CRITICAL GROUPS FOR HOPF ALGEBRA MODULES

DARIJ GRINBERG, JIA HUANG, AND VICTOR REINER

Abstract. This paper considers an invariant of modules over a finite-dimensional Hopf algebra, called the critical group. This generalizes the critical groups of complex finite group representations studied in [1, 11]. A formula is given for the cardinality of the critical group generally, and the critical group for the regular representation is described completely. A key role in the formulas is played by the greatest common divisor of the dimensions of the indecomposable projective representations.

1. Introduction

Every connected finite graph has an interesting isomorphism invariant, called its *critical* or *sandpile group*. This is a finite abelian group, defined as the cokernel of the (reduced) Laplacian matrix of the graph. Its cardinality is the number of spanning trees in the graph, and it has distinguished coset representatives related to the notion of *chip-firing* on graphs ([17], [24]). In recent work motivated by the classical McKay correspondence, a similar critical group was defined by Benkart, Klivans and the third author [1] (and studied further by Gaetz [11]) for complex representations of a finite group. They showed that the critical group of such a representation has many properties in common with that of a graph.

The current paper was motivated in trying to understanding the role played by semisimplicity for the group representations. In fact, we found that much of the theory generalizes not only to arbitrary finite group representations in any characteristic, but even to representations of finite-dimensional Hopf algebras[1].

Thus we start in Section 2 by reviewing modules V for a Hopf algebra A which is finite-dimensional over an algebraically closed field $\mathbb{F}$. This section also defines the critical group $K(V)$ as follows: if $n := \dim V$, and if A has $\ell + 1$ simple modules, then the cokernel of the map L_V on the Grothendieck group $G_0(A) \cong \mathbb{Z}^{\ell+1}$ which multiplies by $n - [V]$ has abelian group structure $\mathbb{Z} \oplus K(V)$.

To develop this further, in Section 3 we show that the vectors in $\mathbb{Z}^{\ell+1}$ giving the dimensions of the simple and indecomposable projective A-modules are left- and right-nullvectors for the map L_V. In the case of a group algebra $A = \mathbb{F}G$ for a finite group G, we extend results from [1] and show that the columns in the *Brauer character tables* for the simple and indecomposable projective modules give complete sets of left- and right-eigenvectors for L_V.

Section 4 uses this to prove the following generalization of a result of Gaetz [11, Ex. 9]. Let $d := \dim A$, and let γ be the greatest common divisor of the dimensions of the $\ell + 1$ indecomposable projective A-modules.

Theorem 1.1. *If $\ell = 0$ then $K(A) = 0$, else $K(A) \cong (\mathbb{Z}/\gamma\mathbb{Z}) \oplus (\mathbb{Z}/d\mathbb{Z})^{\ell-1}$.*

Section 5 proves the following formula for $\#K(V)$, analogous to one for critical groups of graphs.

Theorem 1.2. *Assume $K(V)$ is finite, so that L_V has nullity one. If the characteristic polynomial of L_V factors as $\det(xI - L_V) = x \prod_{i=1}^{\ell}(x - \lambda_i)$, then $\#K(V) = \left|\frac{\gamma}{d}(\lambda_1\lambda_2 \cdots \lambda_\ell)\right|$.*

Section 5 makes this much more explicit in the case of a group algebra $\mathbb{F}G$ for a finite group G, generalizing another result of Gaetz [11, Thm. 3(i)]. Let $p \geq 0$ be the characteristic of the field $\mathbb{F}$. Let p^a be the order

2010 *Mathematics Subject Classification.* 05E10, 16T05, 16T30, 15B48, 20C20.

Key words and phrases. Hopf algebra, chip-firing, sandpile, critical group, Brauer character, modular representation, McKay, M-matrix, Taft Hopf algebra.

Third author supported by NSF grants DMS-1148634, 1601961.

[1]And even further to finite tensor categories, although we will not emphasize this; see Remark 3.13 below.

of the p-Sylow subgroups of G (with p^a to be understood as 1 if $p = 0$), and denote by $\chi_V(g)$ the *Brauer character* value for V on a p-regular element g in G; see Section 3 for definitions.

Corollary 1.3. *For any $\mathbb{F}G$-module V of dimension n with $K(V)$ finite, one has*

$$\#K(V) = \frac{p^a}{\#G} \prod_{g \neq e} (n - \chi_V(g)),$$

where the product runs through a set of representatives g for the non-identity p-regular G-conjugacy classes. In particular, the quantity on the right is a positive integer.

The question of when the abelian group $K(V)$ is *finite*, as opposed to having a free part, occupies Section 6. The crucial condition is a generalization of *faithfulness* for semisimple finite group representations: one needs the A-module V to be *tensor-rich* in the sense that every simple A-module occurs in at least one of its tensor powers $V^{\otimes k}$. In fact, we show that tensor-richness implies something much stronger about the map L_V: its submatrix $\overline{L_V}$ obtained by striking out the row and column indexed by the trivial A-module turns out to be a *nonsingular M-matrix*, that is, the inverse $\left(\overline{L_V}\right)^{-1}$ has all nonnegative entries.

Theorem 1.4. *The following are equivalent for an A-module V.*

(i) *$\overline{L_V}$ is a nonsingular M-matrix.*
(ii) *$\overline{L_V}$ is nonsingular.*
(iii) *L_V has rank ℓ, so nullity* 1.
(iv) *$K(V)$ is finite.*
(v) *V is tensor-rich.*

The question of which A-modules V are tensor-rich is answered completely for group algebras $A = \mathbb{F}G$ via a result of Brauer in Section 7. We suspect that the many questions on finite-dimensional Hopf algebras raised here (Questions 3.12, 5.2, 5.12, 6.9) have good answers in general, not just for group algebras.

1.1. **Notations and standing assumptions.** Throughout this paper, $\mathbb{F}$ will be an algebraically closed field, and A will be a finite-dimensional algebra over $\mathbb{F}$. Outside of Section 2.1, we will further assume that A is a Hopf algebra. We denote by $\dim V$ the dimension of an $\mathbb{F}$-vector space V. Only finite-dimensional A-modules V will be considered. All tensor products are over $\mathbb{F}$.

Vectors v in R^m for various rings R are regarded as column vectors, with v_i denoting their i^{th} coordinate. The (i, j) entry of a matrix M will be denoted $M_{i,j}$. (Caveat lector: Most of the matrices appearing in this paper belong to $\mathbb{Z}^{m \times m'}$ or $\mathbb{C}^{m \times m'}$, even when they are constructed from $\mathbb{F}$-vector spaces. In particular, the rank of such a matrix is always understood to be its rank over $\mathbb{Q}$ or $\mathbb{C}$.)

Let $S_1, S_2, \ldots, S_{\ell+1}$ (resp., $P_1, P_2, \ldots, P_{\ell+1}$) be the inequivalent simple (resp., indecomposable projective) A-modules, with $\operatorname{top}(P_i) := P_i / \operatorname{rad} P_i = S_i$. Define two vectors $\mathbf{s}$ and $\mathbf{p}$ in $\mathbb{Z}^{\ell+1}$ as follows:

$$\mathbf{s} := [\dim(S_1), \ldots, \dim(S_{\ell+1})]^T,$$
$$\mathbf{p} := [\dim(P_1), \ldots, \dim(P_{\ell+1})]^T.$$

2. Finite-dimensional Hopf algebras

2.1. **Finite-dimensional algebras.** Let A be a finite-dimensional algebra over an algebraically closed field $\mathbb{F}$. Unless explicitly mentioned otherwise, we will only consider left A-modules V, with $\dim V := \dim_{\mathbb{F}} V$ finite, and all tensor products $\otimes$ will be over the field $\mathbb{F}$. We recall several facts about such modules; see, e.g., Webb [31, Chap. 7] and particularly [31, Thm. 7.3.9]. The left-regular A-module A has a decomposition

$$A \cong \bigoplus_{i=1}^{\ell+1} P_i^{\dim S_i}. \tag{2.1}$$

For an A-module V, if $[V : S_i]$ denotes the multiplicity of S_i as a composition factor of V, then

$$[V : S_i] = \dim \mathrm{Hom}_A(P_i, V). \tag{2.2}$$

There are two *Grothendieck groups*, $G_0(A)$ and $K_0(A)$:

- The first one, $G_0(A)$, is defined as the quotient of the free abelian group on the set of all isomorphism classes $[V]$ of A-modules V, subject to the relations $[U] - [V] + [W]$ for each short exact sequence $0 \to U \to V \to W \to 0$ of A-modules. This group has a $\mathbb{Z}$-module basis consisting of the classes $[S_1], \ldots, [S_{\ell+1}]$, due to the Jordan-Hölder theorem.
- The second one, $K_0(A)$, is defined as the quotient of the free abelian group on the set of all isomorphism classes $[V]$ of **projective** A-modules V, subject to the relations $[U]-[V]+[W]$ for each direct sum decomposition $V = U \oplus W$ of A-modules. This group has a $\mathbb{Z}$-module basis consisting of the classes $[P_1], \ldots, [P_{\ell+1}]$, due to the Krull-Remak-Schmidt theorem.

Note that (2.1) implies the following.

Proposition 2.1. *For a finite-dimensional algebra A over an algebraically closed field $\mathbb{F}$, in $K_0(A)$, the class $[A]$ of the left-regular A-module has the expansion $[A] = \sum_{i=1}^{\ell+1} (\dim S_i)[P_i]$.*

The two bases of $G_0(A)$ and $K_0(A)$ give rise to group isomorphisms $G_0(A) \cong \mathbb{Z}^{\ell+1} \cong K_0(A)$. There is also a $\mathbb{Z}$-bilinear pairing $K_0(A) \times G_0(A) \to \mathbb{Z}$ induced from $\langle [P], [S] \rangle := \dim \mathrm{Hom}_A(P, S)$. This is a perfect pairing since the $\mathbb{Z}$-basis elements satisfy

$$\langle [P_i], [S_j] \rangle = \dim \mathrm{Hom}_A(P_i, S_j) = [S_j : S_i] = \delta_{i,j}$$

(where (2.2) was used for the second equality). More generally,

$$\langle [P_i], [V] \rangle = \dim \mathrm{Hom}_A(P_i, V) = [V : S_i] \tag{2.3}$$

for any A-module V. There is also a $\mathbb{Z}$-linear map $K_0(A) \to G_0(A)$ which sends the class $[P]$ of a projective A-module P in $K_0(A)$ to the class $[P]$ in $G_0(A)$. This map is expressed in the usual bases by the *Cartan matrix* C of A; this is the integer $(\ell + 1) \times (\ell + 1)$-matrix having entries

$$C_{i,j} := [P_j : S_i] = \dim \mathrm{Hom}_A(P_i, P_j). \tag{2.4}$$

If one chooses orthogonal idempotents e_i in A for which $P_i \cong Ae_i$ as A-modules, then one can reformulate

$$C_{i,j} = \dim \mathrm{Hom}_A(P_i, P_j) = \dim \mathrm{Hom}_A \left(Ae_i, Ae_j\right) = \dim \left(e_i A e_j\right) \tag{2.5}$$

where the last equality used the isomorphism $\mathrm{Hom}_A(Ae, V) \cong eV$ sending $\varphi \mapsto \varphi(1)$, for any A-module V and any idempotent e of A; see, e.g., [31, Prop. 7.4.1 (3)].

Taking dimensions of both sides in (2.1) identifies the dot product of $\mathbf{s}$ and $\mathbf{p}$.

Proposition 2.2. *If A is a finite-dimensional algebra over an algebraically closed field, then $\mathbf{s}^T \mathbf{p} = \dim(A)$.*

Proof. From $\mathbf{s} = [\dim(S_1), \ldots, \dim(S_{\ell+1})]^T$ and $\mathbf{p} = [\dim(P_1), \ldots, \dim(P_{\ell+1})]^T$, we obtain

$$\mathbf{s}^T \mathbf{p} = \sum_{i=1}^{\ell+1} \dim(S_i) \dim(P_i) = \dim \left(\bigoplus_{i=1}^{\ell+1} P_i^{\dim S_i} \right) = \dim A \qquad \text{(by (2.1))}.$$

□

On the other hand, the definition (2.4) of the Cartan matrix C immediately yields the following:

Proposition 2.3. *If A is a finite-dimensional algebra over an algebraically closed field, then $\mathbf{p}^T = \mathbf{s}^T C$.*

2.2. **Hopf algebras.** Let A be a finite-dimensional *Hopf algebra* over an algebraically closed field $\mathbb{F}$, with

- counit $\epsilon : A \longrightarrow \mathbb{F}$,
- coproduct $\Delta : A \longrightarrow A \otimes A$,
- antipode $\alpha : A \longrightarrow A$.

Example 2.4. Our main motivating example is the *group algebra* $A = \mathbb{F}G = \{\sum_{g\in G} c_g g : c_g \in \mathbb{F}\}$, for a finite group G, with $\mathbb{F}$ of arbitrary characteristic. For g in G, the corresponding basis element g of $\mathbb{F}G$ has

$$\epsilon(g) = 1,$$
$$\Delta(g) = g \otimes g,$$
$$\alpha(g) = g^{-1}.$$

Example 2.5. For integers $m, n > 0$ with m dividing n, the *generalized Taft Hopf algebra* $A = H_{n,m}$ is discussed in Cibils [5] and in Li and Zhang [18]. As an algebra, it is a skew group ring [20, Example 4.1.6]

$$H_{n,m} = \mathbb{F}[\mathbb{Z}/n\mathbb{Z}] \ltimes \mathbb{F}[x]/(x^m)$$

for the cyclic group $\mathbb{Z}/n\mathbb{Z} = \{e, g, g^2, \ldots, g^{n-1}\}$ acting on coefficients in a truncated polynomial algebra $\mathbb{F}[x]/(x^m)$, via $gxg^{-1} = \omega^{-1}x$, with ω a primitive n^{th} root of unity in $\mathbb{F}$. That is, the algebra $H_{n,m}$ is the quotient of the free associative $\mathbb{F}$-algebra on two generators g, x, subject to the relations $g^n = 1, x^m = 0$ and $xg = \omega gx$. It has dimension mn, with $\mathbb{F}$-basis $\{g^i x^j : 0 \le i < n \text{ and } 0 \le j < m\}$.

The remainder of its Hopf structure is determined by these choices:

$$\begin{array}{rclrcl} \epsilon(g) &=& 1, & \epsilon(x) &=& 0, \\ \Delta(g) &=& g\otimes g, & \Delta(x) &=& 1\otimes x + x \otimes g, \\ \alpha(g) &=& g^{-1}, & \alpha(x) &=& -\omega^{-1}g^{-1}x. \end{array}$$

Example 2.6. Radford defines in [26, Exercise 10.5.9] a further interesting Hopf algebra, which we will denote $A(n, m)$. Let $n > 0$ and $m \ge 0$ be integers such that n is even and n lies in $\mathbb{F}^\times$. Fix a primitive n^{th} root of unity ω in $\mathbb{F}$. As an algebra, $A(n, m)$ is again a skew group ring

$$A(n, m) = \mathbb{F}[\mathbb{Z}/n\mathbb{Z}] \ltimes \bigwedge_{\mathbb{F}}[x_1, \ldots, x_m],$$

for the cyclic group $\mathbb{Z}/n\mathbb{Z} = \{e, g, g^2, \ldots, g^{n-1}\}$ acting this time on coefficients in an exterior algebra $\bigwedge_{\mathbb{F}}[x_1, \ldots, x_m]$, via $gx_ig^{-1} = \omega x_i$. That is, $A(n, m)$ is the quotient of the free associative $\mathbb{F}$-algebra on $g, x_1, \ldots, x_m$, subject to relations $g^n = 1, x_i^2 = 0, x_ix_j = -x_jx_i$, and $gx_ig^{-1} = \omega x_i$. It has dimension $n2^m$ and an $\mathbb{F}$-basis $\left\{g^i x_J : 0 \le i < n,\ J \subseteq \{1, 2, \ldots, m\}\right\}$ where $x_J := x_{j_1}x_{j_2}\cdots x_{j_k}$ if $J = \{j_1 < j_2 < \cdots < j_k\}$. The remainder of its Hopf structure is determined by these choices:

$$\begin{array}{ll} \epsilon(g) = 1, & \epsilon(x_i) = 0, \\ \Delta(g) = g\otimes g, & \Delta(x_i) = 1 \otimes x_i + x_i \otimes g^{n/2}, \\ \alpha(g) = g^{-1}, & \alpha(x_i) = -x_i g^{n/2}. \end{array}$$

In the special case where $n = 2$, the Hopf algebra $A(2, m)$ is the *Nichols Hopf algebra* of dimension 2^{m+1} defined in Nichols [21]; see also Etingof *et. al.* [10, Example 5.5.7].

Example 2.7. When $\mathbb{F}$ has characteristic p, a *restricted Lie algebra* is a Lie algebra $\mathfrak{g}$ over $\mathbb{F}$, together with a *p-operation* $x \mapsto x^{[p]}$ on $\mathfrak{g}$ satisfying certain properties; see Montgomery [20, Defn. 2.3.2]. The *restricted universal enveloping algebra* $\mathfrak{u}(\mathfrak{g})$ is then the quotient of the usual universal enveloping algebra $\mathfrak{U}(\mathfrak{g})$ by the two-sided ideal generated by all elements $x^p - x^{[p]}$ for x in $\mathfrak{g}$. Since this two-sided ideal is also a Hopf ideal, the quotient $\mathfrak{u}(\mathfrak{g})$ becomes a Hopf algebra over $\mathbb{F}$. The dimension of $\mathfrak{u}(\mathfrak{g})$ is $p^{\dim \mathfrak{g}}$, as it has a PBW-style $\mathbb{F}$-basis of monomials $\{x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}\}_{0\le i_j<p}$ corresponding to a choice of ordered $\mathbb{F}$-basis $(x_1, \ldots, x_m)$ of $\mathfrak{g}$.

We return to discussing general finite-dimensional Hopf algebras A over $\mathbb{F}$.

The counit $\epsilon : A \to \mathbb{F}$ gives rise to the 1-dimensional *trivial A-module* ϵ, which is the vector space $\mathbb{F}$ on which A acts through ϵ. Furthermore, for each A-module V, we can define its subspace of *A-fixed points*:

$$V^A := \{v \in V : av = \epsilon(a)v \text{ for all } a \in A\}.$$

The coproduct Δ gives rise to the *tensor product* $V \otimes W$ of two A-modules V and W, defined via $a(v \otimes w) := \sum a_1 v \otimes a_2 w$, using the Sweedler notation $\Delta(a) = \sum a_1 \otimes a_2$ for $a \in A$ (see, e.g., [26, Sect. 2.1] for an introduction to the Sweedler notation). With this definition, the canonical isomorphisms

$$\epsilon \otimes V \cong V \cong V \otimes \epsilon \tag{2.6}$$

are A-module isomorphisms. The following lemma appears, for example, as [8, Prop. 7.2.2].

Lemma 2.8. *Let V be an A-module.*

(i) *Then, $V \otimes A \cong A^{\oplus \dim V}$ as A-modules.*
(ii) *Also, $A \otimes V \cong A^{\oplus \dim V}$ as A-modules.*

The antipode $\alpha : A \to A$ of the Hopf algebra A is bijective, since A is finite-dimensional; see, e.g., [20, Thm. 2.1.3], [26, Thm. 7.1.14 (b)], [22, Prop. 4], or [10, Prop. 5.3.5]. Hence α is an algebra and coalgebra *anti-automorphism*. In particular, as an algebra, $A \cong A^{\mathrm{opp}}$. For each A-module V, the antipode gives rise to two A-module structures on $\mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F})$: the *left-dual* V^* and the *right-dual* ${}^*V$ of V. They are defined as follows: For $a \in A$, $f \in \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F})$ and $v \in V$, we set

$$(af)(v) := \begin{cases} f(\alpha(a)v), & \text{when regarding } f \text{ as an element of } V^*, \\ f(\alpha^{-1}(a)v), & \text{when regarding } f \text{ as an element of } {}^*V. \end{cases}$$

The following two facts are straightforward exercises in the definitions.

Lemma 2.9. *We have A-module isomorphisms $\epsilon^* \cong {}^*\epsilon \cong \epsilon$.*

Lemma 2.10. *Let V be an A-module. We have canonical A-module isomorphisms ${}^*(V^*) \cong V \cong ({}^*V)^*$.*

For any two A-modules V and W, we define an A-module structure on $\mathrm{Hom}_{\mathbb{F}}(V, W)$ via

$$(a\varphi)(v) := \sum a_1 \varphi(\alpha(a_2)v)$$

for all $a \in A$, $\varphi \in \mathrm{Hom}_{\mathbb{F}}(V, W)$ and $v \in V$. The following result appears, for example, as [32, Lemma 2.2].

Lemma 2.11. *Let V and W be two A-modules. Then, we have an A-module isomorphism*

$$\Phi : W \otimes V^* \xrightarrow{\cong} \mathrm{Hom}_{\mathbb{F}}(V, W) \tag{2.7}$$

sending $w \otimes f$ to the linear map $\varphi \in \mathrm{Hom}_{\mathbb{F}}(V, W)$ that is defined by $\varphi(v) = f(v)w$ for all $v \in V$.

In particular, when $W = \epsilon$, this shows $V^* \cong \mathrm{Hom}_{\mathbb{F}}(V, \epsilon)$.

Next, we shall use a result that is proven in Schneider [28, Lemma 4.1][2]

Lemma 2.12. *Let V and W be two A-modules. Then,* $\mathrm{Hom}_A(V, W) = \mathrm{Hom}_{\mathbb{F}}(V, W)^A$.

The next four results are proven in Appendix 8.

Lemma 2.13. *Let V and W be two A-modules. Then,* $\mathrm{Hom}_A(V, W) \cong \mathrm{Hom}_A(W^* \otimes V, \epsilon)$.

Lemma 2.14. *Let U and V be A-modules. Then, $(U \otimes V)^* \cong V^* \otimes U^*$ and ${}^*(U \otimes V) \cong {}^*V \otimes {}^*U$.*

[2]Schneider makes various assumptions that are not used in the proof.

Lemma 2.15. *For A-modules U, V, and W, one has isomorphisms*

$$\mathrm{Hom}_A(U \otimes V, W) \xrightarrow{\sim} \mathrm{Hom}_A(U, W \otimes V^*), \tag{2.8}$$
$$\mathrm{Hom}_A(V^* \otimes U, W) \xrightarrow{\sim} \mathrm{Hom}_A(U, V \otimes W), \tag{2.9}$$
$$\mathrm{Hom}_A(U \otimes {}^*V, W) \xrightarrow{\sim} \mathrm{Hom}_A(U, W \otimes V), \tag{2.10}$$
$$\mathrm{Hom}_A(V \otimes U, W) \xrightarrow{\sim} \mathrm{Hom}_A(U, {}^*V \otimes W). \tag{2.11}$$

Proposition 2.16. *Any A-module V has* $\dim \mathrm{Hom}_A(V, A) = \dim V$.

Proposition 2.16 implies the following two Hopf algebra facts, to be compared with the two "transposed" algebra facts, Propositions 2.1 and 2.3.

