}Q^{n-2}P\mathbf{a} + \cdots + \lambda_1QP\mathbf{a} + \lambda_0P\mathbf{a} = 0.$$

Multiplying on the left by Q^{n-1} and using $Q^{n-1}P\mathbf{a} = \mathbf{a} \neq 0$ and $Q^n = 0$, we get that $\lambda_0\mathbf{a} = \lambda_0 Q^{n-1}P\mathbf{a} = 0$, thus $\lambda_0 = 0$. Then, left multiplication by Q^{n-2} gives that $\lambda_1\mathbf{a} = \lambda_1 Q^{n-1}P\mathbf{a} = 0$, so $\lambda_1 = 0$. Repeating these left multiplications we get that $\lambda_0 = \lambda_1 = \cdots = \lambda_{n-1} = 0$. We have shown that the columns of A are linearly independent, so A is invertible.

Now, $AE_{n,1} = PA$ and $AS = QA$ implies that $AE_{n,1}A^{-1} = P = \phi(E_{n,1})$ and $ASA^{-1} = Q = \phi(S)$. As we can express $E_{i,j} = S^{n-i}E_{n,1}S^{j-1}$ for all $1 \leq i, j \leq n$, the matrices $E_{n,1}$ and S generate $M_n(\mathbb{F})$ as a $\mathbb{F}$-algebra, and so $AXA^{-1} = \phi(X)$ for all $X \in M_n(\mathbb{F})$. □

3.2 Graded-simple algebras with a descending chain condition

Let $\mathcal{A}$ be a G-graded algebra. We say $\mathcal{A}$ is *simple as a graded algebra*, or *graded-simple* for short, if $\mathcal{A}^2 \neq \{0\}$ and the only two *graded* ideals of $\mathcal{A}$ are $\{0\}$ and $\mathcal{A}$.

One should note that a graded algebra being simple does not imply that the underlying algebra is simple. If we have a simple algebra, then any grading defined on that algebra will make it graded-simple.

We will need the classical Wedderburn theorem and its graded analogue. For a proof of the classical one, see e.g. [11, Corollary. 8.63i].

Theorem 3.4 (Wedderburn Theorem). *Suppose R is a simple associative algebra satisfying the descending chain condition on left ideals. Then $R \cong M_n(\Delta)$ for Δ a division algebra. Furthermore, if $M_n(\Delta) \cong M_{n'}(\Delta')$ then $n = n'$ and $\Delta \cong \Delta'$.*

Graded versions have been given in [1, Thm. 4], [2, Thm. 5.1], [9, Cor. 4.6.7] and [5, Thm. 2.6]. Here we state the latter, which is the most general.

Theorem 3.5. *Let $\mathcal{A}$ be a graded-simple G-graded algebra, satisfying the descending chain condition on graded left ideals, where G is an arbitrary group. Then, there exists a G-graded algebra $\mathcal{D}$ and a graded right $\mathcal{D}$-module V such that $\mathcal{D}$ is a graded-division algebra, V is of finite rank, and $\mathcal{A} \cong \mathrm{End}_{\mathcal{D}}(V)$ as a graded algebra.*

One will note that this is not the exact same formulation as Theorem 3.4. We can, however, restate it in a more comparable form.[2]

[2]Uniqueness will be covered separately in Theorem 3.6.

We can rewrite $\mathrm{End}_{\mathcal{D}}(V)$ in terms of the tensor product of matrix algebras. First, recall that, by Lemma 1.2, we have a $\mathcal{D}$-basis of V consisting of homogeneous elements, say $v_1, \ldots, v_k \in V$, for which we denote $g_i = \deg(v_i)$. Representing endomorphisms of the $\mathcal{D}$-module V with matrices in the standard way, we know that $\mathrm{End}_{\mathcal{D}}(V) \cong M_k(\mathcal{D})$. Explicitly, $r \in \mathrm{End}_{\mathcal{D}}(V)$ is represented by the matrix $(x_{i,j})$ given by

$$rv_j = \sum_{i=1}^{k} v_i x_{i,j}.$$

Now, we know that $\mathcal{A} \cong M_k(\mathcal{D})$. The grading on $M_k(\mathcal{D})$ is inherited from the grading on $\mathrm{End}_{\mathcal{D}}(V)$. Consider the matrix unit $E_{i,j}$ as an endomorphism; it satisfies the relations $E_{i,j}(v_j) = v_i$ and $E_{i,j}(v_{j'}) = 0$ for all $j' \neq j$. Hence, $E_{i,j} \in \mathrm{End}_{\mathcal{D}}(V)_{g_i g_j^{-1}}$. This implies that the subalgebra $M_k(\mathbb{F})$ has the elementary grading with the k-tuple $\mathbf{g} = (g_1, g_2, \ldots, g_k)$ (see equation (1.4)). The grading on the entire $M_k(\mathcal{D})$ is determined as follows: $\deg(E_{i,j} \otimes d) = g_i t g_j^{-1}$ for any $d \in \mathcal{D}_t$. Here we identify $M_k(\mathcal{D})$ with the tensor product $M_k(\mathbb{F}) \otimes \mathcal{D}$ with $E_{i,j} \otimes d$ being identified with the matrix that has d in position (i, j) and 0 elsewhere. Note that if G is abelian, then $g_i t g_j^{-1} = g_i g_j^{-1} t$, so the G-grading on $M_k(\mathbb{F}) \otimes \mathcal{D}$ is a tensor product grading.

If $\mathcal{D}$ is a matrix algebra, $\mathcal{D} \cong M_\ell(\mathbb{F})$, then we can identify $M_k(\mathbb{F}) \otimes \mathcal{D}$ with $M_{k\ell}(\mathbb{F})$ by Kronecker product. The Kronecker product of two matrices, A and B, is defined as the block matrix

$$A \otimes B = \begin{bmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,k}B \\ a_{2,1}B & a_{2,2}B & \cdots & a_{2,k}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{k,1}B & a_{k,2}B & \cdots & a_{k,k}B \end{bmatrix}$$

Conversely, if $\mathcal{A}$ is a matrix algebra $M_n(\mathbb{F})$ then $\mathcal{D}$ must be a matrix algebra $M_\ell(\mathbb{F})$ where $n = k\ell$. Indeed, in this case we have that

$$M_n(\mathbb{F}) \cong M_k(\mathcal{D}).$$

We know that $M_n(\mathbb{F})$ is simple by Lemma 3.1. Hence, by the same lemma, $\mathcal{D}$ is also simple, and furthermore it is finite dimensional. Therefore, we know that $\mathcal{D} \cong M_\ell(\Delta)$ by Theorem 3.4. Thus, we get that

$$\begin{aligned} M_n(\mathbb{F}) &\cong M_k(\mathbb{F}) \otimes M_\ell(\Delta) \\ \Rightarrow M_n(\mathbb{F}) &\cong M_{k\ell}(\Delta). \end{aligned}$$

By Theorem 3.4, we know that this implies that $\Delta \cong \mathbb{F}$ and $k\ell = n$.

If a grading Γ on a matrix algebra $M_n(\mathbb{F})$ makes $M_n(\mathbb{F})$ a graded-division algebra, we will call Γ a *division grading.* This matrix interpretation of Theorem 3.5 provides us with something we already mentioned in Section 1.3, that any grading on a matrix algebra is a combination of an elementary grading and a division grading. Therefore, we can describe a grading on a matrix algebra by a pair $(\mathcal{D}, \kappa)$ of a matrix algebra with a division grading and a multiplicity function $\kappa : G/T \to \mathbb{N}_0$ with finite support where $T = \mathrm{supp}(\mathcal{D})$ (see Lemma 1.3).

