

## A CRITERION FOR THE JACOBSON SEMISIMPLICITY OF THE GREEN RING OF A FINITE TENSOR CATEGORY

ZHIHUA WANG

*Department of Mathematics, Nanjing University,  
Nanjing 210093, China*

*Department of Mathematics, Taizhou University,  
Taizhou 225300, China*

*e-mail: mailzhuhua@126.com*

LIBIN LI

*School of Mathematical Science, Yangzhou University,  
Yangzhou 225002, China*

*e-mail: lbli@yzu.edu.cn*

and YINHUO ZHANG

*Department of Mathematics and Statistics,  
University of Hasselt, Universitaire Campus, 3590 Diepenbeek, Belgium  
e-mail: yinhuo.zhang@uhasselt.be*

(Received 12 March 2017; revised 1 July 2017; accepted 7 August 2017;  
first published online 25 September 2017)

**Abstract.** This paper deals with the Green ring  $\mathcal{G}(\mathcal{C})$  of a finite tensor category  $\mathcal{C}$  with finitely many isomorphism classes of indecomposable objects over an algebraically closed field. The first part of this paper deals with the question of when the Green ring  $\mathcal{G}(\mathcal{C})$ , or the Green algebra  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$  over a field  $K$ , is Jacobson semisimple (namely, has zero Jacobson radical). It turns out that  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$  is Jacobson semisimple if and only if the Casimir number of  $\mathcal{C}$  is not zero in  $K$ . For the Green ring  $\mathcal{G}(\mathcal{C})$  itself,  $\mathcal{G}(\mathcal{C})$  is Jacobson semisimple if and only if the Casimir number of  $\mathcal{C}$  is not zero. The second part of this paper focuses on the case where  $\mathcal{C} = \text{Rep}(\mathbb{k}G)$  for a cyclic group  $G$  of order  $p$  over a field  $\mathbb{k}$  of characteristic  $p$ . In this case, the Casimir number of  $\mathcal{C}$  is computable and is shown to be  $2p^2$ . This leads to a complete description of the Jacobson radical of the Green algebra  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$  over any field  $K$ .

2010 *Mathematics Subject Classification.* 16G70, 16T05, 18D10.

**1. Introduction.** The Green ring of a finite group, or more generally, the Green ring of a tensor category, 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. [3, 7, 9, 14, 16, 25]). After J.A. Green [13] 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 centred 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 [4, 13, 26]). 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 [23, Theorem 5.4] and [24, 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  $\mathcal{C}$  be a finite tensor category with only finitely many non-isomorphic indecomposable objects over an algebraically closed field. The Green ring  $\mathcal{G}(\mathcal{C})$  of  $\mathcal{C}$  is a Frobenius algebra over the ring  $\mathbb{Z}$  of integers with the bilinear form given by dimensions of morphism spaces, see Theorem 3.5. 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  $\mathcal{G}(\mathcal{C})$  related to the almost split sequence ending with  $X$  (if  $X$  is not projective). The Casimir operator of  $\mathcal{G}(\mathcal{C})$  is the map  $c$  from  $\mathcal{G}(\mathcal{C})$  to its centre given by

$$c(x) = \sum_{[X] \in \text{ind}(\mathcal{C})} [X]x\delta_{[X]}^*,$$

where  $\text{ind}(\mathcal{C})$  is the set of all isomorphism classes of indecomposable objects in  $\mathcal{C}$ . 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  $\mathcal{C}$ .

In this paper, the Casimir number of  $\mathcal{C}$  is used to determine whether or not the Green ring  $\mathcal{G}(\mathcal{C})$ , or the Green algebra  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$  over a field  $K$ , is Jacobson semisimple (namely, has zero Jacobson radical). It turns out that  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$  is Jacobson semisimple if and only if the Casimir number of  $\mathcal{C}$  is not zero in  $K$ , see Theorem 3.7. In the special case when the Green ring  $\mathcal{G}(\mathcal{C})$  is a group ring  $\mathbb{Z}G$ , the Casimir number of  $\mathcal{C}$  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 3.7 can be regarded as a version of Maschke's theorem for the Green ring case.

For the Green ring  $\mathcal{G}(\mathcal{C})$  itself,  $\mathcal{G}(\mathcal{C})$  is Jacobson semisimple if and only if the Casimir number of  $\mathcal{C}$  is not zero, see Theorem 3.11. If the Green ring  $\mathcal{G}(\mathcal{C})$  is commutative, then the Jacobson radical of  $\mathcal{G}(\mathcal{C})$  is the set of all nilpotent elements of  $\mathcal{G}(\mathcal{C})$ . As a consequence, Theorem 3.11 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 a finite tensor category  $\mathcal{C}$ . We only focus on the case  $\mathcal{C} = \text{Rep}(\mathbb{k}G)$ , where  $G$  is a cyclic group of order  $p$  and  $\mathbb{k}$  is an algebraically closed field of characteristic  $p$ . By a straightforward computation, we find that the Casimir number of  $\mathcal{C}$  is  $2p^2$ . This shows that the Green ring  $\mathcal{G}(\mathcal{C})$  is Jacobson semisimple, which is a result of J.A. Green [13]. Moreover,  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$  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  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$  explicitly.