Corollary 2.17. *Let A be a finite-dimensional Hopf algebra over an algebraically closed field* $\mathbb{F}$. *Let* P_i, S_i, $\mathbf{p}$, $\mathbf{s}$ *and C be as in Subsection 2.1.*

(i) *The class* $[A]$ *of the left-regular A-module expands in* $G_0(A)$ *as* $[A] = \sum_{i=1}^{\ell+1} (\dim P_i)[S_i]$.
(ii) *The Cartan matrix C has* $C\mathbf{s} = \mathbf{p}$.

Proof. The assertion in (i) follows by noting that for each $i = 1, 2, \ldots, \ell + 1$, one has

$$[A : S_i] = \dim \mathrm{Hom}_A(P_i, A) = \dim (P_i),$$

where the first equality applied (2.2) and the second equality applied Proposition 2.16 with $V = P_i$.

This then helps to deduce assertion (ii), since for each $i = 1, 2, \ldots \ell + 1$, one has

$$(C\mathbf{s})_i = \sum_{j=1}^{\ell+1} C_{ij}\mathbf{s}_j = \sum_{j=1}^{\ell+1} \left[P_j : S_i\right] \dim S_j = \left[\bigoplus_{j=1}^{\ell+1} P_j^{\dim S_j} : S_i\right] = [A : S_i] = \mathbf{p}_i$$

where the second-to-last equality used (2.1), and the last equality is assertion (i). Thus, $C\mathbf{s} = \mathbf{p}$. □

Note that Corollary 2.17 (ii) follows from Proposition 2.3 whenever the Cartan matrix C is symmetric. However, C is not always symmetric, as illustrated by the following example.

Example 2.18. Consider Radford's Hopf algebra $A = A(n, m)$ from Example 2.6, whose algebra structure is the skew group ring $\mathbb{F}[\mathbb{Z}/n\mathbb{Z}] \ltimes \bigwedge_{\mathbb{F}}[x_1, \ldots, x_m]$. In this case, it is not hard to see that the radical of A is the two-sided ideal I generated by $x_1, \ldots, x_m$, with $A/I \cong \mathbb{F}[\mathbb{Z}/n\mathbb{Z}]$, and that A has a system of orthogonal primitive idempotents $\left\{e_k := \frac{1}{n}\sum_{i=0}^{n-1} \omega^{ki} g^i\right\}_{k=0,1,\ldots,n-1}$, where the subscript k can be regarded as an element of $\mathbb{Z}/n\mathbb{Z}$. This gives n indecomposable projective A-modules $\{P_k\}_{k=0,1,\ldots,n-1}$ with $P_k \cong Ae_k$, whose corresponding simple A-modules $\{S_k\}_{k=0,1,\ldots,n-1}$ are the simple modules for the cyclic group algebra $A/I \cong \mathbb{F}[\mathbb{Z}/n\mathbb{Z}]$, regarded as A-modules by inflation.

We compute here the Cartan matrix C for A, using the formulation $C_{i,j} = \dim\left(e_i A e_j\right)$ from (2.5). Recall that A has $\mathbb{F}$-basis $\left\{g^k x_J : 0 \le k < n,\ J \subseteq \{1, 2, \ldots, m\}\right\}$. Using the fact that the $e_0, \ldots, e_{n-1}$ are orthogonal idempotents, and easy calculations such as $e_i g^k = \omega^{-ki} e_i$ and $x_J e_j = e_{j-\#J} x_J$, one concludes that

$$e_i\left(g^k x_J\right)e_j = \omega^{-ki} e_i x_J e_j = \omega^{-ki} e_i e_{j-\#J} x_J = \begin{cases} \omega^{-ki} e_i x_J, & \text{if } i \equiv j - \#J \bmod n, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore $C_{i,j} = \dim\left(e_i A e_j\right) = \#\{J \subseteq \{1, 2, \ldots, m\} : \#J \equiv j - i \bmod n\}$. This matrix C will not be symmetric in general; e.g. for $n = 4$ and $m = 1$, if one indexes rows and columns by e_0, e_1, e_2, e_3, then $C = \begin{bmatrix} 1&1&0&0 \\ 0&1&1&0 \\ 0&0&1&1 \\ 1&0&0&1 \end{bmatrix}$.

2.3. **The Grothendieck ring and the critical group.** The group $G_0(A)$ also has an associative (not necessarily commutative) augmented $\mathbb{Z}$-algebra structure:

- the multiplication is induced from $[V] \cdot [W] := [V \otimes W]$ (which is well-defined, since the tensor bifunctor over $\mathbb{F}$ is exact, and is associative since tensor products are associative),
- the unit element is $1 = [\epsilon]$, the class of the trivial A-module ϵ, and
- the augmentation (algebra) map $G_0(A) \to \mathbb{Z}$ is induced from $[V] \mapsto \dim(V)$.

In many examples that we consider, A will be cocommutative, so that $V \otimes W \cong W \otimes V$, and hence $G_0(A)$ is also commutative. However, Lemma 2.14 shows that there is a ring homomorphism $G_0(A) \to G_0(A)^{\mathrm{opp}}$ sending each $[V]$ to $[V^*]$. Lemma 2.10 furthermore shows that this homomorphism is an isomorphism. Thus, $G_0(A) \cong G_0(A)^{\mathrm{opp}}$ as rings. Consequently, when discussing constructions involving $G_0(A)$ that involve multiplication on the right, we will omit the discussion of the same construction on the left.

The kernel I of the augmentation map, defined by the short exact sequence

$$0 \to I \longrightarrow G_0(A) \longrightarrow \mathbb{Z} \to 0, \tag{2.12}$$

is the (two-sided) *augmentation ideal* of $G_0(A)$. Recalling that the vector $\mathbf{s}$ gave the dimensions of the simple A-modules, then under the additive isomorphism $G_0(A) \cong \mathbb{Z}^{\ell+1}$, the augmentation map $G_0(A) \cong \mathbb{Z}^{\ell+1} \to \mathbb{Z}$ corresponds to the map $\mathbf{x} \mapsto \mathbf{s}^T\mathbf{x}$ that takes dot product with $\mathbf{s}$. Therefore the augmentation ideal $I \subset G_0(A)$ corresponds to the perp sublattice

$$I = \mathbf{s}^{\perp} := \{\mathbf{x} \in \mathbb{Z}^{\ell+1} : \mathbf{s}^T\mathbf{x} = 0\}.$$

We come now to our main definition.

Definition 2.19. Given an A-module V of dimension n, define its *critical group* as the quotient (left-)$G_0(A)$-module of I modulo the principal (left-)ideal generated by $n - [V]$:

$$K(V) := I/G_0(A)(n - [V]) .$$

We are interested in the abelian group structure of $K(V)$, which has some useful matrix reformulations. First, note that the short exact sequence of abelian groups (2.12) is split, since $\mathbb{Z}$ is free abelian. This gives a direct decomposition $G_0(A) = \mathbb{Z} \oplus I$ as abelian groups, which then induces a decomposition

$$G_0(A)/G_0(A)(n - [V]) = \mathbb{Z} \oplus K(V).$$

Second, note that in the ordered $\mathbb{Z}$-basis $([S_1], \ldots, [S_{\ell+1}])$ for $G_0(A)$, one expresses multiplication on the right by $[V]$ via the *McKay matrix* $M = M_V$ in $\mathbb{Z}^{(\ell+1)\times(\ell+1)}$ where $M_{i,j} = [S_j \otimes V : S_i]$. Consequently multiplication on the right by $n - [V]$ is expressed by the matrix $L_V := nI_{\ell+1} - M_V$. Thus the abelian group structure of $K(V)$ can alternately be described in terms of the cokernel of L_V:

$$\mathbb{Z} \oplus K(V) \cong \mathbb{Z}^{\ell+1}/\operatorname{im} L_V, \tag{2.13}$$

$$K(V) \cong \mathbf{s}^{\perp}/\operatorname{im} L_V. \tag{2.14}$$

We will sometimes be able to reformulate $K(V)$ further as the cokernel of an $\ell \times \ell$ submatrix of L_V (see the discussion near the end of Section 6). For this and other purposes, it is important to know about the left- and right-nullspaces of L_V, explored next.

3. Left and right eigenspaces

A goal of this section is to record the observation that, for any A-module V, the vectors $\mathbf{s}$ and $\mathbf{p}$ introduced earlier are always left- and right-eigenvectors for M_V, both having eigenvalue $n = \dim(V)$, and hence left- and right-nullvectors for $L_V = nI_{\ell+1} - M_V$. When $A = \mathbb{F}G$ is the group algebra of a finite group G, we complete this to a full set of left- and right-eigenvectors and eigenvalues: the eigenvalues of M_V turn out to be the *Brauer character values* $\chi_V(g)$, while the left- and right-eigenvectors are the *columns of the Brauer character table* for the simple A-modules and indecomposable projective A-modules, respectively. This interestingly generalizes a well-known story from the McKay correspondence in characteristic zero; see [1, Prop. 5.3, 5.6].

Let us first establish terminology: a *right-eigenvector* (resp. *left-eigenvector*) of a matrix U is a vector v such that $Uv = \lambda v$ (resp. $v^T U = \lambda v^T$) for some scalar λ; notions of left- and right-nullspaces and left- and right-eigenspaces should be intepreted similarly.

We fix an A-module V throughout Section 3; we set $n = \dim(V)$.

3.1. Left-eigenvectors.

Left-eigenvectors of M_V and L_V will arise from the simple A-modules.

Proposition 3.1. *The vector* $\mathbf{s}$ *is a left-eigenvector for* M_V *with eigenvalue* n*, and a left-nullvector for* L_V.

Proof. Letting $M := M_V$, for each $j = 1, 2, \ldots, \ell + 1$, one has

$$n\mathbf{s}_j = \dim(S_j)\dim(V) = \dim(S_j \otimes V) = \sum_{i=1}^{\ell+1} [S_j \otimes V : S_i] \dim(S_i) = \sum_{i=1}^{\ell+1} \dim(S_i) M_{i,j} = (\mathbf{s}^T M)_j. \qquad \square$$

The full left-eigenspace decomposition for M_V and L_V, when $A = \mathbb{F}G$ is a group algebra, requires the notions of p-regular elements and Brauer characters, recalled here.

Definition 3.2. Recall that for a finite group G and a field $\mathbb{F}$ of characteristic $p \geq 0$, an element g in G is *p-regular* if its multiplicative order lies in $\mathbb{F}^\times$. That is, g is p-regular if it is has order coprime to p when $\mathbb{F}$ has characteristic $p > 0$, and *every* g in G is p-regular when $\mathbb{F}$ has characteristic $p = 0$. Let p^a be the order of the p-Sylow subgroups of G, so that $\#G = p^a q$ with $\gcd(p, q) = 1$. (In characteristic zero, set $p^a := 1$ and $q := \#G$.) The order of any p-regular element of G divides q.

To define Brauer characters for G, one first fixes a (cyclic) group isomorphism $\lambda \mapsto \widehat{\lambda}$ between the q^{th} roots of unity in the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$ and the q^{th} roots of unity in $\mathbb{C}$. Then for each $\mathbb{F}G$-module V of dimension n, and each p-regular element g in G, the *Brauer character* value $\chi_V(g) \in \mathbb{C}$ can be defined as follows. Since g is p-regular, it will act semisimply on V by Maschke's theorem, and have eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$ in $\overline{\mathbb{F}}$ which are q^{th} roots of unity when acting on V (or, strictly speaking, when $1 \otimes g$ acts on $\overline{\mathbb{F}} \otimes_{\mathbb{F}} V$). This lets one define $\chi_V(g) := \sum_{i=1}^n \widehat{\lambda_i}$, using the isomorphism fixed earlier. This $\chi_V(g)$ depends only on the conjugacy class of g (not on g itself), and so is also called the *Brauer character value* of V at the conjugacy class of g.

Brauer showed [31, Theorem 9.3.6] that the number $\ell + 1$ of simple $\mathbb{F}G$-modules is the same as the number of p-regular conjugacy classes. He further showed that the map sending $V \longmapsto \chi_V$ induces a ring isomorphism from the Grothendieck ring $G_0(A)$ to $\mathbb{C}^{\ell+1}$, where $\mathbb{C}^{\ell+1}$ is the ring of $\mathbb{C}$-valued class functions on the $\ell + 1$ distinct p-regular G-conjugacy classes, under pointwise addition and multiplication; see [31, Prop. 10.1.3]. One has the accompanying notion of the *Brauer character table* for G, an invertible $(\ell + 1) \times (\ell + 1)$ matrix [31, Theorem 10.2.2] having columns indexed by the p-regular conjugacy classes of G, rows indexed by the simple $\mathbb{F}G$-modules S_i, and entry $\chi_{S_i}(g_j)$ in the row for S_i and column indexed by the conjugacy class of g_j.

Definition 3.3. Given a p-regular element g in G, let $\mathbf{s}(g) = [\chi_{S_1}(g), \ldots, \chi_{S_{\ell+1}}(g)]^T$ be the Brauer character values of the simple $\mathbb{F}G$-modules at g, that is, the column indexed by the conjugacy class of g in the Brauer character table of G. In particular, $\mathbf{s}(e) = \mathbf{s}$, where e is the identity element of G.

Proposition 3.4. *For any p-regular element g in G, the vector* $\mathbf{s}(g)$ *is a left-eigenvector for M_V and L_V, with eigenvalues $\chi_V(g)$ and $n - \chi_V(g)$, respectively.*

Proof. Generalize the calculation from Proposition 3.1, using the fact that $[V] \mapsto \chi_V$ is a ring map:

$$\chi_V(g) \cdot \mathbf{s}(g)_j = \chi_V(g)\chi_{S_j}(g) = \chi_{S_j \otimes V}(g) = \sum_{i=1}^{\ell+1} [S_j \otimes V : S_i] \chi_{S_i}(g) = \sum_{i=1}^{\ell+1} \mathbf{s}(g)_i M_{i,j} = (\mathbf{s}(g)^T M)_j. \qquad \square$$

3.2. **Right-eigenvectors.** Right-eigenvectors for L_V and M_V will come from the indecomposable projective A-modules, as we will see below (Proposition 3.8 and, for group algebras, the stronger Proposition 3.10). First, we shall show some lemmas.

Lemma 3.5. *For any A-module V, and $i, j \in \{1, 2, \ldots, \ell+1\}$, one has*

$$[V \otimes P_j^* : S_i] = [\,{}^*P_i \otimes V : S_j]. \tag{3.1}$$

In particular, taking $V = \epsilon$ gives a "dual symmetry" for the Cartan matrix C of A:

$$[P_j^* : S_i] = [\,{}^*P_i : S_j]. \tag{3.2}$$

Proof. The result follows upon taking dimensions in the following consequence of (2.8) and (2.11):

$$\mathrm{Hom}_A(P_i, V \otimes P_j^*) \cong \mathrm{Hom}_A(P_i \otimes P_j, V) \cong \mathrm{Hom}_A(P_j, {}^*P_i \otimes V). \qquad \square$$

Lemma 3.6. *The following equality holds in the Grothendieck group $G_0(A)$ for any $[V] \in G_0(A)$:*

$$[V \otimes P_j^*] = \sum_{i=1}^{\ell+1} [S_i \otimes V : S_j][P_i^*], \quad \forall j \in \{1, 2, \ldots, \ell+1\}.$$

Proof. By (3.1), the multiplicity of S_k in the left hand side is

$$[V \otimes P_j^* : S_k] = [\,{}^*P_k \otimes V : S_j]. \tag{3.3}$$

However, one also has in $G_0(A)$ that

$$[{}^*P_k \otimes V] = [{}^*P_k] \cdot [V] = \sum_i [{}^*P_k : S_i][S_i] \cdot [V] = \sum_i [{}^*P_k : S_i][S_i \otimes V]$$

and substituting this into (3.3) gives

$$[V \otimes P_j^* : S_k] = \sum_i [S_i \otimes V : S_j][\,{}^*P_k : S_i] = \sum_i [S_i \otimes V : S_j][\,P_i^* : S_k]$$

where we have used (3.2) in the last equality. One can then recognize this last expression as the multiplicity of S_k in the right hand side of the desired equation. $\square$

Lemma 3.7. *Any indecomposable projective A-module P_i has its left-dual P_i^* and right-dual ${}^*P_i$ also indecomposable projective. Consequently, $P_1^*, \ldots, P_{\ell+1}^*$ form a permutation of $P_1, \ldots, P_{\ell+1}$.*

Proof. Lemma 2.10 shows that $V \mapsto V^*$ is an equivalence of categories from the category of (finite-dimensional) A-modules to its opposite category. Since we furthermore have A-module isomorphisms $\left(\bigoplus_i V_i\right)^* \cong \bigoplus V_i^*$ (for finite direct sums) and similarly for right-duals, we thus see that indecomposability is preserved under taking left-duals. It is well-known [10, Prop. 6.1.3] that projectivity is preserved under taking left-duals. Thus P_i^* is also indecomposable projective and so is ${}^*P_i$ by the same argument. Then $P_1^*, \ldots, P_{\ell+1}^*$ form a permutation of $P_1, \ldots, P_{\ell+1}$ since ${}^*(V^*) \cong V$. $\square$

Since $\dim(P_i) = \dim(P_i^*)$, the definition of the vector $\mathbf{p}$ can be rewritten as

$$\mathbf{p} := [\dim(P_1), \ldots, \dim(P_{\ell+1})]^T = \left[\dim(P_1^*), \ldots, \dim(P_{\ell+1}^*)\right]^T.$$

Proposition 3.8. *This $\mathbf{p}$ is a right-eigenvector for M_V with eigenvalue n, and a right-nullvector for L_V.*

Proof. Letting $M := M_V$, for each $j = 1, 2, \ldots, \ell+1$, using Lemma 3.6 one has

$$n\mathbf{p}_j = \dim(V)\dim(P_j^*) = \dim\left(V \otimes P_j^*\right) = \sum_{i=1}^{\ell+1} [S_i \otimes V : S_j] \dim(P_i^*) = \sum_{i=1}^{\ell+1} M_{j,i}\mathbf{p}_i = (M\mathbf{p})_j. \qquad \square$$

In the case of a group algebra $A = \mathbb{F}G$, one has the analogous result to Proposition 3.4.

Definition 3.9. For a p-regular g in G, let $\mathbf{p}^*(g) = [\chi_{P_1^*}(g), \ldots, \chi_{P_{\ell+1}^*}(g)]^T$ be the Brauer character values of the (left-duals of the) indecomposable projective A-modules P_i^* at g. Note that $\mathbf{p}^*(g)$ is a re-ordering of the column indexed by g in the $(\ell+1)\times(\ell+1)$ table of Brauer characters of the indecomposable projective $\mathbb{F}G$-modules, whose (i, j)-entry is $\chi_{P_i}(g_j)$. In particular, $\mathbf{p}^*(e) = \mathbf{p}$, where e is the identity in G. Note that this indecomposable projective Brauer character table is also an invertible matrix [31, Theorem 10.2.2].

Proposition 3.10. *This $\mathbf{p}^*(g)$ is a right-eigenvector for M_V and L_V, with eigenvalues $\chi_V(g)$ and $n - \chi_V(g)$.*

Proof. Generalize the calculation from Proposition 3.8 using the fact that $[V] \mapsto \chi_V$ is a ring map:

$$\chi_V(g)\cdot \mathbf{p}^*(g)_j = \chi_V(g)\chi_{P_j^*}(g) = \chi_{V\otimes P_j^*}(g) = \sum_{i=1}^{\ell+1}[S_i\otimes V : S_j]\chi_{P_i^*}(g) = \sum_{i=1}^{\ell+1} M_{j,i}\mathbf{p}^*(g)_i = (M\mathbf{p}^*(g))_j. \quad \square$$

Remark 3.11. Note that since the Brauer character tables for the simple $\mathbb{F}G$-modules and for the indecomposable projective $\mathbb{F}G$-modules are both invertible, Propositions 3.4 and 3.10 yield full bases for $\mathbb{C}^{\ell+1}$ consisting of right-eigenvectors for M_V or L_V, and of left-eigenvectors for M_V or L_V.

Question 3.12. *Are there analogues of Propositions 3.4, 3.10 for all finite-dimensional Hopf algebras?*

In particular, what plays the role of p-regular elements, and Brauer characters?

One little step towards resolving Question 3.12 is to observe that if a is a group-like element of a finite-dimensional $\mathbb{F}$-Hopf algebra A (that is, $\Delta(a) = a\otimes a$ and $\epsilon(a) = 1$), then the vector $\left[\mathrm{Tr}_{S_1}(a), \mathrm{Tr}_{S_2}(a), \ldots, \mathrm{Tr}_{S_{\ell+1}}(a)\right]^T \in \mathbb{F}^{\ell+1}$ (where $\mathrm{Tr}_W(a)$ stands for the trace of the action of a on an A-module W) is an eigenvector (with eigenvalue $\mathrm{Tr}_V(a)$) for the matrix $(M_V)_{\mathbb{F}}$ obtained by mapping the matrix $M_V \in \mathbb{Z}^{(\ell+1)\times(\ell+1)}$ into $\mathbb{F}^{(\ell+1)\times(\ell+1)}$. This gives us some eigenvectors for this matrix $(M_V)_{\mathbb{F}}$; but we do not know whether they can be lifted to eigenvectors of M_V, and how far they are away from yielding the diagonalization of $(M_V)_{\mathbb{F}}$ (if such a diagonalization even exists).

Remark 3.13. It is perhaps worth noting that many of the previous results which we have stated for a finite-dimensional Hopf algebra A, including Propositions 3.1 and 3.8 on $\mathbf{s}$ and $\mathbf{p}$ as left- and right-nullvectors for L_V, hold in somewhat higher generality. One can replace the category of A-modules with a *finite tensor category* C, replace $G_0(A)$ with the Grothendieck ring $G_0(C)$ of C, and replace the assignment $V \mapsto \dim V$ for A-modules V with the *Frobenius-Perron dimension* as an algebra morphism $\mathsf{FPdim} : G_0(C) \to \mathbb{R}$; see [10, Chapters 1–4]. Most of our arguments mainly use the existence of left- and right-duals V^* and ${}^*V$ for objects V in such a category C, and properties of FPdim.

In fact, we feel that, in the same way that Frobenius-Perron dimension $\mathsf{FPdim}(V)$ is an interesting real-valued invariant of an object in a tensor category, whenever $\mathsf{FPdim}(V)$ happens to be an integer, the critical group $K(V)$ is another interesting invariant taking values in abelian groups.

4. Proof of Theorem 1.1

We next give the structure of the critical group $K(A)$ for the left-regular representation A. We start with a description of its McKay matrix M_A using the Cartan matrix C, and the vectors $\mathbf{s}, \mathbf{p}$ from Subsection 2.1.

