博士后研究报告

论 文 题 目: Hopf代数的Green环及其数值不变量

作 者 姓 名: 王 志 华

专 业 名 称: 基 础 数 学

研 究 方 向: 范 畴 论 与 环 论

合 作 导 师: 刘公祥 教授

二零一九 年 十 月

报告日期: **2019** 年 **10** 月

合 作 导 师: （签字）

Post-doctoral Research Report

Green Rings and Numerical Invariants of Hopf Algebras

Wang Zhihua

Worked with Professor Liu Gongxiang

Fundamental Mathematics

Department of Mathematics, Nanjing University

October, 2019

报 告 题 目: **Hopf代数的Green环及其数值不变量**

基 础 数 学 专 业 博 士 后 姓 名: 王 志 华

合 作 导 师 (姓 名、职 称): 刘 公 祥 教 授

摘 要

在Hopf代数的表示范畴的monoidal结构的研究上, 人们必须考虑将两个对象的张量积分解为不可分解模的直和. 一般而言, 这种分解方法鲜为人知. 为了解决这类问题, 人们把表示的张量积的直和分解式转换为Green环层面的元素乘积公式, 进而研究Green环的环论性质. 本文主要研究有限表示型Hopf代数H的Green环$r(H)$及其Frobenius性质. 这一性质使得人们可以在Green环层面定义Green环(或表示范畴)的数值不变量: Casimir数. 结果表明$r(H)$的Casimir数不为0当且仅当$r(H)$是Jacobson 半单环, $r(H)$ 的Casimir数在域K上不为0当且仅当域K上的Green代数$r(H)\otimes_{\mathbb{Z}}K$为Jacobson半单代数. 本文通过计算一些Green环的Casimir数进而完全刻划了这些Green代数的Jacobson根. 对于fusion范畴的Grothendieck环, 类似可以定义上面的Csimir数. 不同的是Grothendieck环上面的Casimir数总是正整数, 而且可以用来判别pivotal fusion范畴何时是非退化的. 特别地, 如果$\mathcal{C}$为复数域上的spherical fusion范畴, 其Casimir数与Frobenius-Schur指数具有相同的素因子. 这一结果可被视为spherical fusion范畴上的柯西定理的另一版本.

全文分为五章.

第一章给出了一些主要概念和预备知识.

第二章, 利用双线性型这一工具研究有限维Hopf代数的Green环. 当Hopf代数是有限表示型时, 其Green环为整数环$\mathbb{Z}$上的Frobenius代数, 该Frobenius代数的对偶基与Hopf代数表示范畴的几乎可裂序列相关. 第二章还研究了Green环的一些环论性质.

第三章, 研究稳定Green环, 并在上面定义新的双线性型, 刻划了该双线性型何时是非退化的. 如果该双线性型是非退化的, 那么复数域上的稳定Green代数成为类群代数, 并进一步构成双-Frobenius代数.

第四章, 探讨何时Green环$r(H)$, 或Green代数$r(H)\otimes_{\mathbb{Z}}K$是Jacobson半单的. 结果表明Green环$r(H)$上的Casimir数不为0时, Green环$r(H)$ 是Jacobson半单环; Casimir数在域K上不为0时, Green代数$r(H)\otimes_{\mathbb{Z}}K$是Jacobson半单代数. 当Hopf代数是特征为p的域$\Bbbk$上的p阶循环群的群代数$\Bbbk G$时, 计算得知其Casimir数为$2p^2$. 基于此, 完全刻划了任意域K上的Green代数$r(\Bbbk G)\otimes_{\mathbb{Z}}K$的Jacobson根.

第五章, 针对fusion范畴$\mathcal{C}$定义了Grothendieck环$\mathrm{Gr}(\mathcal{C})$上的Casimir数以及另外两个数值不变量. 这些不变量均为正整数并且具备如下性质: 域K上的Grothendieck代数$\mathrm{Gr}(\mathcal{C})\otimes_{\mathbb{Z}}K$为半单代数当且仅当这些数值不变量中任何之一在域$K$中不为0. 这就意味着这些数值不变量具有相同的素因子组成. 对于秩为$n+1$的Verlinde modular范畴$\mathcal{C}$, 经过计算其Casimir数为$2n+4$. 因而Grothendieck代数$\mathrm{Gr}(\mathcal{C})\otimes_{\mathbb{Z}}K$为半单代数当且仅当$2n+4$在域$K$中不为0. 换言之, 第二类型的$(n+1)$-次Dickson多项式$E_{n+1}(X)$在多项式代数$K[X]$中没有重因式. 如果$2n+4$在某一域$K$中为0, 本文以生成子的形式给出了Grothendieck代数$\mathrm{Gr}(\mathcal{C})\otimes_{\mathbb{Z}}K$的Jacobson根. 对于pivotal fusion范畴$\mathcal{C}$, 证明了$\mathcal{C}$是非退化的当且仅当其Casimir数在基域$\Bbbk$上不为0. 对于复数域上的spherical fusion范畴, 其Casimir数与另一数值不变量Frobenius-Schur指数具有相同的素因子. 这一结果可被视为spherical fusion范畴上的柯西定理的另一版本.

关键词: Hopf代数; Green环; Frobenius代数; Jacobson根; Casimir数; 双-Frobenius代数; Verlinde modular范畴; fusion范畴; Grothendieck环; Frobenius-Schur指数.

THESIS: Green Rings and Numerical Invariants of Hopf Algebras

SPECIALIZATION: Fundamental Mathematics

POSTDOCTORAL: Wang Zhihua

CO-SUPERVISOR: Professor Liu Gongxiang

Abstract

In the study of the monoidal structure of a representation category of a Hopf algebra H, one has to consider the decompositions of the tensor product of objects into indecomposables. However, in general, very little is known about how a tensor product of two indecomposables decomposes into a direct sum of indecomposables. One method of addressing this problem is to consider the tensor product as the multiplication of the Green ring $r(H)$ of H, and to study the ring-theoretical properties of the Green ring. In this paper, we study the Frobenius property of $r(H)$ if H is of finite representation type. This enables us to define a numerical invariant, namely, the Casimir number of $r(H)$. We show that this number is not zero if and only if the Green ring $r(H)$ is Jacobson semisimple and this number is not zero in a field K if and only if the Green algebra $r(H) \otimes_{\mathbb{Z}} K$ is semisimple. We compute the Casimir numbers of some Green rings and describe their Jacobson radicals of those Green algebras. For the Grothendieck ring of a fusion category, its Casimir number can be defined similarly. This number is a positive integer and can be used to detect when a pivotal fusion category is non-degenerate. In particular, if $\mathcal{C}$ is a spherical fusion category over the field of complex numbers, its Casimir number and the Frobenius-Schur exponent share the same prime factors. This may be thought of as another statement of the Cauchy theorem for spherical fusion categories.

This paper is divided into five chapters.

In Chapter 1, main notations and preliminaries are stated.

In Chapter 2, we study the Green ring of a finite dimensional Hopf algebra by means of bilinear forms. We show that the Green ring of a Hopf algebra of finite representation type is a Frobenius algebra over $\mathbb{Z}$ with a dual basis associated to almost

split sequences. We next study some ring theoretic properties of the Green ring.

In Chapter 3, on the stable Green ring we define a new bilinear form which is more accurate to determine the bi-Frobenius algebra structure on the stable Green ring. We show that the complexified stable Green algebra is a group-like algebra, and hence a bi-Frobenius algebra, if the bilinear form on the stable Green ring is non-degenerate.

In Chapter 4, we first consider the question of when the Green ring $r(H)$, or the Green algebra $r(H) \otimes_{\mathbb{Z}} K$ over a field K, is Jacobson semisimple. It turns out that $r(H) \otimes_{\mathbb{Z}} K$ is Jacobson semisimple if and only if the Casimir number of $r(H)$ is not zero in K. For the Green ring $r(H)$ itself, $r(H)$ is Jacobson semisimple if and only if the Casimir number of $r(H)$ is not zero. Then we focus on the case where $H = \Bbbk G$ for a cyclic group G of order p over a field $\Bbbk$ of characteristic p. In this case, the Casimir number of $\Bbbk G$ is shown to be $2p^2$. This leads to a complete description of the Jacobson radical of the Green algebra $r(\Bbbk G) \otimes_{\mathbb{Z}} K$ over any field K.

In Chapter 5, we define the Casimir number and another two numerical invariants of a fusion category $\mathcal{C}$. These numerical invariants are all positive integers and admit the property that the Grothendieck algebra $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ over any field K is semisimple if and only if any of these numbers is not zero in K. This means that all these numbers have the same prime factors. If $\mathcal{C}$ is a Verlinde modular category of rank $n+1$, its Casimir number is calculated to be $2n+4$. It follows that the Grothendieck algebra $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ over a field K is semisimple if and only if $2n+4$ is a unit in K. This is equivalent to saying that the $(n+1)$-th Dickson polynomial $E_{n+1}(X)$ of the second kind has no multiple factors in $K[X]$. If $2n+4$ is zero in K, the Jacobson radical of $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ is described explicitly in terms of generators. If moreover $\mathcal{C}$ is pivotal, one obtains a criterion that $\mathcal{C}$ is non-degenerate if and only if the Casimir number of $\mathcal{C}$ is not zero in $\Bbbk$. For the case that $\mathcal{C}$ is a spherical fusion category over the field $\mathbb{C}$ of complex numbers, the Casimir number and the Frobenius-Schur exponent of $\mathcal{C}$ share the same prime factors. This may be thought of as another statement of the Cauchy theorem for spherical fusion categories.

Keywords: Hopf algebra; Green ring; Frobenius algebra; Jacobson radical; Casimir number; Bi-Frobenius algebra; Verlinde modular category; fusion category; Grothendieck ring; Frobenius-Schur exponent.

CONTENTS

摘　要 **i**

Abstract **iii**

Chapter 1 Preliminaries **1**

1.1 Bi-Frobenius algebras 1

1.2 Auslander-Reiten theory 6

Chapter 2 The Green rings of Hopf algebras **9**

2.1 Quantum traces 10

2.2 Bilinear forms on Green rings 20

2.3 Some ring theoretic properties of Green rings 28

Chapter 3 The stable Green rings of Hopf algebras **37**

3.1 The stable Green rings 37

3.2 Bi-Frobenius algebra structure 42

3.3 Applications to Radford Hopf algebras 45

Chapter 4 The Casimir numbers of Hopf algebras **50**

4.1 Introduction 50

4.2 The Jacobson semisimplicity of Green rings 52

4.3 The Casimir number of a finite group 55

Chapter 5 The Casimir numbers of fusion categories **66**

5.1 Introduction 66

5.2 Numerical invariants 68

5.3 The Casimir numbers of Verlinde modular categories 74

5.4 Prime factors of Casimir numbers 83

5.5 Casimir numbers vs. Frobenius-Schur exponents 88

REFERENCES **92**

致 谢 99

Chapter 1 Preliminaries

In this chapter, we first recall the definitions of a Frobenius algebra, a bi-Frobenius algebra and a group-like algebra. After that we shall collect concepts and results from the Auslander-Reiten theory which will be used in other chapters.

§1.1 Bi-Frobenius algebras

Frobenius algebras. Frobenius algebras occur in many different fields of mathematics, such as topological quantum field theory [1], Hopf algebras and quantum Yang-Baxter equations [6, 42]. In the following, the notion of a Frobenius algebra is defined directly over a field $\Bbbk$, although it can also be defined over a commutative ring (e.g., [40, 47]).

Let A be a finite dimensional $\Bbbk$-algebra. We denote by the dual $A^* := \mathrm{Hom}_{\Bbbk}(A, \Bbbk)$. Then A^* has a natural A-A-bimodule structure given by

$$(a \rightharpoonup f \leftharpoonup b)(c) = f(bca), \text{ for } a, b, c \in A,\ f \in A^*.$$

Definition 1.1.1 *(cf. [17, 18]) The pair (A, ϕ) is called a Frobenius algebra provided that $\phi \in A^*$ such that the right A-module morphism $\theta_A : A \to A^*,\ a \mapsto \phi \leftharpoonup a$ is bijective; or equivalently, the left A-module morphism ${}_A\theta : A \to A^*,\ a \mapsto a \rightharpoonup \phi$ is bijective.*

The linear form ϕ is called a *Frobenius homomorphism*. Moreover, A is a *symmetric algebra* provided that A is isomorphic to A^* as A-A-bimodules.

Remark 1.1.2 *If (A, ϕ) is a Frobenius algebra, then $\langle a, b\rangle := \phi(ab)$ for $a, b \in A$, is a non-degenerate associative bilinear form over A. Conversely, if A is equipped with a non-degenerate associative bilinear form $\langle -, -\rangle$, then $\phi := \langle 1, -\rangle$ is a Frobenius homomorphism of A [1, Proposition 1]. Accordingly, one of the equivalent definitions of a Frobenius algebra is that A is Frobenius if and only if A is equipped with a non-degenerate bilinear form $\langle -, -\rangle : A \times A \to \Bbbk$ satisfying the associative $\langle ab, c\rangle = \langle a, bc\rangle$,* *for all $a, b, c \in A$. Moreover, if the bilinear form is symmetric $\langle a, b\rangle = \langle b, a\rangle$ for $a, b \in A$, then A is a symmetric algebra.*

We refer to [21,40,47] for the following basic properties of Frobenius algebras. The $\Bbbk$-linear map θ_A given in Definition 1.1.1 induces the $\Bbbk$-linear isomorphism

$$\Theta : A \otimes A \xrightarrow{id\otimes\theta_A} A \otimes A^* \cong \mathrm{End}_{\Bbbk}(A).$$

Hence there exists a unique element $\sum_{i=1}^{n} a_i \otimes b_i \in A \otimes A$ such that $\Theta(\sum_{i=1}^{n} a_i \otimes b_i) = id_A$. The set $\{a_i, b_i \mid 1 \leq i \leq n\}$ is called a pair of *dual bases* of (A, ϕ). Moreover, (A, ϕ) is symmetric if and only if

$$\sum_{i=1}^{n} a_i \otimes b_i = \sum_{i=1}^{n} b_i \otimes a_i.$$

According to the map Θ given above, we have the following:

$$x = \sum_{i=1}^{n} a_i\phi(b_i x) = \sum_{i=1}^{n} a_i\langle b_i, x\rangle, \text{ for } x \in A, \tag{1.1}$$

or equivalently,

$$x = \sum_{i=1}^{n} \phi(x a_i)b_i = \sum_{i=1}^{n}\langle x, a_i\rangle b_i, \text{ for } x \in A. \tag{1.2}$$

In fact, both of them is equivalent to

$$\langle x, y\rangle = \sum_{i=1}^{n}\langle x, a_i\rangle\langle b_i, y\rangle \tag{1.3}$$

for all $x, y \in A$ (cf. [47]).

Example 1.1.3 *Let H be a finite dimensional Hopf algebra over the field $\Bbbk$. Let $\lambda \in H^*$ be a non-zero left integral and $\Lambda \in H$ a right integral such that $\lambda(\Lambda) = 1$. Then (H, λ) is a Frobenius algebra with a pair of dual bases $\{S(\Lambda_1), \Lambda_2\}$, where $\triangle(\Lambda) = \sum \Lambda_1 \otimes \Lambda_2$. In a similar fashion, one can see that if $\gamma \in H^*$ is a non-zero right integral, then there exists a left integral $\Gamma \in H$ such that $\gamma(\Gamma) = 1$. Then (H, γ) is a Frobenius algebra with a pair of dual bases $\{\Gamma_1, S(\Gamma_2)\}$, where $\triangle(\Gamma) = \sum \Gamma_1 \otimes \Gamma_2$ (cf. [17]). As shown in [46] that H is symmetric if and only if H is unimodular and the square of antipode is inner.*

Let A be a Frobenius algebra over $\mathbb{Z}$. The *Casimir operator* of A (see e.g. [47, Section 3.1]) is the map c from A to its center $Z(A)$ defined by

$$c(a) = \sum_{i=1}^{n} b_i a a_i \text{ for } a \in A.$$

The map c is independent of the choice of a pair of dual bases $\{a_i, b_i \mid 1 \leq i \leq n\}$, because the dual bases depend only on the bilinear form $\langle -, - \rangle$, see [47, Section 1.2.2]. The element $c(1)$ is called the *Casimir element* of A and it depends on $\langle -, - \rangle$ only up to a central unit, see [47, Section 1.2.5]. The image $\operatorname{Im} c$ of c is an ideal of $Z(A)$, called the *Casimir ideal* of A. It does not depend on the choice of the bilinear form, see [47, Section 3.2]. The intersection of $\operatorname{Im} c$ and $\mathbb{Z}$ is an ideal of $\mathbb{Z}$, thus a principal ideal of $\mathbb{Z}$ generated by a non-negative integer. We call this integer the *Casimir number* of A. Obviously, the Casimir number of A does not depend on the choice of the bilinear form on A.

Any $\mathbb{Z}$-algebra morphism $\varepsilon : A \to \mathbb{Z}$ is called an *augmentation* of A. Suppose that the Frobenius $\mathbb{Z}$-algebra A has an augmentation ε. Then any element t of A satisfying $at = \varepsilon(a)t$ for all $a \in A$ is called a *left integral* of A. Similarly, if $ta = \varepsilon(a)t$ for all $a \in R$, then t is called a *right integral* of A. All left integrals of A with respect to ε form a $\mathbb{Z}$-module of rank one generated by $\sum_{i=1}^{n} \varepsilon(a_i)b_i$. Similarly, all right integrals of A with respect to ε form a $\mathbb{Z}$-module of rank one generated by $\sum_{i=1}^{n} \varepsilon(b_i)a_i$, see [47, Section 4.1]. If the set of left integrals of A coincides with the set of right ones, then A is called *unimodular*.

Bi-Frobenius algebras. Let C be a coalgebra over the field $\Bbbk$. Then C has a natural structure of left and right C^*-module under the left action $f \rightharpoonup c = \sum c_1 f(c_2)$, and the right action $c \leftharpoonup f = \sum f(c_1)c_2$, for any $f \in C^*$ and $c \in C$ with $\triangle(c) = \sum c_1 \otimes c_2$. Moreover, for any $c \in C$, the induced maps $c \leftharpoonup : C^* \to C$ and $\rightharpoonup c : C^* \to C$ are morphisms of right and left C^*-modules respectively.

Definition 1.1.4 *(cf. [21,23]) A Frobenius coalgebra is a pair (C, t) where C is a finite dimensional coalgebra and $t \in C$ such that the morphism $t \leftharpoonup : C^* \to C$, $f \mapsto t \leftharpoonup f$ is bijective; or equivalently, the morphism $\rightharpoonup t : C^* \to C$, $f \mapsto f \rightharpoonup t$ is bijective.*

The notion of a Frobenius coalgebra has a nice characterization that is analogue to the characterizations of a Frobenius algebras [20, 22].

The concept of a bi-Frobenius algebra was introduced by Doi and Takeuchi in [23] and further investigated in [20, 22] as a natural generalized of finite dimensional Hopf algebras.

Definition 1.1.5 *(cf. [22]) Let H be a finite dimensional algebra and coalgebra over the field $\Bbbk$, $\phi \in H^*$, $t \in H$. Define the map S by*

$$S : H \to H,\ S(x) = t \leftharpoonup (x \rightharpoonup \phi) = \phi(t_1 x)t_2.$$

The quadruple (H, ϕ, t, S) is called a bi-Frobenius algebra if the following hold:

$(BF1)$ *The counit ε of the coalgebra H is an algebra morphism.*

$(BF2)$ *The unity 1 is a group-like element of H.*

$(BF3)$ *(H, ϕ) is a Frobenius algebra.*

$(BF4)$ *(H, t) is a Frobenius coalgebra.*

$(BF5)$ *S is an anti-algebra and anti-coalgebra morphism, i.e., $S(ab) = S(b)S(a)$, $S(1) = 1$ and $\Delta(S(a)) = \sum S(a_2) \otimes S(a_1)$, $\varepsilon(S(a)) = \varepsilon(a)$.*

The map S given above is necessarily bijective [23], it is called the *antipode* of the bi-Frobenius algebra H. It does not mean a convolution inverse of identity. This is true in the particular situation of Hopf algebras. A pair of dual bases of (H, ϕ, t, S) is given by $\{S^{-1}(t_2), t_1\}$ [21]. Since H is necessary finite dimensional, the $\Bbbk$-linear dual H^* is also an algebra and coalgebra. The comultiplication in H^* is given by

$$\triangle(f)(a \otimes b) = f(ab),$$

for $f \in H^*$ and $a, b \in H$. It can be checked that (H^*, t, ϕ, S^*) becomes a bi-Frobenius algebra. We call it the *dual bi-Frobenius algebra* of H.

Example 1.1.6 *Let H be a finite dimensional Hopf algebra. Choose the right integral $\gamma \in H^*$ and the left integral $\Gamma \in H$ such that $\gamma(\Gamma) = 1$. Then (H, γ, Γ, S) becomes a bi-Frobenius algebra.*

It is interesting to construct bi-Frobenius algebras that are not Hopf algebras. Using known results on the existence of large Hadamard matrices, the author in [36] constructed a class of bi-Frobenius algebras of arbitrarily large dimension satisfying the additional condition

$$S * id = id * S = \varepsilon \tag{1.4}$$

and that are not Hopf algebras. This family of bi-Frobenius algebras satisfying the condition (1.4) is also studied in [59]. There are many other approaches to construct bi-Frobenius algebras that are not Hopf algebras, see e.g., [66, 70]. As we shall see that one of main results of this paper is that the stable Green algebras of certain finite dimensional Hopf algebras are bi-Frobenius algebras that are not Hopf algebras.

Group-like algebras. The notion of a group-like algebra was introduced by Doi in [20] generalizing the group algebra of a finite group and a scheme ring (Bose-Mesner algebra) of a non-commutative association scheme.

Definition 1.1.7 *Let $(A, \varepsilon, \mathbf{b}, *)$ be a quadruple, where A is a finite dimensional algebra over a field $\Bbbk$ with unit 1, ε is an algebra morphism from A to $\Bbbk$, the set $\mathbf{b} = \{b_i \mid i \in I\}$ is a $\Bbbk$-basis of A such that $0 \in I$ and $b_0 = 1$, and $*$ is an involution of the index set I. Then $(A, \varepsilon, \mathbf{b}, *)$ is called a group-like algebra if the following hold:*

(G1) $\varepsilon(b_i) = \varepsilon(b_{i^*}) \neq 0$ *for all* $i \in I$.

(G2) $p_{ij}^k = p_{j^*i^*}^{k^*}$ *for all* $i, j, k \in I$*, where all* p_{ij}^k *are the structure constants for* $\mathbf{b}$ *defined by* $b_i b_j = \sum_{k\in I} p_{ij}^k b_k$.

(G3) $p_{ij}^0 = \delta_{i,j^*}\varepsilon(b_i)$ *for all* $i, j \in I$.

Remark 1.1.8 (1) *Let $(A, \varepsilon, \mathbf{b}, *)$ be a group-like algebra. Then A becomes a coalgebra with a comultiplication given by $\triangle(b_i) = \frac{1}{\varepsilon(b_i)} b_i \otimes b_i$, see [20, Remark 3.2]. Let $\phi \in A^*$ such that $\phi(b_i) = \delta_{0,i}$ and $t = \sum_{i\in I} b_i$. Define the $\Bbbk$-linear map S from A to itself by $S(b_i) = b_{i^*}$ for any $i \in I$. Then (A, ϕ, t, S) becomes a bi-Frobenius algebra with a pair of dual bases $\{b_i, \frac{b_{i^*}}{\varepsilon(b_i)} \mid i \in I\}$.*

(2) *A group-like algebra is not a Hopf algebra in general. If it is, it must be a group algebra, see [36, Corollary 2]. Thus, a bi-Frobenius algebra coming from a group-like algebra is not a Hopf algebra if the underlying algebra is not a group algebra.*

Group-like algebras have some special properties (see e.g., [20]). Group-like algebras of dimension 2 and 3 have been determined in [20]. For group-like algebras of dimension 4, we refer to [21]. If a group-like algebra is also a Hopf algebra, then it needs to be a group algebra [36, Corollary 2]. Because of this, a bi-Frobenius algebra coming from a group-like algebra is not a Hopf algebra if the algebra itself is not a group algebra.

§1.2 Auslander-Reiten theory

The aim of this section is to collect several results about Auslander-Reiten theory which are needed in this paper. For these concepts, we refer to the textbooks [3, 4].

Auslander-Reiten translate. Let A be a finite dimensional algebra over $\Bbbk$ and A-mod (resp. mod-A) the finite dimensional left (resp. right) module category of A. There are several ingredients that go into the topic of Auslander-Reiten translate of A-mod. One is the functor $D : A\text{-mod} \to \text{mod-}A$ which is defined as $DX = \mathrm{Hom}_{\Bbbk}(X, \Bbbk)$, for $X \in A$-mod. We also want to use another functor $\mathrm{Hom}_A(-, A) : A\text{-mod} \to \text{mod-}A$. If M is a left A-module, then $\mathrm{Hom}_A(M, A)$ is a right A-module given by $(fa)(u) = f(u)a$ for $a \in A$, $u \in M$ and $f \in \mathrm{Hom}_A(M, A)$.

Let M be in A-mod and $P_0 \xrightarrow{p_0} M \to 0$ the projective cover of M. We denote by $P_1 \xrightarrow{p_1} \ker p_0$ the projective cover of $\ker p_0$. Then the sequence $P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} M \to 0$ is called a *minimal projective presentation* of M. One can continue the process forever and get what is called a *minimal projective resolution*, but we are only interested in the P_1 and P_0 terms.

Applying the functor $\mathrm{Hom}_A(-, A)$ to $P_1 \xrightarrow{p_1} P_0$, one obtains a right A-module map $p_1^* : \mathrm{Hom}_A(P_0, A) \to \mathrm{Hom}_A(P_1, A)$. The *transpose* of M is defined to be $\mathrm{Tr}(M) := \mathrm{coker}(p_1^*)$ and the *Auslander-Reiten translate* of M is $\mathrm{DTr}(M)$, the dual of transpose of left A-module M.

Almost split sequences. In this subsection we give an introduction to almost split sequences, a special type of short exact sequences of modules which play a central role in the representation theory of artin algebras.

Let X and Y be two A-modules. The morphism $f : M \to N$ is a *split monomorphism* if there exists $g : N \to M$ such that $g \circ f = id_M$, and $f : M \to N$ is a *split epimorphism* if there exists $g : N \to M$ such that $f \circ g = id_N$.

In the following, we introduce some special morphisms, called left and right almost split morphisms, which gives rise in a natural way to the notion of an almost split sequence.

Definition 1.2.1 *The map $f : M \to N$ is called left almost split if f is not a split monomorphism and if there is $g : M \to X$ with g not a split monomorphism, then there is $h : N \to X$ such that $h \circ f = g$. Dually, $f : M \to N$ is called right almost split if f is not split epimorphism and if there is $g : Y \to N$ with g not split epimorphism, then there is $h : Y \to M$ such that $f \circ h = g$.*

We also need the notion of minimality.

Definition 1.2.2 *The map $f : M \to N$ is called left minimal if for all $h : N \to N$ with $h \circ f = f$, then h is an isomorphism. Dually, $f : M \to N$ is called right minimal if for all $h : M \to M$ with $f \circ h = f$, then h is an isomorphism.*

Finally, we say that $f : M \to N$ is *left minimal almost split* if f is both left minimal and left almost split. Similarly, we have the notion of *right minimal almost split*.

Definition 1.2.3 *A short exact sequence $0 \to X \xrightarrow{f} M \xrightarrow{g} Y \to 0$ is called almost split if f is left minimal almost split and g is right minimal almost split.*

The following proposition [4, Proposition 1.14, ChV] gives many equivalent conditions for a short exact sequence to be almost split.

Proposition 1.2.4 *The following are equivalent for a short exact sequence $0 \to X \xrightarrow{f} M \xrightarrow{g} Y \to 0$.*

(1) *The sequence is an almost split sequence.*

(2) *The morphism f is left minimal almost split.*

(3) *The morphism g is right minimal almost split.*

(4) *X is indecomposable and g is right almost split.*

(5) *Y is indecomposable and f is left almost split.*

(6) *X is isomorphic to $DTrY$ and g is right almost split.*

(7) *Y is isomorphic to $TrDX$ and f is left almost split.*

We end with an introduction to the existence and uniqueness of almost split sequence.

Theorem 1.2.5 *[4, Theorem1.15, ChV] We have the following existence of almost split sequence:*

(1) *If Y is an indecomposable non-projective module, then there is an almost split sequence $0 \to X \to M \to Y \to 0$.*

(2) *If X is an indecomposable non-injective module, then there is an almost split sequence $0 \to X \to M \to Y \to 0$.*

An almost split sequence is determined uniquely by either of its end terms in the following sense (cf. [4, Theorem1.16, ChV]).

Theorem 1.2.6 *The following are equivalent for two almost split sequences $0 \to X \xrightarrow{f} M \xrightarrow{g} Y \to 0$ and $0 \to X' \xrightarrow{f'} M' \xrightarrow{g'} Y' \to 0$.*

(1) $X \cong X'$.

(2) $Y \cong Y'$.

(3) *The two sequences are isomorphic (i.e., there is a commutative diagram of the following form with the vertical morphisms isomorphisms)*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X & \xrightarrow{f} & M & \xrightarrow{g} & Y & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & X' & \xrightarrow{f'} & M' & \xrightarrow{g'} & Y' & \longrightarrow & 0. \end{array}$$

Chapter 2 The Green rings of Hopf algebras

Let H be a finite dimensional Hopf algebra and H-mod the category of finite dimensional (left) H-modules. In Section 2.1, we use quantum traces of morphisms of H-modules to characterize when the trivial module $\Bbbk$ is a direct summand of the decomposition of tensor product of any two indecomposable modules (see Theorem 2.1.7). Consequently, we answer the question raised by Cibils [16, Remark 5.8]. In particular, we apply techniques from [35, 73] to determine whether or not the trivial module $\Bbbk$ appears in the decomposition of the tensor product $X \otimes X^*$ (resp. $X^* \otimes X$) for any indecomposable module X. Most results stated in this section are useful for next sections.

In Section 2.2, we follow the approach of [8] and impose three bilinear forms on the Green ring $r(H)$ of the Hopf algebra H. One of them is the bilinear form determined by $\langle [X], [Y] \rangle_1 = \dim_{\Bbbk} \mathrm{Hom}_H(X, Y)$. Another form is $\langle [X], [Y] \rangle_2 = \dim_{\Bbbk} \mathcal{P}(X, Y)$, where $\mathcal{P}(X, Y)$ is the space of morphisms from X to Y factoring through a projective module. We show that the two forms are both non-degenerate and they are essentially the same up to a unit. The third form is $\langle [X], [Y] \rangle_3 = \langle [X], [Y] \rangle_1 - \langle [X], [Y] \rangle_2$. The radical of the form $\langle -, - \rangle_3$ contains the projective ideal $\mathcal{P}$ of $r(H)$ generated by projective H-modules. Under the assumption that H is of finite representation type, we prove that the radical of the form $\langle -, - \rangle_3$ is equal to $\mathcal{P}$ if and only if there are no periodic H-modules of even period.

In Section 2.3, we consider the form $([X], [Y]) := \langle [X], [Y^*] \rangle_1$ on the Green ring $r(H)$ and use the form $(-, -)$ to obtain some results about $r(H)$. The form $(-, -)$ is associative and non-degenerate, and hence $r(H)$ is a Frobenius algebra over $\mathbb{Z}$ if H is of finite representation type. The dual basis of $r(H)$ with respect to the form $(-, -)$ can be described partly by almost split sequences of H-modules. We use the form $(-, -)$ to give several one-sided ideals of $r(H)$ and these ideals provide a little more information about the Jacobson radical and central primitive idempotents of $r(H)$. It is known that the Grothendieck ring $G_0(H)$ of H is a quotient ring of $r(H)$. We describe this quotient ring clearly: $r(H)/\mathcal{P}^{\perp} \cong G_0(H)$, where $\mathcal{P}^{\perp}$ is orthogonal to the projective ideal $\mathcal{P}$ with respect to the form $(-,-)$. This isomorphism will be used in next chapter to characterize when the Jacobson radical of $r(H)$ is equal to the intersection $\mathcal{P}\cap\mathcal{P}^{\perp}$.

Throughout, H is an arbitrary finite dimensional Hopf algebra over an algebraically closed field $\Bbbk$; all H-modules considered here are objects in H-mod, the category of finite dimensional left H-modules. The tensor product $\otimes$ stands for $\otimes_{\Bbbk}$. The notation $M \mid X\otimes Y$ (resp. $M\nmid X\otimes Y$) means that M is (resp. is not) a direct summand of $X\otimes Y$. For the theory of Hopf algebras, we refer to [49, 64].

§2.1 Quantum traces

In the study of the Green ring $r(H)$ of a Hopf algebra H, one of difficult problems is to determine whether or not the trivial module $\Bbbk$ appears in the decomposition of tensor product $X\otimes Y$ for indecomposable modules X and Y. This problem has already been solved in the case of group algebras by Benson and Carlson [7, Theorem 2.1], in the case of involutory Hopf algebras in terms of splitting trace modules [35], and in the case of Hopf algebras with the square of antipode being inner [73, Theorem 2.4]. Motivated by these works, in this section we shall make use of the notion of quantum traces to solve the aforementioned problem for any finite dimension Hopf algebra. In particular, we will look at the special case $X\otimes X^*$ (or $X^*\otimes X$) for X being indecomposable, and give various characterizations for $\Bbbk \mid X\otimes X^*$ or not, which will be used in the next section.

Recall that the Hom-space $\mathrm{Hom}_{\Bbbk}(X,Y)$ is an H-module given by $(hf)(x)=\sum h_1f(S(h_2)x)$, for $x\in X$, $f\in\mathrm{Hom}_{\Bbbk}(X,Y)$ and $h\in H$ with the comultiplication $\triangle(h)=\sum h_1\otimes h_2$. In the special case where Y is the trivial module $\Bbbk$, then $X^*:=\mathrm{Hom}_{\Bbbk}(X,\Bbbk)$ is an H-module given by $(hf)(x)=f(S(h)x)$, for $h\in H$, $x\in X$ and $f\in X^*$. The *evaluation* of X is the morphism $\mathrm{ev}_X: X^*\otimes X\to\Bbbk$ given by $\mathrm{ev}_X(f\otimes x)=f(x)$. The *coevaluation* of X is the morphism $\mathrm{coev}_X:\Bbbk\to X\otimes X^*$ defined by $\mathrm{coev}_X(1)=\sum_i x_i\otimes x_i^*$, where $\{x_i\}$ is a basis of X and $\{x_i^*\}$ is the dual basis in X^*.

The *left quantum trace* of $\theta\in\mathrm{Hom}_H(X,X^{**})$ is defined to be the following composition:

$$\mathrm{Tr}_X^L(\theta) : \Bbbk \xrightarrow{\mathrm{coev}_X} X \otimes X^* \xrightarrow{\theta \otimes id_{X^*}} X^{**} \otimes X^* \xrightarrow{\mathrm{ev}_{X^*}} \Bbbk. \tag{2.1}$$

Similarly, the *right quantum trace* of a morphism $\theta \in \mathrm{Hom}_H(X^{**}, X)$ is defined to be

$$\mathrm{Tr}_X^R(\theta) : \Bbbk \xrightarrow{\mathrm{coev}_{X^*}} X^* \otimes X^{**} \xrightarrow{id_{X^*} \otimes \theta} X^* \otimes X \xrightarrow{\mathrm{ev}_X} \Bbbk. \tag{2.2}$$

Since $\mathrm{End}_H(\Bbbk) \cong \Bbbk$, both $\mathrm{Tr}_X^L(\theta)$ and $\mathrm{Tr}_X^R(\theta)$ are elements in $\Bbbk$.