As of right now, we have a description, not a classification. As such, we need to analyze which of the pairs $(\mathcal{D}, \kappa)$ correspond to isomorphic graded algebras. We will use a definition from [5, Def. 2.9]. Let $\mathcal{D}$ and $\mathcal{D}'$ be graded-division algebras graded by a group G, V a graded right $\mathcal{D}$-module and V' a graded right $\mathcal{D}'$-module. An *isomorphism from* $(\mathcal{D}, V)$ *to* $(\mathcal{D}', V')$ is a pair (ψ_0, ψ_1) where $\psi_0 : \mathcal{D} \to \mathcal{D}'$ is an isomorphism of graded algebras and $\psi_1 : V \to V'$ is an isomorphism of graded spaces such that $\psi_1(vd) = \psi_1(v)\psi_0(d)$ for all $v \in V$, $d \in \mathcal{D}$.

Theorem 3.5 does not give a uniqueness statement necessary for a classification. For that, we need another theorem from [5, Thm. 2.10].

Theorem 3.6. *Let G be a group, and $\mathcal{D}$ and $\mathcal{D}'$ be G-graded algebras that are graded-division algebras. Let V be a graded right $\mathcal{D}$-module and V' be a graded right $\mathcal{D}'$-module, both of finite and nonzero rank. Let $\mathcal{A} = \mathrm{End}_{\mathcal{D}}(V)$ and $\mathcal{A}' = \mathrm{End}_{\mathcal{D}'}(V')$. If $\psi : \mathcal{A} \to \mathcal{A}'$ is an isomorphism of G-graded algebras, then there exists $g \in G$ and an isomorphism (ψ_0, ψ_1) from $({}^{[g^{-1}]}\mathcal{D}^{[g]}, V^{[g]})$ to $(\mathcal{D}', V')$ such that $\psi(r) = \psi_1 r \psi_1^{-1}$ for all $r \in \mathcal{A}$. Conversely, given an isomorphism (ψ_0, ψ_1) from $({}^{[g^{-1}]}\mathcal{D}^{[g]}, V^{[g]})$ to $(\mathcal{D}', V')$, the mapping $\psi : \mathcal{A} \to \mathcal{A}'$ defined by $\psi(r) = \psi_1 r \psi_1^{-1}$ is an isomorphism of G-graded algebras.*

Having classified graded $\mathcal{D}$-modules, we can restate the existence of an isomorphism ψ_1 for a given ψ_0 in terms of the multiplicity functions κ and κ' associated to V and V'. Restating [5, Def. 2.11] in our terms, we will write $(\mathcal{D}, \kappa) \sim (\mathcal{D}', \kappa')$ if there exists $g \in G$ such that $\mathcal{D}' \cong^{[g^{-1}]} \mathcal{D}^{[g]}$, and $\kappa' = \kappa^{[g]}$.

3.3 Division gradings on matrix algebras

We now turn to classifying graded-division algebras themselves, with a focus on the special case of matrix algebras over an algebraically closed field of characteristic zero. Suppose $\mathcal{D}$ is a G-graded, graded-division algebra with one-dimensional homogeneous components and suppose $T = \text{supp}(\mathcal{D})$ is an abelian subgroup. We can then define an *alternating bicharacter* β on T, that is, a mapping $\beta : T \times T \to \mathbb{F}^\times$ with the properties that β is multiplicative in each variable and $\beta(t,t) = 1$ for all $t \in T$.[3] We define it by

$$X_s X_t = \beta(s,t) X_t X_s$$

for $s, t \in T$ and $X_s \in \mathcal{D}_s, X_t \in \mathcal{D}_t$.

This β is a well defined bicharacter as follows. It is well-defined as each $\mathcal{D}_t$ is one-dimensional, $X_t, Y_t \in \mathcal{D}_t \setminus \{0\}$ implies that there exists some $\mu \in \mathbb{F}^\times$ such that $Y_t = \mu X_t$. Therefore, for all $X_s \in \mathcal{D}_s$,

$$X_s Y_t = \beta(s,t) Y_t X_s \iff X_s X_t = \beta(s,t) X_t X_s.$$

As such, $\beta(s,t)$ does not depend on what X_s, X_t we chose. Noting that β is alternating is similarly simple:

$$X_s X_s = \beta(s,s) X_s X_s \Rightarrow \beta(s,s) = 1.$$

We will need to prove that β is multiplicative in the first variable; the proof for the second variable is similar.

$$\begin{aligned}
(X_s X_t) X_u &= \beta(st, u) X_u (X_s X_t) \\
X_s \beta(t,u) X_u X_t &= \beta(st, u) X_u X_s X_t \\
\beta(t,u)\beta(s,u) X_u X_s X_t &= \beta(st,u) X_u X_s X_t \\
\Rightarrow \beta(st,u) &= \beta(s,u)\beta(t,u).
\end{aligned}$$

Any alternating bicharacter is *skew-symmetric* in the multiplicative sense:

$$\beta(t,s) = \beta(s,t)^{-1} \quad \forall s,t \in T.$$

This is easy to prove using the multiplicativity of β as follows:

$$1 = \beta(st,st) = \beta(s,s)\beta(s,t)\beta(t,s)\beta(t,t) = \beta(s,t)\beta(t,s).$$

[3]The assumption of one dimensional components makes $\mathcal{D}$ a so-called *twisted group algebra*, denoted $\mathbb{F}^\sigma T$ where $\sigma : T \times T \to \mathbb{F}^\times$ is a *2-cocycle*. The alternating bicharacter can thus be defined in terms of the cocycle σ by $\beta(s,t) = \frac{\sigma(s,t)}{\sigma(t,s)}$ as in [5, p. 35]. However, any further discussion of this is beyond the scope of this thesis.

We will call β *nondegenerate* if $\beta(s,t) = 1$ for all $t \in T$ implies $s = e$. The *radical* of β is defined as

$$\operatorname{rad}(\beta) := \{s \in T \mid \beta(s,t) = 1 \quad \forall t \in T\}.$$

So β being nondegenerate is the same as stating that $\operatorname{rad}(\beta) = \{e\}$.

Our assumptions that T is abelian and the components of $\mathcal{D}$ are one-dimensional hold if G is abelian and the ground field $\mathbb{F}$ is algebraically closed (see Section 1.3). In this case, finite-dimensional graded-division algebras are classified by pairs (T, β) [6, Sec. 2.2].[4] That is, for any pair (T, β) where T is a finite subgroup of G and β is an alternating bicharacter on T, there is a unique isomorphism class of graded-division algebras. Since we are interested in gradings on matrix algebras, the alternating bicharacter β will be nondegenerate, as we show through a discussion of the center of the algebra $\mathcal{A} = \operatorname{End}_{\mathcal{D}}(V)$.

Lemma 3.7. *Let G be an abelian group and $\mathcal{A} = \operatorname{End}_{\mathcal{D}}(V)$ a G-graded algebra where $\mathcal{D}$ is a graded-division algebra and V is a nonzero graded right $\mathcal{D}$-module of finite rank. Then*

$$\mathcal{Z}(\mathcal{A}) \cong \mathcal{Z}(\mathcal{D}).$$

Proof. Consider the mapping $\Psi : \mathcal{D}^{\mathrm{op}} \to \operatorname{End}^{\mathrm{gr}}_{\mathbb{F}}(V)$ where $\Psi(c) : v \mapsto vc$. Since G is abelian, this is a homomorphism of G-graded algebras where $\mathcal{D}^{\mathrm{op}}$ is the opposite algebra of $\mathcal{D}$, that is, it has the same underlying set but the operation is $(x, y) \mapsto yx$. We thus know that $\ker(\Psi)$ must be a graded ideal of $\mathcal{D}$. However, $\mathcal{D}$ is a graded-division algebra, so the only graded ideals are $\{0\}$ and $\mathcal{D}$. Note that $\Psi(1_{\mathcal{D}}) = \mathrm{id}_V$, so $\ker(\Psi) = \{0\}$ and Ψ is injective.