Proposition 4.1. *Let A be a finite-dimensional Hopf algebra over an algebraically closed field $\mathbb{F}$. Then the McKay matrix M_A of the left-regular representation A takes the form*

$$M_A = C\mathbf{s}\mathbf{s}^T = \mathbf{p}\mathbf{s}^T.$$

Proof. For every A-module V and any $i \in \{1, 2, \ldots, \ell+1\}$, we obtain from[3] Lemma 2.8(i) the equality

$$[V\otimes A : S_i] = \left[A^{\oplus \dim V} : S_i\right] = (\dim V)\,[A : S_i]\,. \tag{4.1}$$

[3]Instead of using Lemma 2.8 (i) here, we could also have used the weaker result that $[V\otimes A] = \dim(V)[A]$ in $G_0(A)$; this weaker result has the advantage of being generalizable to tensor categories [10, Prop. 6.1.11].

Now, we can compute the entries of the McKay matrix M_A:

$$(M_A)_{i,j} = [S_j \otimes A : S_i] = \dim(S_j)[A : S_i] = \dim(S_j)\dim(P_i) = \mathbf{s}_j\mathbf{p}_i = \left(\mathbf{p}\mathbf{s}^T\right)_{i,j}$$

using (4.1) in the second equality, and Corollary 2.17 (i) in the third. Thus $M_A = \mathbf{p}\mathbf{s}^T$ and then $\mathbf{p}\mathbf{s}^T = C\mathbf{s}\mathbf{s}^T$, since $\mathbf{p} = C\mathbf{s}$ from Corollary 2.17 (ii). □

We will deduce the description of $K(A)$ from Proposition 4.1 and the following lemma from linear algebra:

Lemma 4.2. *Let* $\mathbf{s}$ *and* $\mathbf{p}$ *be column vectors in* $\mathbb{Z}^{\ell+1}$ *with* $\ell \geq 1$ *and* $\mathbf{s}_{\ell+1} = 1$. *(In this lemma,* $\mathbf{s}$ *and* $\mathbf{p}$ *are not required to be the vectors from Subsection 1.1.) Set* $d := \mathbf{s}^T\mathbf{p}$ *and assume that* $d \neq 0$. *Let* $\gamma := \gcd(\mathbf{p})$. *Then the matrix* $L := dI_{\ell+1} - \mathbf{p}\mathbf{s}^T$ *has cokernel*

$$\mathbb{Z}^{\ell+1}/\operatorname{im} L \cong \mathbb{Z} \oplus (\mathbb{Z}/\gamma\mathbb{Z}) \oplus (\mathbb{Z}/d\mathbb{Z})^{\ell-1}.$$

We shall now give a proof of Lemma 4.2 using the Smith normal form of a matrix. For a second, more elementary proof, see Section 9.

First proof of Lemma 4.2. Note that $\mathbf{s}^T L = d\mathbf{s}^T - \mathbf{s}^T\mathbf{p}\mathbf{s}^T = d\mathbf{s}^T - d\mathbf{s}^T = 0$. This has two implications. One is that L is singular, so its Smith normal form has diagonal entries $(d_1, d_2, \ldots, d_\ell, 0)$, with d_i dividing d_{i+1} for each i. Hence $\mathbb{Z}^{\ell+1}/\operatorname{im} L \cong \mathbb{Z}\oplus\left(\bigoplus_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}\right)$, and our goal is to show that $(d_1, d_2, \ldots, d_\ell) = (\gamma, d, d, \ldots, d)$.

The second implication is that $\operatorname{im} L \subset \mathbf{s}^\perp$, which we claim lets us reformulate the cokernel of L as follows:

$$\mathbb{Z}^{\ell+1}/\operatorname{im} L \cong \mathbb{Z} \oplus \mathbf{s}^\perp/\operatorname{im}(L), \qquad \left(\text{so that } \mathbf{s}^\perp/\operatorname{im}(L) \cong \bigoplus_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}\right). \tag{4.2}$$

To see this claim, note that $\mathbf{x} \mapsto \mathbf{s}^T\mathbf{x}$ gives a surjection $\mathbb{Z}^{\ell+1} \to \mathbb{Z}$, since $\mathbf{s}_{\ell+1} = 1$, and hence a short exact sequence $0 \to \mathbf{s}^\perp \to \mathbb{Z}^{\ell+1} \to \mathbb{Z} \to 0$. The sequence splits since $\mathbb{Z}$ is a free (hence projective) $\mathbb{Z}$-module, and then the resulting direct sum decomposition $\mathbb{Z}^{\ell+1} = \mathbb{Z} \oplus \mathbf{s}^\perp$ induces the claimed decomposition in (4.2).

Note furthermore that the abelian group $\mathbf{s}^\perp/\operatorname{im}(L)$ is all d-torsion, since for any $\mathbf{x}$ in $\mathbf{s}^\perp$, one has that $\operatorname{im}(L)$ contains $L\mathbf{x} = d\mathbf{x} - \mathbf{p}\mathbf{s}^T\mathbf{x} = d\mathbf{x}$. Therefore each of $(d_1, d_2, \ldots, d_\ell)$ must divide d.

Note that $\gamma = \gcd(\mathbf{p})$ must divide $d = \mathbf{s}^T\mathbf{p}$, and hence we may assume without loss of generality that $\gamma = 1$, after replacing $\mathbf{p}$ with $\frac{1}{\gamma}\mathbf{p}$: this has the effect of replacing d with $\frac{d}{\gamma}$, replacing γ with 1, replacing L with $\frac{1}{\gamma}L$, and $(d_1, d_2, \ldots, d_\ell, 0)$ with $\frac{1}{\gamma}(d_1, d_2, \ldots, d_\ell, 0)$ (since the Smith normal form of $\frac{1}{\gamma}L$ is obtained from that of L by dividing all entries by γ).

Once we have assumed $\gamma = 1$, our goal is to show $(d_1, d_2, \ldots, d_\ell) = (1, d, d, \ldots, d)$. However, since we have seen that each d_i divides d, it only remains to show that $d_1 = 1$, and d divides each of $(d_2, d_3, \ldots, d_\ell)$. To this end, recall (e.g., [9, §12.3 Exer. 35]) that if one defines g_k as the gcd of all $k \times k$ minor subdeterminants of L, then $d_k = \frac{g_k}{g_{k-1}}$. Thus it remains only to show that $g_1 = 1$ and that g_2 is divisible by d.

To see that $g_1 = 1$, we claim 1 lies in the ideal I of $\mathbb{Z}$ generated by the last column $[-\mathbf{p}_1, -\mathbf{p}_2, \ldots, -\mathbf{p}_\ell, d - \mathbf{p}_{\ell+1}]^T$ of L together with the $(1,1)$-entry $L_{1,1} = d - \mathbf{p}_1\mathbf{s}_1$. To see this claim, note that $d = (d - \mathbf{p}_1\mathbf{s}_1) + \mathbf{s}_1 \cdot \mathbf{p}_1$ lies in I, hence $\mathbf{p}_{\ell+1} = d - (d - \mathbf{p}_{\ell+1})$ lies in I, and therefore $1 = \gcd(\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_{\ell+1})$ also lies in I.

To see d divides g_2, we need only to show that each 2×2 minor subdeterminant of $dI - \mathbf{p}\mathbf{s}^T$ vanishes modulo d. This holds, since working modulo d, one can replace $dI - \mathbf{p}\mathbf{s}^T$ by $-\mathbf{p}\mathbf{s}^T$, a rank one matrix. □

We can now prove Theorem 1.1. Recall that its statement involves the number $\ell + 1$ of simple A-modules, the dimension d of A, and the gcd γ of the dimensions of the indecomposable projective A-modules.

Theorem 1.1. *Let* $d := \dim A$ *and* $\gamma := \gcd(\mathbf{p})$. *If* $\ell = 0$ *then* $K(A) = 0$, *else* $K(A) \cong (\mathbb{Z}/\gamma\mathbb{Z}) \oplus (\mathbb{Z}/d\mathbb{Z})^{\ell-1}$.

Proof. The case $\ell = 0$ is somewhat trivial, since M_A, L_A are the 1×1 matrices $[d], [0]$, and $K(A) = 0$.

When $\ell \geq 1$, note that Proposition 2.2 gives $\mathbf{s}^T\mathbf{p} = \dim A = d$, and Proposition 4.1 yields $M_A = \mathbf{p}\mathbf{s}^T$, so that $L_A = dI_{\ell+1} - \mathbf{p}\mathbf{s}^T$. Reindexing $S_1, \ldots, S_{\ell+1}$ so that $S_{\ell+1} = \epsilon$, the result now follows from Lemma 4.2. □

5. Proofs of Theorem 1.2 and Corollary 1.3

We record here a key observation of Lorenzini [16, Prop. 2.1] that leads to a formula for the cardinality of the critical group $K(V)$.

Proposition 5.1 ([16, Prop. 2.1])**.** *Let L be a matrix in $\mathbb{Z}^{(\ell+1)\times(\ell+1)}$, regarded as a linear map $\mathbb{Z}^{\ell+1} \to \mathbb{Z}^{\ell+1}$, of rank ℓ, with characteristic polynomial $x \prod_{i=1}^{\ell}(x - \lambda_i)$, and whose integer right-nullspace* [4] *(resp. left-nullspace) is spanned over $\mathbb{Z}$ by the primitive vector $\mathbf{n}$ (resp. $\mathbf{n}'$) in $\mathbb{Z}^{\ell+1}$. Assume that $\mathbf{n}^T\mathbf{n}' \neq 0$.*

Then, the torsion part K of the cokernel $\mathbb{Z}^{\ell+1}/\operatorname{im} L \cong \mathbb{Z} \oplus K$ has cardinality $\#K = \left|\frac{1}{\mathbf{n}^T\mathbf{n}'}(\lambda_1\lambda_2\cdots\lambda_\ell)\right|$.

Proof. This is a restatement of $\lambda_1\lambda_2\cdots\lambda_\ell = \pm\#K \cdot \left(\mathbf{n}^T\mathbf{n}'\right)$, which is the displayed equation in [16, Prop. 2.1]. (The requirement $n > 1$ is unnecessary.) □

This lets us prove Theorem 1.2 from the Introduction, whose statement we recall here.

Theorem 1.2. *Let $d := \dim A$ and $\gamma := \gcd(\mathbf{p})$. Assume $K(V)$ is finite, so that L_V has nullity one. If the characteristic polynomial of L_V factors as $\det(xI - L_V) = x\prod_{i=1}^{\ell}(x - \lambda_i)$, then $\#K(V) = \left|\frac{\gamma}{d}(\lambda_1\lambda_2\cdots\lambda_\ell)\right|$.*

Proof. From (2.13), we see that $K(V)$ is isomorphic to the torsion part of $\mathbb{Z}^{\ell+1}/\operatorname{im}(L_V)$.

From Proposition 2.2, we obtain $\mathbf{s}^T\mathbf{p} = d(\neq 0)$. Propositions 3.1 and 3.8 exhibit $\mathbf{s}$ and $\mathbf{p}$ as left- and right-nullvectors of L_V in $\mathbb{Z}^{\ell+1}$. Note that $\mathbf{s}$ is primitive, since one of its coordinates is $\dim(\epsilon) = 1$, while $\frac{1}{\gamma}\mathbf{p}$ is also primitive. Since the integer left-nullspace and the integer right-nullspace of L_V are free of rank 1 (because L_V has nullity 1), this shows that $\mathbf{s}$ and $\frac{1}{\gamma}\mathbf{p}$ span these two nullspaces. Then Proposition 5.1 (applied to $\mathbf{n} = \frac{1}{\gamma}\mathbf{p}$ and $\mathbf{n}' = \mathbf{s}$) implies

$$\#K(V) = \left|\frac{1}{\left(\frac{1}{\gamma}\mathbf{p}\right)^T\mathbf{s}}(\lambda_1\lambda_2\cdots\lambda_\ell)\right| = \left|\frac{\gamma}{d}(\lambda_1\lambda_2\cdots\lambda_\ell)\right|.$$ □

The important role played by $\gamma = \gcd(\mathbf{p})$ in Theorem 1.1 and Theorem 1.2 raises the following question.

Question 5.2. *For a finite-dimensional Hopf algebra A over an algebraically closed field, what does the gcd of the dimensions of the indecomposable projective A-modules "mean" in terms of the structure of A?*

We shall answer this question for some Hopf algebras A in Remark 5.11 further below. The following answer for group algebras may be known to experts, but we did not find it in the literature.

Proposition 5.3. *For $A = \mathbb{F}G$ the group algebra of a finite group G, the gcd γ of the dimensions $\mathbf{p}$ of the indecomposable projective $\mathbb{F}G$-modules equals*

- *1 when $\mathbb{F}$ has characteristic zero,*
- *the order of a p-Sylow subgroup of G when $\mathbb{F}$ has characteristic $p > 0$.*

Proof. The statement is obvious in characteristic 0, since $\gamma = 1$, as ϵ is a 1-dimensional projective A-module.

Thus we may assume $\mathbb{F}$ has positive characteristic p. We first claim $\gamma = \gcd(\mathbf{p})$ is a power of p. To deduce this, let C be the Cartan matrix of A. Proposition 2.3 shows that $\mathbf{p}^T = \mathbf{s}^T C$. Multiplying this equation on the right by the *adjugate* matrix $\operatorname{adj}(C)$, whose entries are the cofactors of C, one finds that

$$\mathbf{p}^T \operatorname{adj}(C) = \mathbf{s}^T C \operatorname{adj}(C) = \det(C)\mathbf{s}^T. \tag{5.1}$$

The positive integer γ divides every entry of $\mathbf{p}$, and hence divides every entry on the left of (5.1). Note that $\det(C)$ occurs as an entry on the right of (5.1), so γ divides $\det(C)$, which by a result of Brauer [3, Thm. 1] (also proven in [29, §16.1, Corollary 3] and [7, Theorem (18.25)]) is a power of p. That is, $\gamma = p^b$ for some $b \geq 0$.

[4]The *integer right-nullspace* of L is defined to be the $\mathbb{Z}$-module of all column vectors $u \in \mathbb{Z}^{\ell+1}$ such that $Lu = 0$. The *integer left-nullspace* of L is defined to be the $\mathbb{Z}$-module of all column vectors $u \in \mathbb{Z}^{\ell+1}$ such that $L^T u = 0$.

All that remains is to apply a result of Dickson, asserting that the p-Sylow order p^a for G is the minimum of the powers of p dividing the dimensions $\dim(P_i)$; see Curtis and Reiner [6, (84.15)]. We give a modern argument for this here. Since the p-Sylow order p^a for G divides the dimension of every projective $\mathbb{F}G$-module (see [7, §18, Exer. 5], [31, Cor. 8.1.3]), it also divides $\gamma = p^b$, implying $b \geq a$. For the opposite inequality, since $\#G = p^a q$ where $\gcd(p, q) = 1$, and $\#G = \dim \mathbb{F}G = \dim A = \mathbf{s}^T \mathbf{p}$ by Proposition 2.2, the prime power $p^b = \gamma$ divides $\mathbf{s}^T \mathbf{p} = \#G = p^a q$, and therefore $b \leq a$. Thus $b = a$, so that $\gamma = p^b = p^a$. □

Since the number of simple $\mathbb{F}G$-modules is the number of p-regular G-conjugacy classes, the following is immediate from Theorem 1.1 and Proposition 5.3.

Corollary 5.4. *For the group algebra $A = \mathbb{F}G$ of a finite group G, with $\ell + 1 \geq 2$ different p-regular conjugacy classes, and p-Sylow order p^a, the regular representation A has critical group*

$$K(A) \cong (\mathbb{Z}/p^a\mathbb{Z}) \oplus (\mathbb{Z}/(\#G)\mathbb{Z})^{\ell-1}.$$

Since for group algebras, either of Proposition 3.4 or 3.10 identified the eigenvalues of L_V in terms of the Brauer character values of V, one immediately deduces Corollary 1.3 from the Introduction:

Corollary 1.3. *For any $\mathbb{F}G$-module V of dimension n with $K(V)$ finite, one has*

$$\#K(V) = \frac{p^a}{\#G} \prod_{g \neq e} (n - \chi_V(g)),$$

where the product runs through a set of representatives g for the non-identity p-regular G-conjugacy classes. In particular, the quantity on the right is a positive integer.

Example 5.5. Let us compute what some of the foregoing results say when $A = \mathbb{F}G$ for the symmetric group $G = \mathfrak{S}_4$, and $\mathbb{F}$ has characteristic p, assuming some facts about modular $\mathfrak{S}_N$-representations that can be found, e.g., in James and Kerber [14]. Every field $\mathbb{F}$ is a splitting field for each $\mathfrak{S}_N$, so we may assume $\mathbb{F} = \mathbb{F}_p$. Furthermore one need only consider three cases, namely $p = 2, 3$ and $p \geq 5$, since $\mathbb{F}\mathfrak{S}_N$ is semisimple for $p > N$, and in that case, the theory is the same as in characteristic zero. The simple A-modules can be indexed D^λ where λ are the p-regular partitions of $N = 4$, that is, those partitions having no parts repeated p or more times. For $p = 2, 3$, we have the following Brauer character tables and Cartan matrices (see [31, Example 10.1.5]):

$$p = 2: \qquad \begin{array}{c} \\ D^4 \\ D^{31} \end{array} \begin{array}{c} \begin{matrix} e & (ijk) \end{matrix} \\ \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix} \end{array} \qquad C = \begin{pmatrix} 4 & 2 \\ 2 & 3 \end{pmatrix}$$

$$p = 3: \qquad \begin{array}{c|cccc} & e & (ij) & (ij)(kl) & (ijkl) \\ \hline D^4 & 1 & 1 & 1 & 1 \\ D^{31} & 3 & 1 & -1 & -1 \\ D^{22} & 1 & -1 & 1 & -1 \\ D^{211} & 3 & -1 & -1 & 1 \end{array} \qquad C = \begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

while for $p \geq 5$, the Brauer character table is the ordinary one (and the Cartan matrix C is the identity):

$$\begin{array}{c|ccccc} & e & (ij) & (ij)(kl) & (ijk) & (ijkl) \\ \hline D^4 & 1 & 1 & 1 & 1 & 1 \\ D^{31} & 3 & 1 & 0 & -1 & -1 \\ D^{22} & 2 & 0 & -1 & 2 & 0 \\ D^{211} & 3 & -1 & 0 & -1 & 1 \\ D^{1111} & 1 & -1 & 1 & 1 & -1 \end{array}.$$

In each case, $\mathbf{s}$ is the first column of the Brauer character table, $\mathbf{p}^T = \mathbf{s}^T C$, and $\gamma = \gcd(\mathbf{p})$:

p	$\mathbf{s}$	$\mathbf{p}$	γ
2	$[1,2]^T$	$[8,8]^T$	$8=2^3$
3	$[1,3,1,3]^T$	$[3,3,3,3]^T$	3
≥ 5	$[1,3,2,3,1]^T$	$[1,3,2,3,1]^T$	1

Note that γ is the order p^a of the p-Sylow subgroups for $G = \mathfrak{S}_4$ in each case.

In Section 6 we will show that the critical group $K(V)$ is finite if and only if V is tensor-rich. One can read off which simple $\mathbb{F}\mathfrak{S}_4$-modules $V = D^\lambda$ are tensor-rich using Theorem 7.3 below: this holds exactly when the only $g \in \mathfrak{S}_4$ satisfying $\chi_V(g) = n := \dim V$ is $g = e$. Perusing the above tables, one sees that in each case, the simple modules labeled D^4, D^{22}, D^{1111} are the ones which are not tensor-rich. However, the module $V = D^{31}$ is tensor-rich for each p, and one can use its character values $\chi_V(g)$ to compute $M_V, L_V, K(V)$ and check Corollary 1.3 in each case as follows:

p	M_V for $V=D^{31}$	$L_V = nI - M_V$	Smith form of L_V	$K(V)$	$\#K(V) = \frac{\gamma}{\#G}\prod_{g\neq e}(n-\chi_V(g))$
2	$\begin{pmatrix}0&2\\1&1\end{pmatrix}$	$\begin{pmatrix}2&-2\\-1&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&0\end{pmatrix}$	0	$1 = \frac{8}{24}(2-(-1))$
3	$\begin{pmatrix}0&2&0&1\\1&1&0&1\\0&1&0&2\\0&1&1&1\end{pmatrix}$	$\begin{pmatrix}3&-2&0&-1\\-1&2&0&-1\\0&-1&3&-2\\0&-1&-1&2\end{pmatrix}$	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&4&0\\0&0&0&0\end{pmatrix}$	$\mathbb{Z}/4\mathbb{Z}$	$4 = \frac{3}{24}(3-1)(3-(-1))(3-(-1))$
≥ 5	$\begin{pmatrix}0&1&0&0&0\\1&1&1&1&0\\0&1&0&1&0\\0&1&1&1&1\\0&0&0&1&0\end{pmatrix}$	$\begin{pmatrix}3&-1&0&0&0\\-1&2&-1&-1&0\\0&-1&3&-1&0\\0&-1&-1&2&-1\\0&0&0&-1&3\end{pmatrix}$	$\begin{pmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&4&0\\0&0&0&0&0\end{pmatrix}$	$\mathbb{Z}/4\mathbb{Z}$	$4 = \frac{1}{24}(3-1)(3-0)(3-(-1))(3-(-1))$

The answer $K(D^{31}) \cong \mathbb{Z}/4\mathbb{Z}$ for $p \geq 5$ is also consistent with Gaetz [11, Example 6].

Example 5.6. The above examples with $G = \mathfrak{S}_4$ are slightly deceptive, in that, for each prime p, there exists an $\mathbb{F}\mathfrak{S}_4$-module P_i having $\dim P_i = \gamma = \gcd(\mathbf{p})$. This fails for $G = \mathfrak{S}_5$, e.g., examining $\mathbb{F}_3\mathfrak{S}_5$-modules, one finds that $\mathbf{s} = (1,1,4,4,6)$ and $\mathbf{p} = (6,6,9,9,6)$, so that $\gamma = 3$, but $\dim P_i \neq 3$ for all i.