The paper is organized as follows. In Section 2, we give the definitions of a Frobenius algebra and the Green ring of a finite tensor category. In Section 3, we show that the Green ring  $\mathcal{G}(\mathcal{C})$  is a Frobenius algebra over  $\mathbb{Z}$  if the underlying finite tensor category  $\mathcal{C}$  has finitely many indecomposable objects up to isomorphism. In this case, we describe the Casimir number of  $\mathcal{C}$  and use it to determine when  $\mathcal{G}(\mathcal{C})$ , or

$\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ , is Jacobson semisimple. In Section 4, by applying the results obtained in Section 3 to the Green ring of a finite group  $G$ , we describe the Jacobson radical of the Green algebra of  $G$  completely.

**2. Preliminaries.** Throughout,  $\mathcal{C}$  is a finite tensor category over an algebraically closed field  $\mathbb{k}$ . The tensor product  $\otimes$  stands for  $\otimes_{\mathbb{k}}$ . 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.

**2.1. Frobenius algebras.** The notion of a Frobenius algebra here is defined directly over  $\mathbb{Z}$ , although it can be defined more generally over a commutative ring (see e.g. [20]). Throughout this section,  $R$  is a free  $\mathbb{Z}$ -algebra of finite rank and the dual of  $R$  is  $R^* := \text{Hom}_{\mathbb{Z}}(R, \mathbb{Z})$ . A bilinear form  $(-, -) : R \times R \rightarrow \mathbb{Z}$  is called *associative* if  $(ab, c) = (a, bc)$  for all  $a, b, c \in R$ . It is *symmetric* if  $(a, b) = (b, a)$ ; it is *right* (resp. *left*) *nonsingular* if  $R \rightarrow R^*$  given by  $a \mapsto (-, a)$  (resp.  $a \mapsto (a, -)$ ) is a  $\mathbb{Z}$ -module isomorphism. The form is *nonsingular* if it is both left and right nonsingular. The  $\mathbb{Z}$ -algebra  $R$  is called *Frobenius* if it is equipped with an associative and nonsingular bilinear form and, moreover, *symmetric* if the form is symmetric.

If  $R$  has two  $\mathbb{Z}$ -bases  $\{x_i \mid 1 \leq i \leq n\}$  and  $\{y_i \mid 1 \leq i \leq n\}$  satisfying  $(x_i, y_j) = \delta_{ij}$ , where  $\delta_{ij}$  is the Kronecker symbol, then these two bases are called *dual bases* of  $R$  with respect to  $(-, -)$ . Accordingly, any  $a \in R$  can be written as

$$a = \sum_{i=1}^n (a, y_i)x_i \text{ or } a = \sum_{i=1}^n (x_i, a)y_i. \tag{1}$$

The *Casimir operator* of  $R$  (see e.g. [20, Section 3.1]) is the map  $c$  from  $R$  to its centre  $Z(R)$  defined by

$$c(a) = \sum_{i=1}^n y_i a x_i \text{ for } a \in R.$$

The map  $c$  is independent of the choice of dual bases  $\{x_i \mid 1 \leq i \leq n\}$  and  $\{y_i \mid 1 \leq i \leq n\}$ , because the dual bases depend only on the bilinear form  $(-, -)$ , see [20, Section 1.2.2]. The element  $c(1)$  is called the *Casimir element* of  $R$  and it depends on  $(-, -)$  only up to a central unit, see [20, Section 1.2.5]. The image  $\text{Im } c$  of  $c$  is an ideal of  $Z(R)$ , called the *Casimir ideal* of  $R$ . It does not depend on the choice of the bilinear form, see [20, Section 3.2]. The intersection of  $\text{Im } c$  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  $R$ . Obviously, the Casimir number of  $R$  does not depend on the choice of the bilinear form on  $R$ .

Any  $\mathbb{Z}$ -algebra morphism  $\varepsilon : R \rightarrow \mathbb{Z}$  is called an *augmentation* of  $R$ . Suppose that the Frobenius  $\mathbb{Z}$ -algebra  $R$  has an augmentation  $\varepsilon$ . Then any element  $t$  of  $R$  satisfying  $at = \varepsilon(a)t$  for all  $a \in R$  is called a *left integral* of  $R$ . Similarly, if  $ta = \varepsilon(a)t$  for all  $a \in R$ , then  $t$  is called a *right integral* of  $R$ . All left integrals of  $R$  with respect to  $\varepsilon$  form a  $\mathbb{Z}$ -module of rank one generated by  $\sum_{i=1}^n \varepsilon(x_i)y_i$ . Similarly, all right integrals of  $R$  with respect to  $\varepsilon$  form a  $\mathbb{Z}$ -module of rank one generated by  $\sum_{i=1}^n \varepsilon(y_i)x_i$ , see

[20, Section 4.1]. If the set of left integrals of  $R$  coincides with the set of right ones, then  $R$  is called *unimodular*.

**2.2. Almost split sequences.** Let  $\mathbb{k}$  be an algebraically closed field. A *locally finite* ( $\mathbb{k}$ -linear) *abelian category* over  $\mathbb{k}$  is an additive category whose morphism spaces are finite dimensional, every object has finite length, and every morphism has a kernel and a cokernel. A locally finite abelian category is said to be *finite* if it has only finitely many simple objects  $X_i$  for  $i \in I$ , up to isomorphism, where  $I$  is a finite set, and each simple object  $X_i$  has a projective cover  $P_i$  for any  $i \in I$ . A *finite tensor category* is a finite abelian rigid monoidal category over  $\mathbb{k}$  in which the neutral object  $\mathbf{1}$  is simple (see e.g. [11] for the full definition).