Remark 2.1.1 *Applying the duality functor $*$ to (2.1) and (2.2) respectively, one obtains that $Tr_X^L(\theta) = Tr_{X^*}^R(\theta^*)$ and $Tr_X^R(\theta) = Tr_{X^*}^L(\theta^*)$.*

Remark 2.1.2 *Let P be a projective H-module.*

(1) *If H is not semisimple, then $Tr_P^L(\theta) = 0$ for any $\theta \in Hom_H(P, P^{**})$. Otherwise, the morphism $coev_P$ is a split monomorphism by (2.1). In this case, $\Bbbk \mid P \otimes P^*$. It follows that $\Bbbk$ is projective, and hence H is semisimple, a contradiction. Similarly, if H is not semisimple, then $Tr_P^R(\theta) = 0$ for any $\theta \in Hom_H(P^{**}, P)$.*

(2) *If H is involutory, i.e., $S^2 = id_H$, then the map $\theta : P \to P^{**}$ given by $\theta(x)(f) = f(x)$ for $x \in P$ and $f \in P^*$ is an H-module isomorphism. In this case, $Tr_P^L(\theta) = Tr_P^R(\theta^{-1}) = \dim_{\Bbbk} P$. This implies that an involutory Hopf algebra over a field $\Bbbk$ of characteristic 0 is semisimple (the converse is also true, see [41]). In case the characteristic of $\Bbbk$ is $p > 0$ and H is not semisimple, then $p \mid \dim_{\Bbbk} P$, giving a result of Lorenz [46, Theorem 2.3 (b)].*

Lemma 2.1.3 *Let X be an indecomposable H-module.*

(1) *For any $\theta \in Hom_H(X, X^{**})$, if $Tr_X^L(\theta) \neq 0$, then θ is an isomorphism.*

(2) *For any $\theta \in Hom_H(X^{**}, X)$, if $Tr_X^R(\theta) \neq 0$, then θ is an isomorphism.*

Proof.We only prove Part (1) and the proof of Part (2) is similar. For any integer $m > 0$, the m-th power of the duality functor $*$ on X is denoted X^{*m}. If $\{x_i\}$ is a basis of X, we denote by $\{x_i^{*m}\}$ the basis of X^{*m} dual to the basis $\{x_i^{*m-1}\}$ of X^{*m-1}, i.e., $\langle x_i^{*m}, x_j^{*m-1}\rangle = \delta_{i,j}$. With these notations, we have the following: Let $\mathbf{A}$ be the transformation matrix of the morphism $\theta \in \text{Hom}_H(X, X^{**})$ with respect to the bases $\{x_i\}$ and $\{x_i^{**}\}$. It is clear that $\text{Tr}_X^L(\theta) = \text{Tr}(\mathbf{A})$, the usual trace of the matrix $\mathbf{A}$. Since H is a finite dimensional Hopf algebra, the order of S^2 is finite by Radford's formula on S^4 and the Nichols-Zöller Theorem. Suppose that $S^{2n} = id_H$. Then the map

$$\text{Id} : X^{*2n} \to X, \ \sum_i \lambda_i x_i^{*2n} \mapsto \sum_i \lambda_i x_i$$

is an H-module isomorphism and the transformation matrix of the map Id with respect to the basis $\{x_i^{*2n}\}$ of X^{*2n} and the basis $\{x_i\}$ of X is the identity matrix. Consider the following composition:

$$\Theta : X \xrightarrow{\theta} X^{**} \xrightarrow{\theta^{**}} X^{****} \to \cdots \to X^{*2n-2} \xrightarrow{\theta^{*2n-2}} X^{*2n} \xrightarrow{\text{Id}} X.$$

Note that the matrix of the map Θ from X to itself with respect to the basis $\{x_i\}$ of X is $\mathbf{A}^n$. Since $\text{End}_H(X)$ is local, the map Θ is either nilpotent or isomorphic. If Θ is nilpotent, so is $\mathbf{A}^n$, and hence $\mathbf{A}$ is nilpotent. This implies that $\text{Tr}_X^L(\theta) = \text{Tr}(\mathbf{A}) = 0$, a contradiction. Thus, Θ is an isomorphism, and so is the map θ. □

The following two canonical isomorphisms will be used later.

Lemma 2.1.4 *[5, Lemma 2.1.6] For H-modules X, Y and Z, we have the following canonical isomorphisms functorial in X, Y and Z:*

(1) $\Phi_{X,Y,Z} : Hom_H(X \otimes Y, Z) \to Hom_H(X, Z \otimes Y^*)$, $\Phi_{X,Y,Z}(\alpha) = (\alpha \otimes id_{Y^*}) \circ (id_X \otimes coev_Y)$.

(2) $\Psi_{X,Y,Z} : Hom_H(X, Y \otimes Z) \to Hom_H(Y^* \otimes X, Z)$, $\Psi_{X,Y,Z}(\gamma) = (ev_Y \otimes id_Z) \circ (id_{Y^*} \otimes \gamma)$.

The inverse maps of $\Phi_{X,Y,Z}$ and $\Psi_{X,Y,Z}$, respectively, are $\Phi^{-1}_{X,Y,Z}(\beta) = (id_Z \otimes \text{ev}_Y) \circ (\beta \otimes id_Y)$ for $\beta \in \text{Hom}_H(X, Z \otimes Y^*)$, and $\Psi^{-1}_{X,Y,Z}(\delta) = (id_Y \otimes \delta) \circ (\text{coev}_Y \otimes id_X)$ for $\delta \in \text{Hom}_H(Y^* \otimes X, Z)$. The two canonical isomorphisms satisfy the following properties.

Proposition 2.1.5 *Let X be an indecomposable H-module. For any H-module Y, we have the following:*

(1) *The canonical isomorphism $Hom_H(Y \otimes X^*, \Bbbk) \xrightarrow{\Phi_{Y,X^*,\Bbbk}} Hom_H(Y, X^{**})$ preserves split epimorphisms.*

(2) *The canonical isomorphism* $Hom_H(Y,X) \xrightarrow{\Psi_{Y,X,\Bbbk}} Hom_H(X^* \otimes Y, \Bbbk)$ *reflects split epimorphisms.*

Proof.(1) If the map $\alpha \in \mathrm{Hom}_H(Y \otimes X^*, \Bbbk)$ is a split epimorphism, there is some $\beta \in \mathrm{Hom}_H(\Bbbk, Y \otimes X^*)$ such that $\alpha \circ \beta = id_{\Bbbk}$. For the map β, there is some $\gamma \in \mathrm{Hom}_H(X,Y)$ such that $\beta = \Phi_{\Bbbk,X,Y}(\gamma)$. Note that $\Phi_{Y,X^*,\Bbbk}(\alpha) \circ \gamma \in \mathrm{Hom}_H(X, X^{**})$. It follows that

$$\begin{aligned}
\mathrm{Tr}^L_X(\Phi_{Y,X^*,\Bbbk}(\alpha)\circ\gamma) &= \mathrm{ev}_{X^*} \circ ((\Phi_{Y,X^*,\Bbbk}(\alpha)\circ\gamma) \otimes id_{X^*}) \circ \mathrm{coev}_X \\
&= (id_{\Bbbk} \otimes \mathrm{ev}_{X^*}) \circ (\Phi_{Y,X^*,\Bbbk}(\alpha) \otimes id_{X^*}) \circ (\gamma \otimes id_{X^*}) \circ (id_{\Bbbk} \otimes \mathrm{coev}_X) \\
&= \Phi^{-1}_{Y,X^*,\Bbbk}(\Phi_{Y,X^*,\Bbbk}(\alpha)) \circ \Phi_{\Bbbk,X,Y}(\gamma) \\
&= \alpha \circ \beta = id_{\Bbbk}.
\end{aligned}$$

Thus, $\Phi_{Y,X^*,\Bbbk}(\alpha)\circ\gamma$ is an isomorphism by Lemma 2.1.3, and hence the map $\Phi_{Y,X^*,\Bbbk}(\alpha)$ is a split epimorphism.

(2) If the map $\alpha \in \mathrm{Hom}_H(X^* \otimes Y, \Bbbk)$ is a split epimorphism, there is some $\beta \in \mathrm{Hom}_H(\Bbbk, X^* \otimes Y)$ such that $\alpha \circ \beta = id_{\Bbbk}$. Note that $\Psi^{-1}_{Y,X,\Bbbk}(\alpha) \circ \Psi_{\Bbbk,X^*,Y}(\beta) \in \mathrm{Hom}_H(X^{**}, X)$. It follows that

$$\begin{aligned}
&\mathrm{Tr}^R_X(\Psi^{-1}_{Y,X,\Bbbk}(\alpha) \circ \Psi_{\Bbbk,X^*,Y}(\beta)) \\
&= \mathrm{ev}_X \circ (id_{X^*} \otimes (\Psi^{-1}_{Y,X,\Bbbk}(\alpha) \circ \Psi_{\Bbbk,X^*,Y}(\beta))) \circ \mathrm{coev}_{X^*} \\
&= (\mathrm{ev}_X \otimes id_{\Bbbk}) \circ (id_{X^*} \otimes \Psi^{-1}_{Y,X,\Bbbk}(\alpha)) \circ (id_{X^*} \otimes \Psi_{\Bbbk,X^*,Y}(\beta)) \circ (\mathrm{coev}_{X^*} \otimes id_{\Bbbk}) \\
&= \Psi_{Y,X,\Bbbk}(\Psi^{-1}_{Y,X,\Bbbk}(\alpha)) \circ \Psi^{-1}_{\Bbbk,X^*,Y}(\Psi_{\Bbbk,X^*,Y}(\beta)) \\
&= \alpha \circ \beta = id_{\Bbbk}.
\end{aligned}$$

Thus, $\Psi^{-1}_{Y,X,\Bbbk}(\alpha) \circ \Psi_{\Bbbk,X^*,Y}(\beta)$ is an isomorphism by Lemma 2.1.3, and hence the map $\Psi^{-1}_{Y,X,\Bbbk}(\alpha)$ is a split epimorphism. □

As an immediate consequence of Proposition 2.1.5, we have the following result.

Corollary 2.1.6 *Let* X *and* Y *be two indecomposable* H*-modules.*

(1) *If* $\Bbbk \mid Y \otimes X^*$, *then* $Y \cong X^{**}$.

(2) *If* $\Bbbk \mid X^* \otimes Y$, *then* $Y \cong X$.

Cibils in [16, Remark 5.8] raised the following question: when is the trivial module a direct summand of the tensor product of two indecomposable modules over a finite dimensional Hopf algebra? We are now ready to answer this question using quantum traces.

Theorem 2.1.7 *Let X and Y be two indecomposable H-modules.*

(1) $\Bbbk \mid Y \otimes X^*$ *if and only if there are isomorphisms* $f : X \to Y$ *and* $g : Y \to X^{**}$ *such that* $Tr^L_X(g \circ f) \neq 0$.

(2) $\Bbbk \mid X^* \otimes Y$ *if and only if there are isomorphisms* $f : X^{**} \to Y$ *and* $g : Y \to X$ *such that* $Tr^R_X(g \circ f) \neq 0$.

Proof. We only prove Part (1) and the same argument works for Part (2). If $f : X \to Y$ and $g : Y \to X^{**}$ are two isomorphisms such that $\mathrm{Tr}^L_X(g \circ f) \neq 0$, then

$$0 \neq \mathrm{Tr}^L_X(g \circ f) = \mathrm{ev}_{X^*} \circ (g \otimes id_{X^*}) \circ (f \otimes id_{X^*}) \circ \mathrm{coev}_X.$$

This implies that the map $(f \otimes id_{X^*}) \circ \mathrm{coev}_X : \Bbbk \to Y \otimes X^*$ is a split monomorphism, and hence $\Bbbk \mid Y \otimes X^*$. Conversely, if $\Bbbk \mid Y \otimes X^*$, there are maps $\alpha : \Bbbk \to Y \otimes X^*$ and $\beta : Y \otimes X^* \to \Bbbk$ such that $\beta \circ \alpha = id_{\Bbbk}$. For the map α, by Lemma 2.1.4, there is a map $f : X \to Y$ such that

$$\alpha = \Phi_{\Bbbk,X,Y}(f) = (f \otimes id_{X^*}) \circ (id_{\Bbbk} \otimes \mathrm{coev}_X).$$

For the map β, there is a map $g : Y \to X^{**}$ such that

$$\beta = \Phi^{-1}_{Y,X^*,\Bbbk}(g) = (id_{\Bbbk} \otimes \mathrm{ev}_{X^*}) \circ (g \otimes id_{X^*}).$$

Thus, we have

$$\begin{aligned}\mathrm{Tr}^L_X(g \circ f) &= \mathrm{ev}_{X^*} \circ (g \otimes id_{X^*}) \circ (f \otimes id_{X^*}) \circ \mathrm{coev}_X \\ &= (id_{\Bbbk} \otimes \mathrm{ev}_{X^*}) \circ (g \otimes id_{X^*}) \circ (f \otimes id_{X^*}) \circ (id_{\Bbbk} \otimes \mathrm{coev}_X) \\ &= \beta \circ \alpha = id_{\Bbbk}.\end{aligned}$$

It follows from Lemma 2.1.3 that the composition $g \circ f$ is an isomorphism. Thus, f and g are both isomorphisms. □

Given two H-modules X and Y, one knows little in general about how to decompose the tensor product $X \otimes Y$ into a direct sum of indecomposable modules. However, there are still some rules that the decomposition should follow as shown in the following.

Proposition 2.1.8 *Let X, Y, M be H-modules with X and M indecomposable.*

(1) *If $\Bbbk \mid M \otimes M^*$ and $M \mid X \otimes Y$, then $\Bbbk \mid X \otimes X^*$ and $X \mid M \otimes Y^*$.*

(2) *If $\Bbbk \mid M^* \otimes M$ and $M \mid Y \otimes X$, then $\Bbbk \mid X^* \otimes X$ and $X \mid Y^* \otimes M$.*

Proof.(1) We only prove Part (1) and the proof of Part (2) is similar. The conditions $\Bbbk \mid M \otimes M^*$ and $M \mid X \otimes Y$ imply that $\Bbbk \mid X \otimes Y \otimes M^*$. Suppose $Y \otimes M^* \cong \bigoplus_i N_i^*$ for some indecomposable modules N_i. Then there is an indecomposable module N_i such that $\Bbbk \mid X \otimes N_i^*$. By Theorem 2.1.7 (1), we obtain $X \cong N_i \cong N_i^{**}$. It follows that $\Bbbk \mid X \otimes N_i^* \cong X \otimes X^*$. Note that $\Bbbk \mid M \otimes M^*$ implies that $M \cong M^{**}$. Then $X \cong N_i^{**}$ implies that $X \mid (Y \otimes M^*)^* \cong M \otimes Y^*$, as desired. □

In the rest of this section, H will be a non-semisimple Hopf algebra. We shall take another approach to characterize when the trivial module $\Bbbk$ appears in the decomposition of the tensor product $X^* \otimes X$ (resp. $X \otimes X^*$) for an indecomposable module X. For the special case where the square of the antipode is inner, we refer to [35, 73]. Suppose

$$0 \to \tau(\Bbbk) \to E \xrightarrow{\sigma} \Bbbk \to 0 \tag{2.3}$$

is an almost split sequence ending at the trivial module $\Bbbk$. Tensoring (over $\Bbbk$) the sequence (2.3) with an indecomposable module X, we obtain the following two short exact sequences:

$$0 \to \tau(\Bbbk) \otimes X \to E \otimes X \xrightarrow{\sigma \otimes id_X} X \to 0, \tag{2.4}$$

$$0 \to X \otimes \tau(\Bbbk) \to X \otimes E \xrightarrow{id_X \otimes \sigma} X \to 0. \tag{2.5}$$

We need the following lemma, its proof is straightforward if one applies Lemma 2.1.4.

Lemma 2.1.9 *For H-modules X and Y, the following diagrams are commutative:*

$$\begin{array}{ccc} Hom_H(Y, X \otimes E) & \xrightarrow{(id_X \otimes \sigma)_*} & Hom_H(Y, X) \\ \Psi_{Y,X,E} \downarrow & & \downarrow \Psi_{Y,X,\Bbbk} \\ Hom_H(X^* \otimes Y, E) & \xrightarrow{\sigma_*} & Hom_H(X^* \otimes Y, \Bbbk), \end{array} \tag{2.6}$$

$$\begin{array}{ccc} Hom_H(Y \otimes X, E) & \xrightarrow{\sigma_*} & Hom_H(Y \otimes X, \Bbbk) \\ \Phi_{Y,X,E} \downarrow & & \downarrow \Phi_{Y,X,\Bbbk} \\ Hom_H(Y, E \otimes X^*) & \xrightarrow{(\sigma \otimes id_{X^*})_*} & Hom_H(Y, X^*). \end{array} \tag{2.7}$$

Proposition 2.1.10 *Let X be an indecomposable H-module. The following are equivalent:*

(1) $\Bbbk \nmid X^* \otimes X$

(2) *The map $Hom_H(X^* \otimes X, E) \xrightarrow{\sigma_*} Hom_H(X^* \otimes X, \Bbbk)$ is surjective.*

(3) *The map $Hom_H(X, X \otimes E) \xrightarrow{(id_X \otimes \sigma)_*} Hom_H(X, X)$ is surjective.*

(4) *The map $X \otimes E \xrightarrow{id_X \otimes \sigma} X$ is a split epimorphism.*

(5) *The map $E \otimes X^* \xrightarrow{\sigma \otimes id_{X^*}} X^*$ is a split epimorphism.*

Proof.(1) $\Leftrightarrow$ (2). If $\Bbbk \nmid X^* \otimes X$, then for any $\alpha \in \mathrm{Hom}_H(X^* \otimes X, \Bbbk)$, the map α is not a split epimorphism. Since σ is right almost split from E to $\Bbbk$, there is a map β from $X^* \otimes X$ to E such that $\sigma \circ \beta = \alpha$. This implies that σ_* is surjective. Conversely, if the map σ_* is surjective, then $\Bbbk \nmid X^* \otimes X$. Otherwise, by Theorem 2.1.7 (2), there is an isomorphism $\theta : X^{**} \to X$ such that $\mathrm{Tr}_X^R(\theta) = id_\Bbbk$. For the map $\mathrm{ev}_X : X^* \otimes X \to \Bbbk$, there is some $\beta \in \mathrm{Hom}_H(X^* \otimes X, E)$ such that $\sigma \circ \beta = \mathrm{ev}_X$ since the map σ_* is surjective. It follows that $id_\Bbbk = \mathrm{Tr}_X^R(\theta) = \mathrm{ev}_X \circ (id_{X^*} \otimes \theta) \circ \mathrm{coev}_{X^*} = \sigma \circ \beta \circ (id_{X^*} \otimes \theta) \circ \mathrm{coev}_{X^*}$. We obtain that the map σ is a split epimorphism, a contradiction to the fact that σ is right almost split.

(2) $\Leftrightarrow$ (3). According to the commutative diagram (2.6), we have the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Hom}_H(X, X\otimes E) & \xrightarrow{(id_X\otimes\sigma)_*} & \mathrm{Hom}_H(X,X) \\ {\scriptstyle \Psi_{X,X,E}}\downarrow & & \downarrow{\scriptstyle \Psi_{X,X,\Bbbk}} \\ \mathrm{Hom}_H(X^*\otimes X, E) & \xrightarrow{\sigma_*} & \mathrm{Hom}_H(X^*\otimes X, \Bbbk). \end{array}$$

It follows that σ_* is surjective if and only if $(id_X \otimes \sigma)_*$ is surjective.

(3) $\Leftrightarrow$ (4). If $(id_X \otimes \sigma)_*$ is surjective, for the identity map id_X, there is a map $\alpha \in \mathrm{Hom}_H(X, X\otimes E)$ such that $(id_X\otimes\sigma)_*(\alpha) = id_X$, namely, $(id_X \otimes \sigma)\circ\alpha = id_X$. It follows that $id_X\otimes\sigma$ is a split epimorphism. Conversely, if $id_X\otimes\sigma$ is a split epimorphism, there is $\alpha \in \mathrm{Hom}_H(X, X\otimes E)$ such that $(id_X\otimes\sigma)\circ\alpha = id_X$. For any $\beta \in \mathrm{Hom}_H(X,X)$, we have $(id_X\otimes\sigma)_*(\alpha\circ\beta) = \beta$. It yields that the map $(id_X\otimes\sigma)_*$ is surjective.

(2) $\Leftrightarrow$ (5). Applying the commutative diagram (2.7), we have the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Hom}_H(X^*\otimes X, E) & \xrightarrow{\sigma_*} & \mathrm{Hom}_H(X^*\otimes X, \Bbbk) \\ {\scriptstyle \Phi_{X^*,X,E}}\downarrow & & \downarrow{\scriptstyle \Phi_{X^*,X,\Bbbk}} \\ \mathrm{Hom}_H(X^*, E\otimes X^*) & \xrightarrow{(\sigma\otimes id_{X^*})_*} & \mathrm{Hom}_H(X^*, X^*). \end{array}$$

Thus, σ_* is surjective if and only if $(\sigma\otimes id_{X^*})_*$ is surjective. If $(\sigma\otimes id_{X^*})_*$ is surjective, for the identity map id_{X^*}, there is $\alpha \in \mathrm{Hom}_H(X^*, E\otimes X^*)$ such that $id_{X^*} = (\sigma \otimes id_{X^*})_*(\alpha) = (\sigma\otimes id_{X^*})\circ\alpha$. This implies that $\sigma\otimes id_{X^*}$ is a split epimorphism. Conversely, if $\sigma\otimes id_{X^*}$ is a split epimorphism, there is $\alpha \in \mathrm{Hom}_H(X^*, E\otimes X^*)$ such that $(\sigma \otimes id_{X^*})\circ\alpha = id_{X^*}$. For any $\beta \in \mathrm{Hom}_H(X^*, X^*)$, we obtain that $(\sigma\otimes id_{X^*})_*(\alpha\circ\beta) = \beta$. It follows that the map $(\sigma\otimes id_{X^*})_*$ is surjective. □

Similarly, there are some equivalent conditions for $\Bbbk \nmid X\otimes X^*$. However, we only need the following characterization, which is useful in the study of the Green ring of H.

Proposition 2.1.11 *Let X be an indecomposable H-module. The following are equivalent:*

(1) $\Bbbk \nmid X\otimes X^*$

(2) *The map* $E \otimes X \xrightarrow{\sigma\otimes id_X} X$ *is a split epimorphism.*

Proof. Let Y be indecomposable such that $Y^* \cong X$ (such a Y exists as the order of S^2 is finite). Then $\Bbbk \nmid X \otimes X^*$ if and only if $\Bbbk \nmid (Y^* \otimes Y)^*$ if and only if $\Bbbk \nmid Y^* \otimes Y$. By Proposition 2.1.10, this is precisely $\sigma \otimes id_{Y^*}$ is a split epimorphism, as desired. □

Although we have characterized $\Bbbk \nmid X^* \otimes X$ and $\Bbbk \nmid X \otimes X^*$ respectively in the previous two propositions, we still find the following characterizations of $\Bbbk \mid X^* \otimes X$ and $\Bbbk \mid X \otimes X^*$ useful.

Proposition 2.1.12 *Let X be an indecomposable H-module. The following are equivalent:*

(1) $\Bbbk \mid X^* \otimes X$.

(2) *The map* $X \otimes E \xrightarrow{id_X\otimes\sigma} X$ *is right almost split.*

Proof. If $id_X \otimes \sigma$ is right almost split, it is not a split epimorphism. By Proposition 2.1.10, we have $\Bbbk \mid X^* \otimes X$. Conversely, if $\Bbbk \mid X^* \otimes X$, by Proposition 2.1.10, the map $id_X \otimes \sigma$ is not a split epimorphism. For any $\alpha \in \mathrm{Hom}_H(Y, X)$ which is not split epimorphism, the map $\Psi_{Y,X,\Bbbk}(\alpha) \in \mathrm{Hom}_H(X^* \otimes Y, \Bbbk)$ is also not split epimorphism by Proposition 2.1.5 (2). For the map $\Psi_{Y,X,\Bbbk}(\alpha)$, there is a map $\beta \in \mathrm{Hom}_H(X^* \otimes Y, E)$ such that

$$\sigma \circ \beta = \Psi_{Y,X,\Bbbk}(\alpha)$$

since σ is right almost split. Note that $\Psi^{-1}_{Y,X,E}(\beta) \in \mathrm{Hom}_H(Y, X \otimes E)$. We claim that the map $\Psi^{-1}_{Y,X,E}(\beta)$ satisfies the relation $(id_X \otimes \sigma) \circ \Psi^{-1}_{Y,X,E}(\beta) = \alpha$, and hence $id_X \otimes \sigma$ is right almost split. In fact, the commutative diagram (2.6) states that

$$\Psi_{Y,X,\Bbbk} \circ (id_X \otimes \sigma)_* = \sigma_* \circ \Psi_{Y,X,E}.$$

It follows that

$$\begin{aligned} \alpha &= \Psi^{-1}_{Y,X,\Bbbk}(\sigma \circ \beta) = (\Psi^{-1}_{Y,X,\Bbbk} \circ \sigma_*)(\beta) \\ &= ((id_X \otimes \sigma)_* \circ \Psi^{-1}_{Y,X,E})(\beta) = (id_X \otimes \sigma) \circ \Psi^{-1}_{Y,X,E}(\beta). \end{aligned}$$

This completes the proof. □

Similarly, we have the following result.

Proposition 2.1.13 *Let X be an indecomposable H-module. The following are equivalent:*

(1) $\Bbbk \mid X \otimes X^*$.

(2) *The map $E \otimes X \xrightarrow{\sigma \otimes id_X} X$ is right almost split.*

Proof. If the map $\sigma \otimes id_X$ is right almost split, it is not a split epimorphism. By Proposition 2.1.11, we obtain $\Bbbk \mid X \otimes X^*$. Conversely, if $\Bbbk \mid X \otimes X^*$, then $X \cong X^{**}$ by Theorem 2.1.7 (1). To show that $\sigma \otimes id_X$ is right almost split, we only need to show that $\sigma \otimes id_{X^{**}}$ is right almost split. Note that $\Bbbk \mid X^{**} \otimes X^{***}$. It follows from Proposition 2.1.11 that the map $\sigma \otimes id_{X^{**}}$ is not a split epimorphism. For any $\alpha \in \mathrm{Hom}_H(Y, X^{**})$ which is not a split epimorphism, by Proposition 2.1.5 (1), $\Phi^{-1}_{Y,X^*,\Bbbk}(\alpha) \in \mathrm{Hom}_H(Y \otimes X^*, \Bbbk)$ is also not a split epimorphism. We get a map $\beta \in \mathrm{Hom}_H(Y \otimes X^*, E)$ such that

$$\sigma \circ \beta = \Phi^{-1}_{Y,X^*,\Bbbk}(\alpha)$$

since the map σ is right almost split. In the following, we shall verify that the map $\Phi_{Y,X^*,E}(\beta) \in \mathrm{Hom}_H(Y, E \otimes X^{**})$ satisfies $(\sigma \otimes id_{X^{**}}) \circ \Phi_{Y,X^*,E}(\beta) = \alpha$, and hence the map $\sigma \otimes id_{X^{**}}$ is right almost split. To this end, by replacing X with X^* in commutative diagram (2.7), we obtain that

$$\Phi_{Y,X^*,\Bbbk} \circ \sigma_* = (\sigma \otimes id_{X^{**}})_* \circ \Phi_{Y,X^*,E}.$$

Then

$$\begin{aligned}
\alpha &= \Phi_{Y,X^*,\Bbbk}(\sigma \circ \beta) \\
&= (\Phi_{Y,X^*,\Bbbk} \circ \sigma_*)(\beta) \\
&= ((\sigma \otimes id_{X^{**}})_* \circ \Phi_{Y,X^*,E})(\beta) \\
&= (\sigma \otimes id_{X^{**}}) \circ \Phi_{Y,X^*,E}(\beta).
\end{aligned}$$

Remark 2.1.14 *An indecomposable module satisfying one of the equivalent conditions in Proposition 2.1.12 or in Proposition 2.1.13 is called a splitting trace module, see e.g., [26, 35, 73].*

§2.2 Bilinear forms on Green rings

As shown in [8], an approach to study the Green ring of a finite group is through bilinear forms defined by dimensions of morphism spaces. In this section, we follow the same approach and define similar bilinear forms on the Green ring $r(H)$ of H. As we shall see, these bilinear forms can be used to investigate some properties of $r(H)$ presented in the next section.

Let $F(H)$ be the free abelian group generated by isomorphism classes $[X]$ of all H-modules X. The group $F(H)$ is in fact a ring with a multiplication given by the tensor product $[X][Y] = [X \otimes Y]$. The *Green ring* (or the *representation ring*) $r(H)$ of H is defined to be the quotient ring of $F(H)$ modulo the relations $[X \oplus Y] = [X] + [Y]$, for H-modules X, Y. The identity of the associative ring $r(H)$ is represented by the trivial module $[\Bbbk]$. The set $\mathrm{ind}(H)$ consisting of isomorphism classes of all indecomposable H-modules forms a $\mathbb{Z}$-basis of $r(H)$, see e.g., [13, 19, 39, 43, 65].

The *Grothendieck ring* $G_0(H)$ of H is the quotient ring of $F(H)$ modulo all short exact sequences of H-modules, i.e., $[Y] = [X] + [Z]$ if $0 \to X \to Y \to Z \to 0$ is exact. The Grothendieck ring $G_0(H)$ possesses a $\mathbb{Z}$-basis given by isomorphism classes of simple H-modules. Both $r(H)$ and $G_0(H)$ are augmented $\mathbb{Z}$-algebras with the dimension augmentation. There is a natural ring epimorphism from $r(H)$ to $G_0(H)$ given by

$$\varphi : r(H) \to G_0(H),\ [M] \mapsto \sum_{[V]} [M : V][V], \tag{2.8}$$

where $[M : V]$ is the multiplicity of V in the composition series of M and the sum $\sum_{[V]}$ runs over all non-isomorphic simple H-modules. If H is semisimple, the map φ is the identity map.

Let Z be an indecomposable H-module. If Z is non-projective, there is a unique almost split sequence $0 \to X \to Y \to Z \to 0$ ending at Z. We follow the notation given in [4, Section 4, ChVI] and denote by $\delta_{[Z]}$ the element $[X] - [Y] + [Z]$ in $r(H)$. In case Z is projective, we define $\delta_{[Z]} := [Z] - [\mathrm{rad} Z]$. The following gives a weaker condition for $\delta_{[Z]} = [X] - [Y] + [Z]$ in $r(H)$.

Proposition 2.2.1 *Let Z be an indecomposable non-projective H-module. If $0 \to X \to Y \xrightarrow{\alpha} Z \to 0$ is a short exact sequence and the map α is only right almost split,* *we still have* $\delta_{[Z]} = [X] - [Y] + [Z]$.

Proof. Since the sequence

$$0 \to X \to Y \overset{\alpha}{\to} Z \to 0 \tag{2.9}$$

is exact and the map α is right almost split, it follows from [4, Theorem 2.2, ChI] that the middle term Y has a decomposition $Y = Y_1 \oplus Y_2$ such that the restriction of α to the summand Y_1, denoted $\alpha|_{Y_1}$, is right minimal, and the restriction of α to the summand Y_2 is zero. We obtain that $\alpha|_{Y_1}$ is both right minimal and right almost split. By [4, Proposition 1.12, ChV], the sequence $0 \to \ker(\alpha|_{Y_1}) \overset{\iota}{\to} Y_1 \xrightarrow{\alpha|_{Y_1}} Z \to 0$ is almost split, where ι is the inclusion map. Thus, $\delta_{[Z]} = [\ker(\alpha|_{Y_1})] - [Y_1] + [Z]$. Meanwhile, it is easy to see that the sequence

$$0 \to \ker(\alpha|_{Y_1}) \oplus Y_2 \xrightarrow{\iota \coprod id_{Y_2}} Y_1 \oplus Y_2 \overset{\alpha}{\to} Z \to 0 \tag{2.10}$$

is exact. Applying the short five lemma to the sequences (2.9) and (2.10), we obtain that $X \cong \ker(\alpha|_{Y_1}) \oplus Y_2$. In this case,

$$\begin{aligned} \delta_{[Z]} &= [\ker(\alpha|_{Y_1})] - [Y_1] + [Z] \\ &= [\ker(\alpha|_{Y_1}) \oplus Y_2] - [Y_1 \oplus Y_2] + [Z] \\ &= [X] - [Y] + [Z], \end{aligned}$$

as desired. □

For any two H-modules X and Y, following [8, 52, 72] we define

$$\langle [X], [Y] \rangle_1 := \dim_{\Bbbk} \mathrm{Hom}_H(X, Y).$$

Then, $\langle -, - \rangle_1$ extends to a $\mathbb{Z}$-bilinear form on $r(H)$. The following results can be found from Proposition 4.1, Theorem 4.3 and Theorem 4.4 in [4, ChVI], so we omit their proofs.

Lemma 2.2.2 *The following hold in* $r(H)$*:*

(1) *For any two indecomposable modules* X *and* Z*,* $\langle [X], \delta_{[Z]} \rangle_1 = \delta_{[X],[Z]}$*, where* $\delta_{[X],[Z]}$ *is equal to 1 if* $X \cong Z$*, and 0 otherwise.*

(2) *For any* $x \in r(H)$, $x = \sum_{[M]\in ind(H)} \langle x, \delta_{[M]}\rangle_1 [M]$.

(3) *The set* $\{\delta_{[M]} \mid [M] \in ind(H)\}$ *is linearly independent in* $r(H)$.

(4) H *is of finite representation type if and only if* $\{\delta_{[M]} \mid [M] \in ind(H)\}$ *forms a* $\mathbb{Z}$*-basis of* $r(H)$.

(5) H *is of finite representation type if and only if* $\{\delta_{[M]} \mid [M] \in ind(H)$ *and* M *not projective*$\}$ *forms a* $\mathbb{Z}$*-basis of* $\ker\varphi$, *where* φ *is the map given in (2.8).*

Remark 2.2.3 *It follows from Lemma 2.2.2 (2) that the form* $\langle -,-\rangle_1$ *is non-degenerate in the sense that given* $0 \neq x \in r(H)$, *there is* $y \in r(H)$ *such that* $\langle x, y\rangle_1 \neq 0$. *If* H *is of finite representation type, it can be seen from Lemma 2.2.2 that the set* $\{[M], \delta_{[M]} \mid [M] \in ind(H)\}$ *forms a pair of dual bases of* $r(H)$ *with respect to the form* $\langle -,-\rangle_1$. *In this case, any* x *in* $r(H)$ *can be written as follows:* $x = \sum_{[M]\in ind(H)} \langle [M], x\rangle_1 \delta_{[M]}$.

We use the non-degeneracy of the form $\langle -,-\rangle_1$ to give an equivalent condition for H to be of finite representation type.

Proposition 2.2.4 *A finite dimensional Hopf algebra* H *is of finite representation type if and only if for any indecomposable module* X, *there are only finitely many indecomposable modules* M *such that* $Hom_H(M, X) \neq 0$.

Proof. For any indecomposable module X, if there are only finitely many indecomposable modules M such that $\mathrm{Hom}_H(M, X) \neq 0$, then $\sum_{[M]\in \mathrm{ind}(H)} \dim_{\Bbbk} \mathrm{Hom}_H(M, X)\delta_{[M]}$ is a finite sum. We have the following:

$$\begin{aligned} &\langle [M], [X] - \sum_{[M]\in \mathrm{ind}(H)} \dim_{\Bbbk} \mathrm{Hom}_H(M, X)\delta_{[M]}\rangle_1 \\ = &\langle [M], [X]\rangle_1 - \dim_{\Bbbk} \mathrm{Hom}_H(M, X) = 0. \end{aligned}$$

This implies that $[X] = \sum_{[M]\in \mathrm{ind}(H)} \dim_{\Bbbk} \mathrm{Hom}_H(M, X)\delta_{[M]}$ by the non-degeneracy of the form $\langle -,-\rangle_1$. Thus, $\{\delta_{[M]} \mid [M] \in \mathrm{ind}(H)\}$ is a basis of $r(H)$, and hence H is of finite representation type by Lemma 2.2.2 (4). □

Let $\mathcal{P}(X,Y)$ be the space of morphisms from X to Y which factor through a projective module. By a similar way to [8], we define another bilinear form on $r(H)$ as follows:

$$\langle [X],[Y]\rangle_2 := \dim_{\Bbbk} \mathcal{P}(X,Y).$$

Let $*$ denote the duality operator of $r(H)$ induced by the duality functor: $[X]^* = [X^*]$. Then $*$ is an anti-automorphism of $r(H)$. Obviously, if S^2 of H is inner, then $*$ is an involution [46]. The forms $\langle -,-\rangle_1$ and $\langle -,-\rangle_2$ both have the following properties.