Example 5.7. (This example at least illustrates that γ is not always equal to $\dim(P_i)$ for some i.) Let $A = \mathbb{F}G$ be the group algebra of the symmetric group $G = \mathfrak{S}_5$ over the algebraic closure $\mathbb{F}$ of $\mathbb{F}_3$. By computations in Magma, the Brauer character tables of the simple A-modules and indecomposable projective A-modules are

$$\begin{pmatrix}1&1&1&1&1\\1&-1&1&-1&1\\4&2&0&0&-1\\4&-2&0&0&-1\\6&0&-2&0&1\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}6&0&2&2&1\\6&0&2&-2&1\\9&3&1&-1&-1\\9&-3&1&1&-1\\6&0&-2&0&1\end{pmatrix}$$

where the simple A-modules $S_1,\ldots,S_5$ and the indecomposable projective A-modules $P_1,\ldots,P_5$ are labeled in such a way that S_1 is the trivial A-module and $S_i = \operatorname{top}(P_i)$ for all i. We have $\mathbf{s} = (1,1,4,4,6)$, $\mathbf{p} = (6,6,9,9,6)$, and $\gcd(\mathbf{p}) = 3$ equals the order of a 3-Sylow subgroup of $\mathfrak{S}_5$. The A-module $V = P_4$ is tensor-rich by Proposition 7.1 and Theorem 7.3, since $\chi_V(e) = 9 \neq \chi_V(g)$ for all 3-regular $g \neq e$. We have

$$M_V = \begin{pmatrix} 1 & 0 & 0 & 2 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 2 & 2 & 1 & 4 & 2 \\ 2 & 2 & 4 & 1 & 2 \\ 2 & 2 & 4 & 4 & 3 \end{pmatrix}, \quad L_V = \begin{pmatrix} 8 & 0 & 0 & -2 & 0 \\ 0 & 8 & -2 & 0 & 0 \\ -2 & -2 & 8 & -4 & -2 \\ -2 & -2 & -4 & 8 & -2 \\ -2 & -2 & -4 & -4 & 6 \end{pmatrix}, \quad \overline{L_V} = \begin{pmatrix} 8 & -2 & 0 & 0 \\ -2 & 8 & -4 & -2 \\ -2 & -4 & 8 & -2 \\ -2 & -4 & -4 & 6 \end{pmatrix}.$$

Then $K(V) = \mathbb{Z}^5/\mathrm{im}\, L_V = (\mathbb{Z}/2\mathbb{Z})^3 \oplus \mathbb{Z}/24\mathbb{Z}$ and $\mathbb{Z}^4/\mathrm{im}\, \overline{L_V} = (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/24\mathbb{Z}$, which are different. The eigenvalues of L_V are 0, 8, 8, 10, 12, and $\#K(V) = 2^3 \cdot 24 = 3 \cdot 8^2 \cdot 10 \cdot 12/5!$, as predicted by Theorem 1.2.

Now let $V = S_2$ be the "sign" representation, which is not tensor-rich since $\chi_V(g) = \chi_V(e) = 1$ for some 3-regular $g \neq e$ by the above character table. Computations in Magma show

$$M_V = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad L_V = \begin{pmatrix} 1 & -1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \overline{L_V} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then $\overline{L_V}$ is singular and $K(V) = \mathbb{Z}^2 = \mathbb{Z}^4/\mathrm{im}\, \overline{L_V}$ is infinite.

For $g \in \mathfrak{S}_5$, $\chi_V(g) = 1$ if and only if g is an even permutation. There are 40 even 3-regular permutations in $\mathfrak{S}_5$: the 24 5-cycles, the 15 products of two disjoint 2-cycles, and the identity permutation. These permutations generate the alternating group $N = A_5$. Let $B = \mathbb{F}[G/N]$. Then V is a one-dimensional B-module on which N acts by 1 and $(1,2)N$ acts by -1. As a B-module, V is tensor-rich.

Example 5.8. Working over an algebraically closed field $\mathbb{F}$ of characteristic zero, the generalized Taft Hopf algebra $A = H_{n,m}$ from Example 2.5 has dimension mn. It has $\ell + 1 = n$ projective indecomposable representations $P_1, \ldots, P_n$, each of dimension m, with top $S_i = \mathrm{top}(P_i)$ one-dimensional (see [5, §4] and [18, §2]). Hence in this case, $\gamma = \gcd(\mathbf{p}) = m$ and Theorem 1.1 yields

$$K(A) \cong (\mathbb{Z}/m\mathbb{Z}) \oplus (\mathbb{Z}/mn\mathbb{Z})^{n-2} \qquad \text{for } n \geq 2.$$

Example 5.9. For Radford's Hopf algebra $A = A(n, m)$ from Examples 2.6, 2.18, all indecomposable projectives $\{P_k\}_{k=0}^{n-1}$ are 2^m-dimensional, so $\gamma := \gcd(\mathbf{p}) = 2^m$ and Theorem 1.1 gives

$$K(A) \cong (\mathbb{Z}/2^m\mathbb{Z}) \oplus (\mathbb{Z}/n2^m\mathbb{Z})^{n-2}.$$

Example 5.10. There is a special case of the restricted universal enveloping algebras $A = \mathfrak{u}(\mathfrak{g})$ from Example 2.7 where one has all the data needed for Theorem 1.1. Namely, when $\mathfrak{g}$ is associated to a simple, simply-connected algebraic group $\mathbf{G}$ defined and split over $\mathbb{F}_p$, as in Humphreys [13, Chap. 1], then there is a natural parametrization of the simple A-modules via the set X/pX where $X \cong \mathbb{Z}^{\mathrm{rank}\,\mathfrak{g}}$ is the *weight lattice* for $\mathbf{G}$ or $\mathfrak{g}$. Although the dimensions of the projective indecomposable A-modules P_i are not known completely, they are all divisible by the dimension of one among them, specifically, the *Steinberg module* of dimension p^N where N is the number of *positive roots*; see [13, §10.1]. Consequently, here one has

$$\begin{array}{rlll} \gamma & := \gcd(\mathbf{p}) & = p^N & \\ d & := \dim(A) & = p^{\dim \mathfrak{g}} & \\ \ell + 1 & := \#\{\text{simple } A\text{-modules}\} & = \#X/pX & = p^{\mathrm{rank}\,\mathfrak{g}}, \end{array}$$

and Theorem 1.1 implies

$$K(A) \cong \left(\mathbb{Z}/p^N\mathbb{Z}\right) \oplus \left(\mathbb{Z}/p^{\dim \mathfrak{g}}\mathbb{Z}\right)^{p^{\mathrm{rank}\,\mathfrak{g}}-2}.$$

Remark 5.11. All the above examples of Hopf algebras A share a common interpretation for $\gamma = \gcd(\mathbf{p})$ which we find suggestive. Each has a family of $\mathbb{F}$-subalgebras $B \subset A$, which one is tempted to call *Sylow subalgebras*, with the following properties:

(i) The augmentation ideal $\ker(B \xrightarrow{\epsilon} \mathbb{F})$ is a nil ideal, that is, it consists entirely of nilpotent elements.
(ii) A is free as a left B-module.
(iii) $\dim B = \gamma$.

We claim that properties (i) and (ii) already imply that $\dim B$ *divides* γ (cf. [31, proof of Cor. 8.1.3]): property (i) implies B has only one simple module, namely ϵ, whose projective cover must be B itself, and property (ii) implies that each projective A-module P_i restricts to a projective B-module, which must be of form B^t, so that $\dim B$ divides $\dim P_i$, and hence divides $\gcd(\{\dim P_i\}) = \gamma$. Thus property (iii) implies that B must be *maximal* among subalgebras of A having properties (i),(ii).

- When A is semisimple, then $B = \mathbb{F}1_A$.
- When $A = \mathbb{F}G$ is a group algebra and $\mathbb{F}$ has characteristic p, then $B = \mathbb{F}H$ is the group algebra for any p-Sylow subgroup H.
- When $A = H_{n,m}$ is the generalized Taft Hopf algebra, B is the subalgebra $\mathbb{F}\langle x\rangle$ generated by x, or by any of the elements of the form $g^i x$ for $i = 0, 1, \ldots, n-1$.
- When $A = A(n,m)$ is Radford's Hopf algebra, B is the exterior subalgebra $\Lambda[x_1, \ldots, x_m]$ generated by $x_1, \ldots, x_m$, or various isomorphic subalgebras $\Lambda[g^i x_1, \ldots, g^i x_m]$ for $i \in \mathbb{Z}$.
- When $A = \mathfrak{u}(\mathfrak{g})$ is the restricted universal enveloping algebra for the Lie algebra $\mathfrak{g}$ of a semisimple algebraic group over $\mathbb{F}_p$, then $B = \mathfrak{u}(\mathfrak{n}_+)$ for a nilpotent subalgebra $\mathfrak{n}_+$ in a triangular decomposition $\mathfrak{g} = \mathfrak{n}_- \oplus \mathfrak{h} \oplus \mathfrak{n}_+$.

Question 5.12. *For which finite-dimensional Hopf algebras A over an algebraically closed field $\mathbb{F}$ is there a subalgebra B satisfying properties (i),(ii),(iii) above?*

6. Proof of Theorem 1.4

We recall the statement of the theorem, involving an A-module V of dimension n, with $L_V = nI_{\ell+1} - M_V$ in $\mathbb{Z}^{(\ell+1)\times(\ell+1)}$, and its submatrix $\overline{L_V}$ in $\mathbb{Z}^{\ell\times\ell}$.

Theorem 1.4. *The following are equivalent for an A-module V:*
(i) *$\overline{L_V}$ is a nonsingular M-matrix.*
(ii) *$\overline{L_V}$ is nonsingular.*
(iii) *L_V has rank ℓ, so nullity* 1.
(iv) *$K(V)$ is finite.*
(v) *V is tensor-rich.*

The definitions for V to be tensor-rich and for $\overline{L_V}$ to be a nonsingular M-matrix are given below.

Definition 6.1. Let V be an A-module. Say that V is *rich* if $[V : S_i] > 0$ for every simple A-module S_i. Say that V is *tensor-rich* if for some positive integer t, the A-module $\bigoplus_{k=0}^{t} V^{\otimes k}$ is rich.

Definition 6.2. Let Q be a matrix in $\mathbb{R}^{\ell\times\ell}$ whose off-diagonal entries are nonpositive, that is, $Q_{i,j} \le 0$ for $i \neq j$. Then Q is called a *nonsingular M-matrix* if it is invertible and the entries in Q^{-1} are all nonnegative.

To prove the theorem, we will show the following implications:

$$\begin{array}{ccccccccc} & & & & \text{(iv)} & & & & \\ & & & & \Updownarrow & & & & \\ \text{(i)} & \Rightarrow & \text{(ii)} & \Rightarrow & \text{(iii)} & \Rightarrow & \text{(v)} & \Rightarrow & \text{(i)}, \end{array}$$

after first establishing some inequality notation for vectors and matrices.

Definition 6.3. Given u, v in $\mathbb{R}^m$, write $u \le v$ (resp. $u < v$) if $u_j \le v_j$ (resp. $u_j < v_j$) for all j. Given matrices M, N in $\mathbb{R}^{m\times m'}$, similarly write $M \le N$ (resp. $M < N$) if $M_{i,j} \le N_{i,j}$ (resp. $M_{i,j} < N_{i,j}$) for all i, j.

Note that $u \le v$ and $u \neq v$ do not together imply that $u < v$; similarly for matrices.

6.1. The implication (i) $\Rightarrow$ (ii).

This is trivial from Definition 6.2.

6.2. **The implication (ii) ⇒ (iii).** Since L_V is singular (as $L_V \mathbf{s} = 0$), if its submatrix $\overline{L_V}$ is nonsingular, then L_V has rank ℓ and nullity 1.

6.3. **The equivalence (iii) ⇔ (iv).** For a square integer matrix L_V, having nullity 1 is equivalent to its integer cokernel $\mathbb{Z}^{\ell+1}/\mathrm{im}(L_V) = \mathbb{Z} \oplus K(V)$ having free rank 1, that is, to $K(V)$ being finite.

6.4. **The implication (iii) ⇒ (v).** We prove the contrapositive: not (v) implies not (iii).

To say that (v) fails, i.e., V is *not* tensor-rich, means that the composition factors within the various tensor powers $V^{\otimes k}$ form a nonempty proper subset $\{S_j\}_{j\in J}$ of the set of simple A-modules $\{S_i\}_{i=1,2,\ldots,\ell+1}$. This implies that the McKay matrix M_V has a nontrivial block-triangular decomposition, in the sense that $(M_V)_{i,j} = 0$ for $j \in J$ and $i \notin J$ [5]. This will allow us to apply the following property of nonnegative matrices.

Lemma 6.4. *Let $M \geq 0$ be a nonnegative matrix in $\mathbb{R}^{m\times m}$. Let $\lambda \in \mathbb{R}$. Set $L = \lambda I_m - M$. Let $u \in \mathbb{R}^m$ and $v \in \mathbb{R}^m$ be two column vectors such that $u > 0$, $v > 0$, $u^T L = 0$ and $Lv = 0$.*

Let J be a nonempty proper subset of $\{1, 2, \ldots, m\}$. Assume that

$$M_{i,j} = 0 \qquad \text{for all } i \notin J \text{ and } j \in J. \tag{6.2}$$

Then, $\dim(\ker L) \geq 2$.

Proof. Recall that $L = \lambda I_m - M$. Hence, for all $i \notin J$ and $j \in J$, we have

$$L_{i,j} = (\lambda I_m - M)_{i,j} = \lambda \underbrace{(I_m)_{i,j}}_{\substack{=\delta_{i,j}=0 \\ (\text{since } i\notin J \text{ and } j\in J \\ \text{lead to } i\neq j)}} - \underbrace{M_{i,j}}_{\substack{=0 \\ (\text{by } (6.2))}} = 0. \tag{6.3}$$

On the other hand, for all $i \in J$ and $j \notin J$, we have

$$L_{i,j} = (\lambda I_m - M)_{i,j} = \lambda \underbrace{(I_m)_{i,j}}_{\substack{=\delta_{i,j}=0 \\ (\text{since } i\in J \text{ and } j\notin J \\ \text{lead to } i\neq j)}} - \underbrace{M_{i,j}}_{\substack{\geq 0 \\ (\text{since } M\geq 0)}} \leq 0. \tag{6.4}$$

Define a column vector $v' \in \mathbb{R}^m$ by setting

$$(v')_i = \begin{cases} v_i, & \text{if } i \in J; \\ 0, & \text{if } i \notin J \end{cases} \qquad \text{for all } i \in \{1, 2, \ldots, m\}.$$

---

[5] Assume the contrary. Thus, there exist $i \notin J$ and $j \in J$ such that $(M_V)_{i,j} \neq 0$. Consider these i and j. Since $(M_V)_{i,j} = [S_j \otimes V : S_i]$, this rewrites as $[S_j \otimes V : S_i] \neq 0$. Hence, S_i appears as a composition factor in the A-module $S_j \otimes V$. Therefore, $[S_j \otimes V] = [S_i] + [W]$ in $G_0(A)$ for some A-module W. Consider this W. But we have $[V^{\otimes k} : S_j] > 0$ for some $k \in \mathbb{N}$ (since $j \in J$). Consider this k. Thus, S_j appears as a composition factor in $V^{\otimes k}$. Hence, $[V^{\otimes k}] = [S_j] + [X]$ in $G_0(A)$ for some A-module X. Consider this X. Now, in $G_0(A)$, we have

$$\begin{aligned} \left[V^{\otimes(k+1)}\right] &= \left[V^{\otimes k} \otimes V\right] = \left[V^{\otimes k}\right][V] = ([S_j] + [X])\,[V] \qquad \left(\text{since } \left[V^{\otimes k}\right] = [S_j] + [X]\right) \\ &= \underbrace{[S_j \otimes V]}_{=[S_i]+[W]} + [X \otimes V] = [S_i] + [W] + [X \otimes V] = [S_i \oplus W \oplus X \otimes V]. \end{aligned} \tag{6.1}$$

But if Z is an A-module, then the number $[Z : S_i]$ depends only on the class $[Z] \in G_0(A)$ (but not on Z itself). (Indeed, this follows from (2.3).) Hence, from (6.1), we obtain

$$\left[V^{\otimes(k+1)} : S_i\right] = [S_i \oplus W \oplus X \otimes V : S_i] > 0$$

(since S_i clearly does appear in $S_i \oplus W \oplus X \otimes V$). By the definition of J, this shows that $i \in J$; but this contradicts $i \notin J$. This contradiction completes our proof.

Define a column vector $v'' \in \mathbb{R}^m$ by setting

$$(v'')_i = \begin{cases} 0, & \text{if } i \in J; \\ v_i, & \text{if } i \notin J \end{cases} \qquad \text{for all } i \in \{1, 2, \ldots, m\}.$$

Clearly, $v = v' + v''$. Moreover, the vectors v and v' are linearly independent[6]. Thus, $\dim \operatorname{span}_{\mathbb{R}}(v, v') = 2$.

From $v = v' + v''$, we obtain $Lv = Lv' + Lv''$, so that $Lv' + Lv'' = Lv = 0$ and therefore $Lv' = -Lv''$.

Now, we claim that

$$(Lv')_i \geq 0 \qquad \text{for all } i \in \{1, 2, \ldots, m\}. \tag{6.5}$$

To prove this, we handle the cases $i \in J$ and $i \notin J$ separately:

- Let us consider the case when $i \in J$. In this case, recall that $Lv' = -Lv''$; hence, $(Lv')_i = -(Lv'')_i$. Since
$$\begin{aligned}(Lv'')_i &= \sum_{j=1}^{m} L_{i,j}(v'')_j = \sum_{j=1}^{m} L_{i,j} \begin{cases} 0, & \text{if } j \in J; \\ v_j, & \text{if } j \notin J \end{cases} \qquad \text{(by the definition of } v''\text{)} \\ &= \sum_{j \notin J} \underbrace{L_{i,j}}_{\substack{\leq 0 \\ \text{(by (6.4))}}} \underbrace{v_j}_{\substack{>0 \\ \text{(since } v>0\text{)}}} \leq 0,\end{aligned}$$
this results in $(Lv')_i \geq 0$. Thus, (6.5) is proven when $i \in J$.
- Let us now consider the case when $i \notin J$. In this case,
$$\begin{aligned}(Lv')_i &= \sum_{j=1}^{m} L_{i,j}(v')_j = \sum_{j=1}^{m} L_{i,j} \begin{cases} v_j, & \text{if } j \in J; \\ 0, & \text{if } j \notin J \end{cases} \qquad \text{(by the definition of } v'\text{)} \\ &= \sum_{j \in J} \underbrace{L_{i,j}}_{\substack{=0 \\ \text{(by (6.3))}}} v_j = 0.\end{aligned}$$
Hence, (6.5) is proven when $i \notin J$.

Thus, (6.5) is proven in all cases. Consequently, $Lv' \geq 0$.

Now, recall that $u > 0$. Hence, if $x \in \mathbb{R}^m$ is any column vector satisfying $x \geq 0$ and $u^T x = 0$, then we must have $x = 0$ (because a sum of nonnegative reals can only be 0 if all of its addends are 0). Applying this to $x = Lv'$, we find $Lv' = 0$ (since $Lv' \geq 0$ and $\underbrace{u^T L}_{=0} v' = 0$). Combined with $Lv = 0$, this shows that both v and v' lie in $\ker L$. Therefore, $\ker L \supseteq \operatorname{span}_{\mathbb{R}}(v, v')$. Hence, $\dim(\ker L) \geq \dim \operatorname{span}_{\mathbb{R}}(v, v') = 2$. □

This lets us finish the proof that not (v) implies not (iii): the discussion preceding Lemma 6.4 shows that when V is **not** tensor-rich, one can apply Lemma 6.4 to M_V, with the roles of u, v played by $\mathbf{s}, \mathbf{p}$, and conclude that $L_V = nI_{\ell+1} - M_V$ has nullity at least two.

6.5. **The implication (v) ⇒ (i).** Here we will use a nontrivial fact which is part[7] of the equivalence of two characterizations for nonsingular M-matrices given by Plemmons [25, Thm. 1]; see his conditions F_{15}, K_{34}.

Proposition 6.5. *A matrix $Q \in \mathbb{R}^{\ell \times \ell}$ with nonpositive off-diagonal entries is a nonsingular M-matrix as in Definition 6.2 if and only if there exists $x \in \mathbb{R}^{\ell}$ with both $x > 0$ and $Qx > 0$.*

---

[6]To see this, recall that the vector v has all its coordinates nonzero (since $v > 0$), whereas the vector v' has only a nonempty proper subset of its coordinates nonzero (namely, the coordinates $(v')_i$ for $i \in J$).

[7]See [12] for a more self-contained proof of the implication we are using, namely that if one has a matrix $Q \in \mathbb{R}^{\ell \times \ell}$ with $Q_{i,j} \leq 0$ for $i \neq j$, and a vector $x \in \mathbb{R}^{\ell}$ with both $x > 0$ and $Qx > 0$, then Q is nonsingular.

A few more notations are in order. For x in $\mathbb{R}^{\ell+1}$, let $\overline{x}$ be the vector in $\mathbb{R}^{\ell}$ obtained by forgetting its last coordinate. For M in $\mathbb{R}^{(\ell+1)\times(\ell+1)}$, let $\overline{M}$ be the matrix in $\mathbb{R}^{\ell\times\ell}$ obtained by forgetting its last row and last column.[8] Let $M_{*,k}$ denote the vector which is the k-th column of M.

Proposition 6.6. *For nonnegative matrices $M, N \geq 0$ both in $\mathbb{R}^{(\ell+1)\times(\ell+1)}$, one has $\overline{M} \cdot \overline{N} \leq \overline{MN}$.*

Proof. Compare their (i, j)-entries for $i, j \in \{1, 2, \ldots, \ell\}$:

$$\overline{MN}_{i,j} = (MN)_{i,j} = \sum_{k=1}^{\ell+1} M_{i,k}N_{k,j} = M_{i,\ell+1}N_{\ell+1,j} + \sum_{k=1}^{\ell} M_{i,k}N_{k,j}$$
$$= M_{i,\ell+1}N_{\ell+1,j} + \left(\overline{M} \cdot \overline{N}\right)_{i,j} \geq \left(\overline{M} \cdot \overline{N}\right)_{i,j}. \quad \square$$

The following gives a useful method to produce nonsingular M-matrices, to be applied to $M = M_V$ below.

Proposition 6.7. *Assume one has an eigenvector equation*

$$Mx = \lambda x$$

with a nonnegative matrix $M \geq 0$ in $\mathbb{R}^{(\ell+1)\times(\ell+1)}$, a real scalar λ, and a positive eigenvector $x > 0$ in $\mathbb{R}^{\ell+1}$. Let $\overline{L} := \lambda I_\ell - \overline{M}$.

(i) *One always has $\lambda \geq 0$, and*

$$\overline{M}\overline{x} \leq \lambda\overline{x}.$$

Consequently, $\overline{L}\overline{x} \geq 0$.

(ii) *Under the additional hypothesis that M has positive last column $M_{*,\ell+1} > 0$, then*

$$\overline{M}\overline{x} < \lambda\overline{x}.$$

Consequently, (under this hypothesis) $\overline{L}$ is a nonsingular M-matrix, since both $\overline{x} > 0$ and $\overline{L}\overline{x} > 0$.

(iii) *Let t be a positive integer. Set $\overline{y} := \sum_{k=0}^{t-1} \overline{M}^k \overline{x}$. Then, $\overline{y} > 0$. Under the additional hypothesis (different from (ii)) that the last column of $\sum_{k=0}^{t-1} M^k$ is strictly positive, we also have*

$$\overline{M}\overline{y} < \lambda\overline{y}.$$

Consequently, (under this hypothesis) $\overline{L}$ is a nonsingular M-matrix, since both $\overline{y} > 0$ and $\overline{L}\overline{y} > 0$.

Proof. The nonnegativity $\lambda \geq 0$ follows from $Mx = \lambda x$ since $M \geq 0$ and $x > 0$.

For the remaining assertions in (i) and (ii), note that the first ℓ equations in the system $Mx = \lambda x$ assert

$$\overline{M}\overline{x} + \overline{M_{*,\ell+1}}x_{\ell+1} = \lambda\overline{x}, \qquad \text{where } M_{*,\ell+1} \text{ is the last column vector of } M.$$

Since $x_{\ell+1} > 0$, and since the entries of $M_{*,\ell+1}$ are nonnegative (resp. strictly positive) under the hypotheses in (i) (resp. in (ii)), the remaining assertions in (i) and (ii) follow.