Let  $\mathcal{C}$  be a finite tensor category over  $\mathbb{k}$ . Recall from [22, Section 2.2] that a morphism  $f : X \rightarrow Y$  in  $\mathcal{C}$  is called a *source morphism* if  $f$  is not a section such that every non-section morphism  $X \rightarrow M$  factors through  $f$  and every factorization  $f = h \circ f$  implies that  $h$  is an automorphism of  $Y$ . Dually, A morphism  $g : Y \rightarrow Z$  in  $\mathcal{C}$  is called a *sink morphism* if  $g$  is not a retraction such that every non-retraction morphism  $M \rightarrow Z$  factors through  $g$  and every factorization  $g = g \circ h$  implies that  $h$  is an automorphism of  $Y$ . A source (resp. sink) morphism, if it exists, is unique up to isomorphism. The notion has been introduced originally by Auslander and Reiten under the name minimal left (resp. right) almost split morphism (see e.g. [1]). A short exact sequence  $0 \rightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \rightarrow 0$  in  $\mathcal{C}$  is called an *almost split sequence* if  $f$  is a source morphism and  $g$  is a sink morphism.

It is known that any finite tensor category  $\mathcal{C}$  is equivalent to the representation category of some finite dimensional weak quasi-Hopf algebra over  $\mathbb{k}$ , see [12, Proposition 2.7]. The existence of such an equivalence provides that every indecomposable non-projective object in  $\mathcal{C}$  is always the ending term of an almost split sequence in  $\mathcal{C}$ . More precisely, if  $F$  defines an equivalence between  $\mathcal{C}$  and  $\text{Rep}(H)$  for some finite dimensional weak quasi-Hopf algebra  $H$  over  $\mathbb{k}$ , then for any indecomposable non-projective object  $Z$  in  $\mathcal{C}$ ,  $F(Z)$  is also an indecomposable non-projective representation in  $\text{Rep}(H)$ . Since  $\text{Rep}(H)$  has an almost split sequence  $0 \rightarrow L \rightarrow M \rightarrow F(Z) \rightarrow 0$  ending with  $F(Z)$  and the functor  $F$  is an equivalence of abelian categories, the above sequence is an image of a short exact sequence  $0 \rightarrow X \rightarrow Y \rightarrow Z \rightarrow 0$ , which can be easily verified to be an almost split sequence in  $\mathcal{C}$ . Such an almost split sequence in  $\mathcal{C}$  is unique up to isomorphism. Indeed, an almost split sequence (if it exists) in any additive category is always unique up to isomorphism for a fixed starting term as well as for a fixed ending term (see Theorem 1.4 and Proposition 1.5 in [19]).

**2.3. Green rings.** Let  $F(\mathcal{C})$  be the free abelian group generated by isomorphism classes of objects in the finite tensor category  $\mathcal{C}$ . The abelian group  $F(\mathcal{C})$  admits a ring structure with the multiplication given by the tensor product  $[X][Y] = [X \otimes Y]$ . The *Green ring*  $\mathcal{G}(\mathcal{C})$  of  $\mathcal{C}$  is defined to be the quotient ring of  $F(\mathcal{C})$  modulo the relations  $[X \oplus Y] = [X] + [Y]$  for all objects  $X$  and  $Y$  in  $\mathcal{C}$ . The Green ring  $\mathcal{G}(\mathcal{C})$  is an associative ring with the identity represented by the neutral object  $\mathbf{1}$ . The set  $\text{ind}(\mathcal{C})$  consisting of all isomorphism classes of indecomposable objects in  $\mathcal{C}$  forms a  $\mathbb{Z}$ -basis of  $\mathcal{G}(\mathcal{C})$ . If  $\mathcal{C}$  has a braiding, then  $\mathcal{G}(\mathcal{C})$  is a commutative ring. The reader can refer to [6, 10, 17, 18] for a similar notion of the Green ring of a Hopf algebra.

The Grothendieck ring  $\text{Gr}(\mathcal{C})$  of  $\mathcal{C}$  is the quotient ring of  $F(\mathcal{C})$  modulo all short exact sequences in  $\mathcal{C}$ , i.e.,  $[Y] = [X] + [Z]$  holds in  $\text{Gr}(\mathcal{C})$  if  $0 \rightarrow X \rightarrow Y \rightarrow Z \rightarrow 0$  is exact. The Grothendieck ring  $\text{Gr}(\mathcal{C})$  possesses a basis  $\{[X_i] \mid i \in I\}$  given by isomorphism classes of simple objects in  $\mathcal{C}$ . The Green ring and the Grothendieck ring of  $\mathcal{C}$  are connected by the following natural ring epimorphism:

$$\phi : \mathcal{G}(\mathcal{C}) \rightarrow \text{Gr}(\mathcal{C}), \phi([X]) = \sum_{i \in I} [X : X_i][X_i], \tag{2}$$

where  $[X : X_i]$  is the multiplicity of  $X_i$  in the Jordan-Hölder series of  $X$ . Thus,  $\text{Gr}(\mathcal{C}) \cong \mathcal{G}(\mathcal{C}) / \ker \phi$ . If  $\mathcal{C}$  is semisimple, then  $\phi$  is the identity map.

For any indecomposable object  $Z$  in  $\mathcal{C}$ , if  $Z$  is not projective, there exists a unique almost split sequence  $0 \rightarrow X \rightarrow Y \rightarrow Z \rightarrow 0$  in  $\mathcal{C}$  with the ending term  $Z$ , we follow the notation given in [1, Section 4, ChVI] and denote by  $\delta_{[Z]}$  the element  $[X] - [Y] + [Z]$  in  $\mathcal{G}(\mathcal{C})$ ; if  $Z$  is projective, we write  $\delta_{[Z]} = [Z] - [\text{rad}Z]$ , where  $\text{rad}Z$  is the radical of  $Z$ .