If we restrict the domain of the mapping $\Psi|_{\mathcal{Z}(\mathcal{D})} =: \psi$, we can also restrict the codomain to $\operatorname{End}_{\mathcal{D}}(V)$ by noting that for any $c \in \mathcal{Z}(\mathcal{D})$, $d \in \mathcal{D}$ and $v \in V$,

$$\psi(c)(vd) = vdc = vcd = \psi(c)(v)d,$$

so $\psi(c) \in \operatorname{End}_{\mathcal{D}}(V)$. This is furthermore the largest subdomain of Ψ such that the image is in $\operatorname{End}_{\mathcal{D}}(V)$. If $c \notin \mathcal{Z}(\mathcal{D})$ then there exists $d \in \mathcal{D}$ such that $cd \neq dc$, hence by injectivity of Ψ, there exists $v \in V$ such that

$$vcd \neq vdc \;\Leftrightarrow\; \Psi(c)(vd) \neq \Psi(c)(v)d,$$

[4] For a proof without cohomology, see e.g. [3, Prop. 2.32].

which means that $\Psi(c) \in \mathrm{End}_{\mathcal{D}}(V)$ if and only if $c \in \mathcal{Z}(\mathcal{D})$. Thus $\mathcal{Z}(\mathcal{D})$ is the inverse image of $\mathrm{End}_{\mathcal{D}}(V)$ under Ψ, which implies that $\mathcal{Z}(\mathcal{D})$ is a graded subalgebra of $\mathcal{D}$.[5]

The restriction $\psi : \mathcal{Z}(\mathcal{D}) \to \mathrm{End}_{\mathcal{D}}(V)$ is an injective homomorphism of graded algebras. By fixing a basis of V we can identify $\mathrm{End}_{\mathcal{D}}(V) \cong M_k(\mathcal{D})$. By Lemma 3.2, $\operatorname{im}\psi = \mathcal{Z}(\mathrm{End}_{\mathcal{D}}(V))$. □

Now we characterize the center of $\mathcal{D}$.

Lemma 3.8. *Let G be an abelian group and $\mathcal{D}$ a graded-division algebra graded by G with support T such that $\dim(\mathcal{D}_t) = 1$ for all $t \in T$. Then*

$$\mathcal{Z}(\mathcal{D}) = \bigoplus_{t \in \mathrm{rad}(\beta)} \mathcal{D}_t.$$

Proof. Let $X_s \in \mathcal{D}_s$ for some $s \in \mathrm{rad}(\beta)$ and $X_t \in \mathcal{D}_t$ for some $t \in T$. We then have that

$$X_s X_t = \beta(s,t) X_t X_s = X_t X_s.$$

As X_s commutes with all homogeneous elements, by linearity it commutes with all elements, and thus $X_s \in \mathcal{Z}(\mathcal{D})$, which implies that $\mathcal{D}_s \subset \mathcal{Z}(\mathcal{D})$. Again by linearity, this implies that $\bigoplus_{t \in \mathrm{rad}(\beta)} \mathcal{D}_t \subset \mathcal{Z}(\mathcal{D})$.

Consider $X \in \mathcal{Z}(\mathcal{D})$, $X = X_{s_1} + X_{s_2} + \cdots + X_{s_k}$ where $X_{s_i} \in \mathcal{D}_{s_i}$ and $s_i \neq s_j$ for $i \neq j$. Let $Y_t \in \mathcal{D}_t \setminus \{0\}$ for some $t \in T$. We then have

$$\begin{aligned} XY_t &= Y_t X \\ \left(\sum_{i=1}^{k} X_{s_i}\right) Y_t &= Y_t \left(\sum_{i=1}^{k} X_{s_i}\right) \\ \sum_{i=1}^{k} \beta(t, s_i) Y_t X_{s_i} &= \sum_{i=1}^{k} Y_t X_{s_i}. \end{aligned}$$

Since $\deg(Y_t X_{s_i}) = t s_i$ are distinct for distinct i, we know that $\beta(s_i, t) Y_t X_{s_i} = Y_t X_{s_i}$. As $t \in T$ is arbitrary, that means that $s_i \in \mathrm{rad}(\beta)$ for all i, so $X \in \bigoplus_{t \in \mathrm{rad}(\beta)} \mathcal{D}_t$. □

By Lemmas 3.7 and 3.8 if $\mathcal{A} = \mathrm{End}_{\mathcal{D}}(V)$ is a matrix algebra then the alternating bicharacter β corresponding to $\mathcal{D}$ is nondegenerate. Here we will

[5] This can also be shown directly by an argument similar to the proof of Lemma 3.8.

show that, conversely, if $\beta : T \times T \to \mathbb{F}^\times$ is nondegenerate then there exists a matrix algebra with a division grading that corresponds to (T, β). This can be done using a *symplectic basis* of T, by which we mean a generating set $\{a_i, b_i\}_{i=1}^r$ of T satisfying, for all $1 \leq i, j \leq r$,

$$\beta(a_i, a_j) = 1, \tag{3.2}$$

$$\beta(b_i, b_j) = 1, \tag{3.3}$$

$$\beta(a_i, b_j) = \varepsilon_i^{\delta_{i,j}}, \tag{3.4}$$

$$\mathrm{o}(a_i) = \mathrm{o}(b_i) = \mathrm{o}(\varepsilon_i), \tag{3.5}$$

where $\mathrm{o}(t)$ is the order of an element t, $\delta_{i,j}$ is the Kronecker delta and ε_i is a root of unity in $\mathbb{F}$ (primitive of order $\mathrm{o}(a_i)$).

Lemma 3.9. *If a generating set $B = \{a_1, b_1, a_2, b_2, \ldots, a_r, b_r\}$ of T satisfies equations* (3.2),(3.3),(3.4) *and* (3.5) *then it is a reduced generating set, that is,*

$$T = \langle a_1 \rangle \times \langle b_1 \rangle \times \cdots \times \langle a_r \rangle \times \langle b_r \rangle.$$

Proof. Let $t = a_1^{x_1} b_1^{y_1} \cdots a_r^{x_r} b_r^{y_r}$. Then for each i, we have $\beta(a_i, t) = \varepsilon_i^{y_i}$ and $\beta(t, b_i) = \varepsilon_i^{x_i}$. In view of equation (3.5), the congruence classes of x_i and y_i modulo $\mathrm{o}(a_i) = \mathrm{o}(b_i)$ depend only on t, which shows that B is a reduced generating set. □

The algorithm below is based on the discussion found in [5, p. 35–36].

Algorithm 3.10. *Input: A generating set $\{t_i\}_{i=1}^n$ of a finite abelian group T and a nondegenerate alternating bicharacter β on T.*

Output: A symplectic basis of T with respect to β, say $\{a_i, b_i\}_{i=1}^r$.

Let $T = \mathrm{t}_{p_1}(T) \times \mathrm{t}_{p_2}(T) \times \cdots \times \mathrm{t}_{p_k}(T)$ be the decomposition of T into p_i-torsion subgroups. We can convert an element $t \in T$ into this representation by

$$t \mapsto (t^{w_1}, t^{w_2}, \ldots, t^{w_k})$$

with $0 \leq w_i < \mathrm{o}(t)$ and

$$w_i \equiv 1 \left(\mathrm{mod}\, p_i^{\nu_{p_i}(\mathrm{o}(t))} \right) \quad \text{and} \quad w_i \equiv 0 \left(\mathrm{mod}\, \frac{\mathrm{o}(t)}{p_i^{\nu_{p_i}(\mathrm{o}(t))}} \right),$$

where $\nu_q(n)$ is the q-adic order of n, that is, the greatest integer such that $q^{\nu_q(n)} \mid n$. We can find these w_i through the Chinese Remainder Theorem.