For assertion (iii), note that $\overline{y} = \overline{x} + \sum_{k=1}^{t-1} \overline{M}^k \overline{x}$, and hence $\overline{y} > 0$ follows from the facts that $\overline{x} > 0$ and $\overline{M} \geq 0$. To prove $\overline{M}\overline{y} < \lambda\overline{y}$, we first prove a weak inequality as follows. For each $k = 0, 1, 2, \ldots, t-1$, multiply the inequality in (i) by $\overline{M}^k$, obtaining:

$$\overline{M}^{k+1}\overline{x} \leq \lambda\overline{M}^k\overline{x}. \tag{6.6}$$

Summing this over all k, we find

$$\sum_{k=0}^{t-1} \overline{M}^{k+1}\overline{x} \leq \sum_{k=0}^{t-1} \lambda\overline{M}^k\overline{x}.$$

In view of the definition of $\overline{y}$, this can be rewritten as

$$\overline{M}\overline{y} \leq \lambda\overline{y}. \tag{6.7}$$

[8]This notation will not conflict with the notation $\overline{L_V}$ used (e.g.) in Theorem 1.4 because we shall re-index the simple A-modules in such a way that the last row and the last column of L_V are the ones corresponding to ϵ.

It remains to show that for $1 \leq j \leq \ell$, the inequality in the j^{th} coordinate of (6.7) is strict. For the sake of contradiction, assume $\left(\overline{M}\,\overline{y}\right)_j = \lambda \overline{y}_j$. This forces equalities in the j-th coordinate of (6.6) for $0 \leq k \leq t-1$:

$$\left(\overline{M}^{k+1}\overline{x}\right)_j = \lambda\left(\overline{M}^k\overline{x}\right)_j.$$

This implies via induction on k that $\left(\overline{M}^k\overline{x}\right)_j = \lambda^k \overline{x}_j$, for $k = 0, 1, 2, \ldots, t-1$. Summing on k gives

$$\left(\left(\sum_{k=0}^{t-1}\overline{M}^k\right)\overline{x}\right)_j = \left(\sum_{k=0}^{t-1}\lambda^k\right)\overline{x}_j.$$

However, this contradicts the strict inequality in the j^{th} coordinate in the following:

$$\left(\sum_{k=0}^{t-1}\overline{M}^k\right)\overline{x} \leq \overline{\left(\sum_{k=0}^{t-1}M^k\right)}\overline{x} < \left(\sum_{k=0}^{t-1}\lambda^k\right)\overline{x}. \tag{6.8}$$

The first (weak) inequality in (6.8) comes from the fact that $\overline{M}^k \leq \overline{M^k}$ (which follows by induction from Proposition 6.6), while the second (strict) inequality comes from applying assertion (ii) to the eigenvector equation $\left(\sum_{k=0}^{t-1}M^k\right)x = \left(\sum_{k=0}^{t-1}\lambda^k\right)x$ (which follows from $Mx = \lambda x$). □

We return now to our usual context of a finite-dimensional Hopf algebra A over an algebraically closed field $\mathbb{F}$, and an A-module V of dimension n. Recall the matrices M_V and L_V are given by $(M_V)_{i,j} = [S_j \otimes V : S_i]$ and $L_V := nI_{\ell+1} - M_V$. For the remainder of this section, assume one has indexed the simple A-modules $\{S_i\}_{i=1,2,\ldots,\ell+1}$ such that $S_{\ell+1} = \epsilon$ is the trivial A-module on $\mathbb{F}$. Thus $\overline{M_V}, \overline{L_V}$ come from M_V, L_V by removing the row and column indexed by ϵ.

Richness of V has an obvious reformulation in terms of M_V.

Proposition 6.8. *V is rich if and only if the McKay matrix M_V has positive last column $(M_V)_{*,\ell+1} > 0$.*

Proof. Using (2.6) one has $[V : S_i] = [\epsilon \otimes V : S_i] = [S_{\ell+1} \otimes V : S_i] = (M_V)_{i,\ell+1}$. □

Proof of (v) ⇒ (i). Assuming V is tensor-rich, there is some $t > 0$ for which $W := \bigoplus_{k=0}^t V^{\otimes k}$ is rich. Thus M_W has positive last column $(M_W)_{*,\ell+1} > 0$. In $G_0(A)$, one has $[W] = \sum_{k=0}^t [V]^k$, giving the matrix equation $M_W = \sum_{k=0}^t M_V^k$. Since $M_V\mathbf{p} = n\mathbf{p}$ by Proposition 3.8, one can apply Proposition 6.7(iii), with $M = M_V, \lambda = n, x = \mathbf{p}$, and conclude that $\overline{L_V}$ is a nonsingular M-matrix. □

This completes the proof of Theorem 1.4.

Theorem 1.4 raises certain questions on finite-dimensional Hopf algebras.

Question 6.9. *Let A be a finite-dimensional Hopf algebra over an algebraically closed field.*

(i) *How does one test whether V is tensor-rich in terms of some kind of character theory for A?*
(ii) *Can the nullity of L_V be described in terms of the simple A-modules appearing in $V^{\otimes k}$ for $k \geq 1$?*

Section 7 answers Question 6.9(i) for group algebras $A = \mathbb{F}G$, via Brauer characters.

6.6. **Non-tensor-rich modules as inflations.** Any module V over an algebra B can be regarded as an inflation of a faithful $B/\mathrm{Ann}_B V$-module.[9] A natural question to ask is whether a similar fact holds for tensor-rich modules over Hopf algebras. The annihilator of an A-module is always an ideal, not necessarily a Hopf ideal; thus, a subtler construction is needed. The answer is given by part (iv) of the following theorem, communicated to us by Sebastian Burciu who graciously allowed us to include it in this paper.

[9]The *annihilator* of a B-module V is defined to be the ideal $\{b \in B \mid bV = 0\}$ of B. It is denoted by $\mathrm{Ann}_B V$.
A B-module V is said to be *faithful* if and only if $\mathrm{Ann}_B V = 0$.

Theorem 6.10. *Let V be an A-module. Let ω be the map $A \to A$ sending each $a \in A$ to $a - \epsilon(a)1$. Let $J_V = \bigcap_{k\geq 0} \mathrm{Ann}_A(V^{\otimes k})$.*

(i) *We have $J_V = \omega(\mathrm{LKer}_V)A$, where $\mathrm{LKer}_V = \{a \in A \mid \sum a_1 \otimes a_2 v = a \otimes v \text{ for all } v \in V\}$.*
(ii) *The subspace J_V of A is a Hopf ideal of A, and thus A/J_V is a Hopf algebra.*
(iii) *If $J_V = 0$, then V is tensor-rich.*
(iv) *The A-module V is the inflation of an A/J_V-module via the canonical projection $A \to A/J_V$, and the latter A/J_V-module is tensor-rich.*
(v) *Let J' be any Hopf ideal of A such that the A-module V is the inflation of an A/J'-module via the canonical projection $A \to A/J'$. Then, $J' \subseteq J_V$.*

Note that part (i) of the theorem allows for actually computing J_V, while the definition of J_V itself involves an uncomputable infinite intersection.

Proof of Theorem 6.10. Part (i) is [4, Corollary 2.3.7].

Part (ii) follows from [23, Theorem 7 (i)], since the family $\left(V^{\otimes n}\right)_{n\geq 0}$ of A-modules is clearly closed under tensor products.

Part (iii) is essentially [30, (3)], but let us also prove it for the sake of completeness: Assume that $J_V = 0$. Consider any simple A-module S_i and the corresponding primitive idempotent e_i of A. The A-module $\bigoplus_{k\geq 0} V^{\otimes k}$ is faithful (since its annihilator is $J_V = 0$). Thus, $e_i \cdot \bigoplus_{k\geq 0} V^{\otimes k} \neq 0$. Thus, there exists some $k \geq 0$ such that $e_i V^{\otimes k} \neq 0$. Consider this k. But recall (see, e.g., [31, Prop. 7.4.1 (3)]) that $\mathrm{Hom}_A(Ae, W) \cong eW$ for any A-module W and any idempotent e of A. Thus, $\mathrm{Hom}_A\left(Ae_i, V^{\otimes k}\right) \cong e_i V^{\otimes k} \neq 0$, so that $\dim \mathrm{Hom}_A\left(Ae_i, V^{\otimes k}\right) > 0$. Hence,

$$\left[V^{\otimes k} : S_i\right] = \dim \mathrm{Hom}_A\left(P_i, V^{\otimes k}\right) = \dim \mathrm{Hom}_A\left(Ae_i, V^{\otimes k}\right) > 0.$$

Since we have shown this to hold for each i, we thus conclude that V is tensor-rich.

(iv) Since $J_V \subseteq \mathrm{Ann}_A(V)$, we see immediately that V is the inflation of an A/J_V-module V'. It remains to show that this V' is tensor-rich. But this follows from part (iii), applied to A/J_V, V' and 0 instead of A, V and J_V: Indeed, we have $0 = \bigcap_{k\geq 0} \mathrm{Ann}_{A/J_V}((V')^{\otimes k})$, since $\bigcap_{k\geq 0} \mathrm{Ann}_{A/J_V}((V')^{\otimes k})$ is the projection of $\bigcap_{k\geq 0} \mathrm{Ann}_A(V^{\otimes k}) = J_V$ onto the quotient ring A/J_V, which projection of course is $J_V/J_V = 0$.

(v) We assumed that the A-module V is the inflation of an A/J'-module V' via the canonical projection $A \to A/J'$. Thus, for each $k \geq 0$, the A-module $V^{\otimes k}$ is the inflation of the A/J'-module $(V')^{\otimes k}$ via this projection. Hence, for each $k \geq 0$, we have $J'V^{\otimes k} = 0$. Thus, $J' \subseteq \bigcap_{k\geq 0} \mathrm{Ann}_A(V^{\otimes k}) = J_V$. ◻

6.7. **Avalanche-finiteness.** We digress slightly to discuss *avalanche-finite matrices* and *chip-firing*.

Definition 6.11. An integer nonsingular M-matrix is called an *avalanche-finite* matrix; see [1, §2].

The terminology arises because the integer cokernel $\mathbb{Z}^\ell/\mathrm{im}\, L$ for an avalanche-finite matrix L in $\mathbb{Z}^{\ell\times\ell}$ has certain convenient coset representatives in $(\mathbb{Z}_{\geq 0})^\ell$, characterized via their behavior with respect to the dynamics of a game in which one makes moves (called *chip-firing* or *toppling* or *avalanches*) that subtract columns of L. One such family of coset representatives are called *recurrent*, and the other such family are called *superstable*; see, e.g., [1, §2, Thm. 2.10] for their definitions and further discussion.[10]

Since $L_V = nI_{\ell+1} - M_V$ always has $\overline{L_V}$ in $\mathbb{Z}^{\ell\times\ell}$, Theorem 1.4 has the following immediate consequence.

Proposition 6.12. *For a finite-dimensional Hopf algebra A over an algebraically closed field, any tensor-rich A-module V has $\overline{L_V}$ avalanche-finite.*

The problem in applying this to study the critical group is that $K(V) \cong \mathbf{s}^\perp/\mathrm{im}\, L_V$, which is not always isomorphic to $\mathbb{Z}^\ell/\mathrm{im}\, \overline{L_V}$. Under certain conditions, they are isomorphic, namely when the left-nullvector $\mathbf{s}$ and the right-nullvector $\mathbf{p}$ both have their $(\ell+1)^{st}$ coordinate equal to 1; see [1, §2, Prop. 2.19]. Since we

[10]This terminology harkens back to the theory of chip-firing on graphs (also known as the theory of sandpiles), where analogous notions have been known for longer – see, e.g., [17] or [24].

have indexed the simple A-modules in such a way that $S_{\ell+1} = \epsilon$ is the trivial A-module, this condition is equivalent to the 1-dimensional trivial A-module ϵ being its own projective cover $P_\epsilon = \epsilon$. This, in turn, is known [10, Cor. 4.2.13] to be equivalent to semisimplicity of A. For example, this is always the case in the setting of [1], where $A = \mathbb{F}G$ was a group algebra of a finite group and $\mathbb{F}$ had characteristic zero.

In the case where A is semisimple, many of the results on chip-firing from [1, §5] remain valid, with the same proofs. For example, [1, Prop. 5.16] explains why removing the last entry from the last column of M_V gives a *burning configuration* for the avalanche-finite matrix $\overline{M_V}$, which allows one to easily test when a configuration is recurrent.

7. Tensor-rich group representations

Brauer already characterized tensor-rich $\mathbb{F}G$-modules, though he did not state it in these terms. We need the following fact, well-known when $\mathbb{F}$ has characteristic zero (see, e.g., James and Liebeck [15, Thm. 13.11]), and whose proof works just as well in positive characteristic.

Proposition 7.1. *Given a finite group G and n-dimensional $\mathbb{F}G$-module V, a p-regular element g in G acts as 1_V on V if and only if $\chi_V(g) = n$.*

Proof. The forward implication is clear. For the reverse, if one has $n = \chi_V(g) = \sum_{i=1}^n \widehat{\lambda_i}$, then since each $|\widehat{\lambda_i}| = 1$, the Cauchy-Schwarz inequality implies that the $\widehat{\lambda_i}$ are all equal, and hence they must all equal 1, since they sum to n. But then $\lambda_i = 1$ for all i, which means that g acts as 1_V on V. □

We also need the following fact about Brauer characters; see, e.g., [31, Prop. 10.2.1].

Theorem 7.2. *Given a simple $\mathbb{F}G$-module S having projective cover P, then any $\mathbb{F}G$-module V has*

$$[V : S] = \dim \mathrm{Hom}_{\mathbb{F}G}(P, V) = \frac{1}{\#G} \sum_{\substack{p-regular \\ g \in G}} \overline{\chi}_P(g) \chi_V(g).$$

We come now to the characterization of tensor-rich finite group representations.

Theorem 7.3. *(Brauer* [2, Rmk. 4]*) For $\mathbb{F}$ an algebraically closed field, and G a finite group, an $\mathbb{F}G$-module V is tensor-rich if and only if the only p-regular element acting as 1_V on V is the identity element e of G.*

More precisely, if the only p-regular element in G acting as 1_V is the identity e, and if the Brauer character values $\chi_V(g)$ take on exactly t distinct values, then $\bigoplus_{k=0}^{t-1} V^{\otimes k}$ is rich.

Proof. To see the "only if" direction of the first sentence, note that if some p-regular element $g \neq e$ acts as 1_V on V, then the action of G on V factors through some nontrivial quotient group G/N with $g \in N$, and the same is true for G acting on every tensor power $V^{\otimes k}$. Note that not every simple $\mathbb{F}G$-module can be the inflation of a simple $\mathbb{F}[G/N]$-module through the quotient map $G \to G/N$ in this way, else the columns indexed by e and by g in the Brauer character table of G would be equal, contradicting its invertibility. Therefore not all simple $\mathbb{F}G$-modules can appear in the tensor algebra $T(V)$, that is, V cannot be tensor-rich.

To see the "if" direction of the first sentence, it suffices to show the more precise statement in the second sentence. So assume that the only p-regular element acting as 1_V on V is e, and label the t distinct Brauer character values $\chi_V(g)$ as $a_1, a_2, \ldots, a_t$, where $a_1 = \dim(V) = \chi_V(e)$. Letting A_j denote the set of p-regular elements g for which $\chi_V(g) = a_j$, Proposition 7.1 implies that $A_1 = \{e\}$. Assuming for the sake of contradiction that $\bigoplus_{k=0}^{t-1} V^{\otimes k}$ is not rich, then there exists some simple $\mathbb{F}G$-module S such that for $k = 0, 1, \ldots, t-1$, one has (with P denoting the projective cover of S) the equality

$$0 = [V^{\otimes k} : S] = \dim \mathrm{Hom}_{\mathbb{F}G}(P, V^{\otimes k}) = \frac{1}{\#G} \sum_{\substack{p-\text{regular} \\ g \in G}} \overline{\chi}_P(g) \chi_{V^{\otimes k}}(g) = \frac{1}{\#G} \sum_{j=1}^{t} a_j^k \sum_{g \in A_j} \overline{\chi}_P(g).$$

Multiplying each of these equations by $\#G$, one can rewrite this as a matrix system

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_t \\ a_1^2 & a_2^2 & \cdots & a_t^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{t-1} & a_2^{t-1} & \cdots & a_t^{t-1} \end{bmatrix} \begin{bmatrix} \sum_{g\in A_1} \overline{\chi}_P(g) \\ \vdots \\ \sum_{g\in A_t} \overline{\chi}_P(g) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

The matrix on the left governing the system is an invertible Vandermonde matrix, forcing $\sum_{g\in A_j} \overline{\chi}_P(g) = 0$ for each $j = 1, 2, \dots, t$. However, the $j = 1$ case contradicts $\sum_{g\in A_1} \overline{\chi}_P(g) = \overline{\chi}_P(e) = \dim(P) \neq 0$. □

Corollary 7.4. *Faithful representations V of a finite group G are always tensor-rich.*

In fact, in characteristic zero, Burnside had shown that faithfulness of V is the same as the condition in Theorem 7.3 characterizing tensor-richness. Hence one can always regard a non-faithful G-representation of V as a faithful (and hence tensor-rich) representation of some quotient G/N where N is the kernel of the representation on V. There is a similar reduction in positive characteristic.

Proposition 7.5. *For a finite group representation $\rho : G \longrightarrow GL(V)$ over a field $\mathbb{F}$ of characteristic p,*

- *the subgroup N of G generated by the p-regular elements in* $\ker(\rho)$ *is always normal, and*
- *ρ factors through the representation of the quotient $\overline{\rho} : G/N \longrightarrow GL(V)$ which is tensor-rich.*

Proof. The subgroup N as defined above is normal since its generating set is stable under G-conjugation.

To show that the representation $\overline{\rho} : G/N \longrightarrow GL(V)$ is tensor-rich, by Theorem 7.3 above, it suffices to check that if a coset gN in G/N is both p-regular and has gN in $\ker(\overline{\rho})$ (that is, $g \in \ker(\rho)$), then $g \in N$. The p-regularity means $g^m \in N$ for some m with $\gcd(m, p) = 1$. Recall (e.g., from [31, proof of Lemma 9.3.4]) that one can write $g = ab$ uniquely with a, b both powers of g in which a is p-regular, but b is *p-singular* (that is, b has order a power of p). Since a is a power of g, one has $a \in \ker(\rho)$, and therefore also $a \in N$. Additionally $b^m = a^{-m} g^m$ must also lie in N. Since b is p-singular, say of order p^d, one has $1 = xm + yp^d$ with x, y in $\mathbb{Z}$, and then $b = b^{xm+yp^d} = (b^m)^x (b^{p^d})^y = (b^m)^x \in N$. Hence $g = ab \in N$, as desired. □

Proposition 7.5 implies the following fact, which should be contrasted with Theorem 6.10.

Corollary 7.6. *A non-tensor-rich A-module V for $A = \mathbb{F}G$ the group algebra of a finite group is always a B-module for a proper Hopf quotient $A \twoheadrightarrow B$, namely the group algebra $B = \mathbb{F}[G/N]$, where N is the subgroup generated by the p-regular elements in G that act as 1_V.*

Proof. $B = A/I$ where I is the $\mathbb{F}$-span of $\{g - gn\}_{g\in G, n\in N}$, a two-sided ideal and coideal of $A = \mathbb{F}G$. □

Remark 7.7. These last few results relate to a result of Rieffel [27, Cor. 1], asserting that an A-module V for a finite-dimensional Hopf algebra A that cannot be factored through a proper Hopf quotient must be a *faithful* representation of the algebra A, in the sense that the ring map $A \longrightarrow \mathrm{End}(V)$ is injective. He also shows that this implies V is tensor-rich. However, as he notes there, faithfulness of a finite group representation $G \longrightarrow \mathrm{GL}(V)$ over $\mathbb{F}$ is a weaker condition than faithfulness of the $\mathbb{F}G$-module V in the above sense.

8. Appendix A: Hopf algebra proofs

In this section, we collect proofs for some facts stated in Section 2.2 about Hopf algebras. In fact, we shall prove more general versions of these facts.

To achieve this generality, we will **not** follow the conventions and assumptions made in Subsection 1.1. In particular, we shall not require $\mathbb{F}$ to be algebraically closed. We shall also not require our Hopf algebra A (and its modules) to be finite-dimensional unless we explicitly state so.

Instead, let us make the following standing assumptions: We let A be a Hopf algebra over a field $\mathbb{F}$. We denote its counit, its coproduct, and its antipode by ϵ, Δ and α, respectively (as in Section 2.2). All tensor products are over $\mathbb{F}$. We shall use Sweedler notation for comultiplication in A, writing $\sum a_1 \otimes a_2$ for the coproduct $\Delta(a)$ of any $a \in A$. We denote by $\dim V$ the dimension of an $\mathbb{F}$-vector space V. The word "module" always means "left module".

We recall the following basic properties of Hopf algebras:

- The antipode $\alpha : A \to A$ is an algebra anti-endomorphism and a coalgebra anti-endomorphism of A. (This is proven, e.g., in [8, Proposition 4.2.6] or in [28, Theorem 1.5].)
- If A is finite-dimensional, then the antipode $\alpha : A \to A$ is bijective. (See, e.g., [20, Thm. 2.1.3] or [26, Thm. 7.1.14 (b)] or [22, Prop. 4] or [28, Thm. 2.3. 2)] or [10, Prop. 5.3.5] for proofs of this fact.)
- The vector space $\mathbb{F}$ becomes an A-module, by letting A act on $\mathbb{F}$ through the algebra homomorphism ϵ. This A-module is denoted by ϵ, and called the *trivial A-module*.
- For each A-module V, we define its *subspace of A-fixed points* to be

$$V^A := \{v \in V : av = \epsilon(a)v \text{ for all } a \in A\}.$$

- If V and W are two A-modules, then their tensor product $V \otimes W$ becomes an A-module according to the rule $a(v \otimes w) := \sum a_1 v \otimes a_2 w$ for each $a \in A$, $v \in V$ and $w \in W$. (This can be restated more abstractly as follows: The A-module structure on $V \otimes W$ is obtained from the obvious $A \otimes A$-module structure on $V \otimes W$ by restriction along the $\mathbb{F}$-algebra homomorphism $\Delta : A \to A \otimes A$.)