Proposition 2.2.5 *Let X, Y and Z be H-modules.*

(1) $\langle [X][Y],[Z]\rangle_1 = \langle [X],[Z][Y]^*\rangle_1$ *and* $\langle [X],[Y][Z]\rangle_1 = \langle [Y]^*[X],[Z]\rangle_1$.

(2) $\langle [X][Y],[Z]\rangle_2 = \langle [X],[Z][Y]^*\rangle_2$ *and* $\langle [X],[Y][Z]\rangle_2 = \langle [Y]^*[X],[Z]\rangle_2$.

Proof.(1) It follows from Lemma 2.1.4.

(2) If $\alpha \in \mathrm{Hom}_H(X\otimes Y, Z)$ factors through a projective module P, then $\Phi_{X,Y,Z}(\alpha)$ factors through the projective module $P\otimes Y^*$ by Lemma 2.1.4 (1). Thus, $\Phi_{X,Y,Z}(\mathcal{P}(X\otimes Y,Z)) \subseteq \mathcal{P}(X, Z\otimes Y^*)$. Conversely, for any $\beta \in \mathcal{P}(X, Z\otimes Y^*)$ which factors through a projective module P, by Lemma 2.1.4 (1), the map $\Phi^{-1}_{X,Y,Z}(\beta)$ factors through the projective module $P\otimes Y$. We obtain that $\Phi_{X,Y,Z}(\mathcal{P}(X\otimes Y,Z)) = \mathcal{P}(X, Z\otimes Y^*)$. Similarly, $\Psi_{X,Y,Z}(\mathcal{P}(X, Y\otimes Z)) = \mathcal{P}(Y^*\otimes X, Z)$. We are done. □

Let Ω and Ω^{-1} denote the syzygy functor and cosyzygy functor of H-mod respectively. Namely, ΩM is the kernel of the projective cover $P_M \to M$, and $\Omega^{-1}M$ is the cokernel of the injective envelope $M \to I_M$. Denote by $\delta^*_{[M]}$ the image of $\delta_{[M]}$ under the duality operator $*$ of $r(H)$. The following is a generalization of [8, Proposition 2.1] to the case of the Green ring $r(H)$. We omit the proof since it is similar to the proof of [8, Proposition 2.1].

Lemma 2.2.6 *Let M be an indecomposable H-module and $P_{\Bbbk}$ the projective cover of the trivial module $\Bbbk$. The following hold in $r(H)$:*

(1) $([I_M]-[\Omega^{-1}M])\delta_{[P_{\Bbbk}]} = \delta_{[P_{\Bbbk}]}([I_M]-[\Omega^{-1}M]) = [M]$ *and* $([P_M]-[\Omega M])\delta^*_{[P_{\Bbbk}]} = \delta^*_{[P_{\Bbbk}]}([P_M]-[\Omega M]) = [M]$. *Moreover,* $\delta_{[P_{\Bbbk}]}\delta^*_{[P_{\Bbbk}]} = \delta^*_{[P_{\Bbbk}]}\delta_{[P_{\Bbbk}]} = 1$.

(2) $[M]\delta_{[P_\Bbbk]} = \delta_{[P_\Bbbk]}[M] = [P_M] - [\Omega M]$ *and* $[M]\delta^*_{[P_\Bbbk]} = \delta^*_{[P_\Bbbk]}[M] = [I_M] - [\Omega^{-1}M]$*. Thus,* $\delta_{[P_\Bbbk]}$ *and* $\delta^*_{[P_\Bbbk]}$ *are both central units of* $r(H)$*.*

The following explores a relation between the forms $\langle -,-\rangle_1$ and $\langle -,-\rangle_2$. We refer to [8, Corollary 2.3] for a similar result for the Green ring of a finite group.

Proposition 2.2.7 *Let* X *and* Y *be two* H*-modules.*

(1) $\langle [X],[Y]\rangle_2$ *is equal to the multiplicity of* $P_\Bbbk$ *in the direct sum decomposition of* $Y^*\otimes X$*.*

(2) $\langle [X],[Y]\rangle_2 = \langle [X],[Y]\delta_{[P_\Bbbk]}\rangle_1 = \langle [X]\delta^*_{[P_\Bbbk]},[Y]\rangle_1$.

(3) $\langle [X],[Y]\rangle_1 = \langle [X]\delta_{[P_\Bbbk]},[Y]\rangle_2 = \langle [X],[Y]\delta^*_{[P_\Bbbk]}\rangle_2$.

Proof.(1) For any non-zero morphism $\alpha \in \mathcal{P}(Y^*\otimes X,\Bbbk)$, if α factors through an indecomposable projective module P, then $\alpha = \beta\circ\gamma$ for some $\beta : P \to \Bbbk$ and $\gamma : Y^*\otimes X \to P$. Since β is surjective, P is the projective cover of $\Bbbk$ and hence $P \cong P_\Bbbk$. Note that rad$P_\Bbbk$ is the unique maximal submodule of $P_\Bbbk$. The image of the morphism γ is either contained in rad$P_\Bbbk$ or equal to $P_\Bbbk$. For the former case, $\alpha = \beta\circ\gamma = 0$, a contradiction. Thus, the morphism γ is surjective, and hence $P_\Bbbk$ is a direct summand of $Y^*\otimes X$. Now, if α factors through a projective module P and $P \cong \bigoplus_i P_i$ for some indecomposable projective modules P_i. Then $\alpha = \sum_i \beta_i\circ\gamma_i$ for some $\beta_i : P_i \to \Bbbk$ and $\gamma_i : Y^*\otimes X \to P_i$. We have proved that $\beta_i\circ\gamma_i \neq 0$ if and only if $P_i \cong P_\Bbbk$. It follows that $\dim_\Bbbk \mathcal{P}(Y^*\otimes X,\Bbbk)$ is equal to the multiplicity of $P_\Bbbk$ in the direct sum decomposition of $Y^*\otimes X$, while $\dim_\Bbbk \mathcal{P}(Y^*\otimes X,\Bbbk)$ is equal to $\dim_\Bbbk \mathcal{P}(X,Y)$ by Proposition 2.2.5 (2), as desired.

(2) It follows from Part (1) that $\langle [X],[Y]\rangle_2 = \langle [Y]^*[X],\delta_{[P_\Bbbk]}\rangle_1$. By Proposition 2.2.5, we have

$$\begin{aligned}\langle [Y]^*[X],\delta_{[P_\Bbbk]}\rangle_1 &= \langle [X],[Y]\delta_{[P_\Bbbk]}\rangle_1 = \langle [X]\delta^*_{[P_\Bbbk]}\delta_{[P_\Bbbk]},[Y]\delta_{[P_\Bbbk]}\rangle_1\\ &= \langle [X]\delta^*_{[P_\Bbbk]},[Y]\delta_{[P_\Bbbk]}\delta^*_{[P_\Bbbk]}\rangle_1 = \langle [X]\delta^*_{[P_\Bbbk]},[Y]\rangle_1.\end{aligned}$$

(3) It follows from Part (2) and the fact that $\delta_{[P_\Bbbk]}\delta^*_{[P_\Bbbk]} = \delta^*_{[P_\Bbbk]}\delta_{[P_\Bbbk]} = 1$. $\square$

Corollary 2.2.8 *Let X be an indecomposable H-module and V a simple H-module. Then $\langle [X],[V]\rangle_2 = \delta_{[X],[P_V]}$.*

Proof. It follows from Proposition 2.2.7 that $\langle [X],[V]\rangle_2 = \langle [X],[V]\delta_{[P_\Bbbk]}\rangle_1$. By Lemma 2.2.6, $\langle [X],[V]\delta_{[P_\Bbbk]}\rangle_1 = \langle [X],[P_V]\rangle_1 - \langle [X],[\Omega V]\rangle_1$, which is equal to 1 if $X \cong P_V$, and 0 otherwise. $\square$

Remark 2.2.9 *Let H be of finite representation type. It follows from Proposition 2.2.7 (3) that the set $\{[M]\delta_{[P_\Bbbk]}, \delta_{[M]} \mid [M] \in ind(H)\}$ or $\{[M], \delta_{[M]}\delta^*_{[P_\Bbbk]} \mid [M] \in ind(H)\}$ forms a pair of dual bases of $r(H)$ with respect to the form $\langle -,-\rangle_2$. Hence the form $\langle -,-\rangle_2$ is the same as $\langle -,-\rangle_1$ up to a unit. Namely, $\langle -,-\rangle_1 = \langle -\delta_{[P_\Bbbk]}, -\rangle_2 = \langle -, -\delta^*_{[P_\Bbbk]}\rangle_2$.*

For any two H-modules X and Y, we define

$$\langle [X],[Y]\rangle_3 := \langle [X],[Y]\rangle_1 - \langle [X],[Y]\rangle_2.$$

It follows from Proposition 2.2.7 that

$$\langle [X],[Y]\rangle_3 = \langle [X],[Y](1-\delta_{[P_\Bbbk]})\rangle_1 = \langle [X](1-\delta^*_{[P_\Bbbk]}),[Y]\rangle_1.$$

Moreover, we have the following result.

Proposition 2.2.10 *Let X and Y be two H-modules.*

(1) *If X is projective, then $\langle [X],[Y]\rangle_3 = 0$.*

(2) *If X is indecomposable and non-projective, then*

$$\langle [X],[Y]\rangle_3 = \langle [X],[Y]\rangle_1 + \langle [\Omega^{-1}X],[Y]\rangle_1 - \sum_{[V]}[Y:V]\langle [\Omega^{-1}X],[V]\rangle_1,$$

where the sum $\sum_{[V]}$ runs over all non-isomorphic simple H-modules and $[Y:V]$ is the multiplicity of V in the composition series of Y. In particular, $\langle [X],[Y]\rangle_3 = \langle [X],[Y]\rangle_1$ if Y is simple.

Proof. (1) It follows from the fact that $\mathcal{P}(X,Y) = \mathrm{Hom}_H(X,Y)$ if X is projective.

(2) For any simple H-module V, on the one hand, $\langle [X],[V]\rangle_2 = 0$ by Corollary 2.2.8. On the other hand, $\langle [X],[V]\rangle_2 = \langle [X]\delta^*_{[P_{\Bbbk}]},[V]\rangle_1$, which is equal to $\langle [I_X]-[\Omega^{-1}X],[V]\rangle_1$ by Lemma 2.2.6. It follows that $\langle [I_X],[V]\rangle_1 = \langle [\Omega^{-1}X],[V]\rangle_1$. Now

$$\begin{aligned}\langle [X],[Y]\rangle_3 &= \langle [X](1-\delta^*_{[P_{\Bbbk}]}),[Y]\rangle_1\\ &= \langle [X],[Y]\rangle_1 + \langle [\Omega^{-1}X],[Y]\rangle_1 - \langle [I_X],[Y]\rangle_1\\ &= \langle [X],[Y]\rangle_1 + \langle [\Omega^{-1}X],[Y]\rangle_1 - \sum_{[V]}[Y:V]\langle [I_X],[V]\rangle_1\\ &= \langle [X],[Y]\rangle_1 + \langle [\Omega^{-1}X],[Y]\rangle_1 - \sum_{[V]}[Y:V]\langle [\Omega^{-1}X],[V]\rangle_1,\end{aligned}$$

as desired. □

The *left radical* of the form $\langle -,-\rangle_3$ is the set $\{x\in r(H)\mid \langle x,y\rangle_3=0 \text{ for all } y\in r(H)\}$. This set is exactly the set $\{x\in r(H)\mid x(1-\delta^*_{[P_{\Bbbk}]})=0\}$. Similarly, the *right radical* of the form $\langle -,-\rangle_3$ is exactly the set $\{x\in r(H)\mid x(1-\delta_{[P_{\Bbbk}]})=0\}$. The left and right radicals of the form coincide since $\delta_{[P_{\Bbbk}]}\delta^*_{[P_{\Bbbk}]}=\delta^*_{[P_{\Bbbk}]}\delta_{[P_{\Bbbk}]}=1$. Note that $[P](1-\delta_{[P_{\Bbbk}]})=0$ for any projective module P. Thus, the projective ideal $\mathcal{P}$ of $r(H)$ generated by isomorphism classes of projective H-modules is contained in the radical of the form. For further results about the radical of the form, we need the following lemma.

Lemma 2.2.11 *Let M and Z be two indecomposable H-modules.*

(1) $\langle [M],\delta_{[Z]}\rangle_3 = \delta_{[M],[Z]}+\delta_{[\Omega^{-1}M],[Z]}-\delta_{[I_M],[Z]}$.

(2) $\delta_{[M]} = \begin{cases} -\delta_{[\Omega^{-1}M]}\delta_{[P_{\Bbbk}]}, & M \text{ is not projective};\\ [topM]\delta_{[P_{\Bbbk}]}, & M \text{ is projective}.\end{cases}$

Proof.(1) Note that $\langle [M],\delta_{[Z]}\rangle_3 = \langle [M](1-\delta^*_{[P_{\Bbbk}]}),\delta_{[Z]}\rangle_1$. It follows that

$$\begin{aligned}\langle [M](1-\delta^*_{[P_{\Bbbk}]}),\delta_{[Z]}\rangle_1 &= \langle [M],\delta_{[Z]}\rangle_1 - \langle [I_M]-[\Omega^{-1}M],\delta_{[Z]}\rangle_1\\ &= \langle [M],\delta_{[Z]}\rangle_1 + \langle [\Omega^{-1}M],\delta_{[Z]}\rangle_1 - \langle [I_M],\delta_{[Z]}\rangle_1\\ &= \delta_{[M],[Z]}+\delta_{[\Omega^{-1}M],[Z]}-\delta_{[I_M],[Z]}.\end{aligned}$$

(2) Suppose M is not projective. For any indecomposable module X, we have

$$\begin{aligned}\langle [X], \delta_{[M]} + \delta_{[\Omega^{-1}M]}\delta_{[P_{\Bbbk}]}\rangle_1 &= \langle [X], \delta_{[M]}\rangle_1 + \langle [X]\delta^*_{[P_{\Bbbk}]}, \delta_{[\Omega^{-1}M]}\rangle_1 \text{ by Proposition 2.2.7(2)}\\ &= \langle [X], \delta_{[M]}\rangle_1 + \langle [I_X] - [\Omega^{-1}X], \delta_{[\Omega^{-1}M]}\rangle_1\\ &= \delta_{[X],[M]} - \delta_{[\Omega^{-1}X],[\Omega^{-1}M]} + \delta_{[I_X],[\Omega^{-1}M]}\\ &= 0.\end{aligned}$$

Thus, $\delta_{[M]} = -\delta_{[\Omega^{-1}M]}\delta_{[P_{\Bbbk}]}$ since the form $\langle -, -\rangle_1$ is non-degenerate. Now suppose M is projective, for any indecomposable module X, we have

$$\begin{aligned}\langle [X], \delta_{[M]} - [\mathrm{top}M]\delta_{[P_{\Bbbk}]}\rangle_1 &= \langle [X], \delta_{[M]}\rangle_1 - \langle [X], [\mathrm{top}M]\delta_{[P_{\Bbbk}]}\rangle_1\\ &= \langle [X], \delta_{[M]}\rangle_1 - \langle [X], [\mathrm{top}M]\rangle_2\\ &= \delta_{[X],[M]} - \delta_{[X],[M]} \text{ by Corollary 2.2.8}\\ &= 0.\end{aligned}$$

Thus, $\delta_{[M]} = [\mathrm{top}M]\delta_{[P_{\Bbbk}]}$. □

Recall that an H-module M is called *periodic of period* n if $\Omega^n M \cong M$ for a minimal natural number n (see e.g., [12]).

Theorem 2.2.12 *Let H be of finite representation type. The radical of the form $\langle -, -\rangle_3$ is equal to $\mathcal{P}$ if and only if there are no periodic modules of even period.*

Proof. Note that the projective ideal $\mathcal{P}$ of $r(H)$ is contained in the radical of the form $\langle -, -\rangle_3$. If $\mathcal{P}$ is properly contained in the radical of the form $\langle -, -\rangle_3$, there exist some indecomposable non-projective H-modules M such that $\sum_{[M]} \lambda_{[M]}[M]$ is a non-zero element in the radical of the form. For any indecomposable non-projective module Z, by Lemma 2.2.11 (1), we have $0 = \langle \sum_{[M]} \lambda_{[M]}[M], \delta_{[\Omega^i Z]}\rangle_3 = \lambda_{[\Omega^i Z]} + \lambda_{[\Omega^{i+1} Z]}$, for any $i \geq 0$. It follows that

$$\lambda_{[\Omega^i Z]} = (-1)^i \lambda_{[Z]}, \text{ for any } i \geq 0.$$

This forces $\lambda_{[Z]} = 0$ if Z is a periodic module of odd period. However, $\sum_{[M]} \lambda_{[M]}[M]$ is not zero, implying that there exists a periodic module M of even period with $\lambda_{[M]} \neq 0$. Conversely, suppose the radical of the form $\langle -, -\rangle_3$ is equal to $\mathcal{P}$. We claim that the H-module category has no periodic modules of even period. Otherwise, if M is a periodic module of even period $2s$. It follows from Lemma 2.2.11 (2) that

$$\sum_{i=1}^{2s}(-1)^i\delta_{[\Omega^i M]}(1-\delta^*_{[P_\Bbbk]})=\sum_{i=1}^{2s}(-1)^i(\delta_{[\Omega^i M]}+\delta_{[\Omega^{i-1}M]})=0.$$

Thus, $\sum_{i=1}^{2s}(-1)^i\delta_{[\Omega^i M]}$ belongs to the radical of the form $\langle -,-\rangle_3$. Let $\sum_{i=1}^{2s}(-1)^i\delta_{[\Omega^i M]}=\sum_j\lambda_j[P_j]$ for some indecomposable projective modules P_j. By Remark 2.2.3, $[P_j]$ can be written as $[P_j]=\sum_{[M]\in\mathrm{ind}(H)}\langle [M],[P_j]\rangle_1\delta_{[M]}$. It follows that

$$\sum_{i=1}^{2s}(-1)^i\delta_{[\Omega^i M]}=\sum_j\sum_{[M]\in\mathrm{ind}(H)}\lambda_j\langle [M],[P_j]\rangle_1\delta_{[M]}.$$

Comparing the coefficient of $\delta_{[\Omega^i M]}$ in both two sides of the above equality, we obtain that

$$(-1)^i=\sum_j\lambda_j\dim_\Bbbk \mathrm{Hom}_H(\Omega^i M,P_j)=\sum_j\lambda_j\dim_\Bbbk \mathrm{Ext}^i_H(M,P_j)=0,$$

a contradiction. □

§2.3 Some ring theoretic properties of Green rings

In this section, we use an associative non-degenerate bilinear form to explore some ring theoretic properties of the Green ring $r(H)$ of H. We show that the Green ring $r(H)$ is a Frobenius algebra over $\mathbb{Z}$ if H is of finite representation type. We describe the relation between the Green ring $r(H)$ and the Grothendieck ring $G_0(H)$ of H. We give several one-sided ideals of $r(H)$, which are useful to describe the Jacobson radical and central primitive idempotents of $r(H)$.

Note that the $\mathbb{Z}$-bilinear form $\langle -,-\rangle_1$ is not associative in general. However, we may modify it as follows:

$$([X],[Y]):=\langle [X],[Y]^*\rangle_1=\dim_\Bbbk \mathrm{Hom}_H(X,Y^*). \tag{2.11}$$

Then $(-,-)$ extends to a $\mathbb{Z}$-bilinear form on $r(H)$.

Lemma 2.3.1 *For H-modules X,Y and Z, the form $(-,-)$ satisfies the following:*

(1) $([X][Y],[Z]) = ([X],[Y][Z])$.

(2) $([X],[Y]) = ([Y]^{**},[X])$. *If* S^2 *(the square of antipode) is inner, then* $([X],[Y]) = ([Y],[X])$.

Proof.(1) The associativity of the form follows from Lemma 2.1.4 (1), i.e.,

$$\begin{aligned}([X][Y],[Z]) &= \dim_{\Bbbk} \mathrm{Hom}_H(X \otimes Y, Z^*) \\ &= \dim_{\Bbbk} \mathrm{Hom}_H(X, (Y \otimes Z)^*) \\ &= ([X],[Y][Z]).\end{aligned}$$

(2) The $\Bbbk$-linear isomorphism $\mathrm{Hom}_H(X, Y^*) \cong \mathrm{Hom}_H(Y^{**}, X^*)$ following from Lemma 2.1.4 (see also [46]) implies that $([X],[Y]) = ([Y]^{**},[X])$. If S^2 is inner, the anti-automorphism $*$ of $r(H)$ is an involution. In this case, $([X],[Y]) = ([Y],[X])$. □

The following result can be deduced directly from Lemma 2.2.2.

Lemma 2.3.2 *The following hold in* $r(H)$*:*

(1) *For any two indecomposable modules* X *and* Z, $(\delta^*_{[Z]},[X]) = \delta_{[Z],[X]}$.

(2) *For any* $x \in r(H)$, $x = \sum_{[M]\in ind(H)}(\delta^*_{[M]}, x)[M]$.

(3) *The form* $(-,-)$ *is non-degenerate.*

As an immediate consequence we obtain the following Frobenius property of $r(H)$.

Proposition 2.3.3 *Let* H *be of finite representation type. The Green ring* $r(H)$ *is a Frobenius* $\mathbb{Z}$*-algebra. Moreover,* $r(H)$ *is a symmetric* $\mathbb{Z}$*-algebra if* S^2 *is inner.*

Proof.Note that $r(H)^\vee := \mathrm{Hom}_{\mathbb{Z}}(r(H),\mathbb{Z})$ is a $(r(H),r(H))$-bimodule via $(afb)(x) = f(bxa)$, for $a,b,x \in r(H)$ and $f \in r(H)^\vee$. Since H is of finite representation type, the form $(-,-)$ is associative and non-degenerate with a pair of dual bases $\{\delta^*_{[M]}, [M] \mid [M] \in \mathrm{ind}(H)\}$. Thus, the map ρ from $r(H)$ to $r(H)^\vee$ given by $x \mapsto (-,x)$ is a left $r(H)$-module isomorphism, and hence $r(H)$ is a Frobenius $\mathbb{Z}$-algebra. Moreover, if the square of the antipode is inner, the bilinear form is symmetric and hence ρ is a $(r(H),r(H))$-bimodule isomorphism. It follows that $r(H)$ is a symmetric $\mathbb{Z}$-algebra. □

Remark 2.3.4 *Let H be of finite representation type.*

(1) *The Green ring $r(H)$ is a Frobenius $\mathbb{Z}$-algebra with a pair of dual bases $\{\delta^*_{[M]}, [M] \mid [M] \in ind(H)\}$ with respect to the form $(-,-)$. The equality of Lemma 2.3.2 (2) is now equivalent to the following equality:*

$$x = \sum_{[M]\in ind(H)} (x, [M])\delta^*_{[M]}, \text{ for } x \in r(H).$$

This means that the transformation matrix from the dual basis $\{\delta^*_{[M]} \mid [M] \in ind(H)\}$ to the standard basis $ind(H)$ is an invertible integer matrix with entries $([X],[Y]) = \dim_{\Bbbk} Hom_H(X, Y^*)$ for $[X],[Y] \in ind(H)$.

(2) *If H is semisimple, then S^2 is inner [41] and $\delta^*_{[M]} = [M]^* = [M^*]$. In this case, $r(H) = G_0(H)$ is symmetric (see Proposition 2.3.3) and semiprime [46] with a pair of dual bases $\{[M^*], [M] \mid [M] \in ind(H)\}$. We refer to [72] for more details in the semisimple case.*

The bilinear form $(-,-)$ can be used to describe the relation between the Green ring $r(H)$ and the Grothendieck ring $G_0(H)$ of H. Let $\mathcal{P}^\perp$ be the subgroup of $r(H)$ which is orthogonal to $\mathcal{P}$ with respect to the form $(-,-)$. Then $\mathcal{P}^\perp$ is a two-sided ideal of $r(H)$.

Proposition 2.3.5 *The Grothendieck ring $G_0(H)$ is isomorphic to the quotient ring $r(H)/\mathcal{P}^\perp$.*

Proof. Observe that the natural morphism φ given in (2.8) is surjective. It is sufficient to show that $\ker\varphi = \mathcal{P}^\perp$. Suppose $\sum_{[M]\in \mathrm{ind}(H)} \lambda_{[M]}[M] \in \ker\varphi$, where each $\lambda_{[M]} \in \mathbb{Z}$. Then

$$\sum_{[V]} \sum_{[M]\in \mathrm{ind}(H)} \lambda_{[M]}[M:V][V] = 0.$$

Note that a short exact sequence tensoring over $\Bbbk$ with a projective module P is split. It follows that $[M][P] = \sum_{[V]}[M:V][V][P]$ holds in $r(H)$, and hence

$$(\sum_{[M]\in \mathrm{ind}(H)} \lambda_{[M]}[M], [P]) = (\sum_{[M]\in \mathrm{ind}(H)} \lambda_{[M]}[M][P], [\Bbbk])$$

$$= (\sum_{[V]} \sum_{[M]\in \operatorname{ind}(H)} \lambda_{[M]}[M:V][V][P], [\Bbbk])$$
$$= 0.$$

This implies that $\sum_{[M]\in \operatorname{ind}(H)} \lambda_{[M]}[M] \in \mathcal{P}^{\perp}$. Now, we assume $\sum_{[M]\in \operatorname{ind}(H)} \lambda_{[M]}[M] \in \mathcal{P}^{\perp}$. Note that $[P]y \in \mathcal{P}$ for any $y \in r(H)$ and $[P] \in \mathcal{P}$. We have

$$(\sum_{[M]\in \operatorname{ind}(H)} \lambda_{[M]}[M][P], y) = (\sum_{[M]\in \operatorname{ind}(H)} \lambda_{[M]}[M], [P]y) = 0.$$

This implies that $\sum_{[M]\in \operatorname{ind}(H)} \lambda_{[M]}[M][P] = 0$ as the form $(-,-)$ is non-degenerate. Replacing $[M][P]$ by $\sum_{[V]}[M:V][V][P]$, we obtain the following equality:

$$\sum_{[V]} \sum_{[M]\in \operatorname{ind}(H)} \lambda_{[M]}[M:V][V][P] = 0. \tag{2.12}$$

Note that $\mathcal{P}$ is a $G_0(H)$-module under the action given by $[V][P] = [V \otimes P] \in \mathcal{P}$. Moreover, the $G_0(H)$-module $\mathcal{P}$ is faithful, see [46, Section 3.1]. It follows from (2.12) that $\sum_{[V]} \sum_{[M]\in \operatorname{ind}(H)} \lambda_{[M]}[M:V][V] = 0$, namely, $\sum_{[M]\in \operatorname{ind}(H)} \lambda_{[M]}[M] \in \ker \varphi$. $\square$

Now we turn to the special element $\delta_{[\Bbbk]}$, which plays an important role in the study of the Green ring $r(H)$. For any indecomposable module X, the elements $[X]$, $\delta_{[\Bbbk]}$ and $\delta_{[X]}$ satisfy the following relations.

Theorem 2.3.6 *Let X be an indecomposable H-module.*

(1) $\Bbbk \nmid X^* \otimes X$ *if and only if* $[X]\delta_{[\Bbbk]} = 0$.

(2) $\Bbbk \nmid X \otimes X^*$ *if and only if* $\delta_{[\Bbbk]}[X] = 0$.

(3) $\Bbbk \mid X^* \otimes X$ *if and only if* $[X]\delta_{[\Bbbk]} = \delta_{[X]}$.

(4) $\Bbbk \mid X \otimes X^*$ *if and only if* $\delta_{[\Bbbk]}[X] = \delta_{[X]}$.

Proof.If H is semisimple, then $\Bbbk \mid X^* \otimes X$ and $\Bbbk \mid X \otimes X^*$. In this case, Part (3) and Part (4) hold obviously because $\delta_{[\Bbbk]} = [\Bbbk]$ and $\delta_{[X]} = [X]$. Assume H is not semisimple, we only show Part (1) and Part (3) and the proofs of Part (2) and Part (4) are similar.

(1) If $\Bbbk \nmid X^* \otimes X$, by Proposition 2.1.10, the map $id_X \otimes \sigma$ is a split epimorphism. It follows from (2.5) that $[X \otimes E] = [X \otimes \tau(\Bbbk)] + [X]$, and hence $[X]\delta_{[\Bbbk]} = 0$. Conversely, if $[X]\delta_{[\Bbbk]} = 0$, then $0 = (([X]\delta_{[\Bbbk]})^*, [X]) = (\delta^*_{[\Bbbk]}, [X]^*[X])$. This means that $\Bbbk \nmid X^* \otimes X$.

(3) If $\Bbbk \mid X^* \otimes X$, then the map $id_X \otimes \sigma$ is right almost split by Proposition 2.1.12. It follows from (2.5) and Proposition 2.2.1 that $\delta_{[X]} = [X \otimes \tau(\Bbbk)] - [X \otimes E] + [X] = [X]\delta_{[\Bbbk]}$. Conversely, if $[X]\delta_{[\Bbbk]} = \delta_{[X]}$, then $1 = (\delta^*_{[X]}, [X]) = (([X]\delta_{[\Bbbk]})^*, [X]) = (\delta^*_{[\Bbbk]}, [X]^*[X])$. It follows that $\Bbbk \mid X^* \otimes X$. □

As an application of Theorem 2.3.6, we are able to determine the multiplicity of the trivial module $\Bbbk$ in the decomposition of the tensor product $X \otimes X^*$ and $X^* \otimes X$ respectively. For the case where H is semisimple over the field $\Bbbk$ of characteristic 0, this was done by Zhu [75, Lemma 1], see also [72, Proposition 2.1].

Corollary 2.3.7 *Let X be an indecomposable H-module.*

(1) *The multiplicity of $\Bbbk$ in $X^* \otimes X$ is either 0 or 1.*

(2) *The multiplicity of $\Bbbk$ in $X \otimes X^*$ is either 0 or 1.*

Proof.(1) We only prove Part (1), the proof of Part (2) is similar. Note that the multiplicity of $\Bbbk$ in $X^* \otimes X$ is $(\delta^*_{[\Bbbk]}, [X^*][X])$. By Theorem 2.3.6, we have

$$(\delta^*_{[\Bbbk]}, [X^*][X]) = (([X]\delta_{[\Bbbk]})^*, [X]) = \begin{cases} 0, & \Bbbk \nmid X^* \otimes X, \\ 1, & \Bbbk \mid X^* \otimes X, \end{cases}$$

as desired. □

The following result can be deduced from Theorem 2.3.6.

Proposition 2.3.8 *Let $0 \to X \to Y \to Z \to 0$ be an almost split sequence of H-modules.*

(1) *$\Bbbk \mid Z \otimes Z^*$ if and only if $\Bbbk \mid X \otimes X^*$.*

(2) *$\Bbbk \mid Z^* \otimes Z$ if and only if $\Bbbk \mid X^* \otimes X$.*

Proof. Applying the duality functor $*$ to the almost split sequence $0 \to X \to Y \to Z \to 0$, we get the almost split sequence $0 \to Z^* \to Y^* \to X^* \to 0$, see [4, P144]. Note that both Z and X^* are indecomposable, see [4, Proposition 1.14, ChV]. This implies that $\delta_{[Z]}^* = \delta_{[X^*]}$.

(1) If $\mathbb{k} \mid Z \otimes Z^*$, by Theorem 2.3.6, we have $\delta_{[\mathbb{k}]}[Z] = \delta_{[Z]}$. We claim that $\mathbb{k} \mid X \otimes X^*$. Otherwise, $\mathbb{k} \nmid X \otimes X^*$, and hence $\mathbb{k} \nmid X^{**} \otimes X^*$. This leads to $[X^*]\delta_{[\mathbb{k}]} = 0$ by Theorem 2.3.6. However,

$$1 = (\delta_{[X^*]}^*, [X^*]) = (\delta_{[Z]}^{**}, [X^*]) = ([X^*], \delta_{[Z]}) = ([X^*]\delta_{[\mathbb{k}]}, [Z]) = 0,$$

a contradiction. Conversely, if $\mathbb{k} \mid X \otimes X^*$, then $\mathbb{k} \mid X^{**} \otimes X^*$. This yields that $[X^*]\delta_{[\mathbb{k}]} = \delta_{[X^*]}$. We claim that $\mathbb{k} \mid Z \otimes Z^*$. Otherwise, $\delta_{[\mathbb{k}]}[Z] = 0$ by Theorem 2.3.6. Then

$$1 = (\delta_{[Z]}^*, [Z]) = (\delta_{[X^*]}, [Z]) = ([X^*], \delta_{[\mathbb{k}]}[Z]) = 0,$$

a contradiction.

(2) Applying Part (1) to the almost split sequence $0 \to Z^* \to Y^* \to X^* \to 0$, we may obtain the desired result. □

Denote by $\mathcal{J}_+$ and $\mathcal{J}_-$ the subgroups of $r(H)$ respectively as follows:

$$\mathcal{J}_+ := \mathbb{Z}\{\delta_{[M]} \mid [M] \in \text{ind}(H) \text{ and } \mathbb{k} \mid M \otimes M^*\},$$

$$\mathcal{J}_- := \mathbb{Z}\{\delta_{[M]} \mid [M] \in \text{ind}(H) \text{ and } \mathbb{k} \mid M^* \otimes M\}.$$

By Theorem 2.3.6, $\mathcal{J}_+$ (resp. $\mathcal{J}_-$) is a right (resp. left) ideal of $r(H)$ generated by $\delta_{[\mathbb{k}]}$. Moreover, we have $\mathcal{J}_+^* = \mathcal{J}_-$ and $\mathcal{J}_-^* = \mathcal{J}_+$ by Proposition 2.3.8.

Now let $\mathcal{P}_+$ and $\mathcal{P}_-$ denote the subgroups of $r(H)$ as follows:

$$\mathcal{P}_+ := \mathbb{Z}\{[M] \in \text{ind}(H) \mid \mathbb{k} \nmid M \otimes M^*\},$$

$$\mathcal{P}_- := \mathbb{Z}\{[M] \in \text{ind}(H) \mid \mathbb{k} \nmid M^* \otimes M\}.$$

Then $\mathcal{P}_+$ and $\mathcal{P}_-$ both contain the ideal $\mathcal{P}$ of $r(H)$. It follows from Proposition 2.1.8 that $\mathcal{P}_+$ is a right ideal of $r(H)$ and $\mathcal{P}_-$ is a left ideal of $r(H)$. Obviously, $\mathcal{P}_+^* = \mathcal{P}_-$ and $\mathcal{P}_-^* = \mathcal{P}_+$.

According to the associativity and non-degeneracy of the form $(-,-)$, we have $\mathcal{P}_-x = 0$ if and only if $(\mathcal{P}_-, x) = 0$ if and only if $(x, \mathcal{P}_-) = 0$ since $\mathcal{P}_- = \mathcal{P}_-^{**}$. Similarly, $x\mathcal{P}_+ = 0$ if and only if $(x, \mathcal{P}_+) = 0$ if and only if $(\mathcal{P}_+, x) = 0$. Thus, the right annihilator $r(\mathcal{P}_-)$ of $\mathcal{P}_-$ and left annihilator $l(\mathcal{P}_+)$ of $\mathcal{P}_+$ can be expressed respectively as follows:

$$r(\mathcal{P}_-) := \{x \in r(H) \mid (x, y) = 0 \text{ for all } y \in \mathcal{P}_-\},$$

$$l(\mathcal{P}_+) := \{x \in r(H) \mid (y, x) = 0 \text{ for all } y \in \mathcal{P}_+\}.$$

The relations between these one-sided ideals of $r(H)$ can be described as follows.