The left dual  $X^*$  of any object  $X$  induces a left dual operator on  $\mathcal{G}(\mathcal{C})$  given by  $[X]^* = [X^*]$ . This operator is an anti-automorphism of  $\mathcal{G}(\mathcal{C})$ , since  $(X \otimes Y)^* \cong Y^* \otimes X^*$ . The inverse of this operator under composition is the right dual operator  ${}^*[X] = [{}^*X]$  induced by the right dual  ${}^*X$  of  $X$ , since the left and right duals of  $X$  satisfy  ${}^*(X^*) \cong X \cong ({}^*X)^*$  for any object  $X$  in  $\mathcal{C}$ .

Recall from [12, Section 2.4] that for each object  $X$  of  $\mathcal{C}$  one can define its Frobenius–Perron dimension  $\text{FPdim}(X)$ , which is the largest positive eigenvalue of the matrix of the left or the right multiplication by  $X$ . Since the Frobenius–Perron dimension is additive on exact sequences and multiplicative, the assignment  $[X] \mapsto \text{FPdim}(X)$  extends to an algebra morphism  $\text{FPdim} : \mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{C} \rightarrow \mathbb{C}$  satisfying  $\text{FPdim}([X_i]) > 0$  for any  $i \in I$ . Note that  $\dim_{\mathbb{k}} \text{Hom}_{\mathcal{C}}(P_i, X_j) = 1$  if  $i = j$ , and 0 otherwise. We have

$$\begin{aligned} \text{FPdim}([X]) &= \sum_{j \in I} \text{FPdim}([X_j])[X : X_j] \\ &= \sum_{i, j \in I} \text{FPdim}([X_i])[X : X_j] \dim_{\mathbb{k}} \text{Hom}_{\mathcal{C}}(P_i, X_j) \\ &= \sum_{i \in I} \text{FPdim}([X_i]) \dim_{\mathbb{k}} \text{Hom}_{\mathcal{C}}(P_i, X) > 0. \end{aligned} \tag{3}$$

The regular object of  $\mathcal{C}$  is the element

$$R_{\mathcal{C}} = \sum_{i \in I} \text{FPdim}(X_i)[P_i] \in \mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{C},$$

which satisfies  $R_{\mathcal{C}}[X_i] = [X_i]R_{\mathcal{C}} = \text{FPdim}(X_i)R_{\mathcal{C}}$  for any  $i \in I$  (see [11, Definition 6.1.6]). Moreover, we have  $[X]R_{\mathcal{C}} = R_{\mathcal{C}}[X] = \text{FPdim}(X)R_{\mathcal{C}}$  for any object  $X$  in  $\mathcal{C}$  since any exact sequence in  $\mathcal{C}$  splits after tensoring with a projective object. The Frobenius–Perron dimension of  $\mathcal{C}$  is defined to be

$$\text{FPdim}(\mathcal{C}) = \text{FPdim}(R_{\mathcal{C}}) = \sum_{i \in I} \text{FPdim}([X_i])\text{FPdim}([P_i]).$$

**3. The Frobenius properties of Green rings.** As shown in [3, 24], the Green ring of a finite group or the Green ring of a finite dimensional Hopf algebra can be endowed

with a bilinear form defined by dimensions of morphism spaces. In this section, we follow the same approach and define a similar bilinear form on the Green ring of a finite tensor category.

**3.1. Bilinear forms.** Since there is an equivalence between a finite tensor category  $\mathcal{C}$  and  $\text{Rep}(H)$  for some finite dimensional weak quasi-Hopf algebra  $H$ , many of the technical results of this section can be quoted from Section VI.4 of [1]. However, we reprove them along the same lines for reader’s convenience. We first need the following lemma (see e.g. [2, Lemma 2.1.6]).

LEMMA 3.1. *For all objects  $X, Y, Z$  in  $\mathcal{C}$ , we have the following canonical isomorphisms functorial in  $X, Y$  and  $Z$ :*

- (1)  $\text{Hom}_{\mathcal{C}}(X \otimes Y, Z) \cong \text{Hom}_{\mathcal{C}}(X, Z \otimes Y^*)$ .
- (2)  $\text{Hom}_{\mathcal{C}}(X, Y \otimes Z) \cong \text{Hom}_{\mathcal{C}}(Y^* \otimes X, Z)$ .

For all objects  $X$  and  $Y$  in  $\mathcal{C}$ , we define

$$([X], [Y]) := \dim_{\mathbb{k}} \text{Hom}_{\mathcal{C}}(X, Y^*).$$

Then  $(-, -)$  extends to a  $\mathbb{Z}$ -bilinear form on  $\mathcal{G}(\mathcal{C})$ .

PROPOSITION 3.2. *The bilinear form  $(-, -)$  satisfies the following properties:*

- (1)  $([Y]^*, [X]) = \dim_{\mathbb{k}} \text{Hom}_{\mathcal{C}}(X, Y)$ . In particular,  $([X], *[Y]) = ([Y]^*, [X])$  and  $([X], [Y]) = ([Y]^{**}, [X])$ .
- (2)  $([X][Y], [Z]) = ([X], [Y][Z])$ .