  This concept of tensor products of A-modules satisfies the associativity law (more precisely: if U, V and W are three A-modules, then the canonical $\mathbb{F}$-vector space isomorphism $(U \otimes V) \otimes W \to U \otimes (V \otimes W)$ is an A-module isomorphism), thus allowing us to write tensor products of multiple factors without parenthesizing them. Furthermore, the canonical isomorphisms (2.6) hold for every A-module V. However, the tensor product is not generally commutative (indeed, the A-modules $V \otimes W$ and $W \otimes V$ may be non-isomorphic).
- For any A-module V, the dual space $\operatorname{Hom}_{\mathbb{F}}(V, \mathbb{F})$ becomes an A-module according to the rule $(af)(v) := f(\alpha(a)v)$ for each $a \in A$, $f \in \operatorname{Hom}_{\mathbb{F}}(V, \mathbb{F})$ and $v \in V$. This A-module $\operatorname{Hom}_{\mathbb{F}}(V, \mathbb{F})$ is denoted by V^*, and is called the *left-dual* of V. (This is a well-defined A-module because $\alpha : A \to A$ is an algebra anti-homomorphism.)
- If A is finite-dimensional (so that α is bijective), then there is also another A-module structure on the dual space $\operatorname{Hom}_{\mathbb{F}}(V, \mathbb{F})$ of an A-module V: Namely, we define it by the rule $(af)(v) := f\left(\alpha^{-1}(a)v\right)$ for each $a \in A$, $f \in \operatorname{Hom}_{\mathbb{F}}(V, \mathbb{F})$ and $v \in V$. This A-module $\operatorname{Hom}_{\mathbb{F}}(V, \mathbb{F})$ is denoted by ${}^*V$, and is called the *right-dual* of V. (This is a well-defined A-module because $\alpha^{-1} : A \to A$ is an algebra anti-homomorphism.)
- For any two A-modules V and W, we define an A-module structure on the vector space $\operatorname{Hom}_{\mathbb{F}}(V, W)$ via

$$(a\varphi)(v) := \sum a_1 \varphi(\alpha(a_2)v)$$

  for all $a \in A$, $\varphi \in \operatorname{Hom}_{\mathbb{F}}(V, W)$ and $v \in V$. (See Lemma 8.1 below for a proof of the fact that this is a well-defined A-module structure.) Sometimes, we will simply write $\operatorname{Hom}(V, W)$ for this A-module $\operatorname{Hom}_{\mathbb{F}}(V, W)$.

The following fact is folklore, but an explicit mention is hard to find in the literature:

Lemma 8.1. *Let V and W be two A-modules. For any $a \in A$ and $\varphi \in \operatorname{Hom}_{\mathbb{F}}(V, W)$, define an element $a\varphi \in \operatorname{Hom}_{\mathbb{F}}(V, W)$ by*

$$(a\varphi)(v) := \sum a_1 \varphi(\alpha(a_2)v) \qquad \text{for all } v \in V.$$

This defines an A-module structure on $\operatorname{Hom}_{\mathbb{F}}(V, W)$.

Proof of Lemma 8.1. The definition of $a\varphi$ (for $a \in A$ and $\varphi \in \operatorname{Hom}_{\mathbb{F}}(V, W)$) can be rewritten as follows: $a\varphi$ is the image of a under the composition

$$A \xrightarrow{\Delta} A \otimes A \xrightarrow{\operatorname{id} \otimes \alpha} A \otimes A \longrightarrow \operatorname{Hom}_{\mathbb{F}}(V, W),$$

where the last arrow is the $\mathbb{F}$-linear map $A \otimes A \to \operatorname{Hom}_{\mathbb{F}}(V, W)$ sending each $b \otimes c \in A \otimes A$ to the map $V \to W,\ v \mapsto b\varphi(cv)$. Thus, $a\varphi$ depends $\mathbb{F}$-linearly on a. Also, $a\varphi$ depends $\mathbb{F}$-linearly on φ (this is clear from the definition).

Furthermore, $1\varphi = \varphi$ for each $\varphi \in \operatorname{Hom}_{\mathbb{F}}(V, W)$. (This follows easily from $\Delta(1) = 1 \otimes 1$ and $\alpha(1) = 1$.)

It thus remains to show that $(ab)\varphi = a(b\varphi)$ for any $a \in A$, $b \in A$ and $\varphi \in \operatorname{Hom}_{\mathbb{F}}(V, W)$.

For this purpose, let us fix $a \in A$, $b \in A$ and $\varphi \in \operatorname{Hom}_{\mathbb{F}}(V, W)$. Also, fix $v \in V$.

Now, the definition of $a(b\varphi)$ yields

$$\begin{aligned}(a(b\varphi))(v) &= \sum a_1 \underbrace{(b\varphi)(\alpha(a_2)v)}_{\substack{=\sum b_1\varphi(\alpha(b_2)\alpha(a_2)v) \\ \text{(by the definition of } b\varphi)}} \\ &= \sum\sum a_1 b_1 \varphi\left(\underbrace{\alpha(b_2)\alpha(a_2)}_{\substack{=\alpha(a_2b_2) \\ \text{(since } \alpha \text{ is an algebra anti-endomorphism)}}} v\right) \\ &= \sum\sum a_1b_1\varphi(\alpha(a_2b_2)v) = \sum (ab)_1 \varphi(\alpha((ab)_2)v)\end{aligned}$$

(since one of the axioms of a bialgebra yields $\sum\sum a_1b_1 \otimes a_2b_2 = \sum (ab)_1 \otimes (ab)_2$). Comparing this with

$$((ab)\varphi)(v) = \sum (ab)_1 \varphi(\alpha((ab)_2)v) \qquad \text{(by the definition of } (ab)\varphi),$$

we obtain $((ab)\varphi)(v) = (a(b\varphi))(v)$. Since this holds for all $v \in V$, we thus have $(ab)\varphi = a(b\varphi)$. This completes our proof. □

Let us now generalize Lemma 2.8:

Lemma 8.2. *Let V be an A-module.*

(i) *If A is finite-dimensional, then $V \otimes A \cong A^{\oplus \dim V}$ as A-modules.*
(ii) *Also, $A \otimes V \cong A^{\oplus \dim V}$ as A-modules (independently on the dimension of A).*

Proof of Lemma 8.2. (i) Recall that the antipode $\alpha : A \to A$ is bijective (since A is finite-dimensional). Hence, its inverse α^{-1} is well-defined and an algebra anti-homomorphism (since α is an algebra anti-homomorphism).

The defining property of the antipode α of A shows that

$$\sum a_1\alpha(a_2) = \sum \alpha(a_1)a_2 = \epsilon(a)1$$

for each $a \in A$. Applying the map α^{-1} to this chain of equalities, we obtain

$$\alpha^{-1}\left(\sum a_1\alpha(a_2)\right) = \alpha^{-1}\left(\sum \alpha(a_1)a_2\right) = \alpha^{-1}(\epsilon(a)1).$$

Since α^{-1} is an algebra anti-homomorphism, this can be rewritten as

$$\sum a_2\alpha^{-1}(a_1) = \sum \alpha^{-1}(a_2)a_1 = \epsilon(a)1. \tag{8.1}$$

Let $\underline{V}$ denote V considered as a mere $\mathbb{F}$-vector space, without A-module structure. Then, $\underline{V} \otimes A$ is a well-defined A-module, isomorphic to $A^{\oplus \dim V}$. It remains to prove the isomorphism $V \otimes A \cong \underline{V} \otimes A$.

Define an $\mathbb{F}$-linear map $\Phi : \underline{V} \otimes A \to V \otimes A$ by setting $\Phi(v \otimes b) = \sum b_1 v \otimes b_2$ for all $v \in V$ and $b \in A$. Then, Φ is A-linear (as follows from a straightforward argument using $\sum\sum a_1b_1 \otimes a_2b_2 = \sum (ab)_1 \otimes (ab)_2$).

Define an $\mathbb{F}$-linear map $\Psi : V \otimes A \to \underline{V} \otimes A$ by setting $\Psi(v \otimes b) = \sum \alpha^{-1}(b_1)v \otimes b_2$ for all $v \in V$ and $b \in A$. Then, every $v \in V$ and $b \in A$ satisfy

$$\Phi(\Psi(v \otimes b)) = \Phi\left(\sum \alpha^{-1}(b_1)v \otimes b_2\right) = \sum \underbrace{\Phi\left(\alpha^{-1}(b_1)v \otimes b_2\right)}_{=\sum (b_2)_1 \alpha^{-1}(b_1)v \otimes (b_2)_2} = \sum\sum (b_2)_1 \alpha^{-1}(b_1)v \otimes (b_2)_2$$

$$= \sum \underbrace{\sum (b_1)_2 \alpha^{-1}((b_1)_1)}_{\substack{=\epsilon(b_1)1 \\ \text{(by (8.1), applied to } a=b_1)}} v \otimes b_2 = \sum \epsilon(b_1)1v \otimes b_2 = v \otimes \left(\sum \epsilon(b_1)b_2\right) = v \otimes b$$

(where the fourth equality sign relied on the coassociativity of A in the form $\sum\sum b_1 \otimes (b_2)_1 \otimes (b_2)_2 = \sum\sum (b_1)_1 \otimes (b_1)_2 \otimes b_2$, and the seventh relied on $\sum \epsilon(b_1)b_2 = b$). Thus, $\Phi \circ \Psi = \mathrm{id}$. A similar computation reveals that $\Psi \circ \Phi = \mathrm{id}$, whence we see that Φ and Ψ are mutually inverse bijections. Since Φ is A-linear, they are thus A-isomorphisms, and hence $V \otimes A \cong \underline{V} \otimes A$ is proven.

(ii) A similar argument shows that $A \otimes V \cong A \otimes \underline{V} \cong A^{\oplus \dim V}$ via the isomorphisms $A \otimes \underline{V} \to A \otimes V$, $b \otimes v \mapsto \sum b_1 \otimes b_2 v$ and $A \otimes V \to A \otimes \underline{V}$, $b \otimes v \mapsto \sum b_1 \otimes \alpha(b_2)v$. □

Next, let us generalize Lemma 2.9:

Lemma 8.3. (i) *We have an A-module isomorphism $\epsilon^* \cong \epsilon$.*
(ii) *Assume that A is finite-dimensional. Then, we have an A-module isomorphism ${}^*\epsilon \cong \epsilon$.*

Proof of Lemma 8.3. (i) We have $\epsilon \circ \alpha = \epsilon$ (since α is a coalgebra anti-homomorphism), and thus $\epsilon^* \cong \epsilon$ (via the canonical isomorphism $\mathbb{F}^* \cong \mathbb{F}$).
(ii) From $\epsilon \circ \alpha = \epsilon$, we obtain $\epsilon \circ \alpha^{-1} = \epsilon$, and therefore ${}^*\epsilon \cong \epsilon$. □

Next, we restate and prove Lemma 2.10:

Lemma 8.4. *Assume that A is finite-dimensional. Let V be a finite-dimensional A-module. We have canonical A-module isomorphisms ${}^*(V^*) \cong V \cong ({}^*V)^*$.*

Proof of Lemma 8.4. There is a linear isomorphism $\phi : V \to {}^*(V^*)$ defined by $\phi(v)(f) = f(v)$ for all $v \in V$ and $f \in V^*$. This isomorphism is A-equivariant, since each $a \in A$, $v \in V$ and $f \in V^*$ satisfy

$$(a\phi(v))(f) = \phi(v)(\alpha^{-1}(a)f) = (\alpha^{-1}(a)f)(v) = f(\alpha(\alpha^{-1}(a))v) = f(av) = \phi(av)(f).$$

This proves ${}^*(V^*) \cong V$. The proof of $({}^*V)^* \cong V$ is similar (again, the same ϕ works). □

Next, we shall show a generalization of Lemma 2.11:

Lemma 8.5. *Let V and W be two A-modules. Consider the $\mathbb{F}$-linear map*

$$\Phi : W \otimes V^* \to \mathrm{Hom}_{\mathbb{F}}(V, W) \tag{8.2}$$

sending each $w \otimes f$ (with $w \in W$ and $f \in V^*$) to the linear map $\varphi \in \mathrm{Hom}_{\mathbb{F}}(V, W)$ that is defined by $\varphi(v) = f(v)w$ for all $v \in V$.

(i) *This map Φ is an A-module homomorphism.*
(ii) *Assume that at least one of the vector spaces V and W is finite-dimensional. Then, Φ is an A-module isomorphism, and therefore $W \otimes V^* \cong \mathrm{Hom}_{\mathbb{F}}(V, W)$ as A-modules.*

Proof of Lemma 8.5. (i) Every $v \in V$, $w \in W$, $f \in V^*$ and $a \in A$ satisfy

$$\Phi(a(w \otimes f))(v) = \sum \Phi(a_1 w \otimes a_2 f)(v) = \sum (a_2 f)(v) a_1 w = \sum f(\alpha(a_2)v) a_1 w$$
$$= \sum a_1 f(\alpha(a_2)v) w = \sum a_1 \Phi(w \otimes f)(\alpha(a_2)v) = (a\Phi(w \otimes f))(v).$$

Hence, every $w \in W$, $f \in V^*$ and $a \in A$ satisfy $\Phi(a(w \otimes f)) = a\Phi(w \otimes f)$. By linearity, this entails that every $t \in W \otimes V^*$ and $a \in A$ satisfy $\Phi(at) = a\Phi(t)$. In other words, the map Φ is A-equivariant.

(ii) We have assumed that at least one of the vector spaces V and W is finite-dimensional. Thus, we know from linear algebra that Φ is a vector space isomorphism.[11] Hence, Φ is an A-module isomorphism (since Lemma 8.5 (i) shows that Φ is an A-module homomorphism). □

Corollary 8.6. *For any A-module V, we have $V^* \cong \operatorname{Hom}_{\mathbb{F}}(V, \epsilon)$.*

Proof of Corollary 8.6. Clearly, the A-module ϵ is finite-dimensional. Hence, Lemma 8.5 (ii) (applied to $W = \epsilon$) shows that the map $\Phi : \epsilon \otimes V^* \to \operatorname{Hom}_{\mathbb{F}}(V, \epsilon)$ (defined as in Lemma 8.5) is an A-module isomorphism. Thus, $\operatorname{Hom}_{\mathbb{F}}(V, \epsilon) \cong \epsilon \otimes V^* \cong V^*$ (by (2.6), applied to V^* instead of V) as A-modules. □

The following lemma generalizes Lemma 2.12:

Lemma 8.7. *Let V and W be two A-modules. Then,* $\operatorname{Hom}_A(V, W) = \operatorname{Hom}_{\mathbb{F}}(V, W)^A$.

The following proof of Lemma 8.7 is taken from [28, Lemma 4.1] (where the lemma is stated in far lesser generality, but the proof equally applies in the general setting):

Proof of Lemma 8.7. If $\varphi \in \operatorname{Hom}_A(V, W)$ then $\varphi \in \operatorname{Hom}_{\mathbb{F}}(V, W)^A$, since each $a \in A$ and $v \in V$ satisfy

$$(a\varphi)(v) = \sum a_1 \underbrace{\varphi(\alpha(a_2)v)}_{\substack{=\alpha(a_2)\varphi(v) \\ (\text{since } \varphi \in \operatorname{Hom}_A(V,W))}} = \sum a_1 \alpha(a_2) \varphi(v) = \epsilon(a)\varphi(v).$$

This proves $\operatorname{Hom}_A(V, W) \subseteq \operatorname{Hom}_{\mathbb{F}}(V, W)^A$.

Conversely, let $\psi \in \operatorname{Hom}_{\mathbb{F}}(V, W)^A$. Thus,

$$\epsilon(b)\,\psi = b\psi \qquad \text{for each } b \in A. \tag{8.3}$$

[11] For instance, its inverse can be constructed as follows:

- If V is finite-dimensional, then we can pick a basis $\{v_i\}$ of the $\mathbb{F}$-vector space V, and the corresponding dual basis $\{v_i^*\}$ of V^*. Then, the inverse of Φ can be defined by $\Phi^{-1}(h) = \sum_i h(v_i) \otimes v_i^*$ for all $h \in \operatorname{Hom}_{\mathbb{F}}(V, W)$.
- If W is finite-dimensional, then we can pick a basis $\{w_j\}$ of the $\mathbb{F}$-vector space W, and the corresponding dual basis $\{w_j^*\}$ of W^*. Then, the inverse of Φ can be defined by $\Phi^{-1}(h) = \sum_j w_j \otimes \left(w_j^* \circ h\right)$ for all $h \in \operatorname{Hom}_{\mathbb{F}}(V, W)$.

Using $a = \sum \epsilon(a_1) a_2$, we find

$$\begin{aligned}
\psi(av) &= \psi\left(\sum \epsilon(a_1) a_2 v\right) = \sum \underbrace{\epsilon(a_1)\psi(a_2 v)}_{=(\epsilon(a_1)\psi)(a_2 v)} = \sum \underbrace{(\epsilon(a_1)\psi)}_{\substack{=a_1\psi \\ \text{(by (8.3), applied to } b=a_1)}} (a_2 v) \\
&= \sum \underbrace{(a_1\psi)(a_2 v)}_{\substack{=\sum (a_1)_1 \psi(\alpha((a_1)_2) a_2 v) \\ \text{(by the definition of the } A\text{-action} \\ \text{on } \operatorname{Hom}_{\mathbb{F}}(V,W))}} = \sum \sum (a_1)_1 \psi(\alpha((a_1)_2) a_2 v) \\
&= \sum \sum a_1 \psi(\alpha((a_2)_1)(a_2)_2 v) \\
&\qquad \left(\begin{array}{c}\text{by the coassociativity law } \sum\sum (a_1)_1 \otimes (a_1)_2 \otimes a_2 = \sum\sum a_1 \otimes (a_2)_1 \otimes (a_2)_2 \\ \text{in the coalgebra } A\end{array}\right) \\
&= \sum a_1 \psi\left(\underbrace{\sum \alpha((a_2)_1)(a_2)_2}_{\substack{=\epsilon(a_2)1 \\ \text{(since } \sum \alpha(b_1)b_2 = \epsilon(b)1 \\ \text{for every } b\in A)}} v\right) = \sum a_1 \psi(\epsilon(a_2) v) = \underbrace{\sum a_1 \epsilon(a_2)}_{=a} \psi(v) \\
&= a\psi(v).
\end{aligned}$$

Since this holds for all a and v, we thus conclude that ψ lies in $\operatorname{Hom}_A(V, W)$. Hence, $\operatorname{Hom}_{\mathbb{F}}(V, W)^A \subseteq \operatorname{Hom}_A(V, W)$ is proven. □

Remark 8.8. If A is a Hopf algebra, then $\alpha(A)$ is a Hopf subalgebra of A. As a consequence of our proof of Lemma 8.7, we obtain the following curious fact: If V and W are two A-modules, then $\operatorname{Hom}_{\alpha(A)}(V, W) = \operatorname{Hom}_{\mathbb{F}}(V, W)^A = \operatorname{Hom}_A(V, W)$. In fact, in our proof of Lemma 8.7, we actually showed the two inclusions $\operatorname{Hom}_{\alpha(A)}(V, W) \subseteq \operatorname{Hom}_{\mathbb{F}}(V, W)^A \subseteq \operatorname{Hom}_A(V, W)$. But this chain of inclusions clearly is an equality, since its last term is contained in its first term.

Next, let us generalize Lemma 2.13:

Lemma 8.9. *Let V and W be two A-modules such that W is finite-dimensional. Then,* $\operatorname{Hom}_A(V, W) \cong \operatorname{Hom}_A(W^* \otimes V, \epsilon)$.

Proof of Lemma 8.9. For every $f \in \operatorname{Hom}_{\mathbb{F}}(V, W)$, define a linear functional $\phi(f) \in (W^* \otimes V)^*$ by setting

$$\phi(f)(g \otimes v) = g(f(v)) \qquad \text{for all } g \in W^* \text{ and } v \in V.$$

Thus, we have defined an $\mathbb{F}$-linear map $\phi : \operatorname{Hom}_{\mathbb{F}}(V, W) \to (W^* \otimes V)^*$. This $\mathbb{F}$-linear map is an isomorphism of vector spaces[12]. It is not, in general, an A-module isomorphism. Nevertheless, we claim that it restricts to an isomorphism $\operatorname{Hom}_A(V, W) \to \operatorname{Hom}_A(W^* \otimes V, \epsilon)$. This claim (once proven) will immediately yield Lemma 8.9; thus, it suffices to prove this claim. In other words, it suffices to prove that a map $f \in \operatorname{Hom}_{\mathbb{F}}(V, W)$ belongs to $\operatorname{Hom}_A(V, W)$ if and only if its image $\phi(f)$ belongs to $\operatorname{Hom}_A(W^* \otimes V, \epsilon)$. We shall prove the two directions of this equivalence separately:

[12]Indeed, this map is the composition of the standard isomorphisms $\operatorname{Hom}_{\mathbb{F}}(V, W) \to \operatorname{Hom}_{\mathbb{F}}(V, (W^*)^*) = \operatorname{Hom}_{\mathbb{F}}(V, \operatorname{Hom}_{\mathbb{F}}(W^*, \mathbb{F})) \to \operatorname{Hom}_{\mathbb{F}}(W^* \otimes V, \mathbb{F}) = (W^* \otimes V)^*$. Here, the isomorphism $W \to (W^*)^*$ (arising from the finite-dimensionality of W) was used for the first arrow.

$\Longrightarrow$: Assume that $f \in \operatorname{Hom}_A(V, W)$. Recall that $\sum \alpha(a_1)a_2 = a$ for each $a \in A$. Now, for each $a \in A$, $g \in W^*$ and $v \in V$, we have

$$\phi(f)\,(a(g \otimes v)) = \phi(f)\left(\sum a_1 g \otimes a_2 v\right) = \sum (a_1 g)\,(f\,(a_2 v)) = \sum g\,(\alpha(a_1) f\,(a_2 v)) \tag{8.4}$$

$$= g\left(\sum \alpha(a_1) \underbrace{f\,(a_2 v)}_{\substack{= a_2 f(v) \\ (\text{since } f \in \operatorname{Hom}_A(V,W))}}\right) \tag{8.5}$$

$$= g\left(\underbrace{\sum \alpha(a_1) a_2}_{= \epsilon(a) 1} f\,(v)\right) = \epsilon(a) \underbrace{g\,(f\,(v))}_{= \phi(f)(g \otimes v)} = \epsilon(a)\phi(f)\,(g \otimes v)\,.$$

Thus, $\phi(f)$ belongs to $\operatorname{Hom}_A(W^* \otimes V, \epsilon)$. This proves the $\Longrightarrow$ direction.

$\Longleftarrow$: Assume that $\phi(f)$ belongs to $\operatorname{Hom}_A(W^* \otimes V, \epsilon)$.

Let $a \in A$, $g \in W^*$ and $v \in V$. Then, as in (8.5), we find

$$\phi(f)\,(a(g \otimes v)) = g\left(\sum \alpha(a_1) f\,(a_2 v)\right). \tag{8.6}$$

But $\phi(f)$ belongs to $\operatorname{Hom}_A(W^* \otimes V, \epsilon)$. Hence,

$$\phi(f)\,(a(g \otimes v)) = \epsilon(a) \underbrace{\phi(f)\,(g \otimes v)}_{= g(f(v))} = \epsilon(a) g\,(f\,(v)) = g\,(\epsilon(a) f\,(v))\,.$$

Comparing this with (8.6), we obtain

$$g\left(\sum \alpha(a_1) f\,(a_2 v)\right) = g\,(\epsilon(a) f\,(v))\,.$$

Since this holds for **all** $g \in W^*$, we thus have

$$\sum \alpha(a_1) f\,(a_2 v) = \epsilon(a) f\,(v) \tag{8.7}$$

(since an element $w \in W$ is uniquely determined by its images under all $g \in W^*$).