Proposition 2.3.9 *Let H be of finite representation type.*

(1) $\mathcal{J}_+ = r(\mathcal{P}_-)$.

(2) $\mathcal{J}_- = l(\mathcal{P}_+)$.

Proof. It is sufficient to prove Part (1) and the proof of Part (2) is similar. For any two indecomposable modules X and Y satisfying $\Bbbk \mid X \otimes X^*$ and $\Bbbk \nmid Y^* \otimes Y$, by Theorem 2.3.6, we have

$$(\delta_{[X]}, [Y]) = (\delta_{[\Bbbk]}[X], [Y]) = ([Y^{**}]\delta_{[\Bbbk]}, [X]) = (0, [X]) = 0.$$

This implies that $\mathcal{J}_+ \subseteq r(\mathcal{P}_-)$. For any $x \in r(\mathcal{P}_-)$,

$$\begin{aligned} x &= \sum_{[M]\in \mathrm{ind}(H)} (x, [M])\delta^*_{[M]} \quad \text{by Remark 2.3.4(1)} \\ &= \sum_{\Bbbk \mid M^* \otimes M} (x, [M])\delta^*_{[M]} \quad \text{as } x \in r(\mathcal{P}_-). \end{aligned}$$

We have that $x \in \mathcal{J}_-^* = \mathcal{J}_+$, and hence $r(\mathcal{P}_-) \subseteq \mathcal{J}_+$. □

In the following, we shall use these one-sided ideals to get information about the Jacobson radical and central primitive idempotents of $r(H)$. We first need the following lemma.

Lemma 2.3.10 *For any $x \in r(H)$, we have the following:*

(1) *If $xx^* = 0$, then $x \in \mathcal{P}_+$.*

(2) *If* $x^*x = 0$, *then* $x \in \mathcal{P}_-$.

Proof. It suffices to prove Part (1), the proof of Part (2) is similar. Suppose

$$x = \sum_{\Bbbk | M\otimes M^*} \lambda_{[M]}[M] + \sum_{\Bbbk \nmid M\otimes M^*} \lambda_{[M]}[M],$$

where each $\lambda_{[M]} \in \mathbb{Z}$. By Theorem 2.1.7 (1) and Corollary 2.3.7, the coefficient of the identity $[\Bbbk]$ in the linear expression of xx^* with respect to the basis $\text{ind}(H)$ is $\sum_{\Bbbk | M\otimes M^*} \lambda_{[M]}^2$. Thus, if $xx^* = 0$, then $\lambda_{[M]} = 0$ for any indecomposable module M satisfying $\Bbbk \mid M \otimes M^*$. Hence $x = \sum_{\Bbbk \nmid M\otimes M^*} \lambda_{[M]}[M] \in \mathcal{P}_+$. $\square$

Proposition 2.3.11 *Let H be of finite representation type. If the Green ring $r(H)$ is commutative, then the Jacobson radical $J(r(H))$ of $r(H)$ is contained in $\mathcal{P}_+ \cap \mathcal{P}_-$.*

Proof. Since $r(H)$ is commutative and finitely generated as an algebra over $\mathbb{Z}$, the Jacobson radical $J(r(H))$ is equal to the nilradical of $r(H)$. For any $x \in J(r(H))$, let $x_0 := x$ and $x_{i+1} := x_i x_i^*$ for $i \geq 0$. Then there exists some k such that $x_k = 0$. We write

$$x = \sum_{\Bbbk | M\otimes M^*} \lambda_{[M]}[M] + \sum_{\Bbbk \nmid M\otimes M^*} \lambda_{[M]}[M]$$

and

$$x_1 = xx^* = \sum_{\Bbbk | M\otimes M^*} \mu_{[M]}[M] + \sum_{\Bbbk \nmid M\otimes M^*} \mu_{[M]}[M],$$

for all $\lambda_{[M]}$ and $\mu_{[M]}$ in $\mathbb{Z}$. As shown in the proof of Lemma 2.3.10, the coefficient of $[\Bbbk]$ in $x_1 = xx^*$ is $\mu_{[\Bbbk]} = \sum_{\Bbbk | M\otimes M^*} \lambda_{[M]}^2$ and the coefficient of $[\Bbbk]$ in $x_2 = x_1 x_1^*$ is $\sum_{\Bbbk | M\otimes M^*} \mu_{[M]}^2$. If $\mu_{[\Bbbk]} \neq 0$, then $\sum_{\Bbbk | M\otimes M^*} \mu_{[M]}^2 \neq 0$, and hence $x_2 \neq 0$. Repeating this process, we obtain that $x_i \neq 0$ for any $i \geq 0$. This contradicts to the fact that $x_k = 0$. In view of this, $\mu_{[\Bbbk]} = 0$, and hence $x = \sum_{\Bbbk \nmid M\otimes M^*} \lambda_{[M]}[M] \in \mathcal{P}_+$. Similarly, if $x \in J(r(H))$, then $x \in \mathcal{P}_-$. We obtain that $J(r(H)) \subseteq \mathcal{P}_+ \cap \mathcal{P}_-$. $\square$

Now we are able to locate central primitive idempotents of $r(H)$.

Proposition 2.3.12 *Let e be a central primitive idempotent of $r(H)$. Then either $e \in \mathcal{P}_+ \cap \mathcal{P}_-$ or $1 - e \in \mathcal{P}_+ \cap \mathcal{P}_-$.*

Proof. If e is a central primitive idempotent of $r(H)$, so is e^* since the duality operator $*$ is an anti-automorphism of $r(H)$. It follows that $e = e^*$ or $ee^* = e^*e = 0$. If $ee^* = e^*e = 0$, by Lemma 2.3.10, $e \in \mathcal{P}_+$ and $e \in \mathcal{P}_-$ as well. Now suppose $e = e^*$, and let

$$e = \sum_{\Bbbk | M \otimes M^*} \lambda_{[M]}[M] + \sum_{\Bbbk \nmid M \otimes M^*} \lambda_{[M]}[M].$$

Comparing the coefficients of $[\Bbbk]$ in both sides of the equation $ee^* = e$, we obtain that $\sum_{\Bbbk | M \otimes M^*} \lambda_{[M]}^2 = \lambda_{[\Bbbk]}$. This implies that $\lambda_{[\Bbbk]} = 0$ or 1 and $\lambda_{[M]} = 0$ for all $[M]$ satisfying $[M] \neq [\Bbbk]$ and $\Bbbk \mid M \otimes M^*$. Hence e has the following reduced form

$$e = \lambda_{[\Bbbk]}[\Bbbk] + \sum_{\Bbbk \nmid M \otimes M^*} \lambda_{[M]}[M].$$

In the meanwhile, if we write

$$e = \sum_{\Bbbk | M^* \otimes M} \mu_{[M]}[M] + \sum_{\Bbbk \nmid M^* \otimes M} \mu_{[M]}[M].$$

Then the equation $e^*e = e$ yields that

$$e = \mu_{[\Bbbk]}[\Bbbk] + \sum_{\Bbbk \nmid M^* \otimes M} \mu_{[M]}[M].$$

Thus, $\mu_{[\Bbbk]} = \lambda_{[\Bbbk]}$ which is equal to 0 or 1. We conclude that $e \in \mathcal{P}_+ \cap \mathcal{P}_-$ if $\mu_{[\Bbbk]} = \lambda_{[\Bbbk]} = 0$, and $1 - e \in \mathcal{P}_+ \cap \mathcal{P}_-$ if $\mu_{[\Bbbk]} = \lambda_{[\Bbbk]} = 1$. $\square$

Chapter 3 The stable Green rings of Hopf algebras

In [68, 69] we studied the Green rings of finite dimensional pointed rank one Hopf algebras of both nilpotent and non-nilpotent type respectively. One of the interesting properties possessed by those Green rings is that the complexified stable Green algebras are group-like algebras, and consequently bi-Frobenius algebras, introduced and investigated by Doi and Takeuchi (cf. [20–23]). The notion of a bi-Frobenius algebra is a natural generalization of a finite dimensional Hopf algebra, and possesses many properties that a finite dimensional Hopf algebra does. However, to find more examples of bi-Frobenius algebras, which are not Hopf algebras, is not easy at all.

As we shall see the stable Green rings of finite dimensional Hopf algebras may provide interesting examples of group-like algebras and bi-Frobenius algebras in certain circumstances. Moreover, these bi-Frobenius algebras are themselves transitive fusion rings coming from (not necessary semisimple) stable categories. To do so, our principal technical tools are the bilinear forms on the Green rings introduced in previous chapter, see also [8, 52, 72]. More explicitly, we shall show that the bilinear form $(-,-)$ on the Green ring $r(H)$ described in previous chapter could induce a bilinear form on the stable Green ring of H. The induced form on the stable Green ring is associative, but degenerate in general. We give some equivalent conditions for the non-degeneracy of the form. If the form is non-degenerate, the complexified stable Green algebra is a group-like algebra, and hence a bi-Frobenius algebra. Especially, we consider a special finite dimensional pointed Hopf algebra of rank one, known as a Radford Hopf algebra. We describe the bi-Frobenius algebra structure on the complexified stable Green algebra of the Radford Hopf algebra from the polynomial point of view.

§3.1 The stable Green rings

In this section, we use a bilinear form to study the stable Green ring of H. The Green ring of the stable category H-$\underline{\text{mod}}$ of H is called the stable Green ring of H, denoted $r_{st}(H)$. As the stable category H-$\underline{\text{mod}}$ is a quotient category of H-mod, the stable Green ring $r_{st}(H)$ is indeed a quotient ring of the Green ring $r(H)$, namely, $r_{st}(H) \cong r(H)/\mathcal{P}$ as shown below. This isomorphism enables us to define a new form $[-,-]_{st}$ on $r_{st}(H)$ which is induced from the form $(-,-)$ on $r(H)$. The form $[-,-]_{st}$ is associative but degenerate in general. We determine the left and right radicals of the form $[-,-]_{st}$ respectively, and give several equivalent conditions for the non-degeneracy of the form. Under the assumption that H is of finite representation type, the Green ring $r(H)$ is commutative and the form $[-,-]_{st}$ is non-degenerate, we show that the Jacobson radical of $r(H)$ is equal to $\mathcal{P}\cap\mathcal{P}^{\perp}$ if and only if the Grothendieck ring $G_0(H)$ is semiprime.

Recall that the *stable category* H-$\underline{\text{mod}}$ has the same objects as H-mod does, and the space of morphisms from X to Y in H-$\underline{\text{mod}}$ is the quotient space

$$\underline{\text{Hom}}_H(X,Y) := \text{Hom}_H(X,Y)/\mathcal{P}(X,Y),$$

where $\mathcal{P}(X,Y)$ is the subspace of $\text{Hom}_H(X,Y)$ consisting of morphisms factoring through projective modules. The stable category H-$\underline{\text{mod}}$ is a triangulated [37] monoidal category with the monoidal structure stemming from that of H-mod.

Proposition 3.1.1 *The stable category H-$\underline{\text{mod}}$ is semisimple if and only if any indecomposable H-module is either simple or projective.*

Proof.If any indecomposable H-module is either simple or projective, using the same method as [2, Theorem 2.7], one is able to prove that H-$\underline{\text{mod}}$ is semisimple. Conversely, suppose that H-$\underline{\text{mod}}$ is semisimple. Note that all simple objects of H-$\underline{\text{mod}}$ are those non-projective indecomposable H-modules. If H-mod has an indecomposable object M which is neither simple nor projective, then the indecomposable H-modules M and $\text{Soc}M$ are two simple objects in H-$\underline{\text{mod}}$. Since the inclusion map $\text{Soc}M \to M$ induces a surjective map $M^* \to (\text{Soc}M)^*$, it follows from Proposition 2.2.10 (2) that

$$\dim_{\Bbbk} \underline{\text{Hom}}_H(M^*, (\text{Soc}M)^*) = \langle M^*, (\text{Soc}M)^*\rangle_3 = \langle M^*, (\text{Soc}M)^*\rangle_1 \neq 0.$$

This means that $M^* \cong (\text{Soc}M)^*$ in H-$\underline{\text{mod}}$, so is an isomorphism in H-mod [62, Ch III,Lemma 4.3], a contradiction. $\square$

The Green ring of the stable category H-$\underline{\text{mod}}$ is called the *stable Green ring* of H, denoted $r_{st}(H)$. Obviously, the stable Green ring $r_{st}(H)$ admits a $\mathbb{Z}$-basis consisting of all isomorphism classes of indecomposable non-projective H-modules. As the stable category H-$\underline{\text{mod}}$ is a quotient category of H-mod, the stale Green ring $r_{st}(H)$ can be regarded as the quotient ring of the Green ring $r(H)$.

Proposition 3.1.2 *The stable Green ring $r_{st}(H)$ is isomorphic to the quotient ring $r(H)/\mathcal{P}$.*

Proof. The canonical functor F from H-mod to H-$\underline{\text{mod}}$ given by $F(M) = M$ and $F(\phi) = \underline{\phi}$, for $\phi \in \text{Hom}_H(M, N)$ with the canonical image $\underline{\phi} \in \underline{\text{Hom}}(M, N)$, is a full dense tensor functor. Such a functor induces a ring epimorphism f from $r(H)$ to $r_{st}(H)$ such that $f(\mathcal{P}) = 0$. Hence there is a unique ring epimorphism $\overline{f}$ from $r(H)/\mathcal{P}$ to $r_{st}(H)$ such that $\overline{f}(\overline{x}) = f(x)$, for any $x \in r(H)$ with the canonical image $\overline{x} \in r(H)/\mathcal{P}$. For any two H-modules M and N without nonzero projective direct summands, it follows from [62, Ch III,Lemma 4.3] that $M \cong N$ in H-mod if and only if $M \cong N$ in H-$\underline{\text{mod}}$. From this we conclude that $r_{st}(H)$ is isomorphic to $r(H)/\mathcal{P}$, since there is a one to one correspondence between the indecomposable objects in H-$\underline{\text{mod}}$ and the non-projective indecomposable objects in H-mod. $\square$

We identify $r(H)/\mathcal{P}$ with $r_{st}(H)$ and denote $\overline{x}$ the element in $r_{st}(H)$ for any $x \in r(H)$. Since $(\delta^*_{[\Bbbk]}, x) = 0$ for any $x \in \mathcal{P}$, the linear functional $(\delta^*_{[\Bbbk]}, -)$ on $r(H)$ induces a linear functional on $r_{st}(H)$. Using this functional, we define a form on $r_{st}(H)$ as follows:

$$[\overline{x}, \overline{y}]_{st} := (\delta^*_{[\Bbbk]}, xy), \text{ for } x, y \in r(H). \tag{3.1}$$

It is obvious that the form $[-, -]_{st}$ is associative and $*$-symmetric: $[\overline{x}, \overline{y}]_{st} = [\overline{y}^*, \overline{x}^*]_{st}$.

The *left radical* of the form $[-, -]_{st}$ is the subgroup of $r_{st}(H)$ consisting of $\overline{x} \in r_{st}(H)$ such that $[\overline{x}, \overline{y}]_{st} = 0$ for all $\overline{y} \in r_{st}(H)$. The *right radical* of the form $[-, -]_{st}$ is defined similarly. The form $[-, -]_{st}$ is non-degenerate if and only if the left radical (or equivalently, the right radical) of the form $[-, -]_{st}$ is zero.

Proposition 3.1.3 *The left radical of the form $[-, -]_{st}$ is equal to $\mathcal{P}_+/\mathcal{P}$ and the right radical of the form $[-, -]_{st}$ is equal to $\mathcal{P}_-/\mathcal{P}$.*

Proof.We only consider the left radical of the form $[-,-]_{st}$. For $x, y \in r(H)$, if $x \in \mathcal{P}_+$, then $xy \in \mathcal{P}_+$ since $\mathcal{P}_+$ is a right ideal of $r(H)$. It follows that $[\overline{x}, \overline{y}]_{st} = (\delta^*_{[\Bbbk]}, xy) = 0$, and hence $\overline{x}$ belongs to the left radical of the form $[-,-]_{st}$. Conversely, we suppose that $\overline{x}$ belongs to the left radical of the form $[-,-]_{st}$ for $x = \sum_{[M]\in \mathrm{ind}(H)} \lambda_{[M]}[M]$. The inverse of $*$ under the composition is denoted $\star$. For any $[M] \in \mathrm{ind}(H)$, by Theorem 2.3.6, we have

$$0 = [\overline{x}, \overline{[M]^\star}]_{st} = (\delta^*_{[\Bbbk]}, x[M]^\star) = ([M]^{\star\star\star}\delta^*_{[\Bbbk]}, x) = ((\delta_{[\Bbbk]}[M])^*, x) = \begin{cases} 0, & \Bbbk \nmid M \otimes M^*, \\ \lambda_{[M]}, & \Bbbk \mid M \otimes M^*. \end{cases}$$

This implies that $x = \sum_{\Bbbk \nmid M\otimes M^*} \lambda_{[M]}[M] \in \mathcal{P}_+$. □

Now let $\mathcal{J}$ be the subgroup of $r(H)$ as follows:

$$\mathcal{J} = \mathbb{Z}\{\delta_{[M]} \mid [M] \in \mathrm{ind}(H) \text{ and } M \text{ not projective}\}.$$

Then $\mathcal{J}_+$ and $\mathcal{J}_-$ are both contained in $\mathcal{J}$. If H is of finite representation type, then $\mathcal{J}$ is nothing but $\ker\varphi$ $(= \mathcal{P}^\perp)$ by Lemma 2.2.2 (5). We are now ready to characterize the non-degeneracy of the form $[-,-]_{st}$ using Proposition 3.1.3.

Proposition 3.1.4 *The following statements are equivalent:*

(1) *The form $[-,-]_{st}$ is non-degenerate.*

(2) $\mathcal{P}_+ = \mathcal{P}_- = \mathcal{P}$.

(3) $\mathcal{J}_+ = \mathcal{J}_- = \mathcal{J}$.

(4) *$\mathcal{J}$ is an ideal of $r(H)$ generated by the central element $\delta_{[\Bbbk]}$, the left annihilator $l(\mathcal{J})$ and right annihilator $r(\mathcal{J})$ of $\mathcal{J}$ are both equal to $\mathcal{P}$.*

Proof.It can be seen from Proposition 3.1.3 that Part (1) and Part (2) are equivalent. The equality $\mathcal{P}_+ = \mathcal{P}$ is equivalent to saying that $\Bbbk \nmid M \otimes M^*$ if and only if M is projective, or equivalently, $\Bbbk \mid M \otimes M^*$ if and only if M is not projective, this is precisely $\mathcal{J}_+ = \mathcal{J}$. Similarly, $\mathcal{P}_- = \mathcal{P}$ if and only if $\mathcal{J}_- = \mathcal{J}$.

(1) $\Rightarrow$ (4) If the form $[-,-]_{st}$ is non-degenerate, then $\mathcal{J}_+ = \mathcal{J}_- = \mathcal{J}$. It follows from Theorem 2.3.6 that $\delta_{[\Bbbk]}$ is a central element of $r(H)$ and $\mathcal{J}$ is an ideal of $r(H)$

generated by $\delta_{[\Bbbk]}$. Observe that $\mathcal{J}_+ = \mathcal{J}_- = \mathcal{J}$ implying that $\mathcal{J}^* = \mathcal{J}_-^* = \mathcal{J}_+ = \mathcal{J}$. This deduces that the left and right annihilators of $\mathcal{J}$ coincide: $l(\mathcal{J}) = r(\mathcal{J})$. Let $I := l(\mathcal{J}) = r(\mathcal{J})$. We claim that $I = \mathcal{P}$. The inclusion $\mathcal{P} \subseteq I$ is obvious. We denote $T_{st} = \{\overline{x} \in r_{st}(H) \mid [\overline{x}, 1]_{st} = 0\}$ and $T = \{x \in r(H) \mid \overline{x} \in T_{st}\}$. Then $I \subseteq T$ since $\mathcal{J}x = 0$ if and only if $(\mathcal{J}, x) = 0$. Now I is an ideal of $r(H)$ satisfying $\mathcal{P} \subseteq I \subseteq T$. So $I/\mathcal{P}$ is an ideal of $r_{st}(H)$ contained in $T/\mathcal{P} = T_{st}$. However, T_{st} contains no nonzero ideals of $r_{st}(H)$ since the form $[-,-]_{st}$ is non-degenerate. This implies that $I = \mathcal{P}$.

(4) $\Rightarrow$ (1) If $[\overline{y}, \overline{x}]_{st} = 0$ for any $y \in r(H)$, then $[\overline{x}^*, \overline{y}^*]_{st} = 0$ since the form is $*$-symmetric. We have $0 = [\overline{x}^*, \overline{y}^*]_{st} = (\delta_{[\Bbbk]}^*, x^*y^*) = ((x\delta_{[\Bbbk]})^*, y^*)$ for any $y \in r(H)$. Thus, $x\delta_{[\Bbbk]} = 0$, so $x \in l(\mathcal{J}) = \mathcal{P}$, and hence $\overline{x} = 0$. Similarly, if $[\overline{x}, \overline{y}]_{st} = 0$ for any $y \in r(H)$, then $\overline{x} = 0$. □

Remark 3.1.5 *If the form $[-,-]_{st}$ is non-degenerate, then $\mathcal{J}_+ = \mathcal{J}$ implies that $\Bbbk \mid M \otimes M^*$ for any indecomposable non-projective module M. It deduces that $M \cong M^{**}$ by Theorem 2.1.7 (1). In this case, the operator $*$ on $r_{st}(H)$ is an involution.*

Under certain assumptions we are able to obtain further information about the Jacobson radical of $r(H)$ described as follows.

Theorem 3.1.6 *Let H be of finite representation type such that the Green ring $r(H)$ is commutative and the form $[-,-]_{st}$ on $r_{st}(H)$ is non-degenerate. Then the Jacobson radical $J(r(H))$ of $r(H)$ is equal to $\mathcal{P} \cap \mathcal{P}^{\perp}$ if and only if $G_0(H)$ is semiprime.*

Proof. If $J(r(H)) = \mathcal{P} \cap \mathcal{P}^{\perp}$, it is obvious that $G_0(H)$ is semiprime, since $r(H)/\mathcal{P}^{\perp} \cong G_0(H)$ and the Jacobson radical $J(r(H))$ is the nilradical of $r(H)$. Conversely, the non-degeneracy of the form $[-,-]_{st}$ on $r_{st}(H)$ shows that $\mathcal{P}_+ = \mathcal{P}_- = \mathcal{P}$. This implies that $J(r(H)) \subseteq \mathcal{P}$ by Proposition 2.3.11. If $G_0(H)$ is semiprime, then the isomorphism $G_0(H) \cong r(H)/\mathcal{P}^{\perp}$ implies that $J(r(H)) \subseteq \mathcal{P}^{\perp}$, so we obtain that $J(r(H)) \subseteq \mathcal{P} \cap \mathcal{P}^{\perp}$. The inclusion $\mathcal{P} \cap \mathcal{P}^{\perp} \subseteq J(r(H))$ is obvious, since any element of $\mathcal{P} \cap \mathcal{P}^{\perp}$ has square zero which can be deduced from the non-degeneracy of the form $(-,-)$. □

Remark 3.1.7 *The map $\varphi : r(H) \to G_0(H)$ given in (2.8) restricting to the ideal $\mathcal{P}$ gives rise to the Cartan map $\varphi|_{\mathcal{P}} : \mathcal{P} \to G_0(H)$, whose kernel is exactly* $\ker(\varphi|_{\mathcal{P}}) =$

$\mathcal{P} \cap \ker \varphi = \mathcal{P} \cap \mathcal{P}^{\perp}$.

Example 3.1.8 *If H is a finite dimensional pointed Hopf algebra of rank one (e.g., Taft algebras [14], generalized Taft algebras [44] and Radford Hopf algebras [69]), then $G_0(H)$ is semiprime and the form $[-,-]_{st}$ on $r_{st}(H)$ is non-degenerate since $\mathcal{P}_+ = \mathcal{P}_- = \mathcal{P}$. It follows that $J(r(H)) = \mathcal{P} \cap \mathcal{P}^{\perp} = \ker(\varphi|_{\mathcal{P}})$, which is a principal ideal, see [68, 69] for details.*

§3.2 Bi-Frobenius algebra structure

In this section, we always assume that H is a finite dimensional non-semisimple Hopf algebra of finite representation type and the form $[-,-]_{st}$ on $r_{st}(H)$ is non-degenerate. In this case, we show that the complexified stable Green algebra $R_{st}(H) := \mathbb{C} \otimes_{\mathbb{Z}} r_{st}(H)$ admits a group-like algebra structure, hence it is a bi-Frobenius algebra.

Let $\{[X_i] \mid i \in \mathbb{I}\}$ be the set of all non-projective indecomposable modules in $\mathrm{ind}(H)$. By definition $0 \in \mathbb{I}$ since $[X_0] := [\Bbbk]$ is not projective. Note that X is not projective if and only if X^* is not projective. Thus, the duality functor $*$ of H-mod induces an involution (see Remark 3.1.5) on the index set $\mathbb{I}$ defined by $[X_{i^*}] := [X_i^*]$ for any $i \in \mathbb{I}$.

Proposition 3.2.1 *The stable Green ring $r_{st}(H)$ is a transitive fusion ring with respect to the basis $\{\overline{[X_i]} \mid i \in \mathbb{I}\}$.*

Proof. It is straightforward to verify that $r_{st}(H)$ satisfies the conditions of a fusion ring given in [28, Definition 3.1.7], where the group homomorphism τ from $r_{st}(H)$ to $\mathbb{Z}$ is determined by $\tau(\overline{x}) = (\delta^*_{[\Bbbk]}, x)$ for any $\overline{x} \in r_{st}(H)$. The stable Green ring $r_{st}(H)$ is transitive ([28, Definition 3.3.1]): for any $i, j \in \mathbb{I}$, there exist $k, l \in \mathbb{I}$ such that $\overline{[X_j][X_k]}$ and $\overline{[X_l][X_j]}$ contain $\overline{[X_i]}$ with a nonzero coefficient. In fact, we have $\Bbbk \mid X_j \otimes X_j^*$ since $\mathcal{P}_+ = \mathcal{P}_- = \mathcal{P}$. This implies that $X_i \mid X_j \otimes X_j^* \otimes X_i$. Then we may find an indecomposable non-projective module X_k in $X_j^* \otimes X_i$ such that $X_i \mid X_j \otimes X_k$. Similarly, $X_i \mid X_i \otimes X_j^* \otimes X_j$, then there exists some X_l in $X_i \otimes X_j^*$ such that $X_i \mid X_l \otimes X_j$. □

Remark 3.2.2 *The stable Green ring $r_{st}(H)$ is a fusion ring under the condition that the form $[-,-]_{st}$ on $r_{st}(H)$ is non-degenerate. However, the stable category H-$\underline{mod}$ is not necessary semisimple by Proposition 3.1.1. A typical example is that the stable category of any Taft algebra of dimension n^2 for $n > 2$ is not semisimple, while the stable Green ring of the Taft algebra is a fusion ring.*

The fact that $r_{st}(H)$ is a transitive fusion ring enables us to define the Frobenius-Perron dimension of $\overline{[X_i]}$ for any $i \in \mathbb{I}$. Let $\text{FPdim}(\overline{[X_i]})$ be the maximal nonnegative eigenvalue of the matrix of the left multiplication by $\overline{[X_i]}$ with respect to the basis $\{\overline{[X_i]} \mid i \in \mathbb{I}\}$ of $r_{st}(H)$. Then $\text{FPdim}(\overline{[X_i]})$ is called the *Frobenius-Perron dimension* of $\overline{[X_i]}$. Extending FPdim linearly from the basis $\{\overline{[X_i]} \mid i \in \mathbb{I}\}$ of $r_{st}(H)$ to $R_{st}(H)$, we obtain a functional $\text{FPdim} : R_{st}(H) \to \mathbb{C}$. The functional FPdim has the following properties, see Proposition 3.3.4, Proposition 3.3.6 and Proposition 3.3.9 in [28].

Proposition 3.2.3 *For any $i \in \mathbb{I}$, we have the following:*

(1) *$FPdim(\overline{[X_i]}) \geq 1$.*

(2) *The functional $FPdim : R_{st}(H) \to \mathbb{C}$ is a ring homomorphism.*

(3) *$FPdim(\overline{[X_i]}) = FPdim(\overline{[X_{i^*}]})$.*

Let $x_i := \text{FPdim}(\overline{[X_i]})\overline{[X_i]}$ for any $i \in \mathbb{I}$. Then $\mathbf{b} = \{x_i \mid i \in \mathbb{I}\}$ is a basis of $R_{st}(H)$.

Theorem 3.2.4 *The quadruple $(R_{st}(H), FPdim, \mathbf{b}, *)$ is a group-like algebra.*

Proof. We need to verify the conditions (G1)-(G3) given in Definition 1.1.7. The condition (G1) is obvious. To verify the condition (G2), we have

$$x_i^* = \text{FPdim}(\overline{[X_i]})(\overline{[X_i]})^* = \text{FPdim}(\overline{[X_{i^*}]})\overline{[X_{i^*}]} = x_{i^*}. \tag{3.2}$$

Now for $i, j \in \mathbb{I}$, we suppose that

$$x_i x_j = \sum_{k \in \mathbb{I}} p_{ij}^k x_k, \tag{3.3}$$

where $p_{ij}^k \in \mathbb{C}$. On the one hand, applying the duality operator $*$ to the equality (3.3) and using (3.2), we obtain that $x_{j^*}x_{i^*} = \sum_{k\in\mathbb{I}} p_{ij}^k x_{k^*}$. On the other hand, we have $x_{j^*}x_{i^*} = \sum_{l\in\mathbb{I}} p_{j^*i^*}^l x_l$. It follows that $p_{ij}^k = p_{j^*i^*}^{k^*}$ for any $i, j, k \in \mathbb{I}$. Now we verify the condition (G3):

$$\begin{aligned} p_{ij}^0 &= \mathrm{FPdim}(\overline{[X_i]})\mathrm{FPdim}(\overline{[X_j]})(\delta_{[\Bbbk]}^*, [X_i][X_j]) \\ &= \mathrm{FPdim}(\overline{[X_i]})\mathrm{FPdim}(\overline{[X_j]})([X_j]^{**}\delta_{[\Bbbk]}^*, [X_i]) \\ &= \mathrm{FPdim}(\overline{[X_i]})\mathrm{FPdim}(\overline{[X_j]})(\delta_{[X_{j^*}]}^*, [X_i]) \\ &= \mathrm{FPdim}(\overline{[X_i]})\mathrm{FPdim}(\overline{[X_j]})\delta_{i,j^*} \\ &= \delta_{i,j^*}\mathrm{FPdim}(x_i). \end{aligned}$$

Therefore, the condition (G3) is satisfied. □

As noted in Remark 1.1.8, a group-like algebra is a bi-Frobenius algebra. Now let us look at the bi-Frobenius algebra structure induced from the group-like algebra structure on $R_{st}(H)$. The integral ϕ is given by $\phi(x_i) = \delta_{0,i}$, for $i \in \mathbb{I}$. Equivalently,

$$\phi(\overline{[X_i]}) = \begin{cases} 1, & i = 0, \\ 0, & i \neq 0. \end{cases}$$

The set $\{x_i, \frac{x_i^*}{\mathrm{FPdim}(x_i)} \mid i \in \mathbb{I}\}$ forms a pair of dual bases of $(R_{st}(H), \phi)$. This is equivalent to saying that $\{\overline{[X_i]}, \overline{[X_{i^*}]} \mid i \in \mathbb{I}\}$ is a pair of dual bases of $R_{st}(H)$ with respect to the integral ϕ. From the observation above, we conclude that the integral ϕ is nothing but the map determined by the form $[-,-]_{st}$, namely, $\phi(\overline{x}) = [\overline{x}, 1]_{st}$ for $\overline{x} \in R_{st}(H)$.

The stable Green algebra $R_{st}(H)$ is a coalgebra with the counit given by FPdim, and the comultiplication $\triangle$ defined by $\triangle(x_i) = \frac{1}{\mathrm{FPdim}(x_i)} x_i \otimes x_i$, or equivalently,

$$\triangle(\overline{[X_i]}) = \frac{1}{\mathrm{FPdim}(\overline{[X_i]})}\overline{[X_i]} \otimes \overline{[X_i]},$$

for $i \in \mathbb{I}$. Let $t = \sum_{i\in\mathbb{I}} x_i = \sum_{i\in\mathbb{I}} \mathrm{FPdim}(\overline{[X_i]})\overline{[X_i]}$. Then t is an integral of $R_{st}(H)$ associated to the counit FPdim. Now $(R_{st}(H), t)$ becomes a Frobenius coalgebra. Define a map $S : R_{st}(H) \to R_{st}(H)$ by $S(x_i) = x_{i^*}$, that is, $S(\overline{[X_i]}) = \overline{[X_{i^*}]}$ for $i \in \mathbb{I}$. The map S is exactly the duality operator $*$ on $R_{st}(H)$. It is an anti-algebra and anti-coalgebra morphism, so is an antipode of $R_{st}(H)$. Now the quadruple $(R_{st}(H), \phi, t, S)$ forms a bi-Frobenius algebra which is in general not a Hopf algebra.

§3.3 Applications to Radford Hopf algebras

In this section, we apply results obtained in previous section to the stable Green ring of a Radford Hopf algebra. In this case, the bilinear form $[-,-]_{st}$ is non-degenerate, and hence the complexified stable Green algebra admits a bi-Frobenius algebra structure. We describe this structure in detail from the point of view of polynomials.

Given two integers $m > 1$ and $n > 1$. Let ω be a primitive mn-th root of unity and H an algebra generated by g and y subject to relations

$$g^{mn} = 1,\ yg = \omega^{-m}gy,\ y^n = g^n - 1.$$

Then H is a Hopf algebra whose comultiplication $\triangle$, counit ε, and antipode S are given respectively by

$$\triangle(y) = y \otimes g + 1 \otimes y,\ \varepsilon(y) = 0,\ S(y) = -yg^{-1},$$

$$\triangle(g) = g \otimes g,\ \varepsilon(g) = 1,\ S(g) = g^{-1}.$$

The Hopf algebra H is called a Radford Hopf algebra, which was introduced by Radford [57] so as to give an example of Hopf algebra whose Jacobson radical is not a Hopf ideal.

The Green ring and the stable Green ring of the Radford Hopf algebra H can be presented by generators and relations. Let $\mathbb{Z}[Y, Z, X_1, X_2, \cdots, X_{m-1}]$ be a polynomial ring over $\mathbb{Z}$ in variables $Y, Z, X_1, X_2, \cdots, X_{m-1}$. The Green ring $r(H)$ of H is isomorphic to the quotient ring of $\mathbb{Z}[Y, Z, X_1, X_2, \cdots, X_{m-1}]$ modulo the ideal generated by the elements from (3.4) to (3.6) (see [69, Theorem 8.2]):

$$Y^n - 1,\ (1 + Y - Z)F_n(Y, Z),\ YX_1 - X_1,\ ZX_1 - 2X_1, \tag{3.4}$$

$$X_1^j - n^{j-1}X_j,\ \text{for } 1 \leq j \leq m - 1, \tag{3.5}$$

$$X_1^m - n^{m-2}(1 + Y + \cdots + Y^{n-1})F_n(Y, Z), \tag{3.6}$$

where $F_n(Y, Z)$ is a Dickson polynomial (of the second type) defined recursively by $F_1(Y, Z) = 1$, $F_2(Y, Z) = Z$ and $F_k(Y, Z) = ZF_{k-1}(Y, Z) - YF_{k-2}(Y, Z)$ for $k \geq 3$.