*Proof.* (1) Using Lemma 3.1, we have

$$\begin{aligned} \dim_{\mathbb{k}} \text{Hom}_{\mathcal{C}}(X, Y) &= \dim_{\mathbb{k}} \text{Hom}_{\mathcal{C}}(\mathbf{1} \otimes X, Y) = \dim_{\mathbb{k}} \text{Hom}_{\mathcal{C}}(\mathbf{1}, Y \otimes X^*) \\ &= \dim_{\mathbb{k}} \text{Hom}_{\mathcal{C}}(Y^* \otimes \mathbf{1}, X^*) = ([Y]^*, [X]). \end{aligned}$$

In particular,  $([X], *[Y]) = \dim_{\mathbb{k}} \text{Hom}_{\mathcal{C}}(X, Y) = ([Y]^*, [X])$  and  $([X], [Y]) = ([X], *[Y]^*) = ([Y]^{**}, [X])$ .

(2) The associativity of the form also follows from Lemma 3.1, namely,

$$\begin{aligned} ([X][Y], [Z]) &= \dim_{\mathbb{k}} \text{Hom}_{\mathcal{C}}(X \otimes Y, Z^*) = \dim_{\mathbb{k}} \text{Hom}_{\mathcal{C}}(X, Z^* \otimes Y^*) \\ &= \dim_{\mathbb{k}} \text{Hom}_{\mathcal{C}}(X, (Y \otimes Z)^*) = ([X], [Y][Z]). \end{aligned} \quad \square$$

For any  $[X] \in \text{ind}(\mathcal{C})$ , denote by  $\delta_{[X]}^*$  the image of  $\delta_{[X]}$  under the left dual operator  $*$  of  $\mathcal{G}(\mathcal{C})$ . We have the following result, which is similar to Proposition 4.1 and Theorem 4.2 of [1, ChVI, Section 4].

PROPOSITION 3.3. *The following holds in  $\mathcal{G}(\mathcal{C})$ :*

- (1) For indecomposable objects  $Z$  and  $M$  in  $\mathcal{C}$ ,  $(\delta_{[Z]}^*, [M]) = 1$  if  $Z \cong M$ , and 0 if  $Z \not\cong M$ .
- (2) For any  $x \in \mathcal{G}(\mathcal{C})$ ,  $x = \sum_{[X] \in \text{ind}(\mathcal{C})} (\delta_{[X]}^*, x) [X]$ .
- (3) The set  $\{\delta_{[X]}^* \mid [X] \in \text{ind}(\mathcal{C})\}$  and  $\{\delta_{[X]} \mid [X] \in \text{ind}(\mathcal{C})\}$  are both  $\mathbb{Z}$ -linearly independent.
- (4) The form  $(-, -)$  is non-degenerate in the sense that  $(y, x) = 0$  (resp.  $(x, y) = 0$ ) for all  $y \in \mathcal{G}(\mathcal{C})$  implies that  $x = 0$ .

*Proof.* (1) If  $Z$  is not projective, there exists an almost split sequence

$$0 \rightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \rightarrow 0$$

ending with  $Z$  such that  $g$  is a sink morphism. Applying the functor  $\text{Hom}_C(M, -)$  to this sequence, we obtain the following exact sequence:

$$0 \rightarrow \text{Hom}_C(M, X) \xrightarrow{\text{Hom}_C(M, f)} \text{Hom}_C(M, Y) \xrightarrow{\text{Hom}_C(M, g)} \text{ImHom}_C(M, g) \rightarrow 0.$$

Denote by  $\text{rad}_C(M, Z)$  the set of all morphisms from  $M$  to  $Z$  which are not isomorphic. We claim that  $\text{ImHom}_C(M, g) = \text{rad}_C(M, Z)$ . Indeed, for any  $\alpha \in \text{ImHom}_C(M, g)$ , there exists some  $\beta \in \text{Hom}_C(M, Y)$  such that  $\alpha = g \circ \beta$ . In this case,  $\alpha$  is not an isomorphism since  $g$  is not a retraction. Conversely, for any  $\alpha \in \text{rad}_C(M, Z)$ ,  $\alpha$  is not a retraction. Since  $g$  is a sink morphism, there exists some  $\beta \in \text{Hom}_C(M, Y)$  such that  $\alpha = g \circ \beta$ . Thus,  $\alpha \in \text{ImHom}_C(M, g)$ . Now  $\text{ImHom}_C(M, g) = \text{rad}_C(M, Z)$ , we have

$$\begin{aligned} (\delta_{[Z]}^*, [M]) &= ([X]^*, [M]) - ([Y]^*, [M]) + ([Z]^*, [M]) \\ &= \dim_{\mathbb{k}} \text{Hom}_C(M, X) - \dim_{\mathbb{k}} \text{Hom}_C(M, Y) + \dim_{\mathbb{k}} \text{Hom}_C(M, Z) \\ &= \dim_{\mathbb{k}} \text{Hom}_C(M, Z) - \dim_{\mathbb{k}} \text{rad}_C(M, Z) \\ &= \begin{cases} 1, & M \cong Z; \\ 0, & M \not\cong Z. \end{cases} \end{aligned}$$

If  $Z$  is projective and  $M \not\cong Z$ , then  $\text{Hom}_C(M, Z) = \text{Hom}_C(M, \text{rad}Z)$ , and hence

$$\begin{aligned} (\delta_{[Z]}^*, [M]) &= ([Z]^*, [M]) - ([\text{rad}Z]^*, [M]) \\ &= \dim_{\mathbb{k}} \text{Hom}_C(M, Z) - \dim_{\mathbb{k}} \text{Hom}_C(M, \text{rad}Z) \\ &= 0. \end{aligned}$$

If  $Z$  is projective and  $M \cong Z$ , then  $\text{Hom}_C(Z, \text{rad}Z) = \text{rad}_C(Z, Z)$ , and hence

$$\begin{aligned} (\delta_{[Z]}^*, [Z]) &= ([Z]^*, [Z]) - ([\text{rad}Z]^*, [Z]) \\ &= \dim_{\mathbb{k}} \text{Hom}_C(Z, Z) - \dim_{\mathbb{k}} \text{Hom}_C(Z, \text{rad}Z) \\ &= \dim_{\mathbb{k}} \text{Hom}_C(Z, Z) - \dim_{\mathbb{k}} \text{rad}_C(Z, Z) \\ &= 1. \end{aligned}$$

Part (2) and Part (3) follow from Part (1).