If $s \in \mathrm{t}_{p_i}(T)$ and $t \in \mathrm{t}_{p_j}(T)$ for $i \neq j$ then, since β is a bicharacter, we have $\beta(s,t)^{\mathrm{o}(s)} = 1 = \beta(s,t)^{\mathrm{o}(t)}$, which implies $\beta(s,t) = 1$. Hence, if we construct a symplectic basis for each $\mathrm{t}_{p_i}(T)$, we can combine them into a single symplectic basis for T. As such, we may assume without loss of generality that T is a q-group where q is prime.

Let $\{t_1, t_2, \dots, t_n\}$ be a generating set of T. We will proceed with a modified version of the Gram-Schmidt process. Let the exponent of T be q^N. As β is a bicharacter, we know that $\beta(s,t)$ is a q^N-th root of unity for all $s, t \in T$. Fix a primitive q^N-th root of unity ω. We will proceed by induction.

Pick i, j such that $\beta(t_i, t_j) = \omega^m$ and $\nu_q(m)$ is minimal. As β is alternating, we have $i \neq j$, so without loss of generality, assume that $i = 1$ and $j = 2$. We now modify each t_i for $i \neq 1, 2$. Consider

$$\beta(t_1, t_i t_1^{x_i} t_2^{y_i}) = \beta(t_1, t_i)\beta(t_1, t_1^{x_i})\beta(t_1, t_2^{y_i}) = \beta(t_1, t_i)\omega^{m y_i}$$

and

$$\beta(t_2, t_i t_1^{x_i} t_2^{y_i}) = \beta(t_2, t_i)\beta(t_2, t_1^{x_i})\beta(t_2, t_2^{y_i}) = \beta(t_2, t_i)\omega^{-m x_i}.$$

As we know that, for all i, j, $\beta(t_i, t_j)$ is a power of ω^m by the minimality of $\nu_q(m)$, let $\beta(t_1, t_i) = \omega^{v_i m}$ and $\beta(t_2, t_i) = \omega^{u_i m}$ for all $i > 2$. Putting $y_i = -v_i$ and $x_i = u_i$, our two expressions above will equal 1. If $t_i t_1^{x_i} t_2^{y_i} = e$, then we will discard that t_i. Otherwise, let $t_i' = t_i t_1^{x_i} t_2^{y_i}$. This gives us a new generating set $\{t_1, t_2, t_3', t_4', \dots, t_{n'}'\}$.

Repeating this procedure we get a new generating set, say $B = \{t_1, \dots, t_n\}$. Note that n is even as otherwise t_n is in the radical of β. Let $n = 2r$ and denote $a_i = t_{2i-1}$ and $b_i = t_{2i}$.

Return $B = \{a_1, b_1, a_2, b_2, \dots, a_r, b_r\}$.

Now we must show B is a symplectic basis. Note that conditions (3.2) and (3.3) as well as (3.4) for $i \neq j$ are immediate by construction. Thus, all we need are conditions (3.4) for $i = j$ and (3.5), both of which we can derive at the same time. For all i, the scalar $\beta(a_i, b_i) = \omega^{m_i}$, for some $0 \leq m_i < q^N$, and will thus be a primitive n_i-th root of unity for $n_i = q^{N-\nu_q(m_i)}$. Note here that a_i is orthogonal to all basis elements except b_i and vice-versa. Therefore,

$$1 = \beta(a_i, b_i)^{n_i} = \beta(a_i^{n_i}, b_i) = \beta(a_i, b_i^{n_i}).$$

Thus $a_i^{n_i} \in \operatorname{rad}\beta$ as it is orthogonal to all basis elements, so $\mathrm{o}(a_i) \mid n_i$. On the other hand, as β is a bicharacter, $n_i \mid \mathrm{o}(a_i)$, so $\mathrm{o}(a_i) = n_i$ and similarly $\mathrm{o}(b_i) = n_i$, which gives us conditions (3.4) and (3.5). $\square$

We now have several corollaries.

Corollary 3.11. *If a finite abelian group T admits a nondegenerate alternating bicharacter then there exists an abelian group A such that $T \cong A \times A$.*

Proof. Let $A = \langle a_1, a_2, \ldots, a_r \rangle$ and $B = \langle b_1, b_2, \ldots, b_r \rangle$. By Lemma 3.9, we have $T = A \times B$, $A = \langle a_1 \rangle \times \cdots \times \langle a_r \rangle$ and $B = \langle b_1 \rangle \times \cdots \times \langle b_r \rangle$. As $\mathrm{o}(a_i) = \mathrm{o}(b_i)$, we have $A \cong B$, and therefore $T \cong A \times A$. □

Corollary 3.12. *Given a pair (T, β) where T is a finite abelian subgroup of G and β is a nondegenerate alternating bicharacter on T, there exists a division G-grading Γ on a matrix algebra $M_\ell(\mathbb{F})$ with one dimensional components and support T (hence $\ell^2 = |T|$) such that for any $X_s, X_t \in M_\ell(\mathbb{F})$ with $\deg(X_s) = s$, $\deg(X_t) = t$, we have $X_s X_t = \beta(s,t) X_t X_s$.*

Proof. Let $\{a_1, b_1, a_2, b_2, \ldots, a_r, b_r\}$ be a symplectic basis of T. Define $\varepsilon_j := \beta(a_j, b_j)$; this is a primitive ℓ_j-th root of unity for $\ell_j = \mathrm{o}(a_j)$. Let $\ell = \prod_{j=1}^{r} \ell_j$ and identify $M_{\ell_1}(\mathbb{F}) \otimes \cdots \otimes M_{\ell_r}(\mathbb{F})$ with $M_\ell(\mathbb{F})$ by Kronecker product. Define a generating set $\{X_{a_j}, X_{b_j}\}_{j=1}^{r}$ of the algebra $M_\ell(\mathbb{F})$ by

$$X_{a_j} := I^{\otimes(j-1)} \otimes X_{\ell_j} \otimes I^{\otimes(r-j)} \quad \text{and} \quad X_{b_j} := I^{\otimes(j-1)} \otimes Y_{\ell_j} \otimes I^{\otimes(r-j)},$$

where X_{ℓ_j} and Y_{ℓ_j} are the generalized Pauli matrices of order ℓ_j as per (1.5). Note that by Lemma 1.1, for each j, the monomials $\{X_{\ell_j}^u Y_{\ell_j}^v \mid 0 \le u, v < \ell_j\}$ form a basis of $M_{\ell_j}(\mathbb{F})$, and so certain monomials in X_{a_i} and X_{b_j} form a basis of $M_\ell(\mathbb{F})$, which gives us a T-grading. Explicitly, we define a grading on $M_\ell(\mathbb{F})$ by taking for each $t \in T$ the homogeneous component spanned by the element $X_t \in M_\ell(\mathbb{F})$ defined as follows. By Lemma 3.9 there is a unique decomposition of t in terms of the symplectic basis, say $t = a_1^{u_1} b_1^{v_1} \cdots a_r^{u_r} b_r^{v_r}$ where $0 \le u_j, v_j < \ell_j$. Then we set

$$X_t := X_{a_1}^{u_1} X_{b_1}^{v_1} X_{a_2}^{u_2} X_{b_2}^{v_2} \cdots X_{a_r}^{u_r} X_{b_r}^{v_r} = \bigotimes_{j=1}^{r} X_{\ell_j}^{u_j} Y_{\ell_j}^{v_j}.$$