More precisely, the polynomial $F_k(y,z)$ can be expressed as follows (see [14, Lemma 3.11]):

$$F_k(Y,Z) = \sum_{i=0}^{[\frac{k-1}{2}]} (-1)^i \binom{k-1-i}{i} Y^i Z^{k-1-2i}.$$

The Grothendieck ring $G_0(H)$ is isomorphic to the quotient of $\mathbb{Z}[Y, X_1, X_2, \cdots, X_{m-1}]$ modulo the ideal generated by $Y^n - 1, YX_1 - X_1, X_1^j - n^{j-1}X_j$ for $1 \leq j \leq m-1$ and $X_1^m - n^{m-1}(1 + Y + \cdots + Y^{n-1})$ (see [69, Corollary 8.3]).

The stable Green ring $r_{st}(H)$ of H is isomorphic to the stable Green ring of a Taft algebra of dimension n^2 (see [69, Section 7]), while the latter is isomorphic to the quotient ring $\mathbb{Z}[Y,Z]/I$, where I is an ideal of $\mathbb{Z}[Y,Z]$ generated by $Y^n - 1$ and $F_n(Y,Z)$ (see [68, Proposition 6.1]).

The form $[-,-]_{st}$ on $r_{st}(H)$ is non-degenerate (see Example 3.1.8). As shown in previous section, there is a bi-Frobenius algebra structure on the complexified stable Green algebra $\mathbb{C} \otimes_{\mathbb{Z}} r_{st}(H) \cong \mathbb{C}[Y,Z]/I$. In the following, we shall describe the bi-Frobenius algebra structure on $\mathbb{C}[Y,Z]/I$ using a new basis rather than the canonical basis consisting of indecomposable non-projective H-modules. We need the following inverse version of Dickson polynomials.

Lemma 3.3.1 *[68, Lemma 6.4] For any $j \geq 1$, we have*

$$Z^j = \sum_{k=0}^{[\frac{j}{2}]} \binom{j}{k} \frac{j+1-2k}{j+1-k} Y^k F_{j+1-2k}(Y,Z).$$

Denote by $y^i z^j$ the image of $Y^i Z^j$ under the natural map $\mathbb{C}[Y,Z] \to \mathbb{C}[Y,Z]/I$. Then the set $\{y^i z^j \mid 0 \leq i \leq n-1, 0 \leq j \leq n-2\}$ forms a basis of $\mathbb{C}[Y,Z]/I$. By Lemma 3.3.1, the following equation holds in $\mathbb{C}[Y,Z]/I$:

$$y^i z^j = \sum_{k=0}^{[\frac{j}{2}]} \binom{j}{k} \frac{j+1-2k}{j+1-k} y^{i+k} F_{j+1-2k}(y,z).$$

Thus, $\{y^i F_j(y,z) \mid 0 \leq i \leq n-1, 1 \leq j \leq n-1\}$ is a basis of $\mathbb{C}[Y,Z]/I$. In the following, we shall use this basis to describe the bi-Frobenius algebra structure on the algebra $\mathbb{C}[Y,Z]/I$. Following from [68, Remark 4.4 (3)] we have

$$y^i F_j(y,z) y^k F_l(y,z) = \sum_{t=\zeta(j,l)}^{\min\{j,l\}-1} y^{i+k+t} F_{j+l-1-2t}(y,z), \tag{3.7}$$

where $\zeta(j,l)=0$ if $j+l-1<n$, and $\zeta(j,l)=j+l-n$ if $j+l-1\geq n$.

Define the following two maps $\varepsilon:\mathbb{C}[Y,Z]/I\to\mathbb{C}$ by

$$\varepsilon(y^iF_j(y,z))=F_j(1,2\cos\frac{\pi}{n})$$

and $\triangle:\mathbb{C}[Y,Z]/I\to\mathbb{C}[Y,Z]/I\otimes\mathbb{C}[Y,Z]/I$ by

$$\triangle(y^iF_j(y,z))=\frac{1}{F_j(1,2\cos\frac{\pi}{n})}y^iF_j(y,z)\otimes y^iF_j(y,z).$$

Then both ε and $\triangle$ are well-defined since $F_n(1,2\cos\frac{\pi}{n})=0$ (see [69, Theorem 7.3]). Moreover, it is straightforward to check that $(\triangle\otimes id)\triangle=(id\otimes\triangle)\triangle$ and $(id\otimes\varepsilon)\triangle=id=(\varepsilon\otimes id)\triangle$. Hence $(\mathbb{C}[Y,Z]/I,\triangle,\varepsilon)$ is a coalgebra.

Define the linear map $\phi:\mathbb{C}[Y,Z]/I\to\mathbb{C}$ by

$$\phi(y^iF_j(y,z))=\begin{cases}1, & i=0,j=1,\\ 0, & \text{otherwise.}\end{cases}$$

Then $(\mathbb{C}[Y,Z]/I,\phi)$ is a Frobenius algebra and

$$\{y^iF_j(y,z),y^{1-i-j}F_j(y,z)\mid 0\leq i\leq n-1,1\leq j\leq n-1\}$$

forms a pair of dual bases of $\mathbb{C}[Y,Z]/I$ with respect to the integral ϕ.

Denote by $t=\sum_{i=0}^{n-1}\sum_{j=1}^{n-1}F_j(1,2\cos\frac{\pi}{n})y^iF_j(y,z)$. Then

$$\triangle(t)=\sum t_1\otimes t_2=\sum_{i=0}^{n-1}\sum_{j=1}^{n-1}y^iF_j(y,z)\otimes y^iF_j(y,z).$$

Define the linear map $S:\mathbb{C}[Y,Z]/I\to\mathbb{C}[Y,Z]/I$ by

$$S(f)=\sum\phi(t_1f)t_2=\sum_{i=0}^{n-1}\sum_{j=1}^{n-1}\phi(y^iF_j(y,z)f)y^iF_j(y,z).$$

We have the following result.

Theorem 3.3.2 *The quadruple* $(\mathbb{C}[Y,Z]/I,\phi,t,S)$ *is a bi-Frobenius algebra.*

Proof. To prove that $(\mathbb{C}[Y,Z]/I,\phi,t,S)$ is a bi-Frobenius algebra, we only need to show that $\triangle(1)=1\otimes 1$, the counit ε is an algebra morphism and the map S is an anti-algebra as well as anti-coalgebra automorphism according to [22, Lemma 1.2]. Indeed, the former two conclusions are obviously true. By the definition of S and the equality (3.7), we have

$$\begin{aligned} S(y^k F_l(y,z)) &= \sum_{i=0}^{n-1}\sum_{j=1}^{n-1} \phi(y^i F_j(y,z) y^k F_l(y,z)) y^i F_j(y,z) \\ &= \sum_{i=0}^{n-1}\sum_{j=1}^{n-1} \phi(\sum_{t=\zeta(j,l)}^{\min\{j,l\}-1} y^{i+k+t} F_{j+l-1-2t}(y,z)) y^i F_j(y,z). \end{aligned}$$

By the definition of ϕ, we have $\phi(y^{i+k+t}F_{j+l-1-2t}(y,z)) = 1$ if and only if i, j and t satisfy $n \mid i+k+t$ and $j+l-1-2t = 1$. Note that $t \leq \min\{j,l\} - 1$. The equality $j+l-1-2t = 1$ implies that $j = l$. In this case, $t = l-1$ and $n \mid i+k+l-1$. It follows that $S(y^k F_l(y,z)) = y^{1-k-l}F_l(y,z)$ and S maps the basis to its dual basis, hence the map S is bijective. In particular, $S(1) = 1$ and

$$\begin{aligned} S(y^i F_j(y,z) y^k F_l(y,z)) &= S(\sum_{t=\zeta(j,l)}^{\min\{j,l\}-1} y^{i+k+t} F_{j+l-1-2t}(y,z)) \\ &= \sum_{t=\zeta(j,l)}^{\min\{j,l\}-1} y^{1-(i+k+t)-(j+l-1-2t)} F_{j+l-1-2t}(y,z) \\ &= y^{1-i-j} F_j(y,z) y^{1-k-l} F_l(y,z) \\ &= S(y^i F_j(y,z)) S(y^k F_l(y,z)). \end{aligned}$$

We conclude that S is an anti-algebra map since $\mathbb{C}[Y,Z]/I$ is a commutative algebra. In addition,

$$(\varepsilon \circ S)(y^i F_j(y,z)) = \varepsilon(y^{1-i-j} F_j(y,z)) = \varepsilon(y^i F_j(y,z))$$

and

$$\begin{aligned} (\triangle \circ S)(y^i F_j(y,z)) &= \triangle(y^{1-i-j} F_j(y,z)) \\ &= \frac{1}{F_j(1, 2\cos\frac{\pi}{n})} y^{1-i-j} F_j(y,z) \otimes y^{1-i-j} F_j(y,z) \\ &= ((S \otimes S) \circ \triangle^{\mathrm{op}})(y^i F_j(y,z)). \end{aligned}$$

It follows that S is an anti-coalgebra map on $\mathbb{C}[Y,Z]/I$.

Remark 3.3.3 *Note that* $\{y^i z^j \mid 0 \leq i \leq n-1, 0 \leq j \leq n-2\}$ *is a basis of* $\mathbb{C}[Y,Z]/I$*. Using this basis we are able to describe the bi-Frobenius algebra structure on* $(\mathbb{C}[Y,Z]/I, \phi, t, S)$ *as follows:*

- $\triangle(y^iz^j) = \sum_{k=0}^{\lfloor\frac{j}{2}\rfloor}\begin{pmatrix} j \\ k \end{pmatrix}\frac{j+1-2k}{(j+1-k)F_{j+1-2k}(1,2\cos\frac{\pi}{n})}y^{i+k}F_{j+1-2k}(y,z)\otimes y^{i+k}F_{j+1-2k}(y,z);$
- $\phi(y^iz^j) = \begin{cases} \begin{pmatrix} j \\ \frac{j}{2} \end{pmatrix}\frac{2}{j+2}, & 2 \mid j \ \ and\ n \mid i+\frac{j}{2}, \\ 0, & otherwise; \end{cases}$
- $t = \sum_{i=0}^{n-1}\sum_{j=1}^{n-1}F_j(1,2\cos\frac{\pi}{n})y^iF_j(y,z);$
- $S(y^iz^j) = \sum_{k=0}^{\lfloor\frac{j}{2}\rfloor}\begin{pmatrix} j \\ k \end{pmatrix}\frac{j+1-2k}{j+1-k}y^{k-i-j}F_{j+1-2k}(y,z).$

Chapter 4 The Casimir numbers of Hopf algebras

This chapter deals with the question of when the Green ring $r(H)$, or the Green algebra $r(H) \otimes_{\mathbb{Z}} K$ over a field K, is Jacobson semisimple (namely, has zero Jacobson radical). It turns out that $r(H) \otimes_{\mathbb{Z}} K$ is Jacobson semisimple if and only if the Casimir number of $r(H)$ is not zero in K. For the Green ring $r(H)$ itself, $r(H)$ is Jacobson semisimple if and only if the Casimir number of $r(H)$ is not zero. Then we focus on the cases where $H = \Bbbk G$ for a cyclic group G of order p over a field $\Bbbk$ of characteristic p. In this case, the Casimir number is computed. This leads to a complete description of the Jacobson radical of the Green algebra $r(\Bbbk G) \otimes_{\mathbb{Z}} K$ over any field K.

§4.1 Introduction

The Green ring of a finite group, or more generally, the Green ring of a Hopf algebra, has attracted much attention when it was realized that the Green ring provides one context for studying the problem of decomposing a tensor product into a direct sum of indecomposables (see e.g. [8,14,19,34,39,71]). After J.A. Green [33] first showed that the Green ring has no nonzero nilpotent elements for any cyclic p-group over a field of characteristic p, much subsequent works have centered on the nilpotency problem, that is, whether or not the Green ring possesses nonzero nilpotent elements.

The nilpotency problem has been completely solved for the Green ring of a finite group. It was shown that when the base field is of characteristic p, the Green ring of a finite group G contains nonzero nilpotent elements unless the Sylow p-subgroups of G are cyclic or elementary abelian 2-groups (see [7, 33, 74]). For the Green ring of a Hopf algebra, if H is a finite dimensional pointed Hopf algebra of rank one, then all nilpotent elements of the Green ring of H form a principal ideal, which is nothing but the Jacobson radical of the Green ring (see [68, Theorem 5.4] and [69, Theorem 6.3]). The proofs given for the above results were heavily computational, and neither explained properties of nilpotent elements, nor indicated a criterion for detecting them.

Let H be a finite dimensional Hopf algebra over an algebraically closed field $\Bbbk$. If H is of finite representation type, then the Green ring $r(H)$ of H is a Frobenius algebra over the ring $\mathbb{Z}$ of integers with the bilinear form given by dimensions of morphism spaces, see Proposition 2.3.3. The pair of dual bases associated with this bilinear form is the set consisting of isomorphism classes of indecomposable objects $[X]$ together with $\delta^*_{[X]}$, an element in $r(H)$ related to the almost split sequence ending with X (if X is not projective). The Casimir operator of $r(H)$ is the map c from $r(H)$ to its center given by

$$c(x) = \sum_{[X]\in \mathrm{ind}(H)} [X]x\delta^*_{[X]},$$

where $\mathrm{ind}(H)$ is the set of all isomorphism classes of indecomposable H-modules. The intersection of the image of c and $\mathbb{Z}$ is a principal ideal of $\mathbb{Z}$ generated by a non-negative integer and this integer is called the Casimir number of $r(H)$.

In this chapter, the Casimir number of $r(H)$ is used to determine whether or not the Green ring $r(H)$, or the Green algebra $r(H) \otimes_{\mathbb{Z}} K$ over a field K, is Jacobson semisimple (namely, has zero Jacobson radical). It turns out that $r(H)\otimes_{\mathbb{Z}}K$ is Jacobson semisimple if and only if the Casimir number of $r(H)$ is not zero in K, see Theorem 4.2.1 below. In the special case when the Green ring $r(H)$ is a group ring $\mathbb{Z}G$, the Casimir number is exactly the order of G. This recovers the classical Maschke's theorem which states that $\mathbb{Z}G \otimes_{\mathbb{Z}} K = KG$ is Jacobson semisimple if and only if the order of G is not zero in K. In view of this, Theorem 4.2.1 can be regarded as a version of Maschke's theorem for the Green ring case.

For the Green ring $r(H)$ itself, $r(H)$ is Jacobson semisimple if and only if the Casimir number of $r(H)$ is not zero, see Theorem 4.2.5 below. If the Green ring $r(H)$ is commutative, then the Jacobson radical of $r(H)$ is the set of all nilpotent elements of $r(H)$. As a consequence, Theorem 4.2.5 gives a characterization of a commutative Green ring without nonzero nilpotent elements. In particular, this characterization works for the Green ring of a finite group of finite representation type.

In general, it is difficult to calculate the Casimir number of the Green ring $r(H)$. We only focus on the case $H = \Bbbk G$, where G is a cyclic group of order p and $\Bbbk$ is an algebraically closed field of characteristic p. By a straightforward computation, we find that the Casimir number of $r(\Bbbk G)$ is $2p^2$. This shows that the Green ring $r(\Bbbk G)$

is Jacobson semisimple, which is a result of J.A. Green [33]. Moreover, $r(\Bbbk G) \otimes_{\mathbb{Z}} K$ is Jacobson semisimple if and only if the characteristic of K is not equal to 2 or p. In the case where K is of characteristic 2 or p, we use the factorization of the Dickson polynomials to describe the Jacobson radical of $r(\Bbbk G) \otimes_{\mathbb{Z}} K$ explicitly.

This chapter is organized as follows. In Section 4.2, we describe the Casimir number of $r(H)$ and use it to determine when $r(H)$, or $r(H) \otimes_{\mathbb{Z}} K$, is Jacobson semisimple. In Section 4.3, by applying the results obtained in Section 4.2 to the Green ring of a finite group G, we describe the Jacobson radical of the Green algebra $r(\Bbbk G) \otimes_{\mathbb{Z}} K$ completely.

Throughout this chapter, H is a finite dimensional Hopf algebra which is of finite representation type over an algebraically closed field $\Bbbk$. The letters $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ stand respectively for the ring of integers, the field of rationals, and the field of complex numbers. For a prime number p, the symbol $\mathbb{F}_p$ stands for the finite field consisting of p elements.

§4.2 The Jacobson semisimplicity of Green rings

Recall that for any indecomposable H-module Z, if Z is not projective, there exists a unique almost split sequence $0 \to X \to Y \to Z \to 0$ with the ending term Z, we denote by $\delta_{[Z]}$ the element $[X] - [Y] + [Z]$ in $r(H)$; if Z is projective, we write $\delta_{[Z]} = [Z] - [\mathrm{rad} Z]$, where $\mathrm{rad} Z$ is the radical of Z.

For any $[X] \in \mathrm{ind}(H)$, denote by $\delta^*_{[X]}$ the image of $\delta_{[X]}$ under the dual operator $*$ of $r(H)$. Since H is of finite representation type, the Green ring $r(H)$ is a Frobenius algebra over $\mathbb{Z}$, and all notions for Frobenius $\mathbb{Z}$-algebras make sense for $r(H)$. More precisely, the Casimir operator of $r(H)$ is the map c from $r(H)$ to its center $Z(r(H))$ given by

$$c(x) = \sum_{[X] \in \mathrm{ind}(H)} [X] x \delta^*_{[X]} \text{ for } x \in r(H).$$

The Casimir element of $r(H)$ is $c(1) = \sum_{[X] \in \mathrm{ind}(\mathcal{C})} [X] \delta^*_{[X]}$. In particular,

$$\dim_{\Bbbk}(c(1)) = \dim_{\Bbbk} H.$$

The Casimir number of $r(H)$ is defined to be the non-negative integer m satisfying

$\mathbb{Z} \cap \operatorname{Im} c = (m)$. This number is an invariant of H-module category under tensor equivalence because it does not depend on the choice of a bilinear form on $r(H)$. From this number one is able to determine when $r(H)$, or the algebra $r(H) \otimes_{\mathbb{Z}} K$ over a field K is Jacobson semisimple.

Theorem 4.2.1 *The Green algebra $r(H) \otimes_{\mathbb{Z}} K$ over a field K is Jacobson semisimple if and only if the Casimir number of $r(H)$ is not zero in K.*

Proof. If $K = \mathbb{F}_p$, then the algebra $r(H) \otimes_{\mathbb{Z}} \mathbb{F}_p$ is separable (namely, Jacobson semisimple) if and only if $(p) \not\supseteq \operatorname{Im} c \cap \mathbb{Z}$, see [47, Proposition 6]. If $K = \mathbb{Q}$, then $r(H) \otimes_{\mathbb{Z}} \mathbb{Q}$ is separable if and only if $\operatorname{Im} c = Z(r(H))$ by Higman's theorem [38, Theorem 1], or equivalently, $c(x) = 1$ for some $x \in r(H) \otimes_{\mathbb{Z}} \mathbb{Q}$. This is equivalent to saying that $c(mx) = m$, where m is a positive integer such that $mx \in r(H)$. Precisely, $\mathbb{Z} \cap \operatorname{Im} c \neq 0$. For a general field K, since $\mathbb{Q}$ (resp. $\mathbb{F}_p$) is a perfect field, any field extension $\mathbb{Q} \subseteq K$ (resp. $\mathbb{F}_p \subseteq K$) is separable. This implies that $r(H) \otimes_{\mathbb{Z}} K$ is Jacobson semisimple if and only if $r(H) \otimes_{\mathbb{Z}} \mathbb{Q}$ (resp. $r(H) \otimes_{\mathbb{Z}} \mathbb{F}_p$) is Jacobson semisimple. We have completed the proof. □

If $\mathbb{Z} \cap \operatorname{Im} c = (m)$, then there exists some $x \in r(H)$ such that $c(x) = m$. Applying dimension to this equality, we have

$$m = \dim_{\Bbbk}(c(x)) = \dim_{\Bbbk}(x) \dim_{\Bbbk}(c(1)) = \dim_{\Bbbk}(x) \dim_{\Bbbk} H. \tag{4.1}$$

It means that the Casimir number m of $r(H)$ is divisible by $\dim_{\Bbbk} H$. This is a result of [47, Proposition 22(a)]. In particular, we have the following corollary:

Corollary 4.2.2 *If a prime p divides the dimension of H, then $r(H) \otimes_{\mathbb{Z}} K$ is not Jacobson semisimple for any field K of characteristic p.*

Remark 4.2.3 *Let G be a finite group and $\mathcal{C}$ the discrete tensor category associated to G. Namely, the set of objects of $\mathcal{C}$ is G, the tensor functor is given by $g \otimes h = gh$ for $g, h \in G$, and $Hom_{\mathcal{C}}(g, h) = id_g$ if $g = h$, and $\emptyset$ if $g \neq h$. The Green ring of $\mathcal{C}$ is the group ring $\mathbb{Z}G$, and $\mathbb{Z} \cap \operatorname{Im} c = (m)$, where m is the order of G. It follows from Theorem 4.2.1 that $\mathbb{Z}G \otimes_{\mathbb{Z}} K = KG$ is Jacobson semisimple if and only if m is not* *zero in K. This is exactly the well-known Maschke's theorem. From this point of view, Theorem 4.2.1 can be viewed as the Green ring version of Maschke's theorem.*

An interesting result is that the Casimir number of $r(H)$ can also be used to determine when the Green ring $r(H)$ is Jacobson semisimple. To see this, we need the following lemma.

Lemma 4.2.4 *Let $J(r(H))$ be the Jacobson radical of $r(H)$ and $pr(H)$ the ideal of $r(H)$ generated by a prime p.*

(1) *We have $(J(r(H))^n \subseteq pr(H)$ for some integer n.*

(2) *If $\mathbb{Z} \cap \operatorname{Im} c = (m)$ and $p \nmid m$, then $J(r(H)) \subseteq pr(H)$.*

Proof.(1) The ring isomorphism $r(H)/pr(H) \cong r(H) \otimes_{\mathbb{Z}} \mathbb{F}_p$ shows that the quotient $r(H)/pr(H)$ is a finite ring. So the Jacobson radical $J(r(H)/pr(H))$ of $r(H)/pr(H)$ is nilpotent [48, Proposition IV.7]. The canonical ring epimorphism $\pi : r(H) \to r(H)/pr(H)$ yields that $\pi(J(r(H))) \subseteq J(r(H)/pr(H))$, so $\pi(J(r(H)))$ is nilpotent. Thus, there exists a positive integer n such that $(J(r(H)))^n$ is contained in the kernel of π, namely, $(J(r(H)))^n \subseteq pr(H)$.

(2) If the prime p satisfies $p \nmid m$, then $r(H) \otimes_{\mathbb{Z}} \mathbb{F}_p$ is Jacobson semisimple by Theorem 4.2.1. In this case, $\pi(J(r(H))) \subseteq J(r(H)/pr(H)) = 0$. This implies that $J(r(H)) \subseteq pr(H)$. □

Theorem 4.2.5 *The Green ring $r(H)$ is Jacobson semisimple if and only if the Casimir number of $r(H)$ is not zero.*

Proof.Assume that the Jacobson radical $J(r(H))$ of $r(H)$ is zero. Consider the finite dimensional algebra $r(H) \otimes_{\mathbb{Z}} \mathbb{Q}$ over $\mathbb{Q}$. We first show that the Jacobson radical $J(r(H) \otimes_{\mathbb{Z}} \mathbb{Q})$ of $r(H) \otimes_{\mathbb{Z}} \mathbb{Q}$ is zero. For any $x \in J(r(H) \otimes_{\mathbb{Z}} \mathbb{Q})$, there exists a nonzero integer n such that $nx \in r(H) \cap J(r(H) \otimes_{\mathbb{Z}} \mathbb{Q})$. For any $y, z \in r(H)$, we have $y(nx)z \in r(H) \cap J(r(H) \otimes_{\mathbb{Z}} \mathbb{Q})$. Since $J(r(H) \otimes_{\mathbb{Z}} \mathbb{Q})$ is nilpotent, $1 - y(nx)z$ is invertible in $r(H)$. This means that $nx \in J(r(H)) = 0$, and hence $x = 0$. Now $J(r(H) \otimes_{\mathbb{Z}} \mathbb{Q}) = 0$ and the algebra $r(H) \otimes_{\mathbb{Z}} \mathbb{Q}$ is Jacobson semisimple, it follows from

Theorem 4.2.1 that the Casimir number of $r(H)$ is not zero in $\mathbb{Q}$, so it is a nonzero integer. Conversely, if the Casimir number of $r(H)$ is $m \neq 0$, then the set Ω consisting of all primes p such that $p \nmid m$ is an infinite set. For any $x \in J(r(H))$, we may write $x = d\sum_{[X]\in \mathrm{ind}(\mathcal{C})} \lambda_{[X]}[X]$, where $d \in \mathbb{Z}$ and all integer coefficients $\lambda_{[X]}$ are coprime. By Lemma 4.2.4 (2) we have $J(r(H)) \subseteq pr(H)$ for all $p \in \Omega$. It follows that $p \mid d$ for all $p \in \Omega$. Thus, $d = 0$, and hence $x = 0$. $\square$

If the Green ring $r(H)$ is commutative, then the Jacobson radical of $r(H)$ is the set of all nilpotent elements of $r(H)$. As a consequence, Theorem 4.2.5 gives a characterization of a commutative Green ring without nonzero nilpotent elements. In particular, if H is a finite group of finite representation type, then the Green ring $r(H)$ is commutative. In this case, the Green ring $r(H)$ has no nonzero nilpotent elements if and only if the Casimir number of $r(H)$ is not zero.

§4.3 The Casimir number of a finite group

In this section we determine the Casimir number of the Green ring of a finite group, and then use it to describe the Jacobson radical of the Green algebra over a field K.

From now on p is an odd prime, $\Bbbk$ is an algebraically closed field of characteristic p, and G is a cyclic group of order p. The group algebra $\Bbbk G$ is isomorphic to the quotient of the polynomial algebra $\Bbbk[X]$ modulo the ideal $(X^p - 1)$ generated by $X^p - 1$ or $(X-1)^p$:

$$\Bbbk G \cong \Bbbk[X]/(X^p - 1) \cong \Bbbk[X]/(X-1)^p,$$

where the latter is a commutative Nakayama local algebra over $\Bbbk$. Let $M_i = \Bbbk[X]/(X-1)^i$ for $i = 1, \cdots, p$. Then $\{M_1, M_2, \cdots, M_p\}$ is a complete set of indecomposable $\Bbbk G$-modules up to isomorphism [4, ChV, Section 4]. Here, each M_i is self-dual since M_i is the unique indecomposable module of dimension i up to isomorphism. Note that M_1 is the trivial $\Bbbk G$-module.

We follow from [4, ChV, Section 4] and present almost split sequences of $\Bbbk G$-modules as follows. The almost split sequence ending with the trivial module M_1

is

$$0 \to M_1 \to M_2 \to M_1 \to 0,$$

and the almost split sequence ending with M_i is

$$0 \to M_i \to M_{i+1} \oplus M_{i-1} \to M_i \to 0 \text{ for } 1 < i < p.$$

Note that the sequence

$$0 \to M_i \to M_2 \otimes M_i \to M_i \to 0$$

is also an almost split sequence ending with M_i for $1 \leq i < p$ (see [4, ChV, Theorem 4.7]). The uniqueness of an almost split sequence shows that $M_2 \otimes M_i \cong M_{i+1} \oplus M_{i-1}$ for $1 < i < p$. We also have $M_2 \otimes M_p \cong 2M_p$. This leads to the product $[M_2][M_i] = [M_{i-1}] + [M_{i+1}]$ for $1 < i < p$, and $[M_2][M_p] = 2[M_p]$ in the Green ring $r(\Bbbk G)$ of $\Bbbk G$. The product $[M_i][M_j]$ in $r(\Bbbk G)$ can be described as follows.

Lemma 4.3.1 *For $1 \leq i, j \leq p$, we have*

(1) *If $i + j \leq p$, then $[M_i][M_j] = \sum_{t=0}^{\min\{i,j\}-1} [M_{i+j-1-2t}]$.*

(2) *If $i + j \geq p + 1$, then $[M_i][M_j] = (i + j - p)[M_p] + \sum_{t=i+j-p}^{\min\{i,j\}-1} [M_{i+j-1-2t}]$.*

Proof. This can be proved by induction on $i + j$, or see [68, Proposition 4.2] for a similar result. □

Let $\mathbb{Z}[X_2, \cdots, X_p]$ be a polynomial ring over $\mathbb{Z}$ with variables $X_2, \cdots, X_p$ and I the ideal of $\mathbb{Z}[X_2, \cdots, X_p]$ generated by

$$X_2^2 - X_3 - 1, X_2X_3 - X_4 - X_2, \cdots, X_2X_{p-1} - X_p - X_{p-2}, X_2X_p - 2X_p.$$

We have

$$r(\Bbbk G) \cong \mathbb{Z}[X_2, \cdots, X_p]/I,$$

where the isomorphism is given by $[M_i] \mapsto \overline{X_i}$ for $i = 2, 3, \cdots, p$ (see [4, ChV, Proposition 4.11]). Actually, the Green ring $r(\Bbbk G)$ is isomorphic to a polynomial ring over

$\mathbb{Z}$ with one variable modulo a relation. To see this, we recall the Dickson polynomials of the second kind defined recursively as follows:

$$E_0(X) = 1, E_1(X) = X, \text{and } E_{i+1}(X) = XE_i(X) - E_{i-1}(X) \text{ for } i \geq 1. \tag{4.2}$$

Then $E_n(X)$ can be written explicitly as

$$E_n(X) = \sum_{i=0}^{[\frac{n}{2}]} \binom{n-i}{i} (-1)^i X^{n-2i}$$

for $n \geq 0$ (see e.g. [13, Eq.(1.2)]).

Proposition 4.3.2 *We have* $r(\Bbbk G) \cong \mathbb{Z}[X]/((X-2)E_{p-1}(X))$.

Proof. Consider the following ring epimorphism

$$\psi : \mathbb{Z}[X_2, \cdots, X_p] \to \mathbb{Z}[X]/((X-2)E_{p-1}(X)),$$
$$g(X_2, \cdots, X_p) \mapsto \overline{g(E_1(X), \cdots, E_{p-1}(X))}.$$

By (4.2) we have $\psi(I) = 0$. This induces a ring epimorphism $\overline{\psi}$ from $\mathbb{Z}[X_2, \cdots, X_p]/I$ to $\mathbb{Z}[X]/((X-2)E_{p-1}(X))$ such that the following diagram is commutative:

$$\begin{array}{ccc} \mathbb{Z}[X_2, \cdots, X_p] & \xrightarrow{\psi} & \mathbb{Z}[X]/((X-2)E_{p-1}(X)) \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \overline{\psi}} & \\ \mathbb{Z}[X_2, \cdots, X_p]/I, & & \end{array}$$

where π is the canonical ring epimorphism. Define another ring morphism φ from $\mathbb{Z}[X]$ to $\mathbb{Z}[X_2, \cdots, X_p]/I$ by $\varphi(f(X)) = \overline{f(X_2)}$. By induction on i one is able to check that $\overline{E_{i-1}(X_2)} = \overline{X_i}$ holds in $\mathbb{Z}[X_2, \cdots, X_p]/I$ for $i = 2, 3, \cdots, p$. Thus, φ is surjective. In particular,

$$\varphi((X-2)E_{p-1}(X)) = \overline{(X_2-2)E_{p-1}(X_2)} = \overline{(X_2-2)X_p} = 0.$$

Hence φ induces a ring epimorphism $\overline{\varphi}$ from $\mathbb{Z}[X]/((X-2)E_{p-1}(X))$ to $\mathbb{Z}[X_2, \cdots, X_p]/I$ such that the following diagram is commutative:

$$\begin{array}{ccc} \mathbb{Z}[X] & \xrightarrow{\varphi} & \mathbb{Z}[X_2, \cdots, X_p]/I \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \overline{\varphi}} & \\ \mathbb{Z}[X]/((X-2)E_{p-1}(X)) & & \end{array}$$

Now it is straightforward to check that $\overline{\psi} \circ \overline{\varphi} = id$ and $\overline{\varphi} \circ \overline{\psi} = id$, as desired. $\square$

The almost split sequences of $\Bbbk G$-modules are useful to calculate dimensions of morphism spaces. We illustrate it here, although it is not closely related to the topic of this section. According to the notion of $\delta_{[M]}$, we have

$$\delta_{[M_i]} = \begin{cases} 2 - [M_2], & i = 1; \\ 2[M_i] - [M_{i+1}] - [M_{i-1}], & 1 < i < p; \\ [M_p] - [M_{p-1}], & i = p. \end{cases}$$

In particular, we have $\delta_{[M_i]} = \delta_{[M_1]}[M_i]$ for $1 \leq i < p$ and $\delta_{[M_1]}[M_p] = 0$. This gives the following relation between the bases $\{\delta_{[M_i]} \mid 1 \leq i \leq p\}$ and $\{[M_i] \mid 1 \leq i \leq p\}$ of $r(\Bbbk G)$:

$$\begin{pmatrix} \delta_{[M_1]} \\ \delta_{[M_2]} \\ \vdots \\ \delta_{[M_{p-1}]} \\ \delta_{[M_p]} \end{pmatrix} = \begin{pmatrix} 2 & -1 & & & \\ -1 & 2 & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & -1 & 2 & -1 \\ & & & -1 & 1 \end{pmatrix} \begin{pmatrix} [M_1] \\ [M_2] \\ \vdots \\ [M_{p-1}] \\ [M_p] \end{pmatrix}.$$

Note that

$$\begin{pmatrix} 2 & -1 & & & \\ -1 & 2 & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & -1 & 2 & -1 \\ & & & -1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & \cdots & 2 & 2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 2 & \cdots & p-1 & p-1 \\ 1 & 2 & \cdots & p-1 & p \end{pmatrix}$$

whose (i,j)-entry is $\min\{i,j\}$. We have

$$[M_i] = \sum_{j=1}^{p} ([M_i], [M_j]) \delta^*_{[M_j]} = \sum_{j=1}^{p} \dim_{\Bbbk} \operatorname{Hom}_{\Bbbk G}(M_i, M_j) \delta_{[M_j]}$$

since the dual operator $*$ on $r(\Bbbk G)$ is the identity map. It follows that

$$\dim_{\Bbbk} \operatorname{Hom}_{\Bbbk G}(M_i, M_j) = \min\{i, j\}.$$

The Casimir operator c of $r(\Bbbk G)$ is given by

$$c(x) = \sum_{i=1}^{p} [M_i] x \delta^*_{[M_i]} = \sum_{i=1}^{p} [M_i] x \delta_{[M_i]} = xc(1) \text{ for } x \in r(\Bbbk G)$$

since $r(\Bbbk G)$ is commutative. To determine the Casimir number of $r(\Bbbk G)$, we need to describe the Casimir element $c(1)$ of $r(\Bbbk G)$.

Lemma 4.3.3 *The Casimir element* $c(1) = [M_p] + 2\sum_{i=1}^{p}(-1)^{i-1}(p-i)[M_i]$.