(4) If  $(y, x) = 0$  for all  $y \in \mathcal{G}(C)$ , then  $(\delta_{[X]}^*, x) = 0$  for all  $[X] \in \text{ind}(C)$ . It follows from Part (2) that  $x = 0$ . If  $(x, y) = 0$  for all  $y \in \mathcal{G}(C)$ , then  $x = 0$  since  $(x, {}^*y) = (y^*, x)$  by Proposition 3.2 (1).  $\square$

We have the following result which is similar to Theorems 4.3 and 4.4 of [1, ChVI, Section 4].

**PROPOSITION 3.4.** *The following statements are equivalent:*

- (1) *The set  $\text{ind}(C)$  is finite.*
- (2) *The set  $\{\delta_{[X]} \mid [X] \in \text{ind}(C)\}$  forms a basis of  $\mathcal{G}(C)$ .*
- (3) *The set  $\{\delta_{[X]} \mid [X] \in \text{ind}(C) \text{ and } X \text{ is not projective}\}$  forms a basis of  $\ker \phi$ , where  $\phi$  is the map given in (2).*

*Proof.* (1) $\Rightarrow$ (2) For any  $x \in \mathcal{G}(\mathcal{C})$ , we have  $x = \sum_{[X] \in \text{ind}(\mathcal{C})} (\delta_{[X]}^*, x)[X]$  by Proposition 3.3 (2). If  $\text{ind}(\mathcal{C})$  is a finite set, then  $y = \sum_{[X] \in \text{ind}(\mathcal{C})} (x, [X])\delta_{[X]}^*$  is a finite sum and hence an element in  $\mathcal{G}(\mathcal{C})$ . In this case,  $(y, [X]) = (x, [X])$  for all  $[X] \in \text{ind}(\mathcal{C})$ . It follows from Proposition 3.3 (4) that  $x = y$ , and hence  $x$  is a  $\mathbb{Z}$ -linear combination of the set  $\{\delta_{[X]}^* \mid [X] \in \text{ind}(\mathcal{C})\}$ . We conclude that  $\{\delta_{[X]}^* \mid [X] \in \text{ind}(\mathcal{C})\}$ , or equivalently,  $\{\delta_{[X]} \mid [X] \in \text{ind}(\mathcal{C})\}$  is a basis of  $\mathcal{G}(\mathcal{C})$ , since it is linearly independent by Proposition 3.3 (3).

(2) $\Rightarrow$ (1) Since  $\{\delta_{[X]}^* \mid [X] \in \text{ind}(\mathcal{C})\}$  is a basis of  $\mathcal{G}(\mathcal{C})$ , it is also a basis of the algebra  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{C}$  over  $\mathbb{C}$ . Suppose the regular object of  $\mathcal{C}$  has the form  $R_{\mathcal{C}} = \sum_{[X] \in \text{ind}(\mathcal{C})} \lambda_{[X]}\delta_{[X]}^*$ , where the number of nonzero summands is finite. To verify that  $\text{ind}(\mathcal{C})$  is a finite set, it is enough to show that  $\lambda_{[X]} \neq 0$  for any  $[X] \in \text{ind}(\mathcal{C})$ . Indeed,

$$(R_{\mathcal{C}}, [X]) = \left( \sum_{[X] \in \text{ind}(\mathcal{C})} \lambda_{[X]}\delta_{[X]}^*, [X] \right) = \lambda_{[X]}.$$

On the other hand, since  $R_{\mathcal{C}} = \sum_{i \in I} \text{FPdim}(X_i)[P_i]$ , it follows from (3) that

$$(R_{\mathcal{C}}, [X]) = \sum_{i \in I} \text{FPdim}(X_i) \dim_{\mathbb{k}} \text{Hom}_{\mathcal{C}}(P_i, X^*) = \text{FPdim}(X^*) > 0.$$

Thus,  $\lambda_{[X]} > 0$  for any  $[X] \in \text{ind}(\mathcal{C})$ .

(2) $\Rightarrow$ (3) We only need to show that  $\ker \phi$  is spanned by  $\{\delta_{[X]} \mid [X] \in \text{ind}(\mathcal{C}) \text{ and } X \text{ is not projective}\}$  since this set is already linearly independent. For any  $x \in \ker \phi$ , suppose that  $x = \sum_{[X] \in \text{ind}(\mathcal{C})} \lambda_{[X]}\delta_{[X]}$ . Note that  $\phi(\delta_{[X]}) = 0$  if  $X$  is not projective; and  $\phi(\delta_{[P_i]}) = [X_i]$  for any  $i \in I$ . It follows that  $0 = \phi(x) = \sum_{i \in I} \lambda_{[P_i]}\delta_{[P_i]}$ , and hence  $\lambda_{[P_i]} = 0$  for any  $i \in I$ , as desired.