As we saw at the beginning of this section, the relation $X_s X_t = \beta'(s,t) X_t X_s$ defines a bicharacter $\beta' : T \times T \to \mathbb{F}^\times$. We only need to check that $\beta = \beta'$. It is sufficient to check they coincide on the symplectic basis, so we have to look at the commutation relations among the generators of the algebra $\{X_{a_j}, X_{b_j}\}_{j=1}^{r}$. These generators commute in all cases except the pairs X_{a_j} and X_{b_j}, and for these pairs, we have from Section 1.3 that $X_j Y_j = \varepsilon_j Y_j X_j$.

$$\begin{aligned} X_{a_j} X_{b_j} &= (I \otimes \cdots \otimes X_{\ell_j} \otimes \cdots \otimes I)(I \otimes \cdots \otimes Y_{\ell_j} \otimes \cdots \otimes I) \\ &= I \otimes \cdots \otimes X_{\ell_j} Y_{\ell_j} \otimes \cdots \otimes I \\ &= \varepsilon_j (I \otimes \cdots \otimes Y_{\ell_j} X_{\ell_j} \otimes \cdots \otimes I) = \beta(a_j, b_j) X_{b_j} X_{a_j}. \end{aligned}$$

□

In summary, if G is abelian and $\mathbb{F}$ is algebraically closed, then matrix algebras with a division G-grading are classified up to isomorphism by the pairs (T, β) where T is a finite subgroup of G and $\beta : T \times T \to \mathbb{F}^\times$ is a nondegenerate alternating bicharacter on T (see [5, Thm. 2.15] for a complete proof). Thus, we can classify G-gradings on matrix algebras by the triples (T, β, κ) where T and β are as above and $\kappa : G/T \to \mathbb{N}_0$ has finite support. The matrix algebra associated to the triple (T, β, κ) will be $M_n(\mathbb{F})$ where $n = k\ell$ for $k = |\kappa| := \sum_{x \in G/T} \kappa(x)$ and $\ell = \sqrt{|T|}$. Two such triples, (T, β, κ) and (T', β', κ'), correspond to isomorphic graded algebras if and only if $(\mathcal{D}, \kappa) \sim (\mathcal{D}', \kappa')$, that is, if and only if $T' = T$, $\beta' = \beta$ and $\kappa' = \kappa^{[g]}$ for some $g \in G$.

3.4 The bicharacter on the character group

We now want to obtain an algorithm to compute the triple (T, β, κ) associated to a given grading on a matrix algebra. To this end, we define a bicharacter $\widehat{\beta}$ on $\widehat{G}$ related to β, which was first discussed in [4, Sec. 2]. For the remainder of the chapter we assume that $\mathbb{F}$ is algebraically closed and of characteristic zero and G is abelian.

As T is a finite abelian group, we know that $T \cong \widehat{T}$. The bicharacter β gives us a specific isomorphism as follows. Let $\grave{\beta} : T \to \widehat{T}$ be defined by $(\grave{\beta}(s))(t) = \beta(s, t)$. Note that $\grave{\beta}$ is a group homomorphism by β being a bicharacter and is an isomorphism by $|T| = |\widehat{T}|$ and

$$\ker \grave{\beta} = \{ s \in T \mid \beta(s, t) = 1, \ \forall t \in T \} = \operatorname{rad} \beta,$$

which is trivial as β is nondegenerate.

As any character $\chi \in \widehat{G}$ can be restricted to a character on T, we can define a map $\widehat{G} \to T$ by sending each $\chi \in \widehat{G}$ to $t_\chi := \grave{\beta}^{-1}(\chi|_T)$, that is, $\chi(t) = \beta(t_\chi, t)$ for all $t \in T$. Note that this map is surjective as the restriction map $\widehat{G} \to \widehat{T}$ given by $\chi \mapsto \chi|_T$ is surjective by Lemma and $\grave{\beta}^{-1}$ is an isomorphism. Define an alternating bicharacter $\widehat{\beta} : \widehat{G} \times \widehat{G} \to \mathbb{F}^\times$ by

$$\widehat{\beta}(\chi, \psi) := \beta(t_\chi, t_\psi).$$

Note that this bicharacter is *not* nondegenerate unless $T = G$. In fact, we have a the following:

Lemma 3.13. $T^\perp = \operatorname{rad} \widehat{\beta}$.

Proof. For any $\chi, \psi \in \widehat{G}$, we have

$$\widehat{\beta}(\chi, \psi) = \beta(t_\chi, t_\psi) = \chi(t_\psi)$$

Therefore, $\widehat{\beta}(\chi, \psi)$ holds for all $\psi \in \widehat{G}$ if and only if $\chi(t) = 1$ for all $t \in T$, as the map $\widehat{G} \to T$ is surjective from above. Thus, $\chi \in T^\perp$ if and only if $\chi \in \operatorname{rad} \widehat{\beta}$. $\square$

This $\widehat{\beta}$ is closely related to the Noether-Skolem operators associated to the action of $\widehat{G}$ by automorphisms (see Section 2.1) of a G-graded matrix algebra $\mathcal{A}$. As we know from Section 3.2, $\mathcal{A} \cong M_k(\mathbb{F}) \otimes \mathcal{D}$ as a graded algebra, where $M_k(\mathbb{F})$ has an elementary grading with a k-tuple $\mathbf{g} = (g_1, g_2, \ldots, g_k)$ and $\mathcal{D}$ is a matrix algebra with a division grading. Let (T, β) be the pair associated to $\mathcal{D}$. Recall that $\mathbf{g}$ defines κ, as $\kappa(x)$ is the number of times x appears in the list of cosets $g_1T, \ldots, g_kT$.

Lemma 3.14. *Fix $0 \neq X_t \in \mathcal{D}_t$ for each $t \in T$. Then, for each $\chi \in \widehat{G}$, the automorphism $\eta_\Gamma(\chi) \in \operatorname{Aut}(\mathcal{A})$ is the conjugation by*

$$u_\chi := \operatorname{diag}(\chi(g_1), \chi(g_2), \ldots, \chi(g_k)) \otimes X_{t_\chi},$$

that is, $\eta_\Gamma(\chi)(a) = u_\chi a u_\chi^{-1}$ for all $a \in \mathcal{A}$.

Proof. We clearly have that $u_\chi^{-1} = \operatorname{diag}(\chi(g_1)^{-1}, \chi(g_2)^{-1}, \ldots, \chi(g_k)^{-1}) \otimes X_{t_\chi}^{-1}$. The algebra $\mathcal{A}$ is spanned by homogeneous elements of the form $E_{i,j} \otimes X_t$, with $\deg(E_{i,j} \otimes X_t) = g_i g_j^{-1} t$. Conjugating this element by u_χ gives us

$$\begin{aligned}
u_\chi(E_{i,j} \otimes X_t)u_\chi^{-1} &= (\operatorname{diag}(\chi(g_1), \ldots, \chi(g_k)) \otimes X_{t_\chi})(E_{i,j} \otimes X_t)u_\chi^{-1} \\
&= (\chi(g_i)E_{i,j} \otimes X_{t_\chi}X_t)(\operatorname{diag}(\chi(g_1)^{-1}, \ldots, \chi(g_k)^{-1}) \otimes X_{t_\chi}^{-1}) \\
&= \chi(g_i)\chi(g_j)^{-1} E_{i,j} \otimes X_{t_\chi} X_t X_{t_\chi}^{-1} \\
&= \chi(g_i g_j^{-1}) E_{i,j} \otimes \beta(t_\chi, t) X_t \\
&= \chi(g_i g_j^{-1}) E_{i,j} \otimes \chi(t) X_t \\
&= \chi(g_i g_j^{-1} t)(E_{i,j} \otimes X_t) = \eta_\Gamma(\chi)(E_{i,j} \otimes X_t).
\end{aligned}$$

The result follows. □

We will call such u_χ (defined up to a non-zero scalar factor) the *Noether-Skolem operator* associated to χ. Note that each u_χ is diagonalizable, as $X_t^{o(t)}$ (being an element of $\mathcal{D}_e$) is a scalar matrix, and hence the minimal polynomial of X_t has no repeated roots.