Now, let $b \in A$ and $v \in V$. Then, using the axiom $b = \sum \epsilon(b_1) b_2$, we find

$$f(bv) = f\left(\sum \epsilon(b_1) b_2 v\right) = \sum \epsilon(b_1) f\,(b_2 v) = \sum \epsilon(b_1) 1 f\,(b_2 v) = \sum \sum (b_1)_1 \alpha((b_1)_2) f\,(b_2 v)$$

$$\left(\text{by the antipode axiom } \epsilon(a) 1 = \sum a_1 \alpha(a_2), \text{ applied to } a = b_1\right)$$

$$= \sum b_1 \underbrace{\sum \alpha((b_2)_1) f\,((b_2)_2 v)}_{\substack{= \epsilon(b_2) f(v) \\ (\text{by (8.7), applied to } a = b_2)}}$$

$$\left(\text{by the coassociativity law } \sum \sum (b_1)_1 \otimes (b_1)_2 \otimes b_2 = \sum b_1 \otimes \sum (b_2)_1 \otimes (b_2)_2\right)$$

$$= \sum b_1 \epsilon(b_2) f\,(v) = bf\,(v)\,.$$

Hence, f is A-linear, i.e., belongs to $\operatorname{Hom}_A(V, W)$. This proves the $\Longleftarrow$ direction. Hence, Lemma 8.9 is proven. ◻

We next generalize Lemma 2.14:

Lemma 8.10. *Let U and V be A-modules, at least one of which is finite-dimensional.*

(i) *We have $(U \otimes V)^* \cong V^* \otimes U^*$.*

(ii) *Assume that A is finite-dimensional. Then,* $^*(U \otimes V) \cong {}^*V \otimes {}^*U$.

Proof of Lemma 8.10. (i) There is a linear map $\phi : V^* \otimes U^* \to (U \otimes V)^*$ given by $\phi(g \otimes f)(u \otimes v) = f(u)g(v)$ for all $u \in U$, $v \in V$, $f \in U^*$, and $g \in V^*$. This linear map ϕ is an $\mathbb{F}$-vector space isomorphism (since at least one of U and V is finite-dimensional)[13]. We shall now show that this isomorphism is A-equivariant. Indeed, for any $a \in A$, $g \in V^*$, $f \in U^*$, $u \in U$ and $v \in V$, we have

$$\phi\left(\underbrace{a(g \otimes f)}_{=\sum a_1 g \otimes a_2 f}\right)(u \otimes v) = \sum \phi(a_1 g \otimes a_2 f)(u \otimes v) = \sum \underbrace{(a_2 f)(u)}_{=f(\alpha(a_2)u)} \underbrace{(a_1 g)(v)}_{=g(\alpha(a_1)v)} = \sum f(\alpha(a_2)u) g(\alpha(a_1)v)$$
$$= \sum \phi(g \otimes f)(\alpha(a_2)u \otimes \alpha(a_1)v) = \phi(g \otimes f)(\alpha(a)(u \otimes v)) = (a\phi(g \otimes f))(u \otimes v),$$

where the fifth equality sign relied on the fact that $\sum \alpha(a_2) \otimes \alpha(a_1) = \Delta(\alpha(a))$ (which is part of what it means for α to be a coalgebra anti-homomorphism). Hence, $\phi(a(g \otimes f)) = a\phi(g \otimes f)$ for all $a \in A$, $g \in V^*$ and $f \in U^*$ (because we have just shown that the two linear maps $\phi(a(g \otimes f))$ and $a\phi(g \otimes f)$ are equal on all pure tensors). Therefore, $\phi(at) = a\phi(t)$ for all $a \in A$ and $t \in V^* \otimes U^*$ (by linearity). In other words, the isomorphism $\phi : V^* \otimes U^* \to (U \otimes V)^*$ is A-equivariant. Therefore $(U \otimes V)^* \cong V^* \otimes U^*$.

(ii) The proof for $^*(U \otimes V) \cong {}^*V \otimes {}^*U$ is similar.[14] □

Here is another basic property of Hopf algebras:

Lemma 8.11. *Let V be a finite-dimensional A-module. Let $\{v_i\}$ be a basis for the $\mathbb{F}$-vector space V, and $\{v_i^*\}$ the dual basis for V^*. Identify $V \otimes \epsilon$ with V and $\epsilon \otimes V^*$ with V^* as usual. Then*

(i) $\sum_i v_i \otimes v_i^*(v) = v$ *for all* $v \in V$,
(ii) $\sum_i v^*(v_i) \otimes v_i^* = v^*$ *for all* $v^* \in V^*$, *and*
(iii) $a \sum_i v_i \otimes v_i^* = \epsilon(a) \sum_i v_i \otimes v_i^*$ *for all* $a \in A$.

Proof of Lemma 8.11. (i) and (ii) are just restatements of the identities $\sum_i v_i^*(v) v_i = v$ and $\sum_i v^*(v_i) v_i^* = v^*$, which are known facts from linear algebra.

(iii) The identity map id_V belongs to $\mathrm{Hom}_A(V, V) = \mathrm{Hom}_{\mathbb{F}}(V, V)^A$ (by Lemma 8.7). But Lemma 8.5 (ii) provides an A-module isomorphism $\Phi : V \otimes V^* \xrightarrow{\cong} \mathrm{Hom}_{\mathbb{F}}(V, V)$. The image of the element $\sum_i v_i \otimes v_i^* \in V \otimes V^*$ under this isomorphism Φ is id_V (because each $v \in V$ satisfies $\left(\Phi\left(\sum_i v_i \otimes v_i^*\right)\right)(v) = \sum_i v_i^*(v) v_i = v = \mathrm{id}_V(v)$), which belongs to $\mathrm{Hom}_A(V, V) = \mathrm{Hom}_{\mathbb{F}}(V, V)^A$. Hence, $\sum_i v_i \otimes v_i^*$ must belong to $(V \otimes V^*)^A$. In other words, $a \sum_i v_i \otimes v_i^* = \epsilon(a) \sum_i v_i \otimes v_i^*$ for all $a \in A$. This proves part (iii). □

The next lemma generalizes Lemma 2.15:

Lemma 8.12. *Let U, V, and W be A-modules such that V and W are finite-dimensional. Then, one has isomorphisms*

$$\mathrm{Hom}_A(U \otimes V, W) \xrightarrow{\sim} \mathrm{Hom}_A(U, W \otimes V^*), \tag{8.8}$$

$$\mathrm{Hom}_A(V^* \otimes U, W) \xrightarrow{\sim} \mathrm{Hom}_A(U, V \otimes W). \tag{8.9}$$

Assume furthermore that A is finite-dimensional. Then, one has isomorphisms

$$\mathrm{Hom}_A(U \otimes {}^*V, W) \xrightarrow{\sim} \mathrm{Hom}_A(U, W \otimes V), \tag{8.10}$$

$$\mathrm{Hom}_A(V \otimes U, W) \xrightarrow{\sim} \mathrm{Hom}_A(U, {}^*V \otimes W). \tag{8.11}$$

[13]The quickest way to prove this is to recall that both duals and tensor products commute with finite direct sums, so we can reduce the proof to the case when one of U and V is $\mathbb{F}$; but this case is obvious.

[14] Indeed, the isomorphism is provided by the same map ϕ. The computation is also identical, except that α is replaced by α^{-1} (which, too, is a coalgebra anti-homomorphism). The finite-dimensionality of A is used to ensure that α^{-1} exists (and the right-duals are well-defined).

Proof of Lemma 8.12. Notice that V^*, $W \otimes V^*$ and $V \otimes W$ are finite-dimensional (since V and W are finite-dimensional).

One only need check (8.8) and (8.9), since then replacing V by ${}^*V$ yields (8.10) and (8.11) (thanks to Lemma 8.4).

We have

$$\begin{aligned}\operatorname{Hom}(U \otimes V, W) &\cong W \otimes (U \otimes V)^* \qquad \text{(by Lemma 8.5 (ii))}\\ &\cong W \otimes V^* \otimes U^* \qquad \text{(by Lemma 8.10 (i))}\\ &\cong \operatorname{Hom}(U, W \otimes V^*) \qquad \text{(by Lemma 8.5 (ii))}.\end{aligned}$$

Now, (8.8) holds since

$$\begin{aligned}\operatorname{Hom}_A(U \otimes V, W) &= \operatorname{Hom}(U \otimes V, W)^A \qquad \text{(by Lemma 8.7)}\\ &\cong \operatorname{Hom}(U, W \otimes V^*)^A \qquad (\text{since } \operatorname{Hom}(U \otimes V, W) \cong \operatorname{Hom}(U, W \otimes V^*))\\ &= \operatorname{Hom}_A(U, W \otimes V^*) \qquad \text{(by Lemma 8.7)}.\end{aligned}$$

Furthermore, (8.9) holds since

$$\begin{aligned}\operatorname{Hom}_A(V^* \otimes U, W) &\cong \operatorname{Hom}_A(W^* \otimes V^* \otimes U, \epsilon) \qquad \text{(by Lemma 8.9)}\\ &\cong \operatorname{Hom}_A((V \otimes W)^* \otimes U, \epsilon) \qquad (\text{since Lemma 8.10 (i) yields } (V \otimes W)^* \cong W^* \otimes V^*)\\ &\cong \operatorname{Hom}_A(U, V \otimes W) \qquad \text{(by Lemma 8.9)}.\end{aligned}$$

Remark: Here is an alternative proof of (8.9): Fix a basis $\{v_i\}$ for the $\mathbb{F}$-vector space V, and the corresponding dual basis $\{v_i^*\}$ of V^*.

For each $f \in \operatorname{Hom}(V^* \otimes U, W)$, we define $\phi(f) \in \operatorname{Hom}(U, V \otimes W)$ by

$$\phi(f)(u) = \sum_i v_i \otimes f(v_i^* \otimes u), \quad \forall u \in U.$$

This defines a linear map $\phi : \operatorname{Hom}(V^* \otimes U, W) \to \operatorname{Hom}(U, V \otimes W)$. (Its definition uses a choice of bases, but ϕ itself is independent of this choice, since the tensor $\sum_i v_i \otimes v_i^*$ does not depend on the choice of basis $\{v_i\}$.)

Conversely, if $g \in \operatorname{Hom}(U, V \otimes W)$ then define $\psi(g) \in \operatorname{Hom}(V^* \otimes U, W)$ by

$$\psi(g)(v^* \otimes u) = (v^* \otimes \mathrm{id})(g(u)), \quad \forall u \in U, \ \forall v^* \in V^*.$$

This defines a linear map $\psi : \operatorname{Hom}(U, V \otimes W) \to \operatorname{Hom}(V^* \otimes U, W)$.

The maps ϕ and ψ are inverses of each other since Lemma 8.11 implies

$$\phi(\psi(g))(u) = \sum_i v_i \otimes \psi(g)(v_i^* \otimes u) = \sum_i v_i \otimes (v_i^* \otimes \mathrm{id})(g(u)) = g(u),$$

$$\psi(\phi(f))(v^* \otimes u) = (v^* \otimes \mathrm{id})(\phi(f)(u)) = \sum_i v^*(v_i) \otimes f(v_i^* \otimes u) = f(v^* \otimes u).$$

It thus remains to show that $\phi(\operatorname{Hom}_A(U \otimes V, W)) \subseteq \operatorname{Hom}_A(U, W \otimes V^*)$ and $\psi(\operatorname{Hom}_A(U, W \otimes V^*)) \subseteq \operatorname{Hom}_A(U \otimes V, W)$.

Suppose f is A-linear. Let $a \in A$ and $u \in U$. Then

$$a\phi(f)(u) = \sum_i \sum a_1 v_i \otimes a_2 f(v_i^* \otimes u) = \sum_i \sum a_1 v_i \otimes f(a_2' v_i^* \otimes a_2'' u).$$

Combining this with Lemma 8.11 we have, for any $v^* \in V^*$,

$$\begin{aligned}(v^* \otimes \mathrm{id})(a\phi(f)(u)) &= \sum_i \sum f(v^*(a_1 v_i) a_2' v_i^* \otimes a_2'' u) = \sum f(\epsilon(a_1) v^* \otimes a_2 u)\\ &= f(v^* \otimes au) = \sum_i v^*(v_i) \otimes f(v_i^* \otimes au) = (v^* \otimes \mathrm{id})(\phi(f)(au)).\end{aligned}$$

This implies $a\phi(f)(u) = \phi(f)(au)$. Thus $\phi(f)$ is A-linear. Hence, $\phi(\operatorname{Hom}_A(U \otimes V, W)) \subseteq \operatorname{Hom}_A(U, W \otimes V^*)$.

Now suppose g is A-linear. Let $a \in A$, $u \in U$, and $v^* \in V^*$. Writing $g(u) = \sum_i v^{(i)} \otimes w^{(i)}$, we have

$$\begin{aligned}
\psi(g)(a(v^* \otimes u)) &= \sum \psi(g)(a_1 v^* \otimes a_2 u) = \sum (a_1 v^* \otimes \mathrm{id})(g(a_2 u)) \\
&= \sum (a_1 v^* \otimes \mathrm{id})(a_2 g(u)) = \sum (a_1 v^* \otimes \mathrm{id}) \sum_i a_2' v^{(i)} \otimes a_2'' w^{(i)} \\
&= \sum \sum_i v^*(\alpha(a_1) a_2' v^{(i)}) \otimes a_2'' w^{(i)} = \sum \sum_i v^*(\epsilon(a_1) v^{(i)}) \otimes a_2 w^{(i)} \\
&= \sum \sum_i v^*(v^{(i)}) \otimes \epsilon(a_1) a_2 w^{(i)} = \sum_i v^*(v^{(i)}) \otimes a w^{(i)} \\
&= a \sum_i v^*(v^{(i)}) \otimes w^{(i)} = a((v^* \otimes \mathrm{id})(g(u))) = a\psi(g)(v^* \otimes u).
\end{aligned}$$

Thus, $\psi\left(\mathrm{Hom}_A(U, W \otimes V^*)\right) \subseteq \mathrm{Hom}_A(U \otimes V, W)$. Therefore (8.9) holds.

The advantage of this alternative proof of (8.9) is that it gets by without using the finite-dimensionality of W. Hence, the isomorphism (8.9) holds even if W is not finite-dimensional (as long as V is finite-dimensional).

The isomorphism (8.8) also holds in this generality (i.e., requiring only V to be finite-dimensional, not W). Here is an outline of how to prove this: It clearly suffices to prove the isomorphism $\mathrm{Hom}(U \otimes V, W) \cong \mathrm{Hom}(U, W \otimes V^*)$ (because this isomorphism was the crucial step in our above proof). In view of the isomorphism $W \otimes V^* \cong \mathrm{Hom}(V, W)$ (a consequence of Lemma 8.5 (ii)), this boils down to proving the isomorphism $\mathrm{Hom}(U \otimes V, W) \cong \mathrm{Hom}(U, \mathrm{Hom}(V, W))$. But this isomorphism is well-known: It is provided by the $\mathbb{F}$-vector space isomorphism

$$\begin{aligned}
&\mathrm{Hom}(U \otimes V, W) \to \mathrm{Hom}(U, \mathrm{Hom}(V, W)), \\
&\qquad F \mapsto (\text{the map } U \to \mathrm{Hom}(V, W) \text{ sending each } u \in U \text{ to the map } V \to W \\
&\qquad\qquad \text{sending each } v \in V \text{ to } F(u \otimes v)),
\end{aligned}$$

whose A-equivariance can be proven by a somewhat tedious but straightforward computation.[15] ◻

Let us now extend Proposition 2.16. To wit, Proposition 2.16 will follow from part (ii) of the following fact:

Proposition 8.13. *Let A be a finite-dimensional Hopf algebra.*

(i) *We have* $\dim\left(A^A\right) = 1$.

(ii) *Let V be a finite-dimensional A-module. Then,* $\dim \mathrm{Hom}_A(V, A) = \dim V$.

Proposition 8.13 (i) is actually the well-known fact (see, e.g., [26, Thm. 10.2.2 (a)]) that the vector space of left integrals of the finite-dimensional Hopf algebra A is 1-dimensional. Nevertheless, we shall give a proof, as it is easy using what has been done before.

Proof of Proposition 8.13. Let V be a finite-dimensional A-module. Lemma 8.5 (ii) (applied to $W = A$) shows that $A \otimes V^* \cong \mathrm{Hom}_{\mathbb{F}}(V, A)$ as A-modules. But Lemma 8.2 (ii) (applied to V^* instead of V) yields $A \otimes V^* \cong A^{\oplus \dim(V^*)} = A^{\oplus \dim V}$ as A-modules. Hence, $\mathrm{Hom}_{\mathbb{F}}(V, A) \cong A \otimes V^* \cong A^{\oplus \dim V}$ as A-modules. Now, Lemma 8.7 (applied to $W = A$) yields

$$\begin{aligned}
\mathrm{Hom}_A(V, A) = \mathrm{Hom}_{\mathbb{F}}(V, A)^A &\cong \left(A^{\oplus \dim V}\right)^A \qquad \left(\text{since } \mathrm{Hom}_{\mathbb{F}}(V, A) \cong A^{\oplus \dim V}\right) \\
&\cong \left(A^A\right)^{\oplus \dim V} \qquad \left(\text{since the functor } W \mapsto W^A \text{ preserves direct sums}\right)
\end{aligned}$$

as $\mathbb{F}$-vector spaces. Taking dimensions, we thus find

$$\dim \mathrm{Hom}_A(V, A) = \dim\left(\left(A^A\right)^{\oplus \dim V}\right) = \dim\left(A^A\right) \dim V. \tag{8.12}$$

Now, forget that we fixed V. It is well-known that $\mathrm{Hom}_A(A, A) \cong A$ as $\mathbb{F}$-vector spaces (indeed, the map $\mathrm{Hom}_A(A, A) \to A,\ f \mapsto f(1)$ is an isomorphism). Hence, $\dim A = \mathrm{Hom}_A(A, A) = \dim\left(A^A\right) \dim A$ (by

[15]The computation uses the fact that α is a coalgebra anti-homomorphism.

(8.12), applied to $V = A$). We can cancel $\dim A$ from this equality (since $\dim A > 0$), and thus obtain $1 = \dim\left(A^A\right)$. This proves Proposition 8.13 (i).

(ii) From (8.12), we obtain $\dim \operatorname{Hom}_A(V, A) = \underbrace{\dim\left(A^A\right)}_{=1} \dim V = \dim V$. □

We record a curious corollary of Proposition 8.13, which we will not use below but we find worth observing.

Corollary 8.14. *Let e be an idempotent in the finite-dimensional Hopf algebra A. Then,* $\dim(Ae) = \dim(eA)$.

Proof. A well-known fact (see, e.g., [31, Prop. 7.4.1 (3)]) says that $\dim \operatorname{Hom}_A(Ae, U) = \dim(eU)$ for any A-module U. Applying this to $U = A$, we obtain $\dim \operatorname{Hom}_A(Ae, A) = \dim(eA)$. But Proposition 8.13 (ii) (applied to $V = Ae$) yields $\dim \operatorname{Hom}_A(Ae, A) = \dim(Ae)$. Hence, $\dim(Ae) = \dim \operatorname{Hom}_A(Ae, A) = \dim(eA)$. □

9. Appendix B: an elementary proof of Lemma 4.2

In this section, we shall give a second proof of Lemma 4.2, using nothing but basic linear algebra. Besides its elementary nature, this proof has the additional advantage of providing an explicit construction of the isomorphism claimed in Lemma 4.2 under some circumstances (e.g., if two entries of $\mathbf{s}$ equal 1).

We prepare by showing some lemmas about $\mathbb{Z}$-modules.

Lemma 9.1. *Let m be a positive integer. Let $(e_1, e_2, \ldots, e_m)$ be the standard basis of the $\mathbb{Z}$-module $\mathbb{Z}^m$ (consisting of column vectors). Let $w \in \mathbb{Z}^m$ be a column vector. Let $g = \gcd(w)$. (Here and below, $\gcd(w)$ denotes the greatest common divisor of the entries of w.) Then, there exists some $B \in \mathrm{GL}_m(\mathbb{Z})$ such that $Bw = ge_1$.*

Proof. This is a well-known fact, but let us sketch a proof. An operation on vectors in $\mathbb{Z}^m$ (that is, a map $\mathbb{Z}^m \to \mathbb{Z}^m$) is called an *elementary operation* if and only if

- it is a *negation operation*, which means that it multiplies an entry of the vector by -1; **or**
- it is an *addition operation*, which means that it adds an integer multiple of an entry of the vector to another entry; **or**
- it is a *swap operation*, which means that it swaps two entries of the vector.

It is well-known that each composition of elementary operations can be rewritten as left multiplication by some matrix in $\mathrm{GL}_m(\mathbb{Z})$ (i.e., as the map $v \mapsto Bv$ for some $B \in \mathrm{GL}_m(\mathbb{Z})$). Hence, if we can prove that the vector ge_1 can be obtained from w by a sequence of elementary operations, then we will be done.

But proving this is easy: Start with the vector w. Then, apply negation operations to turn all its entries nonnegative. Then, apply addition operations (specifically, subtracting entries from other entries) to ensure that at most one of its entries is nonzero[16]. Finally, apply a swap operation to ensure that this nonzero entry is the first entry (if it was not already). The resulting vector has the form pe_1 for some $p \in \mathbb{Z}$. Consider this p. But elementary operations do not change the greatest common divisor of the entries of a vector. Hence, $\gcd(pe_1) = \gcd(w)$ (since we obtained pe_1 from w by elementary operations). Since p is nonnegative, we have $\gcd(pe_1) = p$, so that $p = \gcd(pe_1) = \gcd(w) = g$ and thus $pe_1 = ge_1$. Hence, we have obtained the vector ge_1 from w by a sequence of elementary operations (since we have obtained the vector pe_1 in this way). As we have said above, this proves the lemma. □

Lemma 9.2. *Let m be a positive integer. Let $d \in \mathbb{Z}$, and let $w \in \mathbb{Z}^m$ be a column vector. Let $\gamma = \gcd(d, \gcd(w))$. Then,*

$$\mathbb{Z}^m / (d\mathbb{Z}^m + \mathbb{Z}w) \cong (\mathbb{Z}/\gamma\mathbb{Z}) \oplus (\mathbb{Z}/d\mathbb{Z})^{m-1}.$$

[16]This can be done as follows: As long as our vector has (at least) two nonzero entries, we can apply an addition operation (namely, subtracting the smaller of these two entries from the larger) to obtain a new vector, whose entries are still all nonnegative, but whose sum of entries is smaller than that of the previous vector. We can repeat this step until no two nonzero entries remain (which is destined to happen, since the sum of entries cannot keep decreasing forever).

Proof. Let $g = \gcd(w)$. Thus, $\gcd(d, g) = \gcd(d, \gcd(w)) = \gamma$. Now, $\mathbb{Z}d + \mathbb{Z}g = \mathbb{Z}\underbrace{\gcd(d, g)}_{=\gamma} = \mathbb{Z}\gamma$.