(3) $\Rightarrow$ (2) For any  $x \in \mathcal{G}(\mathcal{C})$ , we only need to show that  $x$  is spanned by the set  $\{\delta_{[X]} \mid [X] \in \text{ind}(\mathcal{C})\}$  since this set is linearly independent. Suppose that  $x = \sum_{[X] \in \text{ind}(\mathcal{C})} \lambda_{[X]}[X]$ . Consider the element  $x_0 = \sum_{i \in I} \sum_{[X] \in \text{ind}(\mathcal{C})} \lambda_{[X]}[X : X_i]\delta_{[P_i]}$ . Since  $\phi(x) = \phi(x_0)$ , we have  $x - x_0 \in \ker \phi$  which is spanned by the set  $\{\delta_{[X]} \mid [X] \in \text{ind}(\mathcal{C}) \text{ and } X \text{ is not projective}\}$ . Thus,  $x$  is spanned by the set  $\{\delta_{[X]} \mid [X] \in \text{ind}(\mathcal{C})\}$ .  $\square$

We summarize the main result of this section as follows:

**THEOREM 3.5.** *If  $\mathcal{C}$  is a finite tensor category with only finitely many indecomposable objects up to isomorphism, then the Green ring  $\mathcal{G}(\mathcal{C})$  is a Frobenius  $\mathbb{Z}$ -algebra.*

*Proof.* Since  $\text{ind}(\mathcal{C})$  is finite, the set  $\{\delta_{[X]}^* \mid [X] \in \text{ind}(\mathcal{C})\}$  is a basis of  $\mathcal{G}(\mathcal{C})$  by Proposition 3.4 (2). Consider the  $\mathbb{Z}$ -linear map from  $\mathcal{G}(\mathcal{C})$  to its dual  $\mathcal{G}(\mathcal{C})^*$  given by  $x \mapsto (x, -)$  or  $x \mapsto (-, x)$ . This map is injective by Proposition 3.3 (4) and surjective by Proposition 3.3 (1). Thus, the Green ring  $\mathcal{G}(\mathcal{C})$  is equipped with an associative and nonsingular bilinear form  $(-, -)$  with dual bases  $\{\delta_{[X]}^* \mid [X] \in \text{ind}(\mathcal{C})\}$  and  $\text{ind}(\mathcal{C})$ . Hence  $\mathcal{G}(\mathcal{C})$  is a Frobenius  $\mathbb{Z}$ -algebra.  $\square$

**REMARK 3.6.** If  $\mathcal{C}$  is a fusion category, then  $\text{ind}(\mathcal{C}) = \{[X_i] \mid i \in I\}$ , which is the set of isomorphism classes of simple objects of  $\mathcal{C}$ , and  $\delta_{[X_i]}^* = [X_i]^*$  for any  $i \in I$ . In this case,  $\{[X_i]^* \mid i \in I\}$  and  $\{[X_i] \mid i \in I\}$  form dual bases of  $\mathcal{G}(\mathcal{C})$  with respect to the form  $(-, -)$  and the Green ring  $\mathcal{G}(\mathcal{C})$  coincides with the Grothendieck ring  $\text{Gr}(\mathcal{C})$ , which is a fusion ring in the sense of [11, Definition 3.1.7].

Let  $\mathcal{C}$  be a finite tensor category with only finitely many indecomposable objects up to isomorphism. The regular object  $R_{\mathcal{C}}$  of  $\mathcal{C}$  is an integral of  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{C}$  with respect

to the augmentation  $\text{FPdim}$ . Indeed, the algebra  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{C}$  is a Frobenius algebra over  $\mathbb{C}$ , and any  $x \in \mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{C}$  can be written as

$$x = \sum_{[X] \in \text{ind}(\mathcal{C})} (\delta_{[X]}^*, x)[X] \text{ or } x = \sum_{[X] \in \text{ind}(\mathcal{C})} (x, [X])\delta_{[X]}^*. \tag{4}$$

By Section 2.1, a left integral with respect to  $\text{FPdim}$  is up to a scalar the following element

$$\sum_{[X] \in \text{ind}(\mathcal{C})} \text{FPdim}([X])\delta_{[X]}^* = \sum_{[X] \in \text{ind}(\mathcal{C})} (R_{\mathcal{C}}, [X])\delta_{[X]}^* = R_{\mathcal{C}},$$

and a right integral with respect to  $\text{FPdim}$  is up to a scalar the element

$$\sum_{[X] \in \text{ind}(\mathcal{C})} \text{FPdim}(\delta_{[X]}^*)[X] = \sum_{i \in I} \text{FPdim}(X_i)[P_i] = R_{\mathcal{C}}.$$

Thus, the left and right integral spaces coincide and  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{C}$  is unimodular under the augmentation  $\text{FPdim}$ .