We will now see that the commutation relation between two such operators, u_χ and u_ψ, is given by $\widehat{\beta}$:

$$\begin{aligned}
u_\chi u_\psi &= (\operatorname{diag}(\chi(g_1),\dots,\chi(g_k))\otimes X_{t_\chi})(\operatorname{diag}(\psi(g_1),\dots,\psi(g_k))\otimes X_{t_\psi})\\
&= \operatorname{diag}(\chi(g_1)\psi(g_1),\dots,\chi(g_k)\psi(g_k))\otimes X_{t_\chi}X_{t_\psi}\\
&= \operatorname{diag}(\psi(g_1)\chi(g_1),\dots,\psi(g_k)\chi(g_k))\otimes \beta(t_\chi,t_\psi)X_{t_\psi}X_{t_\chi}\\
&= \widehat{\beta}(\chi,\psi)(\operatorname{diag}(\psi(g_1),\dots,\psi(g_k))\otimes X_{t_\psi})(\operatorname{diag}(\chi(g_1),\dots,\chi(g_k))\otimes X_{t_\chi})\\
&= \widehat{\beta}(\chi,\psi)u_\psi u_\chi.
\end{aligned}$$

Thus, if we have the Noether-Skolem operators, we can compute $\widehat{\beta}$ as their commutation factor. These operators are also nicely behaved with respect to the grading itself.

Lemma 3.15. *For any $\chi \in \widehat{G}$, u_χ is homogeneous and* $\deg(u_\chi) = t_\chi$*. Moreover, if $K \subset \widehat{G}$ is a set of characters such that $K^\perp = \{e\}$, then $\langle \deg(u_\chi) \mid \chi \in K\rangle = T$.*

Proof. Note that $\operatorname{diag}(\chi(g_1),\dots,\chi(g_k)) \in M_k(\mathbb{F})$ is of degree e as $M_n(\mathbb{F})$ is endowed with an elementary grading, and $X_{t_\chi} \in \mathcal{D}$ is of degree t_χ. Thus, $\deg(u_\chi) = \deg(\operatorname{diag}(\chi(g_1),\dots,\chi(g_k)))\deg(X_{t_\chi}) = t_\chi$.

Now, let $X = \{\chi|_T \mid \chi \in K\} \subset \widehat{T}$. Clearly as $K^\perp = \{e\}$ we have $X^\perp = \{e\}$. By Corollary 2.10, this implies $\langle X\rangle = \{e\}^\perp = \widehat{T}$. From above, we know that for $\chi \in \widehat{G}$, $\deg(u_\chi) = t_\chi = \grave{\beta}^{-1}(\chi|_T)$, where $\grave{\beta}$ is an isomorphism between T and $\widehat{T}$. Since the set X generates $\widehat{T}$, its preimage $\deg(u_\chi)$, $\chi \in K$, will generate T. □

3.5 Computing the canonical form of a grading on a matrix algebra

Now we put together our previous results to formulate an algorithm to compute the canonical form of a grading by a finitely generated abelian group G

on a matrix algebra. To be specific, we work over the ground field of complex numbers, $\mathbb{C}$. We denote the imaginary unit by $\mathbf{i}$.

Let $\Gamma : \mathcal{A} = \bigoplus_{g\in G} \mathcal{A}_g$ be a G-grading on a matrix algebra $\mathcal{A} = M_n(\mathbb{C})$. Let $\mathcal{B} = \{X_1, \ldots, X_{n^2}\}$ be a graded basis of $\mathcal{A}$, with $\deg(X_i) = h_i$. By Theorem 2.2 we can write

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r} \times \mathbb{Z}^m$$

where $n_1 \geq 2$ and $n_i \mid n_{i+1}$. From here on, we will consider elements of G as elements of $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r} \times \mathbb{Z}^m$, and express them as integer vectors with $r + m$ components.

By the discussion in Subsection 2.2.2 we have

$$\widehat{G} \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r} \times (\mathbb{C}^\times)^m.$$

This allows us to define a point-separating set of characters $\{\chi_j\}_{j=0}^r$ as follows: for $1 \leq j \leq r$, let

$$\chi_j(w_1, w_2, \ldots, w_r, w_{r+1} \ldots, w_{r+m}) := \exp\left(\frac{2\pi \mathbf{i} w_j}{n_j}\right). \tag{3.6}$$

These are trivial on the free part and separate points in the torsion part of the grading group. We also define

$$\chi_0(w_1, w_2, \ldots, w_r, w_{r+1} \ldots, w_{r+m}) := 2^{w_{r+1}} 3^{w_{r+2}} \cdots p_m^{w_{r+m}} \tag{3.7}$$

where p_j is the j-th prime number. This character is trivial on the torsion part and separates points in the free part of the grading group.

Using the Szigeti–van Wyk algorithm reviewed in Section 3.1, we can now efficiently compute the invertible matrices $\{U_{\chi_j}\}_{j=0}^r$ such that

$$\eta_\Gamma(\chi_j)(X) = U_{\chi_j} X U_{\chi_j}^{-1} \quad \text{for all } X \in M_n(\mathbb{C}).$$

Note that $\eta_\Gamma(\chi)(X)$ can be computed by expressing X in terms of the basis $\mathcal{B}$: if $X = \sum_{i=1}^{n^2} \xi_i X_i$ then

$$\eta_\Gamma(\chi)(X) = \sum_{i=1}^{n^2} \xi_i \chi(h_i) X_i.$$

These Noether-Skolem operators allow us to calculate the bicharacter $\widehat{\beta} : \widehat{G} \times \widehat{G} \to \mathbb{C}^\times$ associated to β by

$$\widehat{\beta}(\chi_i, \chi_j) I_n := U_{\chi_i} U_{\chi_j} U_{\chi_i}^{-1} U_{\chi_j}^{-1}.$$

Note that the factor $(\mathbb{C}^\times)^m$ lies in $\operatorname{rad} \widehat{\beta}$ by Lemma 3.13, since any element of $(\mathbb{C}^\times)^m$ (for example, χ_0) has trivial restriction to $\mathrm{t}(G)$ and $T \subset \mathrm{t}(G)$. We will represent $\widehat{\beta}$ through the integer matrix $B = [b_{i,j}]_{1 \le i,j \le r}$, defined by

$$b_{i,j} := \frac{n_r \ln\bigl(\widehat{\beta}(\chi_i, \chi_j)\bigr)}{2\pi\mathbf{i}}, \tag{3.8}$$

where we take the principal branch cut for $\ln(z)$.[6] If $\chi = \prod_{j=1}^r \chi_j^{x_j}$ and $\psi = \prod_{j=1}^r \chi_j^{y_j}$ where $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^r$ and z_j denotes the j-th component of the vector $\mathbf{z}$, then we can write:

$$\widehat{\beta}(\chi, \psi) = \omega^{\mathbf{x}^\top B \mathbf{y}} \quad \text{where} \quad \omega = \exp\left(\frac{2\pi\mathbf{i}}{n_r}\right).$$

Thus, $\psi \in \operatorname{rad} \widehat{\beta}$ if and only if $B\mathbf{y} \equiv 0 \pmod{n_r}$. As B is an integer matrix, we can use the Smith Canonical Form of B to compute solutions of this system of congruences as follows.