Proof. Firstly, it is straightforward to check (by Lemma 4.3.1) that

$$\sum_{i=1}^{\frac{p-1}{2}}[M_i]^2 = \sum_{i=1}^{\frac{p-1}{2}}(\frac{p+1}{2}-i)[M_{2i-1}] = \sum_{i=\frac{p+1}{2}}^{p-1}[M_i]^2.$$

Using this equality we have:

$$\begin{aligned}
c(1) &= \sum_{i=1}^{p}[M_i]\delta_{[M_i]} = \delta_{[M_1]}\sum_{i=1}^{p-1}[M_i]^2 + [M_p]([M_p]-[M_{p-1}]) \\
&= [M_p] + \delta_{[M_1]}(\sum_{i=1}^{\frac{p-1}{2}}[M_i]^2 + \sum_{i=\frac{p+1}{2}}^{p-1}[M_i]^2) \\
&= [M_p] + 2\delta_{[M_1]}\sum_{i=1}^{\frac{p-1}{2}}[M_i]^2 \\
&= [M_p] + 2\delta_{[M_1]}\sum_{i=1}^{\frac{p-1}{2}}(\frac{p+1}{2}-i)[M_{2i-1}] \\
&= [M_p] + 2(2-[M_2])\sum_{i=1}^{\frac{p-1}{2}}(\frac{p+1}{2}-i)[M_{2i-1}] \\
&= [M_p] + 2\sum_{i=1}^{\frac{p-1}{2}}(\frac{p+1}{2}-i)(2[M_{2i-1}]-[M_{2i}]-[M_{2i-2}]) \\
&= [M_p] + 2\sum_{i=1}^{p}(-1)^{i-1}(p-i)[M_i].
\end{aligned}$$

The proof is completed. □

Note that $\{\delta_{[M_t]} \mid t = 1, 2, \cdots, p\}$ and $\{[M_t] \mid t = 1, 2, \cdots, p\}$ form dual bases of $r(\Bbbk G)$. For any $x \in r(\Bbbk G)$, $c(x)$ has the form $c(x) = \sum_{t=1}^{p}(\delta_{[M_t]}, c(x))[M_t]$. Thus, the coefficient of $[M_t]$ in the linear expression of $c(x)$ is $(\delta_{[M_t]}, c(x))$. Next, we need to compute $(\delta_{[M_t]}, c(x))$ for $1 \le t \le p$.

Lemma 4.3.4 *If* $x = \sum_{j=1}^{p} \lambda_j [M_j]$, *then* $(\delta_{[M_p]}, c(x)) = \sum_{i=1}^{\frac{p+1}{2}} (2i-1)\lambda_{2i-1}$.

Proof. By Lemma 4.3.3 we have

$$\begin{aligned} c(x) = c(1)x &= ([M_p] + 2\sum_{i=1}^{p}(-1)^{i-1}(p-i)[M_i])\sum_{j=1}^{p}\lambda_j[M_j] \\ &= \sum_{j=1}^{p} j\lambda_j[M_p] + 2\sum_{i,j=1}^{p}(-1)^{i-1}(p-i)\lambda_j[M_i][M_j] \\ &= \sum_{j=1}^{p} j\lambda_j[M_p] + 2\sum_{i+j=p+1}^{2p}(-1)^{i-1}(p-i)(i+j-p)\lambda_j[M_p] + \sum_{i=1}^{p-1}\mu_i[M_i], \end{aligned}$$

where the last equality follows from Lemma 4.3.1 (2) with some $\mu_i \in \mathbb{Z}$. Then

$$\begin{aligned} (\delta_{[M_p]}, c(x)) &= \sum_{j=1}^{p} j\lambda_j + 2\sum_{i+j=p+1}^{2p}(-1)^{i-1}(p-i)(i+j-p)\lambda_j \\ &= \sum_{j=1}^{p} j\lambda_j + 2\sum_{j=1}^{p}\sum_{i=p+1-j}^{p}(-1)^{i-1}(p-i)(i+j-p)\lambda_j \\ &= \sum_{j=1}^{p} j\lambda_j + 2\sum_{j=1}^{p}\sum_{k=1}^{j}(-1)^{k-j}(j-k)k\lambda_j. \end{aligned}$$

Note that

$$\sum_{k=1}^{j}(-1)^k(j-k)k = \begin{cases} 0, & 2 \nmid j; \\ -\frac{j}{2}, & 2 \mid j. \end{cases}$$

Thus,

$$(\delta_{[M_p]}, c(x)) = \sum_{j=1}^{p} j\lambda_j - \sum_{2|j, j=1}^{p} j\lambda_j = \sum_{2\nmid j, j=1}^{p} j\lambda_j = \sum_{i=1}^{\frac{p+1}{2}}(2i-1)\lambda_{2i-1}.$$

We have completed the proof. □

To describe $(\delta_{[M_t]}, c(x))$ for $1 \le t \le p-1$, we need some preparations. The left multiplication by $[M_t]$ with respect to the basis $\{[M_1], [M_2], \cdots, [M_p]\}$ corresponds to a matrix $\mathbf{M}_t$. That is,

$$[M_t]\begin{pmatrix}[M_1]\\ [M_2]\\ \vdots \\ [M_p]\end{pmatrix} = \mathbf{M}_t \begin{pmatrix}[M_1]\\ [M_2]\\ \vdots \\ [M_p]\end{pmatrix}.$$

If we denote by $\mathbf{E}_{i,j}$ the square matrix of order p with (i,j)-entry 1, and 0 otherwise, then $\mathbf{M}_t$ can be written explicitly as follows:

$$\begin{aligned}\mathbf{M}_t &= \mathbf{E}_{1,t} + \mathbf{E}_{2,t+1} + \mathbf{E}_{3,t+2} + \cdots + \mathbf{E}_{p-t,p-1} \\ &+ \mathbf{E}_{2,t-1} + \mathbf{E}_{3,t} + \mathbf{E}_{4,t+1} + \cdots + \mathbf{E}_{p-t+1,p-2} \\ &+ \mathbf{E}_{3,t-2} + \mathbf{E}_{4,t-1} + \mathbf{E}_{5,t} + \cdots + \mathbf{E}_{p-t+2,p-3} \\ &+ \cdots \\ &+ \mathbf{E}_{t,1} + \mathbf{E}_{t+1,2} + \mathbf{E}_{t+2,3} + \cdots + \mathbf{E}_{p-1,p-t} \\ &+ t\mathbf{E}_{p,p} + (t-1)\mathbf{E}_{p-1,p} + (t-2)\mathbf{E}_{p-2,p} + \cdots + \mathbf{E}_{p-t+1,p} \\ &= \sum_{s=1}^{t}\sum_{r=1}^{p-t} \mathbf{E}_{s+r-1,t+r-s} + \sum_{s=1}^{t}(t+1-s)\mathbf{E}_{p-s+1,p}.\end{aligned} \tag{4.3}$$

Lemma 4.3.5 *If* $x = \sum_{j=1}^{p} \lambda_j [M_j]$, *then*

$$(\delta_{[M_t]}, c(x)) = 2(p-t)\sum_{i=1}^{t}(-1)^{t+i} i\lambda_i + 2t\sum_{i=t+1}^{p-1}(-1)^{t+i}(p-i)\lambda_i$$

for $1 \le t \le p-1$.

Proof.Let $[M_i][M_j] = \sum_{t=1}^{p} N_{ij}^t [M_t]$ for $N_{ij}^t \in \mathbb{Z}$. For $1 \le i,j,t \le p-1$, the associativity of the form $(-,-)$ over $r(H)$ together with the commutativity of $r(\Bbbk G)$ shows that

$$\begin{aligned}N_{ij}^t &= (\delta_{[M_t]}, [M_i][M_j]) = (\delta_{[M_1]}[M_t], [M_i][M_j]) \\ &= (\delta_{[M_1]}[M_j], [M_t][M_i]) = (\delta_{[M_j]}, [M_t][M_i]) \\ &= N_{ti}^j.\end{aligned} \tag{4.4}$$

Consequently, we have:

$$\begin{aligned}c(x) = c(1)x &= ([M_p] + 2\sum_{i=1}^{p}(-1)^{i-1}(p-i)[M_i])\sum_{j=1}^{p}\lambda_j[M_j] \\ &= \mu_1[M_p] + 2\sum_{i,j=1}^{p-1}(-1)^{i-1}(p-i)\lambda_j[M_i][M_j] \quad (\text{for some } \mu_1 \in \mathbb{Z}) \\ &= \mu_1[M_p] + 2\sum_{i,j=1}^{p-1}(-1)^{i-1}(p-i)\lambda_j\sum_{t=1}^{p}N_{ij}^t[M_t]\end{aligned}$$

$$= \mu_2[M_p] + 2\sum_{i,j,t=1}^{p-1}(-1)^{i-1}(p-i)\lambda_j N_{ij}^t[M_t] \quad (\text{for some } \mu_2 \in \mathbb{Z})$$
$$= \mu_2[M_p] + 2\sum_{i,j,t=1}^{p-1}(-1)^{i-1}(p-i)\lambda_j N_{ti}^j[M_t] \quad \text{by (4.4).}$$

Thus,

$$(\delta_{[M_t]}, c(x)) = 2\sum_{i,j=1}^{p-1}(-1)^{i-1}(p-i)\lambda_j N_{ti}^j \quad \text{for} \quad 1 \le t \le p-1.$$

Let $\widehat{\mathbf{M}}_t$ be the submatrix of $\mathbf{M}_t$ obtained by deleting the p-th column and row. By (4.3) we have $\widehat{\mathbf{M}}_t = \sum_{s=1}^{t}\sum_{r=1}^{p-t}\mathbf{E}_{s+r-1,t+r-s}$. The matrix $\widehat{\mathbf{M}}_t$ is symmetric and

$$\begin{aligned}
(\delta_{[M_t]}, c(x)) &= 2\sum_{i,j=1}^{p-1}(-1)^{i-1}(p-i)\lambda_j N_{ti}^j \\
&= 2\begin{pmatrix}\lambda_1 & \lambda_2 & \cdots & \lambda_{p-1}\end{pmatrix}\widehat{\mathbf{M}}_t\begin{pmatrix} p-1 \\ -(p-2) \\ \vdots \\ (-1)^{p-2}\end{pmatrix} \\
&= 2\begin{pmatrix}\lambda_1 & \lambda_2 & \cdots & \lambda_{p-1}\end{pmatrix}\sum_{s=1}^{t}\sum_{r=1}^{p-t}\mathbf{E}_{s+r-1,t+r-s}\begin{pmatrix} p-1 \\ -(p-2) \\ \vdots \\ (-1)^{p-2}\end{pmatrix} \\
&= 2\sum_{s=1}^{t}\sum_{r=1}^{p-t}(-1)^{t+r-s-1}(p-t-r+s)\lambda_{s+r-1} \\
&= 2(p-t)\sum_{i=1}^{t}(-1)^{t+i}i\lambda_i + 2t\sum_{i=t+1}^{p-1}(-1)^{t+i}(p-i)\lambda_i.
\end{aligned}$$

We are done. □

The Casimir number of $r(\Bbbk G)$ can be presented as follows:

Theorem 4.3.6 *The Casimir number of $r(\Bbbk G)$ is $2p^2$.*

Proof. Let $x = \sum_{j=1}^{p}\lambda_j[M_j]$. Then $c(x) = \sum_{t=1}^{p}(\delta_{[M_t]}, c(x))[M_t]$. If $c(x) \in \mathbb{Z}$, then

$(\delta_{[M_t]}, c(x)) = 0$ for $t = 2, 3, \cdots, p$. However,

$$(\delta_{[M_t]}, c(x)) = 2(p-t)\sum_{i=1}^{t}(-1)^{t+i} i\lambda_i + 2t\sum_{i=t+1}^{p-1}(-1)^{t+i}(p-i)\lambda_i \tag{4.5}$$

for $t = 2, 3, \cdots, p-1$ (see Lemma 4.3.5), and

$$(\delta_{[M_p]}, c(x)) = \sum_{i=1}^{\frac{p+1}{2}}(2i-1)\lambda_{2i-1}$$

(see Lemma 4.3.4). This gives a system of equations with variables $\lambda_1, \cdots, \lambda_p$. Consider the following equations:

$$\begin{cases} (\delta_{[M_{p-1}]}, c(x)) = 0 \\ (\delta_{[M_{p-2}]}, c(x)) = 0. \end{cases}$$

Using (4.5) it is not hard to see that $\lambda_{p-1} = 0$. Similarly, the system of equations

$$\begin{cases} (\delta_{[M_{p-2}]}, c(x)) = 0 \\ (\delta_{[M_{p-3}]}, c(x)) = 0 \end{cases}$$

together with $\lambda_{p-1} = 0$ shows that $\lambda_{p-2} = 0$. Repeating this argument we obtain that $\lambda_{p-1} = \lambda_{p-2} = \cdots = \lambda_3 = 0$. Now the system of equations

$$\begin{cases} (\delta_{[M_2]}, c(x)) = 0 \\ (\delta_{[M_p]}, c(x)) = 0 \end{cases}$$

can be simplified as follows:

$$\begin{cases} -\lambda_1 + 2\lambda_2 = 0 \\ \lambda_1 + p\lambda_p = 0. \end{cases}$$

It follows that $\lambda_1 = 2p\mu$, $\lambda_2 = p\mu$, $\lambda_p = -2\mu$ for $\mu \in \mathbb{Z}$. In this case,

$$\begin{aligned}(\delta_{[M_1]}, c(x)) &= 2(p-1)\lambda_1 + 2\sum_{i=2}^{p-1}(-1)^{1+i}(p-i)\lambda_i \\ &= 2(p-1)\lambda_1 - 2(p-2)\lambda_2 \\ &= 2p^2\mu.\end{aligned}$$

We conclude that $\operatorname{Im} c \cap \mathbb{Z} = (2p^2)$. $\square$

Since the Casimir number of $r(\Bbbk G)$ is $2p^2 \neq 0$, the Green ring $r(\Bbbk G)$ is Jacobson semisimple. This is exactly a result of J.A. Green [33]. For the Green algebra $r(\Bbbk G)\otimes_{\mathbb{Z}} K$, it follows from Theorem 4.2.1 that $r(\Bbbk G)\otimes_{\mathbb{Z}} K$ is Jacobson semisimple if and only if the characteristic of K is not equal to 2 or p. In the following, we use the factorization of the Dickson polynomials to determine the generators of the Jacobson radical of $r(\Bbbk G)\otimes_{\mathbb{Z}} K$, or equivalently, $K[X]/((X-2)E_{p-1}(X))$ (see Proposition 4.3.2) in the cases where K is of characteristic 2 or p.

Proposition 4.3.7 *If the characteristic of K is p, then the Jacobson radical of the Green algebra $K[X]/((X-2)E_{p-1}(X))$ is a principal ideal generated by $\overline{X^2-4}$.*

Proof. We have the decomposition $E_{p-1}(X) = (X-2)^{\frac{p-1}{2}}(X+2)^{\frac{p-1}{2}}$ in $K[X]$ [13, Theorem 3.1 (2)]. Thus, the polynomial $(X-2)E_{p-1}(X)$ has only two distinct prime factors $X-2$ and $X+2$. Since $K[X]$ is a principal ideal domain and every nonzero prime ideal is maximal, the Jacobson radical of $K[X]/((X-2)E_{p-1}(X))$ is a principal ideal generated by $\overline{(X-2)(X+2)}$, which is the product of distinct prime factors of $(X-2)E_{p-1}(X)$. □

Proposition 4.3.8 *If the characteristic of K is 2, then the Jacobson radical of the Green algebra $K[X]/((X-2)E_{p-1}(X))$ is a principal ideal generated by*

$$\sum_{i=0}^{[\frac{p-1}{2}]} \begin{pmatrix} p-1-i \\ i \end{pmatrix} (-1)^i \overline{X^{\frac{p+1}{2}-i}}.$$

Proof. Since the characteristic of K is 2, we have the following isomorphism:

$$K[X]/((X-2)E_{p-1}(X)) \cong K[X]/(XE_{p-1}(X)).$$

The Dickson polynomial $E_{p-1}(X)$ in $K[X]$ can be written as

$$E_{p-1}(X) = \sum_{i=0}^{[\frac{p-1}{2}]} \begin{pmatrix} p-1-i \\ i \end{pmatrix} (-1)^i X^{p-1-2i} = (f(X))^2,$$

where

$$f(X) = \sum_{i=0}^{[\frac{p-1}{2}]} \begin{pmatrix} p-1-i \\ i \end{pmatrix} (-1)^i X^{\frac{p-1}{2}-i}$$

and it has no multiple factors in $K[X]$, see [9, Theorem 6]. It follows that the Jacobson radical of $K[X]/(XE_{p-1}(X))$ is a principal ideal generated by $\overline{Xf(X)}$. We have completed the proof. □

Chapter 5 The Casimir numbers of fusion categories

Let $\mathcal{C}$ be a fusion category over an algebraically closed field $\Bbbk$ of arbitrary characteristic. The Casimir number and another two numerical invariants of $\mathcal{C}$ are considered in this chapter. These numerical invariants are all positive integers and admit the property that the Grothendieck algebra $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ over any field K is semisimple if and only if any of these numbers is not zero in K. This means that all these numbers have the same prime factors. If moreover $\mathcal{C}$ is pivotal, one obtains a criterion that $\mathcal{C}$ is non-degenerate if and only if any one of these numbers is not zero in $\Bbbk$. For the case that $\mathcal{C}$ is a spherical fusion category over the field $\mathbb{C}$ of complex numbers, these numbers and the Frobenius-Schur exponent of $\mathcal{C}$ all share the same prime factors. This may be thought of as another statement of the Cauchy theorem for spherical fusion categories.

§5.1 Introduction

A fusion category $\mathcal{C}$ over a field $\Bbbk$ is called *non-degenerate* if the global dimension $\dim(\mathcal{C})$ of $\mathcal{C}$ is not zero in $\Bbbk$. Since $\dim(\mathcal{C})$ is automatically not zero in a field $\Bbbk$ of characteristic zero, this notation is only considered in a field $\Bbbk$ of positive characteristic. A crucial property of non-degenerate fusion categories is that they can be lifted to the case of characteristic zero (see e.g. [29, Section 9]). It is interesting to know when a fusion category over a field of positive characteristic is non-degenerate. Ostrik stated that a spherical fusion category $\mathcal{C}$ over a field $\Bbbk$ is non-degenerated, if the Grothendieck algebra $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} \Bbbk$ is semisimple (see [54, Proposition 2.9]). It has been proved by Shimizu that a pivotal fusion category $\mathcal{C}$ over an algebraically closed field $\Bbbk$ is non-degenerate if and only if its Grothendieck algebra $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} \Bbbk$ is semisimple (see [60, Theorem 6.5]).

In this chapter we first pay attention to the question when the Grothendieck algebra $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} \Bbbk$ is semisimple for any fusion category $\mathcal{C}$ over an algebraically closed field $\Bbbk$. To solve this question, in Section 5.2 we associate any fusion category $\mathcal{C}$ with three positive integers: $m_{\mathcal{C}}$, $n_{\mathcal{C}}$ and $d_{\mathcal{C}}$, where the first one is the Casimir number of $\mathcal{C}$ and the last one is the determinant of the matrix of left multiplication by $\sum_{i\in I} X_i X_{i^*}$ with respect to the basis $\{X_i\}_{i\in I}$ of $\operatorname{Gr}(\mathcal{C})$. These numbers provide a semisimplicity criterion on Grothendieck algebras, namely, the Grothendieck algebra $\operatorname{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ over any field K is semisimple if and only if any one of these numbers is not zero in K. This leads to a result that the three numbers $m_{\mathcal{C}}$, $n_{\mathcal{C}}$ and $d_{\mathcal{C}}$ have the same prime factors. The semisimplicity criterion for Grothendieck algebras together with Shimizu's work [60, Theorem 6.5] gives a criterion for a pivotal fusion category to be non-degenerate. That is, a pivotal fusion category $\mathcal{C}$ over a field $\Bbbk$ is non-degenerate if and only if one of the numbers $m_{\mathcal{C}}$, $n_{\mathcal{C}}$ and $d_{\mathcal{C}}$ is not zero in $\Bbbk$.

The Casimir number of a special kind of Verlinde modular category $\mathcal{C}$ of rank $n+1$ is calculated to be $2n+4$ in Section 5.3. It follows that the Grothendieck algebra $\operatorname{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ over a field K is semisimple if and only if $2n+4$ is a unit in K. This is equivalent to saying that the $(n+1)$-th Dickson polynomial $E_{n+1}(X)$ of the second kind has no multiple factors in $K[X]$. If $2n+4$ is zero in K, we use the factorizations of Dickson polynomials to describe the Jacobson radical of $\operatorname{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ explicitly

As these numbers $m_{\mathcal{C}}$, $n_{\mathcal{C}}$ and $d_{\mathcal{C}}$ have the same prime factors, in Section 5.4 we only focus on the Casimir number $m_{\mathcal{C}}$ of a fusion category $\mathcal{C}$. We give some results concerning prime factors of the Casimir number of representation categories of semisimple Hopf algebras. In particular, for a semisimple and cosemisimple Hopf algebra H, we show that the Casimir number of the representation category of the Drinfeld double $D(H)$ shares the same prime factors with those of $\dim_{\Bbbk} H$. We also reveal a relationship between the Casimir number $m_{\mathcal{C}}$ of a fusion category $\mathcal{C}$ and the Casimir number $m_{\widetilde{\mathcal{C}}}$ of the pivotalization $\widetilde{\mathcal{C}}$ of $\mathcal{C}$. We show that the former is a factor of the latter. This gives a result that any non-degenerate fusion category over a field $\Bbbk$ has a nonzero Casimir number in $\Bbbk$. However, the converse is not known to be true.

The Frobenius-Schur exponent of a spherical fusion category $\mathcal{C}$ has been defined in [51, Definition 5.1] as a minimal positive integer satisfying certain properties. In the case that the ground field is the field $\mathbb{C}$ of complex numbers, the Cauchy theorem for spherical fusion categories asserts that the prime ideals dividing the global dimension dim($\mathcal{C}$) and those dividing the Frobenius-Schur exponent of $\mathcal{C}$ are the same in the ring of algebraic integers [10, Theorem 3.9]. We prove in Section 5.5 that the Casimir number and the Frobenius-Schur exponent of $\mathcal{C}$ have the same prime factors, which may be considered as another statement of the Cauchy theorem for spherical fusion categories.

§5.2 Numerical invariants

In this section, all fusion categories are defined over an algebraically closed field $\Bbbk$ of arbitrary characteristic. We first introduce some numerical invariants of a fusion category $\mathcal{C}$, and then use them to describe when the Grothendieck algebra $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ over any field K is semisimple.

Let $\mathcal{C}$ be a fusion category over $\Bbbk$ and $\{X_i\}_{i\in I}$ the set of isomorphism classes of simple objects of $\mathcal{C}$. The Grothendieck ring $\mathrm{Gr}(\mathcal{C})$ of $\mathcal{C}$ is an associative unital ring with a multiplication induced by the tensor product on $\mathcal{C}$, namely,

$$X_iX_j := [X_i \otimes X_j] = \sum_{k\in I} N_{ij}^k X_k,$$

where N_{ij}^k, called the *fusion coefficient* of $\mathrm{Gr}(\mathcal{C})$, is the multiplicity of X_k in the Jordan-Hölder series of $X_i \otimes X_j$. The duality functor $*$ of $\mathcal{C}$ induces an involution on $\mathrm{Gr}(\mathcal{C})$, namely, $(X_iX_j)^* = X_j^*X_i^*$ and $(X_i)^{**} = X_i$ for $i, j \in I$. We write $(X_i)^* = X_{i^*}$ for convenience. In view of this, the duality functor $*$ induces a permutation on the index set I.

There is an associative symmetric and non-degenerate $\mathbb{Z}$-bilinear form $(-,-)$ on $\mathrm{Gr}(\mathcal{C})$ defined by

$$(X_i, X_j) = \dim_{\Bbbk} \mathrm{Hom}(X_i, X_j^*) = \delta_{i,j^*},$$

where δ_{i,j^*} is the Kronecker symbol. This form is also $*$-invariant, namely, $(X_i, X_j) = (X_i^*, X_j^*)$ for all $i, j \in I$. Thus, $\mathrm{Gr}(\mathcal{C})$ is a symmetric $*$-algebra over $\mathbb{Z}$. The pair of dual bases with respect to the form $(-,-)$ is the set $\{X_i, X_{i^*}\}_{i\in I}$ satisfying the following equality:

$$\sum_{i\in I} X_i \otimes X_{i^*} = \sum_{i\in I} X_{i^*} \otimes X_i.$$

Note that $N_{ij}^k = (X_iX_j, X_{k^*})$ hold for all $i, j, k \in I$. It follows from

$$(X_iX_j, X_{k^*}) = (X_{i^*}X_k, X_{j^*}) = (X_kX_{j^*}, X_{i^*})$$

that $N_{ij}^k = N_{i^*k}^j = N_{kj^*}^i$. Using this equality one is able to check that

$$\sum_{i\in I} X_j X_i \otimes X_{i^*} = \sum_{i\in I} X_i \otimes X_{i^*} X_j, \tag{5.1}$$

$$\sum_{i\in I} X_i X_j \otimes X_{i^*} = \sum_{i\in I} X_i \otimes X_j X_{i^*}. \tag{5.2}$$

Recall that the *Casimir operator* (see e.g. [47, Section 3.1]) of the Grothendieck ring $\mathrm{Gr}(\mathcal{C})$ is the map c from $\mathrm{Gr}(\mathcal{C})$ to its center $Z(\mathrm{Gr}(\mathcal{C}))$ given by

$$c(a) = \sum_{i\in I} X_i a X_{i^*} \text{ for } a \in \mathrm{Gr}(\mathcal{C}).$$

The element $c(1) = \sum_{i\in I} X_i X_{i^*}$, depending on $(-,-)$ only up to a central unit of $\mathrm{Gr}(\mathcal{C})$ (see [47, Section 1.2.5]), is called the *Casimir element* of $\mathrm{Gr}(\mathcal{C})$. It is well known that the image $\mathrm{Im}c$ of c is an ideal of $Z(\mathrm{Gr}(\mathcal{C}))$ and is called the *Higman ideal* of $\mathrm{Gr}(\mathcal{C})$.

The element $c(1) = \sum_{i\in I} X_i X_{i^*}$, as an element in $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q}$, is central invertible (see the proof of [28, Lemma 9.3.10]), hence there exists a unique central invertible element b in $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q}$ such that $c(1)b = 1$. Suppose $b = \sum_{i\in I} \frac{m_i}{n_i} X_i$, where m_i and n_i form a pair of coprime integers for each $i \in I$. Denote by $n_{\mathcal{C}} > 0$ the least common multiple of n_i for all $i \in I$. Then $bn_{\mathcal{C}} \in \mathrm{Gr}(\mathcal{C})$ and $n_{\mathcal{C}} = c(1)bn_{\mathcal{C}} = c(bn_{\mathcal{C}})$. This means that $n_{\mathcal{C}} \in \mathbb{Z} \cap \mathrm{Im}c$, and hence $\mathbb{Z} \cap \mathrm{Im}c \neq \{0\}$.

Since the intersection $\mathbb{Z} \cap \mathrm{Im}c$ is a nonzero principle ideal of $\mathbb{Z}$, the positive generator of $\mathbb{Z} \cap \mathrm{Im}c$ (denoted by $m_{\mathcal{C}}$) is called the *Casimir number* of $\mathcal{C}$. Namely, $\mathbb{Z} \cap \mathrm{Im}c = (m_{\mathcal{C}})$ for $m_{\mathcal{C}} > 0$. The element a satisfying $c(a) = m_{\mathcal{C}}$ is not unique in general. It is easy to see that the element a satisfying $c(a) = m_{\mathcal{C}}$ is unique if and only if the map c is injective, if and only if $\mathrm{Gr}(\mathcal{C})$ is commutative. The Casimir number $m_{\mathcal{C}}$ always divides the number $n_{\mathcal{C}}$ since we have seen that $n_{\mathcal{C}} \in \mathbb{Z} \cap \mathrm{Im}c$. If $\mathrm{Gr}(\mathcal{C})$ is commutative, we have $m_{\mathcal{C}} = n_{\mathcal{C}}$.

Observe that the matrix $[c(1)]$ of left multiplication by $c(1)$ with respect to the basis $\{X_i\}_{i\in I}$ of $\mathrm{Gr}(\mathcal{C})$ is a positive definite integer matrix (see [47, Proposition 8]). It follows that the determinant $d_{\mathcal{C}} := \det[c(1)]$, called the *determinant* of $\mathcal{C}$, is always a positive integer.

Remark 5.2.1 (1) *If two fusion categories are monoidally equivalent under a monoidal functor, then this functor induces an isomorphism preserving fusion coefficients* *between the Grothendieck rings of fusion categories. Thus, equivalent fusion categories lead to the same Casimir numbers and the same determinants.*

(2) *Let H_1 and H_2 be two finite dimensional semisimple Hopf algebras over $\Bbbk$. If H_1 and H_2 are twisted of each other in the sense that $H_1 = H_2$ as algebras and $H_2 = (H_1)_\Omega$ for some 2-pseudo-cocycle Ω, then the Grothendieck rings $Gr(H_1)$ and $Gr(H_2)$ share the same fusion coefficients (see [53, Theorem 4.1]). It turns out that the Casimir number or the determinant of representation category of H_1 is the same as that of H_2. In other words, the Casimir number or the determinant of representation category of a semisimple Hopf algebra is stable under twisting.*

(3) *The notation of the Casimir number of a fusion category defined here is indeed a special case of the notation of Casimir number defined over a representation category of a finite dimensional Hopf algebra, see Section 4.2.*

Proposition 5.2.2 *Let $\mathcal{C}$ be a fusion category over $\Bbbk$. For any field K, the following statements are equivalent:*

(1) *The determinant $d_{\mathcal{C}} \neq 0$ in K.*

(2) *The number $n_{\mathcal{C}} \neq 0$ in K.*

(3) *The Casimir number $m_{\mathcal{C}} \neq 0$ in K.*

(4) *The Grothendieck algebra $Gr(\mathcal{C}) \otimes_{\mathbb{Z}} K$ is semisimple.*

Proof.(1) $\Rightarrow$ (2): Let $c(1) = \sum_{i \in I} X_i X_{i^*}$ denote the Casimir element of $\mathrm{Gr}(\mathcal{C})$. Suppose the characteristic polynomial of the integer matrix $[c(1)]$ is

$$f(x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_{n-1} x + \alpha_n,$$

where n is the cardinality of I. Then $f(x) \in \mathbb{Z}[x]$ and $\alpha_n = \pm d_{\mathcal{C}}$. By the Cayley-Hamilton's theorem, the operator of left multiplication by $c(1)$ satisfies that

$$0 = f(c(1)) = c(1)(c(1)^{n-1} + \alpha_1 c(1)^{n-2} + \cdots + \alpha_{n-1}) + \alpha_n = c(1)a + \alpha_n,$$

where $a = c(1)^{n-1} + \alpha_1 c(1)^{n-2} + \cdots + \alpha_{n-1}$. Thus, $c(1)a = -\alpha_n = \mp d_{\mathcal{C}} \in \mathbb{Z}$. By the definition of $n_{\mathcal{C}}$, we have $n_{\mathcal{C}} \mid d_{\mathcal{C}}$. Now $d_{\mathcal{C}} \neq 0$ in K implies that $n_{\mathcal{C}} \neq 0$ in K.

(2) $\Rightarrow$ (3): It follows from $m_{\mathcal{C}} \mid n_{\mathcal{C}}$.

(3) $\Rightarrow$ (4): Note that there exists some $a \in \mathrm{Gr}(\mathcal{C})$ such that $\sum_{i\in I} X_i a X_{i^*} = m_{\mathcal{C}}$. Denote by $A := \mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ and consider $\sum_{i\in I} X_i \frac{a}{m_{\mathcal{C}}} \otimes X_{i^*} \in A \otimes A$. Obviously,

$$\sum_{i\in I} X_i \frac{a}{m_{\mathcal{C}}} X_{i^*} = 1 \text{ and } \sum_{i\in I} bX_i \frac{a}{m_{\mathcal{C}}} \otimes X_{i^*} = \sum_{i\in I} X_i \frac{a}{m_{\mathcal{C}}} \otimes X_{i^*} b$$

holds for any $b \in A$, see (5.1). Thus, $\sum_{i\in I} X_i \frac{a}{m_{\mathcal{C}}} \otimes X_{i^*}$ is a separable idempotent of A, and hence A is a separable K-algebra. It is well known that any separable K-algebra is a semisimple K-algebra (see e.g., [11]).

(4) $\Rightarrow$ (1): Let $\mathrm{Tr}(a)$ be the trace of the operator of left multiplication by $a \in A$. Since A is semisimple, the bilinear form $\langle a, b\rangle = \mathrm{Tr}(ab)$ on A is non-degenerate. This implies that the matrix $[a_{ij}]$ for $a_{ij} = \langle X_i, X_j\rangle$ is an invertible matrix in K. Let c_{ij} be the (i,j)-entry of $[c(1)]$. Then

$$\begin{aligned}
c_{ij} &= (\sum_{k\in I} X_k X_{k^*} X_i, X_{j^*}) = \sum_{k\in I} (X_i X_{j^*} X_k, X_{k^*}) \\
&= \sum_{k,s\in I} (N_{ij^*}^s X_s X_k, X_{k^*}) = \sum_{k,s\in I} N_{ij^*}^s (X_s X_k, X_{k^*}) \\
&= \sum_{k,s\in I} N_{ij^*}^s N_{sk}^k = \sum_{s\in I} N_{ij^*}^s \mathrm{Tr}(X_s) \\
&= \mathrm{Tr}(\sum_{s\in I} N_{ij^*}^s X_s) = \mathrm{Tr}(X_i X_{j^*}) \\
&= a_{ij^*}.
\end{aligned}$$

That is, the matrix $[c(1)]$ differs from the matrix $[a_{ij}]$ only by permutations of columns. It follows that $[c(1)]$ is an invertible matrix in K and $\det[c(1)] = d_{\mathcal{C}} \neq 0$ in K. □

Remark 5.2.3 (1) *The proof of* (4) $\Rightarrow$ (1) *in Proposition 5.2.2 comes from the proof of [54, Proposition 2.9]. From this proof one is able to see that* $d_{\mathcal{C}} = \pm\det[a_{ij}]$*, where* $a_{ij} = Tr(X_i X_j)$ *for* $i, j \in I$.

(2) *The result that* $Gr(\mathcal{C}) \otimes_{\mathbb{Z}} K$ *is semisimple if and only if* $m_{\mathcal{C}} \neq 0$ *in* K *is essentially the Higman's theorem applied to the Frobenius algebra* $Gr(\mathcal{C}) \otimes_{\mathbb{Z}} K$ *(see [38, Theorem*

1] or [47, Proposition 6]). This result can also be deduced directly from Theorem 4.2.1.

(3) *Any one of the statements of Proposition 5.2.2 is equivalent to the result that $c(1) = \sum_{i \in I} X_i X_{i^*}$ is invertible in $Gr(\mathcal{C}) \otimes_{\mathbb{Z}} K$ (see [63, Theorem 3.8]).*

It can be seen from the proof of (1) $\Rightarrow$ (2) in Proposition 5.2.2 that $n_{\mathcal{C}} \mid d_{\mathcal{C}}$. Together with $m_{\mathcal{C}} \mid n_{\mathcal{C}}$ we may see that $m_{\mathcal{C}} \mid n_{\mathcal{C}}$ and $n_{\mathcal{C}} \mid d_{\mathcal{C}}$. Moreover, if the field K is of characteristic p, it follows from Proposition 5.2.2 that $p \nmid d_{\mathcal{C}}$ if and only if $p \nmid n_{\mathcal{C}}$, if and only if $p \nmid m_{\mathcal{C}}$. This gives the following relationship among the numbers $m_{\mathcal{C}}$, $n_{\mathcal{C}}$ and $d_{\mathcal{C}}$:

Theorem 5.2.4 *The Casimir number $m_{\mathcal{C}}$, the number $n_{\mathcal{C}}$ and the determinant $d_{\mathcal{C}}$ of a fusion category $\mathcal{C}$ have the same prime factors.*

Recall from [60, Theorem 6.5] that a pivotal fusion category $\mathcal{C}$ over a field $\Bbbk$ is non-degenerate (i.e., the global dimension $\dim(\mathcal{C})$ of $\mathcal{C}$ is not zero in $\Bbbk$) if and only if its Grothendieck algebra $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} \Bbbk$ is semisimple. This result together with Proposition 5.2.2 gives a criterion for non-degenerate pivotal fusion categories:

Proposition 5.2.5 *A pivotal fusion category $\mathcal{C}$ over a field $\Bbbk$ is non-degenerate if and only if any one of these numbers $m_{\mathcal{C}}$, $n_{\mathcal{C}}$ and $d_{\mathcal{C}}$ is not zero in $\Bbbk$.*

The rest of this section provides some fusion categories whose determinants or Casimir numbers can be explicitly described.