Let $(e_1, e_2, \ldots, e_m)$ be the standard basis of the $\mathbb{Z}$-module $\mathbb{Z}^m$ (consisting of column vectors). Then, $\mathbb{Z}de_1 + \mathbb{Z}ge_1 = \underbrace{(\mathbb{Z}d + \mathbb{Z}g)}_{=\mathbb{Z}\gamma} e_1 = \mathbb{Z}\gamma e_1$.

Lemma 9.1 shows that there exists some $B \in \mathrm{GL}_m(\mathbb{Z})$ such that $Bw = ge_1$. Consider this B. Left multiplication by B is an automorphism of the $\mathbb{Z}$-module $\mathbb{Z}^m$ (since $B \in \mathrm{GL}_m(\mathbb{Z})$) and sends the submodule $d\mathbb{Z}^m$ to $d\mathbb{Z}^m$ while sending the submodule $\mathbb{Z}w$ to $\mathbb{Z}\underbrace{Bw}_{=ge_1} = \mathbb{Z}ge_1$. Hence, it induces an isomorphism $\mathbb{Z}^m/(d\mathbb{Z}^m + \mathbb{Z}w) \to \mathbb{Z}^m/(d\mathbb{Z}^m + \mathbb{Z}ge_1)$. Thus,

$$\begin{aligned}
\mathbb{Z}^m/(d\mathbb{Z}^m + \mathbb{Z}w) &\cong \mathbb{Z}^m/(d\mathbb{Z}^m + \mathbb{Z}ge_1) = \mathbb{Z}^m/((\mathbb{Z}de_1 + \mathbb{Z}de_2 + \cdots + \mathbb{Z}de_m) + \mathbb{Z}ge_1) \\
&\qquad (\text{since } d\mathbb{Z}^m = \mathbb{Z}de_1 + \mathbb{Z}de_2 + \cdots + \mathbb{Z}de_m) \\
&= \mathbb{Z}^m/\left(\underbrace{(\mathbb{Z}de_1 + \mathbb{Z}ge_1)}_{=\mathbb{Z}\gamma e_1} + (\mathbb{Z}de_2 + \mathbb{Z}de_3 + \cdots + \mathbb{Z}de_m)\right) \\
&= \mathbb{Z}^m/(\mathbb{Z}\gamma e_1 + (\mathbb{Z}de_2 + \mathbb{Z}de_3 + \cdots + \mathbb{Z}de_m)) \\
&= (\mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \cdots \oplus \mathbb{Z}e_m)/(\mathbb{Z}\gamma e_1 \oplus \mathbb{Z}de_2 \oplus \mathbb{Z}de_3 \oplus \cdots \oplus \mathbb{Z}de_m) \\
&\cong \underbrace{(\mathbb{Z}e_1/\mathbb{Z}\gamma e_1)}_{\cong \mathbb{Z}/\gamma\mathbb{Z}} \oplus \underbrace{(\mathbb{Z}e_2/\mathbb{Z}de_2) \oplus (\mathbb{Z}e_3/\mathbb{Z}de_3) \oplus \cdots \oplus (\mathbb{Z}e_m/\mathbb{Z}de_m)}_{\cong (\mathbb{Z}/d\mathbb{Z})^{m-1}} \\
&\cong (\mathbb{Z}/\gamma\mathbb{Z}) \oplus (\mathbb{Z}/d\mathbb{Z})^{m-1}.
\end{aligned}$$

□

Lemma 9.3. *Let $m > 1$ be an integer. Let $u \in \mathbb{Z}^m$ and $v \in \mathbb{Z}^m$ be two column vectors such that $v_1 = 1$. Let $\gamma = \gcd(u)$, and set $d = v^T u \in \mathbb{Z}$. Let $L = dI_m - uv^T \in \mathbb{Z}^{m \times m}$. Then,*

$$\mathbb{Z}^m/\operatorname{im} L \cong \mathbb{Z} \oplus (\mathbb{Z}/\gamma\mathbb{Z}) \oplus (\mathbb{Z}/d\mathbb{Z})^{m-2}.$$

Proof. Let $(e_1, e_2, \ldots, e_m)$ be the standard basis of the $\mathbb{Z}$-module $\mathbb{Z}^m$. Recall that $L = dI_m - uv^T$. Hence, for each $i \in \{1, 2, \ldots, m\}$, we have

$$Le_i = \left(dI_m - uv^T\right) e_i = de_i - u \underbrace{v^T e_i}_{=v_i} = de_i - uv_i.$$

Applying this to $i = 1$, we obtain $Le_1 = de_1 - u \underbrace{v_1}_{=1} = de_1 - u$.

Now, for each $i \in \{1, 2, \ldots, m\}$, define a vector $q_i \in \mathbb{Z}^m$ by $q_i = e_i - v_i e_1$. Then, each $i \in \{1, 2, \ldots, m\}$ satisfies

$$\begin{aligned}
Lq_i = L(e_i - v_i e_1) &= \underbrace{Le_i}_{=de_i - uv_i} - v_i \underbrace{Le_1}_{=de_1 - u} = (de_i - uv_i) - v_i (de_1 - u) \\
&= d\underbrace{(e_i - v_i e_1)}_{=q_i} = dq_i. \qquad (9.1)
\end{aligned}$$

Note that the definition of q_1 yields $q_1 = e_1 - \underbrace{v_1}_{=1} e_1 = e_1 - e_1 = 0$. Hence, $\sum_{i=1}^m u_i q_i = \sum_{i=2}^m u_i q_i + u_1 \underbrace{q_1}_{=0} = \sum_{i=2}^m u_i q_i$. Thus,

$$\sum_{i=2}^m u_i q_i = \sum_{i=1}^m u_i \underbrace{q_i}_{=e_i - v_i e_1} = \sum_{i=1}^m u_i (e_i - v_i e_1) = \underbrace{\sum_{i=1}^m u_i e_i}_{=u} - \underbrace{\sum_{i=1}^m u_i v_i}_{=v^T u = d} e_1$$

$$= u - de_1 = -\underbrace{(de_1 - u)}_{=Le_1} = -Le_1. \tag{9.2}$$

Let u' be the vector $[u_2, u_3, \ldots, u_m]^T \in \mathbb{Z}^{m-1}$. Recall that

$$d = v^T u = \underbrace{v_1}_{=1} u_1 + v_2 u_2 + v_3 u_3 + \cdots + v_m u_m = u_1 + \underbrace{v_2 u_2 + v_3 u_3 + \cdots + v_m u_m}_{\substack{\in \gcd(u')\mathbb{Z} \\ (\text{since } u_i \in \gcd(u')\mathbb{Z} \text{ for all } i>1)}} \in u_1 + \gcd(u')\mathbb{Z}.$$

Hence, $d \equiv u_1 \mod \gcd(u')\mathbb{Z}$. Thus, $\gcd(d, \gcd(u')) = \gcd(u_1, \gcd(u')) = \gcd(u) = \gamma$.

We shall identify the $\mathbb{Z}$-module $\mathbb{Z}^{m-1}$ with the $\mathbb{Z}$-submodule $\operatorname{span}_{\mathbb{Z}}(e_2, e_3, \ldots, e_m)$ of $\mathbb{Z}^m$ by equating each vector $[p_2, p_3, \ldots, p_m]^T \in \mathbb{Z}^{m-1}$ with $p_2 e_2 + p_3 e_3 + \cdots + p_m e_m \in \operatorname{span}_{\mathbb{Z}}(e_2, e_3, \ldots, e_m)$. From this point of view, we have $u' = u_2 e_2 + u_3 e_3 + \cdots + u_m e_m$ and

$$\mathbb{Z}^m / \left(d\mathbb{Z}^{m-1} + \mathbb{Z}u' \right) \cong \mathbb{Z} \oplus \underbrace{\left(\mathbb{Z}^{m-1} / \left(d\mathbb{Z}^{m-1} + \mathbb{Z}u' \right) \right)}_{\substack{\cong (\mathbb{Z}/\gamma\mathbb{Z}) \oplus (\mathbb{Z}/d\mathbb{Z})^{m-2} \\ (\text{by Lemma 9.2, applied to } m-1 \text{ and } u' \text{ instead of } m \text{ and } w)}}$$

$$\cong \mathbb{Z} \oplus (\mathbb{Z}/\gamma\mathbb{Z}) \oplus (\mathbb{Z}/d\mathbb{Z})^{m-2}. \tag{9.3}$$

Now, we define a $\mathbb{Z}$-linear map $\Phi : \mathbb{Z}^m \to \mathbb{Z}^m$ by setting

$$\Phi(e_i) = \begin{cases} e_1, & \text{if } i = 1; \\ q_i, & \text{if } i > 1 \end{cases} \qquad \text{for all } i \in \{1, 2, \ldots, m\}.$$

This map Φ is tantamount to left multiplication by the matrix $\begin{pmatrix} 1 & -v_2 & -v_3 & \cdots & -v_m \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$ (since $q_i = e_i - v_i e_1$), which is invertible over $\mathbb{Z}$ (since it is upper-unitriangular). Hence, Φ is a $\mathbb{Z}$-module isomorphism.

Next, we are going to show that $\Phi\left(d\mathbb{Z}^{m-1} + \mathbb{Z}u'\right) = \operatorname{im} L$.

Indeed, for each $i \in \{2, 3, \ldots, m\}$, we have

$$\Phi(de_i) = d \underbrace{\Phi(e_i)}_{\substack{=q_i \\ (\text{since } i>1)}} = dq_i = Lq_i \qquad (\text{by (9.1)}). \tag{9.4}$$

Furthermore, $u' = u_2 e_2 + u_3 e_3 + \cdots + u_m e_m = \sum_{i=2}^m u_i e_i$, so that

$$\Phi(u') = \Phi\left(\sum_{i=2}^m u_i e_i \right) = \sum_{i=2}^m u_i \underbrace{\Phi(e_i)}_{\substack{=q_i \\ (\text{since } i>1)}} = \sum_{i=2}^m u_i q_i = -Le_1 \qquad (\text{by (9.2)}). \tag{9.5}$$

But the map Φ is an isomorphism. Thus,

$$\begin{aligned}\mathbb{Z}^m &= \Phi(\mathbb{Z}^m) = \Phi\left(\operatorname{span}_{\mathbb{Z}}(e_1, e_2, e_3, \ldots, e_m)\right) \\ &= \operatorname{span}_{\mathbb{Z}}(\Phi(e_1), \Phi(e_2), \Phi(e_3), \ldots, \Phi(e_m)) = \operatorname{span}_{\mathbb{Z}}(e_1, q_2, q_3, \ldots, q_m)\end{aligned}$$

(since the definition of Φ yields $\Phi(e_1) = e_1$ and $\Phi(e_i) = q_i$ for each $i > 1$). Hence,

$$L(\mathbb{Z}^m) = L\left(\operatorname{span}_{\mathbb{Z}}(e_1, q_2, q_3, \ldots, q_m)\right) = \operatorname{span}_{\mathbb{Z}}(Le_1, Lq_2, Lq_3, \ldots, Lq_m). \tag{9.6}$$

On the other hand,

$$\begin{aligned}d\mathbb{Z}^{m-1} + \mathbb{Z}u' &= \underbrace{\mathbb{Z}u'}_{=\operatorname{span}_{\mathbb{Z}}(u')} + \underbrace{d\mathbb{Z}^{m-1}}_{\substack{=d\operatorname{span}_{\mathbb{Z}}(e_2,e_3,\ldots,e_m) \\ =\operatorname{span}_{\mathbb{Z}}(de_2,de_3,\ldots,de_m)}} = \operatorname{span}_{\mathbb{Z}}(u') + \operatorname{span}_{\mathbb{Z}}(de_2, de_3, \ldots, de_m) \\ &= \operatorname{span}_{\mathbb{Z}}(u', de_2, de_3, \ldots, de_m)\end{aligned}$$

and thus

$$\begin{aligned}\Phi\left(d\mathbb{Z}^{m-1} + \mathbb{Z}u'\right) &= \Phi\left(\operatorname{span}_{\mathbb{Z}}(u', de_2, de_3, \ldots, de_m)\right) \\ &= \operatorname{span}_{\mathbb{Z}}(\Phi(u'), \Phi(de_2), \Phi(de_3), \ldots, \Phi(de_m)) \\ &= \operatorname{span}_{\mathbb{Z}}(-Le_1, Lq_2, Lq_3, \ldots, Lq_m) \qquad \text{(by (9.5) and (9.4))} \\ &= \operatorname{span}_{\mathbb{Z}}(Le_1, Lq_2, Lq_3, \ldots, Lq_m) = L(\mathbb{Z}^m) \qquad \text{(by (9.6))} \\ &= \operatorname{im} L.\end{aligned}$$

Thus, the isomorphism $\Phi : \mathbb{Z}^m \to \mathbb{Z}^m$ induces an isomorphism $\mathbb{Z}^m / \left(d\mathbb{Z}^{m-1} + \mathbb{Z}u'\right) \to \mathbb{Z}^m / \operatorname{im} L$. Hence,

$$\mathbb{Z}^m / \operatorname{im} L \cong \mathbb{Z}^m / \left(d\mathbb{Z}^{m-1} + \mathbb{Z}u'\right) \cong \mathbb{Z} \oplus (\mathbb{Z}/\gamma\mathbb{Z}) \oplus (\mathbb{Z}/d\mathbb{Z})^{m-2} \qquad \text{(by (9.3))}. \qquad \square$$

Proof of Lemma 4.2. Lemma 4.2 would follow by applying Lemma 9.3 to $m = \ell + 1$, $u = \mathbf{p}$, $v = \mathbf{s}$, except for a minor inconvenience: Lemma 4.2 assumes $\mathbf{s}_{\ell+1} = 1$, whereas Lemma 9.3 assumes $v_1 = 1$. However, this is merely a notational distinction, and can be straightened out by relabeling the indices (we leave the details to the reader). □

10. Appendix C: Some more observations on gcds

In this short appendix, we relate the gcds of the entries of the vectors $\mathbf{s}$ and $\mathbf{p}$ to expansions of $[A]$ in the Grothendieck groups $K_0(A)$ and $G_0(A)$. This relation (which does not require A to be a Hopf algebra) was found as a side result in our study of the critical group, but did not turn out to be useful for the latter. We record it here merely to avoid losing it.

Proposition 10.1. *Let A be a finite-dimensional $\mathbb{F}$-algebra, with $\mathbb{F}$ algebraically closed. (We do not require A to be a Hopf algebra here.) Let P_i, S_i, $\mathbf{p}$, $\mathbf{s}$ and C be as in Subsection 2.1.*

(i) *The class $[A]$ of the left-regular A-module lies in* $\gcd(\mathbf{s}) \cdot K_0(A)$.
(ii) *When $A \cong A^{\text{opp}}$ as rings, the class $[A]$ of the left-regular A-module lies in* $\gcd(\mathbf{p}) \cdot G_0(A)$.

Proof. Assertion (i) follows since (2.1) shows $[A] = \sum_{i=1}^{\ell+1} \dim(S_i)[P_i]$ in $K_0(A)$.

(ii) We have $[A] = \sum_{i=1}^{\ell+1} [A : S_i][S_i]$ in $G_0(A)$. Hence, it is enough to show that $\gcd(\mathbf{p}) \mid [A : S_i]$ for each $i \in \{1, 2, \ldots, \ell+1\}$. So let us fix i. Choose a primitive idempotent $e_i \in A$ such that $P_i \cong Ae_i$. The hypothesis $A \cong A^{\text{opp}}$ shows that there is a ring isomorphism $\phi : A \to A^{\text{opp}}$. The image of the primitive idempotent e_i under this isomorphism ϕ must be another primitive idempotent e_j of A, and furthermore we have $\phi(e_i A) = Ae_j$, whence $\dim(e_i A) = \dim(Ae_j)$. Now, (2.2) yields

$$[A : S_i] = \dim \operatorname{Hom}_A(P_i, A) = \dim \operatorname{Hom}_A(Ae_i, A) = \dim(e_i A) = \dim(Ae_j) = \dim P_j \text{ for some } P_j.$$

Here the third equality used the $\mathbb{F}$-linear isomorphism $\operatorname{Hom}_A(Ae_i, V) \cong e_i V$ (defined for each A-module V) which sends φ to $\varphi(e_i)$. Since P_j is projective, we have $\gcd(\mathbf{p}) \mid \dim P_j = [A : S_i]$, as desired. □

Example 10.2. The matrix algebra $A = \mathrm{Mat}_n(\mathbb{F})$ is semisimple, with only one simple A-module $S_1(= P_1)$ having $\dim(S_1) = n$. Thus in this case, $n = \gcd(\mathbf{s}) = \gcd(\mathbf{p})$, and indeed, $[A] = n[S_1] = n[P_1]$ in $G_0(A)(= K_0(A))$.

Each finite-dimensional Hopf algebra A satisfies $A \cong A^{\mathrm{opp}}$ as rings (via the antipode $\alpha : A \to A^{\mathrm{opp}}$); therefore, Proposition 10.1 (ii) can be applied to any such A. For example, we obtain the following:

Example 10.3. Consider again the generalized Taft Hopf algebra $A = H_{n,m}$ from Example 2.5. As we know from Example 5.8, we have $\gcd(\mathbf{p}) = m$. Hence, Proposition 10.1 (ii) shows that $[A]$ lies in $mG_0(A)$.

Acknowledgements

The authors thank Georgia Benkart, Sebastian Burciu, Pavel Etingof, Jim Humphreys, Radha Kessar, Peter J. McNamara, Hans-Jürgen Schneider, Peter Webb, and Sarah Witherspoon for helpful conversations and references.

References

[1] G. Benkart, C. Klivans, and V. Reiner, Chip firing on Dynkin diagrams and McKay quivers. *Math. Z.* **290** (2018), 615–648. A preprint appears on `arXiv:1601.06849v2`.
[2] R. Brauer, A note on theorems of Burnside and Blichfeldt. *Proc. Amer. Math. Soc.* **15** (1964), 31–34.
[3] R. Brauer, On the Cartan Invariants of Groups of Finite Order. *Annals of Mathematics* **42** (1941), 53–61.
[4] S. Burciu, Kernels of representations and coideal subalgebras of Hopf algebras. *Glasgow Math. J.* **54** (2012), 107–119. A preprint appears on `arXiv:1012.3096v1`.
[5] C. Cibils, A quiver quantum group. *Comm. Math. Phys.* **157** (1993), 459–477.
[6] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics, Vol. XI, Interscience Publishers, a division of John Wiley & Sons, New York, 1962.
[7] C. W. Curtis, I. Reiner, *Methods of Representation Theory, Volume I*, Wiley 1981.
[8] S. Dăscălescu, C. Năstăsescu, S. Raianu, Hopf algebras. An introduction. *Monographs and Textbooks in Pure and Applied Mathematics* **235**. Marcel Dekker, Inc., New York, 2001.
[9] D. Dummit and R.M. Foote, *Abstract algebra*, 3rd edition. John Wiley & Sons, Inc., Hoboken, NJ, 2004.
[10] P. Etingof, S. Gelaki, D. Nikshych, and V. Ostrik, Tensor categories, *Mathematical Surveys and Monographs* **205**. Amer. Math. Soc., Providence, RI, 2015.
[11] C. Gaetz, Critical groups of group representations. *Lin. Alg. Appl.* **508** (2016), 91–99.
[12] D. Grinberg, math.stackexchange answer #2147742 ("Nonsingular M-matrices are nonsingular"), `http://math.stackexchange.com/q/2147742`
[13] J.E. Humphreys, Modular representations of finite groups of Lie type. *London Mathematical Society Lecture Note Series* **326**. Cambridge University Press, Cambridge, 2006.
[14] G. James and A. Kerber, The representation theory of the symmetric group. *Encyclopedia of Mathematics and its Applications* **16**. Addison-Wesley Publishing Co., Reading, Mass., 1981.
[15] G. James and M. Liebeck, *Representations and characters of groups*, Cambridge University Press, New York, 2001.
[16] D. Lorenzini, Smith normal form and Laplacians. *J. Combin. Theory Ser. B* **98** (2008), 1271–1300.
[17] A.E. Holroyd, L. Levine, K. Mészáros, Y. Peres, J. Propp, and D.B. Wilson, Chip-Firing and Rotor-Routing on Directed Graphs, *In and Out of Equilibrium 2, "Progress in Probability"* **60** (2008), 331–364. Updated version available at `arXiv:0801.3306v4`
[18] L. Li and Y. Zhang, The Green rings of the generalized Taft Hopf algebras. Hopf algebras and tensor categories, 275–288, *Contemp. Math.* **585**, Amer. Math. Soc., Providence, RI, 2013.
[19] M. Lorenz, Representations of Finite-Dimensional Hopf Algebras. *Journal of Algebra* **188** (1997), 476–505.
[20] S. Montgomery, Hopf algebras and their actions on rings. *CBMS Regional Conference Series in Mathematics* **82**, 1993.
[21] W.D. Nichols, Bialgebras of type one. *Comm. Algebra* **6** (1978), 1521–1552.
[22] B. Pareigis, When Hopf Algebras Are Frobenius Algebras. *Journal of Algebra* **18** (1971), 588–596.
[23] D. S. Passman, D. Quinn, Burnside's Theorem for Hopf algebras. *Proceedings of the American Mathematical Society* **123** (1995), 327–333.
[24] D. Perkinson, J. Perlman, and J. Wilmes, Primer for the algebraic geometry of sandpiles. *arXiv preprint arXiv:1112.6163v2*, 2011. `arXiv:1112.6163v2`
[25] R.J. Plemmons, M-matrix characterizations. I. Nonsingular M-matrices. *Linear Algebra and Appl.* **18** (1977), 175–188.
[26] D.E. Radford, Hopf Algebras. *Series on Knots and Everything* **49**, World Scientific 2012.
[27] M.A. Rieffel, Burnside's theorem for representations of Hopf algebras. *J. Algebra* **6** (1967), 123–130.
[28] H.-J. Schneider, Lectures on Hopf algebras, lecture notes, 31 March 2006. `http://www.famaf.unc.edu.ar/series/pdf/pdfBMat/BMat31.pdf`

[29] J.-P. Serre, Linear Representations of Finite Groups, *Graduate Texts in Mathematics* **42**, Springer 1977.
[30] R. Steinberg, Complete sets of representations of algebras. *Proc. Amer. Math. Soc.* **13** (1962), 746–747.
[31] P. Webb, A Course in Finite Group Representation Theory. *Cambridge Studies in Advanced Mathematics* **161**, Cambridge University Press, 2016.
[32] S.J. Witherspoon, Cohomology of Hopf algebras. lecture notes, 10 January 2017. http://www.math.tamu.edu/~sjw/pub/hopf-cohom.pdf

School of Mathematics, University of Minnesota, 206 Church St. SE, Minneapolis, MN 55455
Email address: darijgrinberg@gmail.com

Department of Mathematics and Statistics, University of Nebraska at Kearney, Kearney, NE 68849
Email address: huangj2@unk.edu

School of Mathematics, University of Minnesota, 206 Church St. SE, Minneapolis, MN 55455
Email address: reiner@math.umn.edu