Let P, Q, and D be integer matrices such that $PBQ = D$ and $D = \operatorname{diag}(d_1, d_2, \ldots d_r)$. Letting $\mathbf{y} = Q\mathbf{v}$, we rewrite our system of congruences as $D\mathbf{v} \equiv \mathbf{0} \pmod{n_r}$, that is, $d_i v_i \equiv 0 \pmod{n_r}$. Solving this with basic number theory yields $v_i \equiv 0 \pmod{\frac{n_r}{\gcd(d_i, n_r)}}$. Let vector $\mathbf{v}^{(i)}$ have $\frac{n_r}{\gcd(n_r, d_i)}$ in the i-th entry and 0 elsewhere, and take $\mathbf{z}^{(i)} := Q\mathbf{v}^{(i)}$. That is, $\mathbf{z}^{(i)}$ is the i-th column of Q multiplied by $\frac{n_r}{\gcd(n_r, d_i)}$. We then reduce $\mathbf{z}^{(i)}$ modulo n_r, remove redundancy and relabel so that we get a set, say $Z := \{\mathbf{z}^{(1)}, \mathbf{z}^{(2)}, \ldots, \mathbf{z}^{(s)}\} \subset \mathbb{Z}_{n_r}^r$, that generates the nullspace. The corresponding characters in $\operatorname{rad} \widehat{\beta}$ are given by

$$\Psi := \left\{ \psi_i := \prod_{j=1}^r \chi_j^{z_j^{(i)}} \;\middle|\; \mathbf{z}^{(i)} \in Z \right\} \cup \{\chi_0\}. \tag{3.9}$$

Lemma 3.16. $\Psi^\perp = T$.

[6] In fact, the matrix B should be regarded as lying in $M_r(\mathbb{Z}_{n_r})$, and as such it does not matter what branch cut we take. However, for the sake of computation, the principal branch cut is used.

Proof. By Lemma 3.13 we have that $\Psi \subset T^\perp$ and so $T \subset \Psi^\perp$.

Now, note that $\{\chi_0\}^\perp = \mathrm{t}(G)$ and hence $\Psi^\perp \subset \mathrm{t}(G)$. So to prove that $\Psi^\perp \subset T$, we can work with $\mathrm{t}(G)$, that is, replace the elements of Ψ by their restrictions to $\mathrm{t}(G)$. The replacement of G by $\mathrm{t}(G)$ induces a new bicharacter $\widehat{\beta} : \widehat{\mathrm{t}(G)} \times \widehat{\mathrm{t}(G)} \to \mathbb{C}^\times$, which is the original $\widehat{\beta} : \widehat{G} \times \widehat{G} \to \mathbb{C}^\times$ precomposed with two copies of the restriction map $\widehat{G} \to \widehat{\mathrm{t}(G)}$. The radical of the new $\widehat{\beta}$ is generated by $\psi_1|_{\mathrm{t}(G)}, \psi_2|_{\mathrm{t}(G)}, \ldots, \psi_s|_{\mathrm{t}(G)}$. Again by Lemma 3.13, we have that $T^\perp = \operatorname{rad}\widehat{\beta}$ for the new $\widehat{\beta}$ and hence $(\operatorname{rad}\widehat{\beta})^\perp = T$. $\square$

We then can compute the Noether-Skolem operators that correspond to the elements of $\Psi \subset \operatorname{rad}\widehat{\beta}$:

$$C := \left\{ U_i := \prod_{j=1}^{r} U_{\chi_j}^{z_j^{(i)}} \;\middle|\; \mathbf{z}^{(i)} \in Z \right\} \cup \{U_{\chi_0}\}. \tag{3.10}$$

For ease of notation, let $\psi_0 := \chi_0$ and $U_0 := U_{\chi_0}$.

Note that as $\Psi \subset \operatorname{rad}\widehat{\beta}$ the matrices in C commute pairwise and each of them is diagonalizable, they are simultaneously diagonalizable. Consider the simultaneous eigenspace decomposition

$$\mathbb{C}^n = \bigoplus_{\boldsymbol{\mu}} V_{\boldsymbol{\mu}}$$

where $\boldsymbol{\mu} = (\mu_0, \mu_1, \ldots, \mu_s)$ and $V_{\boldsymbol{\mu}} := \{\mathbf{v} \in \mathbb{C}^n \mid U_i(\mathbf{v}) = \mu_i \mathbf{v}, \text{ for all } i\}$.

Recall from Lemma 3.14 that, up to scalar factors, U_i are simultaneously similar to the matrices $\operatorname{diag}(\psi_i(g_1), \psi_i(g_2), \ldots, \psi_i(g_k)) \otimes I_\ell$ for some k-tuple $\mathbf{g} = (g_1, g_2, \ldots, g_k)$ where $k = \frac{n}{\ell}$ and $\ell = \sqrt{|T|}$. The multiplicity function $\kappa : G/T \to \mathbb{N}_0$ is determined up to a shift and given by $\kappa(x)$ being the number of times that x appears in the list of cosets $g_1T, g_2T, \ldots, g_kT$. Thus, the elements g_i are not uniquely determined, only the cosets they represent in G/T are determined up to a shift and reordering. So, in particular, we may assume that $\mathbf{g} = (e, g_2, g_3, \ldots, g_k)$. Let

$$\boldsymbol{\lambda}_i := (\psi_0(g_i), \psi_1(g_i), \ldots, \psi_s(g_i)).$$

Note that $\boldsymbol{\lambda}_1 = \mathbf{1}$ where $\mathbf{1}$ is the vector with all entries equal to 1. Choose a nonzero simultaneous eigenspace $V_{\boldsymbol{\mu}_1}$. Let M be the diagonal matrix whose diagonal entries are the inverses of the entries of $\boldsymbol{\mu}_1$, so that $M\boldsymbol{\mu}_1 = \mathbf{1} = \boldsymbol{\lambda}_1$. Then, all elements g_i satisfying $\boldsymbol{\lambda}_i = M\boldsymbol{\mu}$ are associated to the simultaneous eigenspace $V_{\boldsymbol{\mu}}$, so we let $V_i := V_{\boldsymbol{\mu}}$ for these elements. From Lemma 3.16 we know that Ψ kills T and separates elements of G/T, so $V_i = V_j$ if and only if $g_iT = g_jT$.

By equation (3.9) we know how to evaluate each character in Ψ on an element $g_i \in G$ represented by a vector $\mathbf{w}^{(i)} \in \mathbb{Z}^{r+m}$. To determine g_iT, we now solve for these vectors $\mathbf{w}^{(i)}$. For $j \neq 0$, we have

$$\boldsymbol{\lambda}_i[j] = \psi_j(g_i) = \exp\left(2\pi\mathbf{i}\sum_{i'=1}^{r}\frac{w_{i'}^{(i)}z_{i'}^{(j)}}{n_{i'}}\right) \tag{3.11}$$

and for $j = 0$, we have

$$\boldsymbol{\lambda}_i[0] = \psi_0(g_i) = 2^{w_{r+1}^{(i)}}3^{w_{r+2}^{(i)}}\cdots p_m^{w_{r+m}^{(i)}}. \tag{3.12}$$

where $\boldsymbol{\lambda}_i[j]$ is the j-th entry of $\boldsymbol{\lambda}_i$. Determining the free part of each g_i, that is $(w_{r+1}^{(i)}, w_{r+2}^{(i)}, \dots w_{r+m}^{(i)})$, is thus a matter of prime decomposition.