Example 5.2.6 *Let $\mathcal{C}$ be a pointed fusion category over a field $\Bbbk$. The Grothendieck ring of $\mathcal{C}$ is the group ring $\mathbb{Z}G$ for a finite group G. The Casimir number of $\mathcal{C}$ is the order $|G|$ of G and the determinant of $\mathcal{C}$ is $|G|^{|G|}$. It follows from Proposition 5.2.2 that for any field K, the K-algebra $KG = \mathbb{Z}G \otimes_{\mathbb{Z}} K$ is semisimple if and only if $|G| \neq 0$ in K. This is the Maschke's theorem for group algebras.*

Example 5.2.7 *Let $\mathcal{C}$ be a modular category over a field $\Bbbk$ with isomorphism classes of simple objects $\{X_i\}_{i \in I}$. That is, $\mathcal{C}$ is a spherical fusion category with a braiding c such that the S-matrix $S = [s_{ij}]$ is invertible in $\Bbbk$, where $s_{ij} = Tr(c_{X_j X_i} \circ c_{X_i X_j})$ (see* *e.g. [28, Section 8.14]). Note that* $\dim(X_i) \neq 0$ *in* $\Bbbk$ *for any* $i \in I$ *(see [28, Proposition 4.8.4]). For any* $i \in I$*, the map*

$$h_i : X_j \mapsto \frac{s_{ij}}{\dim(X_i)} \quad \text{for } j \in I$$

defines a homomorphism from Gr($\mathcal{C}$*) to* $\Bbbk$*. In other words,* $\{h_i(X_j)\}_{i\in I}$ *forms all eigenvalues of the matrix* $[X_j]$ *of left multiplication by* X_j *with respect to the basis* $\{X_i\}_{i\in I}$ *of Gr(*$\mathcal{C}$*). Note that all eigenvalues of the matrix* $[c(1)]$ *are* $h_i(c(1))$ *for* $i \in I$*. Moreover,*

$$h_i(c(1)) = h_i(\sum_{j\in I} X_j X_{j^*}) = \sum_{j\in I} h_i(X_j)h_i(X_{j^*}) = \sum_{j\in I} \frac{s_{ij}s_{ij^*}}{\dim(X_i)^2} = \frac{\dim(\mathcal{C})}{\dim(X_i)^2},$$

where the last equality follows from [28, Proposition 8.14.2]. It follows that

$$d_{\mathcal{C}} = \prod_{i\in I} h_i(c(1)) = \frac{(\dim \mathcal{C})^n}{\prod_{i\in I}\dim(X_i)^2},$$

where n *is the cardinality of* I*.*

Example 5.2.8 *Recall from [61] that the near-group category* $\mathcal{C}$ *is a rigid fusion category whose simple objects except for one are invertible. Let* G *be the group of isomorphism classes of invertible objects in* $\mathcal{C}$ *and* X *the isomorphism class of the remaining non-invertible simple object. The Grothendieck ring Gr(*$\mathcal{C}$*) of* $\mathcal{C}$ *obey the following multiplication rule:*

$$g \cdot h = gh, \;\; g \cdot X = X \cdot g = X, \;\; X^2 = \sum_{g\in G} g + \rho X,$$

where $g, h \in G$ *and* ρ *is a positive integer. The matrix* $[c(1)]$ *of left multiplication by* $c(1)$ *with respect to the basis* $G \cup \{X\}$ *of Gr(*$\mathcal{C}$*) can be written explicitly as follows (see [67, Example 3.3]):*

$$[c(1)] = \begin{bmatrix} M & \mathbf{u} \\ \mathbf{u}^t & \rho^2 + 2|G| \end{bmatrix},$$

where M *is a square matrix of size* $|G|$ *whose diagonal elements are all* $|G| + 1$ *and off-diagonal elements are all* 1*,* $\mathbf{u}$ *is a column vector of size* $|G|$ *whose elements are all* ρ*. It is easy to compute that*

$$d_{\mathcal{C}} = \det[c(1)] = (4|G| + \rho^2)|G|^{|G|}.$$

Note that the Casimir number of $\mathcal{C}$ is a minimal positive integer $m_{\mathcal{C}}$ such that

$$\sum_{g\in G} gag^{-1} + XaX = m_{\mathcal{C}} \quad \textit{for some } a \in Gr(\mathcal{C}).$$

Accordingly, the Casimir number $m_{\mathcal{C}}$ and the associated $a \in Gr(\mathcal{C})$ can be determined separately as follows:

Case 1: *If ρ is odd, then $a = (4|G| + \rho^2) - 2\sum_{g\in G} g - \rho X$ and $m_{\mathcal{C}} = (4|G| + \rho^2)|G|$.*

Case 2: *If ρ is even, then $a = \frac{1}{2}(4|G| + \rho^2) - \sum_{g\in G} g - \frac{\rho}{2}X$ and $m_{\mathcal{C}} = \frac{1}{2}(4|G| + \rho^2)|G|$.*

We see that $m_{\mathcal{C}}$ and $d_{\mathcal{C}}$ have the same prime factors for both cases (1) and (2).

§5.3 The Casimir numbers of Verlinde modular categories

In this section, we consider the Casimir number of a Verlinde modular category $\mathcal{C}$ of rank $n+1$ introduced in [28], see also [5]. By heavy computation, we will find that the Casimir number of $\mathcal{C}$ is $2n+4$. It will be shown that the Grothendieck algebra $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ considered here is isomorphic to the quotient algebra $K[X]/(E_{n+1}(X))$, where $E_{n+1}(X)$ is the $(n+1)$-th Dickson polynomial of the second kind. This leads to a byproduct that $E_{n+1}(X)$ has no multiple factors in $K[X]$ if and only if $2n+4$ is a unit in K, although the factorizations of $E_{n+1}(X)$ have been carried out using much lengthier methods [15], see also [9]. In the case when $2n+4$ is zero in K, we use the factorizations of Dickson polynomials to describe the Jacobson radical of $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ explicitly.

Let $\mathfrak{g}$ be a simple complex Lie algebra, n a positive integer and $q = e^{\frac{\pi i}{n+2}}$ a complex number. The *Verlinde modular category* $\mathcal{C}(\mathfrak{g}, q)$ associative with the pair $(\mathfrak{g}, q)$ is "semisimple part" of the representation category of the associated Lusztig quantum group $U_q^L(\mathfrak{g})$, more precisely, the quotient of the subcategory of tilting modules by the subcategory of negligible modules (see [28, Section 8.12.2]).

In the following we only consider the case $\mathfrak{g} = \mathfrak{sl}_2$ and denote the Verlinde modular category $\mathcal{C}(\mathfrak{sl}_2, q)$ by $\mathcal{C}_n(q)$. The simple objects of $\mathcal{C}_n(q)$ are $X_0, X_1, \cdots, X_n$, the irreducible representations of the Lusztig quantum group $\mathfrak{u}_q(\mathfrak{sl}_2)$ (i.e., simple comodules for the quantum function algebra $O_q(SL_2)$ with highest weights $0, 1, \cdots, n$). The tensor product in $\mathcal{C}_n(q)$ is the truncation of the usual tensor product in representation category of $\mathfrak{u}_q(\mathfrak{sl}_2)$, namely, the usual tensor product $X_i \otimes X_j$ modulo a certain "negligible" part of $X_i \otimes X_j$. For instance, $\mathcal{C}_1(q) = \mathrm{Vec}^{\omega}_{\mathbb{Z}/2\mathbb{Z}}$ (where ω is the nontrivial 3-cocycle), $\mathcal{C}_2(q)$ is one of the well-known Ising model categories [25, Appendix B].

The Grothendieck ring $\mathrm{Gr}(\mathcal{C}_n(q))$ of $\mathcal{C}_n(q)$ is the truncated Verlinde ring given in [28, Example 4.10.6] whose multiplication rule is

$$X_iX_j = \sum_{l=\max\{i+j-n,0\}}^{\min\{i,j\}} X_{i+j-2l}. \tag{5.3}$$

This Grothendieck ring is a symmetric Frobenius algebra over $\mathbb{Z}$ with the bilinear form defined by $(X_i, X_j) = \delta_{ij}$. Thus, $\{X_i, X_i \mid 0 \leq i \leq n\}$ forms a pair of dual bases of $\mathrm{Gr}(\mathcal{C}_n(q))$ with respect to the bilinear form $(-,-)$.

The Casimir operator of $\mathrm{Gr}(\mathcal{C}_n(q))$ is the map c from $\mathrm{Gr}(\mathcal{C}_n(q))$ to its center given by

$$c(x) = \sum_{i=0}^{n} X_i x X_i \text{ for } x \in \mathrm{Gr}(\mathcal{C}_n(q)).$$

Since $\mathrm{Gr}(\mathcal{C}_n(q))$ is commutative, we have $c(x) = c(1)x$, where $c(1) = \sum_{i=0}^{n} X_i^2$, which is the Casimir element of $\mathrm{Gr}(\mathcal{C}_n(q))$. The Casimir number of $\mathrm{Gr}(\mathcal{C}_n(q))$ is the non-negative integer m satisfying $\mathbb{Z} \cap \mathrm{Im}c = (m)$. This number is a category invariant of $\mathcal{C}_n(q)$, so is also called the Casimir number of the category $\mathcal{C}_n(q)$. We shall see that the Casimir number of $\mathcal{C}_n(q)$ can be used to detect when the Grothendieck algebra $\mathrm{Gr}(\mathcal{C}_n(q)) \otimes_{\mathbb{Z}} K$ over a field K is semisimple.

In the following, we shall calculate the Casimir number of $\mathcal{C}_n(q)$. Firstly, the Casimir element $c(1)$ of $\mathrm{Gr}(\mathcal{C}_n(q))$ can be described as follows.

Lemma 5.3.1 *We have* $c(1) = \sum_{j=0}^{[\frac{n}{2}]}(n+1-2j)X_{2j}$.

Proof. A direct calculation shows that

$$\begin{aligned} c(1) &= \sum_{j=0}^{[\frac{n}{2}]} X_j^2 + \sum_{j=[\frac{n}{2}]+1}^{n} X_j^2 \\ &= \sum_{j=0}^{[\frac{n}{2}]} \sum_{l=0}^{j} X_{2j-2l} + \sum_{j=[\frac{n}{2}]+1}^{n} \sum_{l=2j-n}^{j} X_{2j-2l} \quad \text{by (5.3)} \end{aligned}$$

$$= \begin{cases} 2(X_0 + (X_0 + X_2) + \cdots + (X_0 + X_2 + \cdots + X_{n-2})) \\ +(X_0 + X_2 + \cdots + X_n), & 2 \mid n \\ 2(X_0 + (X_0 + X_2) + \cdots + (X_0 + X_2 + \cdots + X_{n-1})), & 2 \nmid n \end{cases}$$
$$= \sum_{j=0}^{[\frac{n}{2}]} (n + 1 - 2j) X_{2j}.$$

We complete the proof. □

To describe the $\mathbb{Z}$-linear expression of $c(x)$ for any $x \in \mathrm{Gr}(\mathcal{C}_n(q))$, we need some preparations. The left multiplication by X_i with respect to the basis $\{X_0, X_1, \cdots, X_n\}$ corresponds to a matrix, which is denoted by $\mathbf{X}_i$, namely,

$$X_i \begin{pmatrix} X_0 \\ X_1 \\ \vdots \\ X_n \end{pmatrix} = \mathbf{X}_i \begin{pmatrix} X_0 \\ X_1 \\ \vdots \\ X_n \end{pmatrix}.$$

We denote $\mathbf{E}_{i+1,j+1}$ for $0 \leq i, j \leq n$ the square matrix unit of order $n + 1$ with $(i + 1, j + 1)$-entry 1, and 0 otherwise. Then the matrix $\mathbf{X}_i$ can be written explicitly as follows:

$$\begin{aligned} \mathbf{X}_i = {} & \mathbf{E}_{1,i+1} + \mathbf{E}_{2,i+2} + \mathbf{E}_{3,i+3} + \cdots + \mathbf{E}_{n-i+1,n+1} \\ & + \mathbf{E}_{2,i} + \mathbf{E}_{3,i+1} + \mathbf{E}_{4,i+2} + \cdots + \mathbf{E}_{n-i+2,n} \\ & + \mathbf{E}_{3,i-1} + \mathbf{E}_{4,i} + \mathbf{E}_{5,i+1} + \cdots + \mathbf{E}_{n-i+3,n-1} \\ & + \cdots \\ & + \mathbf{E}_{i+1,1} + \mathbf{E}_{i+2,2} + \mathbf{E}_{i+3,3} + \cdots + \mathbf{E}_{n+1,n-i+1} \\ = {} & \sum_{s=0}^{i} \sum_{t=0}^{n-i} \mathbf{E}_{s+t+1,i+t-s+1}. \end{aligned} \tag{5.4}$$

Let $\delta(i)$ be the function defined over $\mathbb{Z}$ by $\delta(i) = 1$ if i is even, and 0 if i is odd. Then the coefficient of X_i in the linear expression of $c(x)$ has the following form.

Proposition 5.3.2 *Let $x = \sum_{k=0}^{n} \lambda_k X_k$. Then the coefficient of X_i in the linear expression of $c(x)$ is $(n+1-i)\sum_{k=0}^{i}(k+1)\delta(i+k)\lambda_k + (i+1)\sum_{k=i+1}^{n}(n-k+1)\delta(i+k)\lambda_k$.*

Proof.Let $X_jX_k = \sum_{i=0}^{n} N_{jk}^i X_i$. Then $N_{jk}^i = (X_jX_k, X_i) = (X_iX_j, X_k) = N_{ij}^k$ since the form $(-,-)$ is associative and symmetric. It follows that

$$c(x) = c(1)x = \sum_{j,k=0}^{n} (n+1-j)\delta(j)\lambda_k X_j X_k = \sum_{i,j,k=0}^{n} (n+1-j)\delta(j)\lambda_k N_{ij}^k X_i.$$

Thus, the coefficient of X_i in the linear expression of $c(x)$ is $\sum_{j,k=0}^{n}(n+1-j)\delta(j)\lambda_k N_{ij}^k$. Moreover, this coefficient can also be written as follows:

$$\begin{aligned}
&\sum_{j,k=0}^{n} (n+1-j)\delta(j)\lambda_k N_{ij}^k \\
&= (\lambda_0, \lambda_1, \cdots, \lambda_n)\mathbf{X}_i \begin{pmatrix} (n+1)\delta(0) \\ n\delta(1) \\ \vdots \\ \delta(n) \end{pmatrix} \\
&= \sum_{s=0}^{i}\sum_{t=0}^{n-i} (\lambda_0, \lambda_1, \cdots, \lambda_n)\mathbf{E}_{s+t+1, i+t-s+1} \begin{pmatrix} (n+1)\delta(0) \\ n\delta(1) \\ \vdots \\ \delta(n) \end{pmatrix} \quad \text{by (5.4)} \\
&= \sum_{s=0}^{i}\sum_{t=0}^{n-i} (n+1-i-t+s)\delta(i+t-s)\lambda_{s+t}. \qquad (5.5)
\end{aligned}$$

A straightforward computation shows that if $s+t=k \leq i$, then the coefficient of λ_k in (5.5) is $(n+1-i)(k+1)\delta(i+k)$; if $s+t=k>i$, then the coefficient of λ_k in (5.5) is $(i+1)(n-k+1)\delta(i+k)$. Thus, (5.5) is equal to

$$(n+1-i)\sum_{k=0}^{i}(k+1)\delta(i+k)\lambda_k + (i+1)\sum_{k=i+1}^{n}(n-k+1)\delta(i+k)\lambda_k.$$

This completes the proof. □

The main result of this section is presented as follows.

Theorem 5.3.3 *The Casimir number of Verlinde modular category $\mathcal{C}_n(q)$ is $2n+4$.*

Proof.Let $x = \sum_{k=0}^{n} \lambda_k X_k$. It follows from Proposition 5.3.2 that the coefficient α_i of

X_i in the linear expression of $c(x)$ is

$$\alpha_i = (n+1-i)\sum_{k=0}^{i}(k+1)\delta(i+k)\lambda_k + (i+1)\sum_{k=i+1}^{n}(n-k+1)\delta(i+k)\lambda_k,$$

for $0 \leq i \leq n$. If $c(x) \in \mathbb{Z}$, then $\alpha_i = 0$ for $1 \leq i \leq n$. Consider the system of equations

$$\begin{cases} \alpha_n = 0 \\ \alpha_{n-2} = 0 \end{cases}$$

with variables $\lambda_0, \lambda_1, \cdots, \lambda_n$. This implies that $\lambda_n = 0$. Similarly, the system of equations

$$\begin{cases} \alpha_{n-1} = 0 \\ \alpha_{n-3} = 0 \end{cases}$$

together with $\lambda_n = 0$ induces that $\lambda_{n-1} = 0$. Repeating this argument until the following equations:

$$\begin{cases} \alpha_3 = 0 \\ \alpha_1 = 0, \end{cases}$$

we obtain that $\lambda_n = \lambda_{n-1} = \cdots = \lambda_3 = 0$. Now consider the system of equations

$$\begin{cases} \alpha_2 = 0 \\ \alpha_1 = 0. \end{cases}$$

It follows that $\lambda_1 = 0$ and $\lambda_0 = -3\lambda_2$. Thus, the coefficient α_0 of X_0 is

$$\begin{aligned} \alpha_0 &= (n+1)\lambda_0 + \sum_{k=1}^{n}(n-k+1)\delta(k)\lambda_k \\ &= (n+1)\lambda_0 + (n-1)\lambda_2 \\ &= -(2n+4)\lambda_2. \end{aligned}$$

We conclude that the Casimir number of $\mathcal{C}_n(q)$ is $2n+4$. □

Remark 5.3.4 *The maximal non-negative eigenvalue of the matrix $\mathbf{X}_i$ is called the Frobenius-Perron dimension of X_i, denoted FPdim(X_i). Then FPdim induces an algebra morphism from $Gr(\mathcal{C}_n(q))$ to the field $\mathbb{C}$ of complex numbers. Note that*

$$FPdim(X_i) = \frac{q^{i+1} - q^{-i-1}}{q - q^{-1}}$$

for $0 \le i \le n$ *(see [28, Exercise 4.10.7]). Then the Frobenius-Perron dimension of* $\mathcal{C}_n(q)$ *is the number* $FPdim(\mathcal{C}_n(q))$ *defined to be*

$$FPdim(\mathcal{C}_n(q)) = FPdim(c(1)) = \sum_{i=0}^{n}(FPdim(X_i))^2 = \frac{2n+4}{(q-q^{-1})^2}.$$

This shows that

$$2n+4 = FPdim(\mathcal{C}_n(q))(q-q^{-1})^2,$$

which gives a relationship between the Casimir number of $\mathcal{C}_n(q)$ *and the Frobenius-Perron dimension of* $\mathcal{C}_n(q)$*. By the way, this equality can be obtained as well from the following approach: it follows from Theorem 5.3.3 that* $2n+4 = c(1)x$*, where* $x = 3 - X_2$*, applying FPdim to this equality we also obtain that*

$$2n+4 = FPdim(\mathcal{C}_n(q))FPdim(x) = FPdim(\mathcal{C}_n(q))(q-q^{-1})^2.$$

The Casimir number of $\mathcal{C}_n(q)$ can be used to determine the semisimplicity of the Grothendieck algebra $\mathrm{Gr}(\mathcal{C}_n(q)) \otimes_{\mathbb{Z}} K$ over a field K. In the following, we turn to consider the Jacobson radical of $\mathrm{Gr}(\mathcal{C}_n(q)) \otimes_{\mathbb{Z}} K$ in the case when $2n+4$ is zero in K. To this end, we need to present the Grothendieck ring $\mathrm{Gr}(\mathcal{C}_n(q))$ in terms of generators and relations.

Let $\mathbb{Z}[X]$ be a polynomial ring with one variable X over $\mathbb{Z}$ and $(E_{n+1}(X))$ the ideal of $\mathbb{Z}[X]$ generated by the $n+1$-th Dickson polynomial $E_{n+1}(X)$ (see (4.2)). The image of a polynomial $f(X)$ under the natural ring epimorphism $\mathbb{Z}[X] \to \mathbb{Z}[X]/(E_{n+1}(X))$ is denoted by $\overline{f(X)}$. We have the following lemma.

Lemma 5.3.5 *For* $0 \le i, j \le n$*, the equality*

$$\overline{E_i(X)E_j(X)} = \sum_{l=\max\{i+j-n,0\}}^{\min\{i,j\}} \overline{E_{i+j-2l}(X)}$$

holds in $\mathbb{Z}[X]/(E_{n+1}(X))$*.*

Proof. We suppose that $E_s(X) = 0$ if $s < 0$. We proceed by induction on $i+j$ only for the case $0 \le i+j \le n$, and the proof of the case $n \le i+j \le 2n$ is similar. It is obvious that the identity holds for $i+j = 0$. For a fixed $1 \le k \le n-1$, suppose that the identity holds for $1 \le i+j \le k$. We show that it also holds for the case $i+j = k+1$. Note that $(i-1)+j \le k$ and $(i-2)+j \le k$. Applying the induction hypothesis on $(i-1)+j \le k$ and $(i-2)+j \le k$, we obtain the following two equalities:

$$\overline{E_{i-1}(X)E_j(X)} = \sum_{l=\max\{i-1+j-n,0\}}^{\min\{i-1,j\}} \overline{E_{i-1+j-2l}(X)} \tag{5.6}$$

and

$$\overline{E_{i-2}(X)E_j(X)} = \sum_{l=\max\{i-2+j-n,0\}}^{\min\{i-2,j\}} \overline{E_{i-2+j-2l}(X)}. \tag{5.7}$$

Now consider the product $\overline{XE_{i-1}(X)E_j(X)}$ in $\mathbb{Z}[X]/(E_{n+1}(X))$. On the one hand, using (5.6) we get that

$$\begin{aligned}\overline{XE_{i-1}(X)E_j(X)} &= \overline{X} \sum_{l=\max\{i-1+j-n,0\}}^{\min\{i-1,j\}} \overline{E_{i-1+j-2l}(X)} \\ &= \sum_{l=\max\{i-1+j-n,0\}}^{\min\{i-1,j\}} (\overline{E_{i+j-2l}(X)} + \overline{E_{i-2+j-2l}(X)}).\end{aligned}$$

On the other hand, using (5.7) we have

$$\begin{aligned}\overline{XE_{i-1}(X)E_j(X)} &= (\overline{E_i(X)} + \overline{E_{i-2}(X)})\overline{E_j(X)} \\ &= \overline{E_i(X)E_j(X)} + \sum_{l=\max\{i-2+j-n,0\}}^{\min\{i-2,j\}} \overline{E_{i-2+j-2l}(X)}.\end{aligned}$$

It follows that

$$\overline{E_i(X)E_j(X)} = \sum_{l=\max\{i-1+j-n,0\}}^{\min\{i-1,j\}} (\overline{E_{i+j-2l}(X)} + \overline{E_{i-2+j-2l}(X)}) - \sum_{l=\max\{i-2+j-n,0\}}^{\min\{i-2,j\}} \overline{E_{i-2+j-2l}(X)}.$$

By discussing the cases $i-1 < j$, $i-1 = j$ and $i-1 > j$ separately, we obtain that

$$\overline{E_i(X)E_j(X)} = \sum_{l=\max\{i+j-n,0\}}^{\min\{i,j\}} \overline{E_{i+j-2l}(X)}.$$

We complete the proof. □

Theorem 5.3.6 *The Grothendieck ring $Gr(\mathcal{C}_n(q))$ is isomorphic to the quotient ring $\mathbb{Z}[X]/(E_{n+1}(X))$.*

Proof. Consider the $\mathbb{Z}$-linear map θ from $\mathrm{Gr}(\mathcal{C}_n(q))$ to $\mathbb{Z}[X]/(E_{n+1}(X))$ given by $\theta(X_i) = \overline{E_i(X)}$ for $0 \leq i \leq n$. This is a ring epimorphism by Lemma 5.3.5. To see that this map is injective, we suppose $\sum_{i=0}^{n} \lambda_i \overline{E_i(X)} = 0$ for each $\lambda_i \in \mathbb{Z}$, then $\sum_{i=0}^{n} \lambda_i E_i(X) = E_{n+1}(X) f(X)$ for some $f(X) \in \mathbb{Z}[X]$. By comparing the degrees of both two sides of the equality, we obtain that $f(X) = 0$, and hence $\lambda_i = 0$ for $0 \leq i \leq n$. $\square$

The factorizations of $E_{n+1}(X)$ have been carried out using much lengthier methods by W.-S. Chou [15] (see also [9]). According to Theorem 5.3.6, we obtain the following criterion for $E_{n+1}(X)$ without multiple factors in $K[X]$.

Proposition 5.3.7 *The $(n+1)$-th Dickson polynomial $E_{n+1}(X)$ of the second kind has no multiple factors in $K[X]$ if and only if $2n+4$ is a unit in K.*

Proof. We have by Theorem 5.3.6 that $\mathrm{Gr}(\mathcal{C}_n(q)) \otimes_{\mathbb{Z}} K \cong K[X]/(E_{n+1}(X))$. It follows from Theorem 5.3.3 that $2n+4$ is a unit in K if and only if $K[X]/(E_{n+1}(X))$ is semisimple, if and only if $E_{n+1}(X)$ has no multiple factors in $K[X]$, as desired. $\square$

In the following we turn to describe the Jacobson radical of the Grothendieck algebra $\mathrm{Gr}(\mathcal{C}_n(q)) \otimes_{\mathbb{Z}} K$ (or equivalently, $K[X]/(E_{n+1}(X))$) in the case $2n+4$ is zero in K. Note that a product of all distinct irreducible factors of $E_{n+1}(X)$ gives rise to a generator of the Jacobson radical of $K[X]/(E_{n+1}(X))$.

Proposition 5.3.8 *Let the characteristic of K be $p > 2$. If $p \mid 2n+4$, write $n+2 = p^r(m+1)$ where $(p, m+1) = 1$, then the Jacobson radical of $K[X]/(E_{n+1}(X))$ is a principal ideal generated by $\overline{E_m(X)(X^2-4)}$.*

Proof. The decomposition $E_{n+1}(X) = E_m(X)^{p^r}(X^2-4)^{\frac{p^r-1}{2}}$ holds in $K[X]$ (see [9, Section 3]), and the Dickson polynomial $E_m(X)$ has no multiple factors in $K[X]$ by Proposition 5.3.7. It follows that $E_m(X)(X^2-4)$ is a product of all distinct irreducible factors of $E_{n+1}(X)$. We conclude that the Jacobson radical of $K[X]/(E_{n+1}(X))$ is a principal ideal generated by $\overline{E_m(X)(X^2-4)}$. $\square$

Let the characteristic of K be 2. Then the factorizations of the Dickson polynomials of the second kind are a little bit more complicated. If m is even, it follows from [9, Theorem 6] that $E_m(X) = F_m(X)^2$, where

$$F_m(X) = \sum_{j=0}^{\frac{m}{2}} \binom{m-j}{j} (-1)^j X^{\frac{m}{2}-j},$$

which is a product of several distinct irreducible polynomials in $K[X]$, which occur in cliques corresponding to the divisors d of $m+1$ with $d > 1$. To each such d there correspond $\varphi(d)/(2k_d)$ irreducible factors, where φ is the Euler's totient function and k_d is the least positive integer such that $q^{k_d} \equiv \pm 1 (\mathrm{mod}\ d)$. Each of such irreducible factors has the form

$$\prod_{i=0}^{k_d-1} (X - (\zeta_d^{2^i} + \zeta_d^{-2^i}))$$

for some choice of ζ_d, where ζ_d is a primitive d-th root of unity.

Proposition 5.3.9 *Let the characteristic of K be 2.*

(1) *If $n+1$ is even, then the Jacobson radical of $K[X]/(E_{n+1}(X))$ is a principal ideal generated by $\overline{F_{n+1}(X)}$.*

(2) *If $n+1$ is odd, write $n+2 = 2^r(m+1)$, where m is even, then the Jacobson radical of $K[X]/(E_{n+1}(X))$ is a principal ideal generated by $\overline{XF_m(X)}$.*

Proof.(1) If $n+1$ is even, then $F_{n+1}(X)$ is a product of all distinct irreducible factors of $E_{n+1}(X))$ as stated above. Thus, the Jacobson radical of $K[X]/(E_{n+1}(X))$ is a principal ideal generated by $\overline{F_{n+1}(X)}$.

(2) If $n+1$ is odd, write $n+2 = 2^r(m+1)$, where $r \geq 1$ and m is even. In this case,

$$E_{n+1}(X) = X^{2^r-1} E_m(X)^{2^r} = X^{2^r-1} F_m(X)^{2^{r+1}}$$

(see [9, Section 3]). Thus, $XF_m(X)$ can be written as a product of all distinct irreducible factors of $E_{n+1}(X))$, and hence the Jacobson radical of $K[X]/(E_{n+1}(X))$ is a principal ideal generated by $\overline{XF_m(X)}$. □

§5.4 Prime factors of Casimir numbers

Denote by m_H the Casimir number of representation category $\mathrm{Rep}(H)$ of a semisimple Hopf algebra H. In this section, we will give some results concerning prime factors of m_H. Obviously, these results holding for the Casimir number of $\mathrm{Rep}(H)$ also hold for the determinant of $\mathrm{Rep}(H)$ as the two numbers have the same prime factors. Then we show that the Casimir number $m_{\mathcal{C}}$ of a fusion category $\mathcal{C}$ divides the Casimir number $m_{\widetilde{\mathcal{C}}}$ of the pivotalization $\widetilde{\mathcal{C}}$. This is used to prove that any non-degenerate fusion category has a nonzero determinant.

A finite dimensional Hopf algebra H is call *pivotal* if H contains a group-like element g such that $S^2(h) = ghg^{-1}$ for all $h \in H$. The representation category $\mathrm{Rep}(H)$ of a finite dimensional semisimple pivotal Hopf algebra H is a pivotal fusion category.

Proposition 5.4.1 *Let H be a finite dimensional semisimple pivotal Hopf algebra over $\Bbbk$. The Casimir number $m_H \neq 0$ in $\Bbbk$ if and only if $S^2 = id_H$ and $\dim_{\Bbbk} H \neq 0$ in $\Bbbk$.*

Proof. The Casimir number $m_H \neq 0$ in $\Bbbk$ if and only if $\mathrm{Rep}(H)$ is non-degenerate by Proposition 5.2.5, if and only if H is cosemisimple by [29, Section 9.1], if and only if $S^2 = id_H$ and $\dim_{\Bbbk} H \neq 0$ in $\Bbbk$ by [27, Corollary 3.2]. □

Since a finite dimensional semisimple and cosemisimple Hopf algebra H over $\Bbbk$ always satisfies that $S^2 = id_H$ and $\dim_{\Bbbk} H \neq 0$ (see [27, Corollary 3.2]), Proposition 5.4.1 has the following corollary:

Corollary 5.4.2 *Let H be a finite dimensional semisimple and cosemisimple Hopf algebra over $\Bbbk$. The Casimir number m_H is always not zero in $\Bbbk$.*

The following result gives more information about the Casimir number m_H of a semisimple and cosemisimple Hopf algebra H under a certain hypothesis.

Proposition 5.4.3 *Let H be a finite dimensional semisimple and cosemisimple Hopf algebra over $\Bbbk$. If the Grothendieck ring $Gr(H)$ of H is commutative, then the Casimir number m_H and the dimension $\dim_{\Bbbk} H$ have the same prime factors.*

Proof. We turn to prove the determinant d_H and the dimension $\dim_{\Bbbk} H$ have the same prime factors. We first consider the case $\mathrm{char}(\Bbbk) = 0$. The set of isomorphism classes of simple objects of $\mathrm{Rep}(H)$ is denoted by $\{X_i\}_{i\in I}$. Since the Grothendieck ring $\mathrm{Gr}(H)$ is commutative, it follows from [47, Proposition 20] that all eigenvalues of the matrix $[c(1)]$ of left multiplication by $c(1) = \sum_{i\in I} X_i X_{i^*}$ with respect to the basis $\{X_i\}_{i\in I}$ of $\mathrm{Gr}(H)$ are positive integers, and moreover, all these eigenvalues divide $\dim_{\Bbbk} H$. In particular, $\dim_{\Bbbk} H$ is itself the largest eigenvalue of $[c(1)]$ (see [47, Proposition 8]). On the other hand, the determinant d_H is obtained by multiplying all these eigenvalues. Thus, d_H and $\dim_{\Bbbk} H$ have the same prime factors.

For the case $\mathrm{char}(\Bbbk) = p > 0$, we denote $\mathcal{O}$ the ring of Witt vectors of $\Bbbk$ and K the field of fractions of $\mathcal{O}$. For the semisimple and cosemisimple Hopf algebra H, using the lifting Theorem [27, Theorem 2.1] we may construct a Hopf algebra A over $\mathcal{O}$ which is free of rank $\dim_{\Bbbk} H$ as an $\mathcal{O}-$module such that A/pA is isomorphic to H as a Hopf algebra. The Hopf algebra $A_0 := A \otimes_{\mathcal{O}} K$ is a semisimple and cosemisimple Hopf algebra over the field K of characteristic 0 with the same Grothendieck ring as for H. It follows that the Grothendieck ring $\mathrm{Gr}(A_0)$ is commutative and the determinant d_{A_0} of $\mathrm{Rep}(A_0)$ is equal to the determinant d_H of $\mathrm{Rep}(H)$. By the same argument as for the case of $\mathrm{char}(\Bbbk) = 0$, we may see that the determinant d_{A_0} and $\dim_K A_0$ have the same prime factors. Note that $\dim_K A_0 = \dim_K(A \otimes_{\mathcal{O}} K)$ which is equal to $\dim_{\Bbbk} H$ since the Hopf algebra A over $\mathcal{O}$ is free of rank $\dim_{\Bbbk} H$ and $\mathcal{O}$ as a discrete valuation ring is a unique factorization domain. We conclude that d_H and $\dim_{\Bbbk} H$ have the same prime factors. □

Applying Proposition 5.4.3 to the Drinfeld double of a semisimple and cosemisimple Hopf algebra, we have the following result:

Theorem 5.4.4 *Let H be a finite dimensional semisimple and cosemisimple Hopf algebra over $\Bbbk$ and $D(H)$ the Drinfeld double of H. The Casimir number $m_{D(H)}$ and the dimension $\dim_{\Bbbk} H$ have the same prime factors.*

Proof. The representation category of the Drinfeld double $D(H)$ is a modular fusion category over $\Bbbk$, since $D(H)$ is a quasitriangular semisimple and cosemisimple Hopf algebra (see [49, Corollary 10.3.13]). It follows that the Grothendieck ring $\mathrm{Gr}(D(H))$

of $D(H)$ is a commutative ring. By Proposition 5.4.3, the Casimir number $m_{D(H)}$ and the dimension $\dim_{\Bbbk} D(H) = (\dim_{\Bbbk} H)^2$ have the same prime factors. This gives the desired result. $\square$

In the following, we describe a relationship between the Casimir number $m_{\mathcal{C}}$ of a fusion category $\mathcal{C}$ and the Casimir number $m_{\widetilde{\mathcal{C}}}$ of $\widetilde{\mathcal{C}}$, where $\widetilde{\mathcal{C}}$ is the pivotalization of $\mathcal{C}$ stated below.