Computing the torsion part, $\mathbf{x}^{(i)} := (w_1^{(i)}, w_2^{(i)}, \dots, w_r^{(i)})$, is more involved. Letting $d_{i'} := \frac{n_r}{n_{i'}}$, we can rewrite equation (3.11) as follows:

$$\boldsymbol{\lambda}_i[j] = \exp\left(\frac{2\pi\mathbf{i}}{n_r}\sum_{i'=1}^{r}d_{i'}w_{i'}^{(i)}z_{i'}^{(j)}\right),$$

which reduces to the congruence relation

$$\sum_{i'=1}^{r}d_{i'}z_{i'}^{(j)}w_{i'}^{(i)} \equiv \frac{n_r\ln(\boldsymbol{\lambda}_i[j])}{2\pi\mathbf{i}} \pmod{n_r}. \tag{3.13}$$

We can write the system of congruence relations for $1 \leq j \leq r$ in matrix form using the matrix $A = [a_{j,i'}]_{1\leq j,i'\leq r}$, defined by

$$a_{j,i'} := d_{i'}z_{i'}^{(j)},$$

and the vector $\mathbf{b}^{(i)}$, defined by

$$b_j^{(i)} := \frac{n_r\ln(\boldsymbol{\lambda}_i[j])}{2\pi\mathbf{i}}.$$

With this notation, (3.13) becomes:

$$A\mathbf{x}^{(i)} \equiv \mathbf{b}^{(i)} \pmod{n_r}. \tag{3.14}$$

This system of congruences can be solved with the Smith Canonical Form of A, say $PAQ = D$. Letting $\mathbf{x}^{(i)} = Q\mathbf{y}^{(i)}$ and $\mathbf{c}^{(i)} := P\mathbf{b}^{(i)}$ we rewrite (3.14) in the form $D\mathbf{y}^{(i)} \equiv \mathbf{c}^{(i)} \pmod{n_r}$. As D is diagonal, this is easy to solve for $\mathbf{y}^{(i)}$, which provides us with a solution for $\mathbf{x}^{(i)}$. Once we have a particular solution for the $\mathbf{x}^{(i)}$, which represents the torsion part of g_i, we can combine that with the free part to construct the entire g_i (recall that g_i are determined modulo T). For each such g_i, we have

$$\kappa(g_iT) = \frac{\dim(V_i)}{\sqrt{|T|}}.$$

Computing the other parameters of the grading, namely T and β, is significantly easier. By Lemma 3.15, we know that T is generated by the elements $t_{\chi_i} = \deg(U_{\chi_i})$, $0 \le i \le r$. Noting that $\deg(U_{\chi_0}) = e$, it suffices to take $1 \le i \le r$. As well, by the definition of $\widehat{\beta}$, we know that

$$\beta(t_{\chi_i}, t_{\chi_j}) = \widehat{\beta}(\chi_i, \chi_j) = U_{\chi_i}U_{\chi_j}U_{\chi_i}^{-1}U_{\chi_j}^{-1}.$$

Thus, we can use Algorithm 3.10 on the generating set $\{t_i := t_{\chi_i} \mid 1 \le i \le r\}$ to render this into a symplectic basis of T, giving us a clean representation of both T and β at the same time.

In conclusion, we summarize the process to compute the parameters of the grading on $M_n(\mathbb{C})$:

Algorithm 3.17. *Input: A finitely generated abelian group G and a graded basis $\mathcal{B} = \{X_1, \dots X_{n^2}\}$ of $M_n(\mathbb{C})$ with $\deg(X_i) = h_i \in G$.*

Output: (T, β, κ).

- Define the finite set of characters $\{\chi_i\}_{i=0}^r$ that separate points of G by (3.6) and (3.7).
- Construct the Noether-Skolem matrices for these $\{\chi_i\}_{i=0}^r$, say $\{U_{\chi_i}\}_{i=0}^r$, using the Szigeti–van Wyk algorithm.
- Compute the matrix $B = [b_{i,j}]_{1 \le i,j \le r}$ representing $\widehat{\beta}$ by equation (3.8).
- Use the Smith Canonical Form of B to find generators of the nullspace of B considered as a matrix in $M_r(\mathbb{Z}_{n_r})$.
- Associate to these generators a set of characters in $\operatorname{rad}\widehat{\beta}$ by equation (3.9) and Noether-Skolem operators by equation (3.10).

- Compute the simultaneous eigenspace decomposition

$$\mathbb{C}^n = V_{\boldsymbol{\mu}_1} \oplus V_{\boldsymbol{\mu}_2} \oplus V_{\boldsymbol{\mu}_3} \oplus \cdots .$$

- Let $\boldsymbol{\lambda}_i[j] := \frac{\boldsymbol{\mu}_i[j]}{\boldsymbol{\mu}_1[j]}$. Note that these $\boldsymbol{\lambda}_i$ are distinct for distinct i. To get the $\boldsymbol{\lambda}_i$ and g_i as above, each should be repeated $\frac{\dim(V_{\boldsymbol{\mu}_i})}{\sqrt{|T|}}$ times.

- Use the Smith Canonical Form on the system of congruences (3.14) to determine the torsion part of each g_i.

- Use the prime factor decomposition on equation (3.12) to determine the free part of each g_i.

- $\kappa(g_i T) = \frac{\dim(V_{\boldsymbol{\mu}_i})}{\sqrt{|T|}}$.

- $T = \langle t_i \mid 1 \leq i \leq r \rangle$ where $t_i := \deg(U_{\chi_i})$.

- $\beta(t_i, t_j) = U_{\chi_i} U_{\chi_j} U_{\chi_i}^{-1} U_{\chi_j}^{-1}$.

- Return (T, β, κ). $\square$

Bibliography

[1] Y. A. Bahturin, S. K. Sehgal, and M. V. Zaicev. "Group Gradings on Associative Algebras". In: *Journal of Algebra* 241 (2001), pp. 677–698. DOI: 10.1006/jabr.2000.8643.

[2] Y. A. Bahturin and M. V. Zaicev. "Group Gradings on Matrix Algebras". In: *Canadian Mathematical Bulletin* 45.4 (2002), pp. 499–508. DOI: 10.4153/cmb-2002-051-x.

[3] C. De Naday Hornhardt. "Group Gradings on Classical Lie Superalgebras". PhD thesis. Memorial University, 2020.

[4] A. Elduque and M. Kochetov. "Graded modules over classical simple Lie algebras with a grading". In: *Israel Journal of Mathematics* 207.1 (2015), pp. 229–280. ISSN: 0021-2172.

[5] A. Elduque and M. Kochetov. *Gradings on simple Lie algebras*. Mathematical Surveys and Monographs; no. 189. 2013. ISBN: 9780821898468.

[6] A. Elduque and M. Kochetov. "Gradings on the Lie algebra D_4 revisited". In: *Journal of Algebra* 441 (2015), pp. 441–474.

[7] J. E. Humphreys. *Linear algebraic groups*. 4th ed. Vol. 21. Graduate Texts in Mathematics. Springer, 1995.

[8] T.-Y. Lam. *Lectures on modules and rings*. Vol. 189. Graduate Texts in Mathematics. Springer, 1999.

[9] C. Năstăsescu and F. van Oystaeyen. *Methods of graded rings*. Vol. 1836. Lecture Notes in Mathematics. Springer-Verlag, 2004.

[10] W. K. Nicholson. *Linear Algebra with Applications*. Lyryx Learning Inc., 2020. URL: https://lyryx.com/linear-algebra-applications.

[11] J. J. Rotman. *Advanced modern algebra*. Prentice Hall, 2003.

[12] J. Szigeti and L. van Wyk. "A Constructive Elementary Proof of the Skolem-Noether Theorem for Matrix Algebras". In: *The American Mathematical Monthly* 124.10 (2017), pp. 966–968. DOI: 10.4169/amer.math.monthly.124.10.966. eprint: https://www.tandfonline.com/doi/pdf/10.4169/amer.math.monthly.124.10.966. URL: https://www.tandfonline.com/doi/abs/10.4169/amer.math.monthly.124.10.966.

[13] I.M. Yaglom. *Felix Klein and Sophus Lie: evolution of the idea of symmetry in the Nineteenth Century*. Ed. by Hardy Grant and Abe Shenitzer. Trans. by Sergei Sossinsky. Birkhäuser, 1988.