Let $\mathcal{C}$ be a fusion category over $\Bbbk$. Recall from [29, Theorem 2.6] that there exists an isomorphism $\gamma : id \to * * **$ between the identity and the fourth duality tensor autoequivalences of $\mathcal{C}$. Denote by $\widetilde{\mathcal{C}} := \mathcal{C}^{\mathbb{Z}/2\mathbb{Z}}$ the corresponding equivariantization. More explicitly, simple objects of $\widetilde{\mathcal{C}}$ are pairs (X, α), where X is a simple object of $\mathcal{C}$, and $\alpha : X \to X^{**}$ satisfies $\alpha^{**}\alpha = \gamma_X$. The fusion category $\widetilde{\mathcal{C}}$ has a canonical pivotal structure which is called the *pivotalization* of $\mathcal{C}$ (see [28, Definition 7.21.9] for details). Moreover, the pivotal fusion category $\widetilde{\mathcal{C}}$ is also spherical (see [30, Corollary 7.6]).

To describe any simple object (X, α) of $\widetilde{\mathcal{C}}$, we first fix an isomorphism $\theta : X \to X^{**}$. Since $\mathrm{Hom}(X, X^{**})$ is one dimensional, we may write $\alpha = u\theta$ and $\gamma_X = v\theta^{**}\theta$ for some $u, v \in \Bbbk^{\times}$. Then $\alpha^{**}\alpha = \gamma_X$ implies that $u^2 = v$. Therefore, for each simple object X of $\mathcal{C}$, we only have two choices of α, and if one of them is α then another one is $-\alpha$. In view of this, we may write $(X, \alpha) = X^+$ and $(X, -\alpha) = X^-$. It follows that $\mathbf{1}^+ = \mathbf{1}$, $\mathbf{1}^- \otimes \mathbf{1}^- = \mathbf{1}$, $\dim(\mathbf{1}^-) = -1$, and $X^{\pm} \otimes \mathbf{1}^- = \mathbf{1}^- \otimes X^{\pm} = X^{\mp}$ (see [55, Section 5.1]). Note that the forgetful function $F : \widetilde{\mathcal{C}} \to \mathcal{C}, X^{\pm} \mapsto X$ preserves squared norms of simple objects [28, Remark 7.21.11]. It follows that $\dim(\widetilde{\mathcal{C}}) = 2\dim(\mathcal{C})$.

If $\mathrm{char}(\Bbbk) \neq 2$, the Grothendieck algebra $\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk$ has the following decomposition:

$$\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk = e(\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk) \oplus (1 - e)(\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk), \tag{5.8}$$

where $e = \frac{\mathbf{1} - \mathbf{1}^{-1}}{2}$ is a central idempotent element of $\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk$. It follows from [55, Section 5.1] that

$$\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} \Bbbk \cong (\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk)/e(\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk) \cong (1 - e)(\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk). \tag{5.9}$$

The Casimir number $m_{\mathcal{C}}$ (resp. $d_{\mathcal{C}}$ or $n_{\mathcal{C}}$) and $m_{\widetilde{\mathcal{C}}}$ (resp. $d_{\widetilde{\mathcal{C}}}$ or $n_{\widetilde{\mathcal{C}}}$) have the following relation:

Proposition 5.4.5 *Let $\mathcal{C}$ be a fusion category over $\Bbbk$ and $\widetilde{\mathcal{C}}$ the pivotalization of $\mathcal{C}$.*

(1) $m_{\mathcal{C}} \mid m_{\widetilde{\mathcal{C}}}$.

(2) $n_{\mathcal{C}} \mid n_{\widetilde{\mathcal{C}}}$.

(3) $d_{\mathcal{C}} \mid d_{\widetilde{\mathcal{C}}}$.

Proof.(1) Denote by $\{X_i\}_{i\in I}$ the set of isomorphism classes of simple objects of $\mathcal{C}$. Then $\{X_i^{\pm}\}_{i\in I}$ is the set of isomorphism classes of simple objects of $\widetilde{\mathcal{C}}$. For the Casimir number $m_{\widetilde{\mathcal{C}}}$, there exists some $a \in \mathrm{Gr}(\widetilde{\mathcal{C}})$ such that $\sum_{i\in I} X_i^{\pm} a (X_i^{\pm})^* = m_{\widetilde{\mathcal{C}}}$. Applying the ring morphism $f : \mathrm{Gr}(\widetilde{\mathcal{C}}) \to \mathrm{Gr}(\mathcal{C})$ induced by the forgetful function $F : \widetilde{\mathcal{C}} \to \mathcal{C}$ to this equation, we have $\sum_{i\in I} X_i 2f(a)(X_i)^* = m_{\widetilde{\mathcal{C}}}$. It follows that $m_{\widetilde{\mathcal{C}}} \in \mathbb{Z} \cap \mathrm{Im}c = (m_{\mathcal{C}})$. This gives a proof of Part (1).

(2) The proof is similar to Part (1).

(3) In the Grothendieck ring $\mathrm{Gr}(\widetilde{\mathcal{C}})$ we suppose for any $j \in I$ that

$$\sum_{i\in I} X_i^+ (X_i^+)^* X_j^+ = \sum_{i\in I} \mu_{ij} X_i^+ + \sum_{i\in I} \nu_{ij} X_i^-, \tag{5.10}$$

where $\mu_{ij}, \nu_{ij} \in \mathbb{Z}$. Then for any $j \in I$,

$$\sum_{i\in I} X_i^+ (X_i^+)^* X_j^- = \sum_{i\in I} X_i^+ (X_i^+)^* X_j^+ \mathbf{1}^- = \sum_{i\in I} \mu_{ij} X_i^- + \sum_{i\in I} \nu_{ij} X_i^+.$$

This means that, in the Grothendieck ring $\mathrm{Gr}(\widetilde{\mathcal{C}})$, the matrix of left multiplication by the Casimir element $\sum_{i\in I} X_i^{\pm}(X_i^{\pm})^* = 2\sum_{i\in I} X_i^+(X_i^+)^*$ with respect to the basis $\{X_i^{\pm}\}_{i\in I}$ of $\mathrm{Gr}(\widetilde{\mathcal{C}})$ is

$$2\begin{pmatrix} A & B \\ B & A \end{pmatrix},$$

where $A = (\mu_{ij})_{n\times n}$, $B = (\nu_{ij})_{n\times n}$ and n is the cardinality of I. Thus, the determinant of $\widetilde{\mathcal{C}}$ is

$$d_{\widetilde{\mathcal{C}}} = 2^{2n} \det(A+B)\det(A-B).$$

Applying the homomorphism $f : \mathrm{Gr}(\widetilde{\mathcal{C}}) \to \mathrm{Gr}(\mathcal{C})$ as above to the equation (5.10), we have that $\sum_{i\in I} X_i (X_i)^* X_j = \sum_{i\in I} (\mu_{ij} + \nu_{ij}) X_i$. This shows that, in the Grothendieck ring $\mathrm{Gr}(\mathcal{C})$, the matrix of left multiplication by the Casimir element $\sum_{i\in I} X_i X_i^*$ with respect to the basis $\{X_i\}_{i\in I}$ of $\mathrm{Gr}(\mathcal{C})$ is $A + B$. Thus, the determinant of $\mathcal{C}$ is $d_{\mathcal{C}} = \det(A+B)$, which is a factor of $d_{\widetilde{\mathcal{C}}}$. $\square$

As a consequence, we have the following result:

Proposition 5.4.6 *Let $\mathcal{C}$ be a fusion category over $\Bbbk$ with char$(\Bbbk) \neq 2$. If $\mathcal{C}$ is non-degenerate, then $m_{\mathcal{C}} \neq 0$ in $\Bbbk$.*

Proof. Since $\mathcal{C}$ is non-degenerate, i.e., the global dimension $\dim(\mathcal{C}) \neq 0$ in $\Bbbk$, it follows that $\dim(\widetilde{\mathcal{C}}) = 2\dim(\mathcal{C}) \neq 0$. Thus, the pivotal fusion category $\widetilde{\mathcal{C}}$ is non-degenerate. It follows from Proposition 5.2.5 that $m_{\widetilde{\mathcal{C}}} \neq 0$ in $\Bbbk$. As a result, $m_{\mathcal{C}} \neq 0$ since $m_{\mathcal{C}}$ is a factor of $m_{\widetilde{\mathcal{C}}}$. □

We expect that the converse of Proposition 5.4.6 is also true. One method of addressing this problem is to prove that $\det(A + B)$ and $\det(A - B)$ as stated in Proposition 5.4.5 have the same prime factors. However, the proof seems too hard to be finished. What we can do is the proof of the following statement:

Proposition 5.4.7 *Let $\mathcal{C}$ be a fusion category over $\Bbbk$ with char$(\Bbbk) \neq 2$. Then $\mathcal{C}$ is non-degenerate if and only if the subalgebra $e(Gr(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk)$ is semisimple, where $e = \frac{\mathbf{1}-\mathbf{1}^{-1}}{2}$ is a central idempotent element of $Gr(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk$.*

Proof. The global dimension $\dim(\mathcal{C}) \neq 0$ shows that $\dim(\widetilde{\mathcal{C}}) = 2\dim(\mathcal{C}) \neq 0$. Thus, the Grothendieck algebra $\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk$ of the pivotal fusion category $\widetilde{\mathcal{C}}$ is semisimple by [60, Theorem 6.5]. It follows that the quotient algebra (see (5.8))

$$(\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk)/(1-e)(\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk) \cong e(\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk)$$

is also semisimple. Conversely, consider the element $t = \sum_{i\in I} \dim(eX_i^{\pm})e(X_i^{\pm})^*$. For any $a \in e(\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk)$, it follows from (5.1) that

$$ta = \sum_{i\in I} \dim(eX_i^{\pm})e(X_i^{\pm})^* a = \sum_{i\in I} \dim(eaX_i^{\pm})e(X_i^{\pm})^* = \dim(a)t.$$

Similarly, it follows from (5.2) that $at = \dim(a)t$. Thus, t is an central element of $e(\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk)$ satisfying $t^2 = \dim(t)t = \dim(\widetilde{\mathcal{C}})t = 2\dim(\mathcal{C})t$. If $\dim(\mathcal{C}) = 0$, then the ideal of $e(\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk)$ generated by t is nilpotent, a contradiction to the semisimplicity of $e(\mathrm{Gr}(\widetilde{\mathcal{C}}) \otimes_{\mathbb{Z}} \Bbbk)$. □

§5.5 Casimir numbers vs. Frobenius-Schur exponents

In this section, we shall show that the Casimir number and the Frobenius-Schur exponent of a spherical fusion category over the field $\mathbb{C}$ of complex numbers have the same prime factors.

Let $\mathcal{C}$ be a fusion category over $\Bbbk$ and V a finite dimensional left $\mathrm{Gr}(\mathcal{C})\otimes_{\mathbb{Z}} K$-module over an algebraic closure field K. For any $\varphi \in \mathrm{End}_K(V)$, we define $\mathcal{I}(\varphi) \in \mathrm{End}_K(V)$ by

$$\mathcal{I}(\varphi)(v) = \sum_{i\in I} X_i \varphi(X_{i^*}v) \text{ for } v \in V.$$

Then $\mathcal{I}(\varphi)$ lies in $\mathrm{End}_{\mathrm{Gr}(\mathcal{C})\otimes_{\mathbb{Z}}K}(V)$ and does not depend on the choice of a pair of dual bases of $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ (see [32, Lemma 7.1.10]). If V is a simple $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$-module, then $\mathrm{End}_{\mathrm{Gr}(\mathcal{C})\otimes_{\mathbb{Z}}K}(V) \cong K$. In this case, there exists a unique element $c_V \in K$ such that

$$\mathcal{I}(\varphi) = c_V \mathrm{Tr}(\varphi) id_V \text{ for all } \varphi \in \mathrm{End}_K(V).$$

Such an element c_V only depends on the isomorphism class of V and is called the *Schur element* associated with V (see [32, Theorem 7.2.1]). Note that the semisimplicity criterion stated in [32, Theorem 7.2.6] works for Grothendieck algebras. Namely, the Grothendieck algebra $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ is semisimple if and only if any Schur element associated with a simple module over $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ is not zero in K.

Let V be a simple $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$-module with the Schur element c_V. The character of V is denoted by χ_V. Then $\sum_{i\in I} \chi_V(X_i)X_{i^*}$ is a central element of $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$. This element acts by a scalar f_V on V and by zero on any simple module not isomorphic to V. The scalar f_V is called the *formal codegree* of V (see [56, Lemma 2.3]).

Lemma 5.5.1 *Let V be a simple $Gr(\mathcal{C}) \otimes_{\mathbb{Z}} K$-module with the Schur element c_V and the formal codegree f_V. The action of $\sum_{i,j\in I} X_i X_j X_{i^*} X_{j^*}$ on V is a scalar multiple by $c_V f_V$.*

Proof. For a simple module V over $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$, there is a corresponding algebra morphism

$$\rho_V : \mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K \to \mathrm{End}_K(V),\ \rho_V(a)(v) = av \text{ for } a \in \mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K,\ v \in V.$$

Note that $\mathcal{I}(\varphi)(v) = c_V \mathrm{Tr}(\varphi)v$ holds for any $\varphi \in \mathrm{End}_K(V)$ and $v \in V$. Replacing φ and v in this equality by $\rho_V(X_j)$ and $X_{j^*}v$ respectively, we have $\mathcal{I}(\rho_V(X_j))(X_{j^*}v) = c_V \mathrm{Tr}(\rho_V(X_j))X_{j^*}v$. Summing over all $j \in I$ we have

$$\sum_{j\in I} \mathcal{I}(\rho_V(X_j))(X_{j^*}v) = c_V \sum_{j\in I} \mathrm{Tr}(\rho_V(X_j))X_{j^*}v.$$

Taking into account the definition of $\mathcal{I}$, we have

$$\sum_{i,j\in I} X_i \rho_V(X_j)(X_{i^*}X_{j^*}v) = c_V \sum_{j\in I} \chi_V(X_j)X_{j^*}v.$$

This gives rise to the desired result $\sum_{i,j\in I} X_i X_j X_{i^*} X_{j^*} v = c_V f_V v$ for any $v \in V$. □

Note that $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{C}$ is always semisimple and $\dim(\mathcal{C})$ is always not zero in the field $\mathbb{C}$ of complex numbers. Thus, [60, Theorem 6.5] is trivial if the field $\Bbbk$ is taken to be $\mathbb{C}$. In the following, we shall give a modification version of [60, Theorem 6.5] so that we can use it to present another statement of the Cauchy theorem for spherical fusion categories.

Let $\mathcal{C}$ be a spherical fusion category over $\mathbb{C}$ with isomorphism classes of simple objects $\{X_i\}_{i\in I}$. The Frobenius-Schur exponent of $\mathcal{C}$ has been defined in [51, Definition 5.1] in terms of the higher Frobenius-Schur indicators of objects of $\mathcal{C}$. This exponent, denoted by N, can be regarded as the order of the twist θ of the Drinfeld center $Z(\mathcal{C})$ associated with a pivotal structure of $\mathcal{C}$ (see [51, Theorem 5.5]). Let $\xi_N \in \mathbb{C}$ be a primitive N-th root of unity. Then $\mathbb{Z}[\xi_N]$ is a Dedekind domain and every nonzero proper ideal factors into a product of prime ideal factors. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\xi_N]$. Then $\mathfrak{p}$ is maximal since $\mathbb{Z}[\xi_N]$ is Dedekind. Thus, the quotient ring $\mathbb{Z}[\xi_N]/\mathfrak{p}$ is a field. In this case, $\dim(X) \in \mathbb{Z}[\xi_N]$ (see [51]) can be considered as an element in $\mathbb{Z}[\xi_N]/\mathfrak{p}$ in a natural way.

Theorem 5.5.2 *Let $\mathcal{C}$ be a spherical fusion category over $\mathbb{C}$ with the Frobenius-Schur exponent N. For any prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\xi_N]$, the Casimir number $m_{\mathcal{C}} \neq 0$ in $\mathbb{Z}[\xi_N]/\mathfrak{p}$ if and only if the global dimension $\dim(\mathcal{C}) \neq 0$ in $\mathbb{Z}[\xi_N]/\mathfrak{p}$. Thus, the set of prime ideals dividing the principal ideal generated by $\dim(\mathcal{C})$ is identical to that of $m_{\mathcal{C}}$ in $\mathbb{Z}[\xi_N]$.*

Proof. Note that the Casimir number $m_{\mathcal{C}} = \sum_{i\in I} X_i a X_{i^*}$ for some $a \in \mathrm{Gr}(\mathcal{C})$. Applying dim to this equality, we have $m_{\mathcal{C}} = \dim(\mathcal{C})\dim(a)$. Thus, if $m_{\mathcal{C}} \neq 0$ in $\mathbb{Z}[\xi_N]/\mathfrak{p}$, then

$\dim(\mathcal{C}) \neq 0$ in $\mathbb{Z}[\xi_N]/\mathfrak{p}$. Conversely, if $\dim(\mathcal{C}) \neq 0$ in $\mathbb{Z}[\xi_N]/\mathfrak{p}$, so is $\dim(\mathcal{C}) \neq 0$ in K, where K is an algebraic closure of the field $\mathbb{Z}[\xi_N]/\mathfrak{p}$. Let $Z(\mathcal{C})$ be the Drinfeld center of $\mathcal{C}$. Since $\dim(\mathcal{C}) \neq 0$ in K, it follows from [50, Section 5] that $Z(\mathcal{C})$ is a modular category and $\dim(Z(\mathcal{C})) = \dim(\mathcal{C})^2 \neq 0$ in K. If we denote $\mathrm{Irr}(Z(\mathcal{C}))$ the set of isomorphism classes of simple objects of $Z(\mathcal{C})$ and n the cardinality of $\mathrm{Irr}(Z(\mathcal{C}))$, then by Example 5.2.7 the determinant of $Z(\mathcal{C})$ is

$$d_{Z(\mathcal{C})} = \frac{\dim(Z(\mathcal{C}))^n}{\prod_{Y\in\mathrm{Irr}(Z(\mathcal{C}))} \dim(Y)^2} \neq 0.$$

Note that $d_{Z(\mathcal{C})}$ is the determinant of the matrix of left multiplication by the Casimir element $\sum_{Y\in\mathrm{Irr}(Z(\mathcal{C}))} YY^*$. It follows that $\sum_{Y\in\mathrm{Irr}(Z(\mathcal{C}))} YY^*$ is an invertible element in $\mathrm{Gr}(Z(\mathcal{C}))\otimes_{\mathbb{Z}} K$. Note that the forgetful tensor functor $F : Z(\mathcal{C}) \to \mathcal{C}$ induces an algebra morphism $f : \mathrm{Gr}(Z(\mathcal{C})) \otimes_{\mathbb{Z}} K \to \mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ whose image is contained in the center of $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$. In particular, from the proof of [56, Lemma 3.1] we may see that

$$f(\sum_{Y\in\mathrm{Irr}(Z(\mathcal{C}))} YY^*) = \sum_{i,j\in I} X_i X_j X_{i^*} X_{j^*}.$$

Thus, $\sum_{i,j\in I} X_i X_j X_{i^*} X_{j^*}$ is a central invertible element in $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$. This together with Lemma 5.5.1 shows that $c_V \neq 0$ for any simple $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$-module V. We conclude that $\mathrm{Gr}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ is semisimple by [32, Theorem 7.2.6], and hence $m_{\mathcal{C}} \neq 0$ in K by Proposition 5.2.2. This gives the desired result that $m_{\mathcal{C}} \neq 0$ in $\mathbb{Z}[\xi_N]/\mathfrak{p}$. □

We are now ready to state the relationship between the Casimir number $m_{\mathcal{C}}$ and the Frobenius-Schur exponent N of $\mathcal{C}$.

Theorem 5.5.3 *Let $\mathcal{C}$ be a spherical fusion category over $\mathbb{C}$. The Casimir number $m_{\mathcal{C}}$ and the Frobenius-Schur exponent N of $\mathcal{C}$ have the same prime factors.*

Proof. For the Casimir number $m_{\mathcal{C}}$, there is some $a \in \mathrm{Gr}(\mathcal{C})$ such that $\sum_{i\in I} X_i a X_{i^*} = m_{\mathcal{C}}$. Applying dim to this equality, we have $\dim(\mathcal{C})\dim(a) = m_{\mathcal{C}}$ in $\mathbb{Z}[\xi_N]$. Note that (N) and $(\dim(\mathcal{C}))$ are two principal ideals of $\mathbb{Z}[\xi_N]$ having the same prime ideal factors (see [10, Theorem 3.9]). If $p \mid N$ for a prime number p, then there exists a prime ideal factor $\mathfrak{p}$ of (N) such that $\mathfrak{p} \cap \mathbb{Z} = (p)$. In this case, $\mathfrak{p}$ is also a prime ideal factor of $(\dim(\mathcal{C}))$. Moreover, $(\dim(\mathcal{C})) \cap \mathbb{Z} \subseteq \mathfrak{p} \cap \mathbb{Z} = (p)$. It follows from

$m_{\mathcal{C}} = \dim(\mathcal{C})\dim(a)$ that $m_{\mathcal{C}} \in (\dim(\mathcal{C})) \cap \mathbb{Z} \subseteq (p)$, and hence $p \mid m_{\mathcal{C}}$. Conversely, if $p \nmid N$ for a prime p, we need to show that $p \nmid m_{\mathcal{C}}$. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\xi_N]$ such that $\mathfrak{p} \cap \mathbb{Z} = (p)$. Then $(N) \nsubseteq \mathfrak{p}$ since $p \nmid N$. This implies that $(\dim(\mathcal{C})) \nsubseteq \mathfrak{p}$. Especially, $0 \neq \dim(\mathcal{C}) \in \mathbb{Z}[\xi_N]/\mathfrak{p}$. It follows from Theorem 5.5.2 that $m_{\mathcal{C}} \neq 0$ in $\mathbb{Z}[\xi_N]/\mathfrak{p}$. In other words, $m_{\mathcal{C}} \notin \mathfrak{p} \cap \mathbb{Z} = (p)$ and hence $p \nmid m_{\mathcal{C}}$. □

Remark 5.5.4 *Let* (N) *and* $(\dim(\mathcal{C}))$ *be principal ideals of* $\mathbb{Z}[\xi_N]$ *generated by* N *and* $\dim(\mathcal{C})$*, respectively. The statement of [10, Theorem 3.9] that* (N) *and* $(\dim(\mathcal{C}))$ *have the same prime ideal factors is called the Cauchy theorem for a spherical fusion category. Indeed, applying this to the case* $\mathcal{C} = Rep(G)$ *for a finite group* G*, we obtain the classical Cauchy theorem for finite groups:* $\dim(\mathcal{C}) = |G|$ *and* $N = exp(G)$ *have the same prime factors. Now, Theorem 5.5.3 shows that all of the numbers* $m_{\mathcal{C}}$*,* $n_{\mathcal{C}}$*,* $d_{\mathcal{C}}$ *and the Frobenius-Schur exponent* N *of* $\mathcal{C}$ *have the same prime factors. This may be thought of as another statement of the Cauchy theorem for spherical fusion categories.*

REFERENCES

[1] L. Abrams, Two-dimensional topological quantum field theories and Frobenius algebras, J. Knot Theory Ramifications **5** (5) (1996): 569-587.

[2] N. Andruskiewitsch, I. Angiono, A. G. Iglesias, et al, From Hopf algebras to tensor categories, Conformal field theories and tensor categories, Springer Berlin Heidelberg, (2014): 1-31.

[3] I. Assem, D. Simson, A. Skowronski, Elements of the representation theory of associative algebras: Techniques of representation theory, Cambridge University Press, 2006.

[4] M. Auslander, I. Reiten, S. O. Smalϕ, Representation theory of Artin algebras, Cambridge Studies in Advanced Mathematics, Vol.**36**, Cambridge, 1994.

[5] B. Bakalov, A. A. Kirillov, Lectures on tensor categories and modular functors, University Series Lectures, Vol. **21** AMS Providence, 2001.

[6] K. Beidar, Y. Fong, A. Stolin, On Frobenius algebras and the quantum Yang-Baxter equation, Trans. Amer. Math. Soc. **349** (9) (1997): 3823-3836.

[7] D. J. Benson, J. F. Carlson, Nilpotent elements in the Green ring, J. Algebra **104** (1986): 329-350.

[8] D. J. Benson, R. A. Parker, The Green ring of a finite group, J. Algebra **87** (1984): 290-331.

[9] M. Bhargava, M. E. Zieve, Factoring Dickson polynomials over finite fields, Finite Fields Appl. **5** (2) (1999): 103-111.

[10] P. Bruillard, S. H. Ng, E. Rowell, Z. Wang, Rank-finiteness for modular categories, J. Amer. Math. Soc. **29** (3) (2016): 857-881.

[11] S. Caenepeel, Bogdan Ion, G. Militaru, The structure of Frobenius algebras and separable algebras, K-theory **19** (4) (2000): 365-402.

[12] J. F. Carlson, The dimensions of periodic modules over modular group algebras, Ill. J. Math. **23** (2) (1979): 295-306.

[13] H. Chen, The Green ring of Drinfeld double $D(H_4)$, Algebras and Representation Theory **17** (5) (2014): 1457-1483.

[14] H. Chen, F. V. Oystaeyen and Y. Zhang, The Green rings of Taft algebras, Proc. Amer. Math. Soc. **142** (2014): 765-775.

[15] W. S. Chou, The factorization of Dickson polynomials over finite fields, Finite Fields Appl. **3** (1997): 84-96.

[16] C. Cibils, A quiver quantum group, Commun. Math. Phys. **157** (1993): 459-477.

[17] M. Cohen, S. Westreich, Structure constants related to symmetric Hopf algebras, J. Algebra **324** (2010): 3219-3240.

[18] C. W. Curtis, I. Reiner, Methods of representation theory, vol. **1**, Wiley-Interscience, New York, 1981.

[19] E. Darpö, M. Herschend, On the representation ring of the polynomial algebra over perfect field, Math. Z **265** (2011): 605-615.

[20] Y. Doi, Bi-Frobenius algebras and group-like algebras, Lecture notes in pure and applied Mathematics (2004): 143-156.

[21] Y. Doi, Group-like algebras and their representations, Commun. Algebra **38** (7) (2010): 2635-2655.

[22] Y. Doi, Substructures of bi-Frobenius algebras, J. Algebra **256** (2002): 568-582.

[23] Y. Doi, M. Takeuchi, BiFrobenius algebras, Contemp. Math. **267** (2000): 67-98.

[24] M. Domokos and T. H. Lenagan, Representation rings of quantum groups, J. Algebra **282** (2004): 103-128.

[25] V. Drinfeld, S. Gelaki, D. Nikshych, V. Ostrik, On braided fusion categories I, Selecta Mathematica (N. S.) **16** (2010): 1-119.

[26] K. Erdmann, E. L. Green, N. Snashall, R. Taillefer, Representation theory of the Drinfeld doubles of a family of Hopf algebras, J. Pure Appl. Algebra **204** (2) (2006): 413-454.

[27] P. Etingof, S. Gelaki, On finite-dimensional semisimple and cosemisimple Hopf algebras in positive characteristic, Int. Math. Res. Not. IMRN **16** (1998): 851-864.

[28] P. Etingof, S. Gelaki, D. Nikshych, V. Ostrik, Tensor categories, Mathematical Surveys and Monographs, **205**, AMS, Providence, 2015.

[29] P. Etingof, D. Nikshych, V. Ostrik, On fusion categories, Ann. of Math. **162** (2005): 581-642.

[30] P. Etingof, D. Nikshych, V. Ostrik, An analogue of Radford's S^4 formula for finite tensor categories, Int. Math. Res. Not. IMRN **54** (2004): 2915-2933.

[31] P. Etingof, V. Ostrik, Finite tensor categories, Mosc. Math. J. **4** (3) (2004): 627-654.

[32] M. Geck, G. Pfeiffer, Characters of finite Coxeter groups and Iwahori-Hecke algebras, New York: Oxford University Press, 2000.

[33] J. A. Green, A transfer theorem for mudular representations, J. Algebra **1** (1964): 73-84.

[34] J. A. Green, The modular representation algebra of a finite group, Ill. J. Math. **6** (4) (1962): 607-619.

[35] E. L. Green, E. N. Marcos, Ø. Solberg, Representations and almost split sequences for Hopf algebras, Representation theory of algebras (Cocoyoc, 1994) (1996): 237-245.

[36] M. Haim, Group-like algebras and Hadamard matrices, J. Algebra **308** (2007): 215-235.

[37] D. Happel, Triangulated categories in the representation of finite dimensional algebras, Cambridge University Press, 1988.

[38] D. G. Higman, On orders in separable algebras, Canad. J. Math. **7** (1955): 509-515.

[39] H. Huang, F. V. Oystaeyen, Y. Yang, Y. Zhang, The Green rings of pointed tensor categories of finite type, J. Pure Appl. Algebra **218** (2014): 333-342.

[40] L. Kadison, A. A. Stolin, Separability and Hopf algebras, Contemp. Math. **259** (1999): 279-298.

[41] R. G. Larson, D. E. Radford, Semisimple cosemisimple Hopf algebras, Amer. J. Math. **109** (1987): 187-195.

[42] R. G. Larson, M. Sweedler, An associative orthogonal bilinear form for Hopf algebras, Amer. J. Math. **91** (1969): 75-93.

[43] Y. Li, N. Hu, The Green rings of the 2-rank Taft algebra and its two relatives twisted, J. Algebra **410** (2014): 1-35.

[44] L. Li, Y. Zhang, The Green rings of the generalized Taft Hopf algebras, Contemp. Math. **585** (2013): 275-288.

[45] S. Liu, Auslander-Reiten theory in a Krull-Schmidt category, The S*ão* Paulo Journal of Mathematical Sciences **4** (3) (2010): 425-472.

[46] M. Lorenz, Representations of finite-dimensional Hopf algebras, J. Algebra **188** (1997): 476-505.

[47] M. Lorenz, Some applications of Frobenius algebras to Hopf algebras, Contemp. Math. **537** (2011): 269-289.

[48] B. R. McDonald, Finite rings with identity, Vol. **28**, Marcel Dekker Incorporated, 1974.

[49] S. Montgomery, Hopf Algebras and their actions on rings, CBMS Series in Math., Vol. **82**, AMS, Providence, 1993.

[50] M. M*ü*ger, From subfactors to categories and topology. II. The quantum double of tensor categories and subfactors, J. Pure Appl. Algebra **180** (1-2) (2003): 159-219.

[51] S. H. Ng, P. Schauenburg, Frobenius-Schur indicators and exponents of spherical categories, Adv. Math. **211** (1) (2007): 34-71.

[52] W.D. Nichols, M. B. Richmond, The Grothendieck algebra of a Hopf algebra I, Commun. Algebra **26** (4) (1998): 1081-1095.

[53] D. Nikshych, K_0-rings and twisting of finite dimensional semisimple Hopf algebras, Commun. Algebra **26** (1) (1998): 321-342.

[54] V. Ostrik, On symmetric fusion categories in positive characteristic, arXiv: 1503.01492.

[55] V. Ostrik, Pivotal fusion categories of rank 3, Mosc. Math. J. **15** (2) (2015): 373-396.

[56] V. Ostrik, On formal codegrees of fusion categories, Math. Res. Lett. **16** (5) (2009): 895-901.

[57] D. E. Radford, On the coradical of a finite-dimensional Hopf algebra, Proc. Amer. Math. Soc. **53** (1) (1975): 9-15.

[58] C. M. Ringel, Tame Algebras and Integral Quadratic Forms, Lecture Notes in Mathematics, Vol. **1099**, Springer Berlin Heidelberg, 1984.

[59] W. F. Santos, M. Haim, Radford's formula for biFrobenius algebras and applications, Commun. Algebra **36** (4) (2008): 1301-1310.

[60] K. Shimizu, The monoidal center and the character algebra, J. Pure Appl. Algebra **221** (9) (2017): 2338-2371.

[61] J. Siehler, Near-group categories, Alg. Geom. Topol. **3** (2) (2003): 719-775.

[62] A. Skowroński, K. Yamagata, Frobenius algebras, European Mathematical Society, 2011.

[63] Y. Sommerhäuser, On Kaplansky's fifth conjecture, J. Algebra **204** (1998): 202-224.

[64] M. E. Sweedler, Hopf Algebras, Benjamin, New York, 1969.

[65] M. Wakui, Various structures associated to the representation categories of eight-dimensional nonsemisimple Hopf algebras, Algebras and Representation Theory **7** (2004): 491-515.

[66] Y. Wang, X. Chen, Construct non-graded bi-Frobenius algebras via quivers, Science in China Series A: Mathematics **50** (3) (2007): 450-456.

[67] Z. Wang, L. Li, On realization of fusion rings from generalized Cartan matrices. Acta Mathematica Sinica, English Series **33** (3) (2017): 362-376.

[68] Z. Wang, L. Li, Y. Zhang, Green rings of pointed rank one Hopf algebras of nilpotent type, Algebras and Representation Theory **17** (6) (2014): 1901-1924.

[69] Z. Wang, L. Li, Y. Zhang, Green rings of pointed rank one Hopf algebras of non-nilpotent type, J. Algebra **449** (2016): 108-137.

[70] Y. Wang, P. Zhang, Construct bi-Frobenius algebras via quivers, Tsukuba J. Math. **28** (1) (2004): 215-227.

[71] S. J. Witherspoon, The representation ring of the quantum double of a finite group, J. Algebra **179** (1996): 305-329.

[72] S. J. Witherspoon, The representation ring and the centre of a Hopf algebra, Canad. J. Math. **51** (4) (1999): 881-896.

[73] S. Yang, Finite dimensional representations of u-Hopf algebras, Commun. Algebra **29** (12) (2001): 5359-5370.

[74] J. Zemanek, Nilpotent elements in representation rings, J. Algebra **19** (1971): 453-469.

[75] Y. Zhu, Hopf algebras of prime dimension, Int. Math. Res. Not. IMRN **1** (1994): 53-59.

E-mail address: mailzhihua@126.com

Papers published during my postdoctor program

1. Zhihua Wang, Libin Li, Yinhuo Zhang, A criterion for the Jacobson semisimplicity of the Green ring of a finite tensor category, Glasg. Math. J., 2018, 60(1): 253-272.

2. Zhihua Wang, The corepresentation ring of a pointed Hopf algebra of rank one, Journal of Algebra and Its Applications, 2018, 17(12): P21, 1850236.

3. Zhihua Wang, Li Libin, Representations of the quantum matrix algebra Mq(2) arising from Ore extensions, Southeast Asian Bulletin of Mathematics, 2018, 42(2): 293-306.

4. Zhihua Wang, Li Libin, Double Frobenius algebras, Frontiers of Mathematics in China, 2018, 13(2): 399-415.

5. 王志华, 李立斌, 张印火, 基于Benson-Carlson商环的双Frobenius代数的构造，中国科学: 数学, 2018, 48: 471-482.

6. 王志华,李立斌, Verlinde模性范畴上的Casimir数及其应用,数学学报, 2018, 61(1): 59-66.

7. Zhihua Wang, Calabi-Yau objects in the stable category of a finite dimensional pointed Hopf algebra of rank one, 数学进展, 2017, 46(6): 888-896.

8. Zhihua Wang, Libin Li, On realization of fusion rings from generalized Cartan matrices, Acta Math Sinica, 2017, 33(3): 362-376.

致 谢

光阴似箭, 博士后阶段即将结束, 在南大进站期间收获颇多.

首先感谢我的合作导师刘公祥教授, 感谢他在科研上对我的指导和帮助, 在讨论班、项目申报、论文指导等方面刘教授都给予我极大的帮助与鼓励. 刘老师渊博的知识, 严谨的治学态度, 深邃的洞察力和诲人不倦的精神都深深地影响了我, 并激励我在今后的科研工作中不忘初心、继续前行.

感谢丁南庆教授、秦厚荣教授、朱晓胜教授、黄兆泳教授以及杨东教授, 感谢他们给予我的指导和帮助.

感谢南京大学数学系以及数学系全体工作人员, 感谢他们创造了如此优越的学习环境和氛围.

最后, 感谢我的父母和妻儿, 是你们的理解、关心与支持, 才能让我在科研的道路上心无旁骛走到今天. 我觉得亏欠你们太多, 你们的健康与快乐是我最大的心愿.

王 志 华

2019 年 10 月