**3.2. The Jacobson semisimplicity of Green rings.** In this subsection,  $\mathcal{C}$  is always a finite tensor category with only finitely many indecomposable objects up to isomorphism over an algebraically closed field  $\mathbb{k}$ . In this case, the Green ring  $\mathcal{G}(\mathcal{C})$  of  $\mathcal{C}$  is a Frobenius algebra over  $\mathbb{Z}$ , and all notions given in Section 2.1 make sense for  $\mathcal{G}(\mathcal{C})$ . More precisely, the Casimir operator of  $\mathcal{G}(\mathcal{C})$  is the map  $c$  from  $\mathcal{G}(\mathcal{C})$  to its centre  $Z(\mathcal{G}(\mathcal{C}))$  given by

$$c(x) = \sum_{[X] \in \text{ind}(\mathcal{C})} [X]x\delta_{[X]}^* \text{ for } x \in \mathcal{G}(\mathcal{C}).$$

The Casimir element of  $\mathcal{G}(\mathcal{C})$  is  $c(1) = \sum_{[X] \in \text{ind}(\mathcal{C})} [X]\delta_{[X]}^*$ . In particular,

$$\text{FPdim}(c(1)) = \text{FPdim}(R_{\mathcal{C}}) = \text{FPdim}(\mathcal{C}).$$

The Casimir number of  $\mathcal{C}$  is defined to be the Casimir number of  $\mathcal{G}(\mathcal{C})$ , namely, the non-negative integer  $m$  satisfying  $\mathbb{Z} \cap \text{Im } c = (m)$ . This number is an invariant of  $\mathcal{C}$  under tensor equivalence because it does not depend on the choice of a bilinear form on  $\mathcal{G}(\mathcal{C})$ . From this number one is able to determine when  $\mathcal{G}(\mathcal{C})$ , or the algebra  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$  over a field  $K$  is Jacobson semisimple.

**THEOREM 3.7.** *The Green algebra  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$  over a field  $K$  is Jacobson semisimple if and only if the Casimir number of  $\mathcal{C}$  is not zero in  $K$ .*

*Proof.* If  $K = \mathbb{F}_p$ , then the algebra  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{F}_p$  is separable (namely, Jacobson semisimple) if and only if  $(p) \not\subseteq \text{Im } c \cap \mathbb{Z}$ , see [20, Proposition 6]. If  $K = \mathbb{Q}$ , then  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q}$  is separable if and only if  $\text{Im } c = Z(\mathcal{G}(\mathcal{C}))$  by Higman’s theorem [15, Theorem 1], or equivalently,  $c(x) = 1$  for some  $x \in \mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q}$ . This is equivalent to saying that  $c(mx) = m$ , where  $m$  is a positive integer such that  $mx \in \mathcal{G}(\mathcal{C})$ . Precisely,  $\mathbb{Z} \cap \text{Im } c \neq 0$ . 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  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$  is Jacobson semisimple if and only if  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q}$  (resp.  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{F}_p$ ) is Jacobson semisimple. We have completed the proof. □

If  $\mathbb{Z} \cap \text{Im } c = (m)$ , then there exists some  $x \in \mathcal{G}(\mathcal{C})$  such that  $c(x) = m$ . Applying  $\text{FPdim}$  to this equality, we have

$$m = \text{FPdim}(c(x)) = \text{FPdim}(x)\text{FPdim}c(1) = \text{FPdim}(x)\text{FPdim}(\mathcal{C}). \tag{5}$$

It means that the Casimir number  $m$  of  $\mathcal{C}$  is divisible by  $\text{FPdim}(\mathcal{C})$ . In particular, we have the following result which is a generalization of [20, Proposition 22(a)].

**COROLLARY 3.8.** *If  $\mathcal{C} = \text{Rep}(H)$  for a finite dimensional quasi-Hopf algebra  $H$  of finite representation type, then*

- (1) *The dimension of  $H$  divides the Casimir number of  $\mathcal{C}$ .*
- (2) *If a prime  $p$  divides the dimension of  $H$ , then  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$  is not Jacobson semisimple for any field  $K$  of characteristic  $p$ .*

*Proof.* (1) If  $\mathcal{C} = \text{Rep}(H)$  for a finite dimensional quasi-Hopf algebra  $H$ , then  $\text{FPdim}(\mathcal{C}) = \dim_k(H)$  and  $\text{FPdim}(X) = \dim_k(X)$  for any object  $X$  in  $\mathcal{C}$  (see [11, Proposition 6.1.14]). In this case, Part (1) follows directly from (5).

(2) It follows from Part (1) and Theorem 3.7. □

**REMARK 3.9.** 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  $\text{Hom}_{\mathcal{C}}(g, h) = id_g$  if  $g = h$ , and  $\emptyset$  if  $g \neq h$ . The Green ring of  $\mathcal{C}$  is the group ring  $\mathbb{Z}G$ , and  $\mathbb{Z} \cap \text{Im } c = (m)$ , where  $m$  is the order of  $G$ . It follows from Theorem 3.7 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 3.7 can be viewed as the Green ring version of Maschke’s theorem.

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

**LEMMA 3.10.** *Let  $J(\mathcal{G}(\mathcal{C}))$  be the Jacobson radical of  $\mathcal{G}(\mathcal{C})$  and  $p\mathcal{G}(\mathcal{C})$  the ideal of  $\mathcal{G}(\mathcal{C})$  generated by a prime  $p$ .*

- (1) *We have  $(J(\mathcal{G}(\mathcal{C})))^n \subseteq p\mathcal{G}(\mathcal{C})$  for some integer  $n$ .*
- (2) *If  $\mathbb{Z} \cap \text{Im } c = (m)$  and  $p \nmid m$ , then  $J(\mathcal{G}(\mathcal{C})) \subseteq p\mathcal{G}(\mathcal{C})$ .*

*Proof.* (1) The ring isomorphism  $\mathcal{G}(\mathcal{C})/p\mathcal{G}(\mathcal{C}) \cong \mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{F}_p$  shows that the quotient  $\mathcal{G}(\mathcal{C})/p\mathcal{G}(\mathcal{C})$  is a finite ring. So the Jacobson radical  $J(\mathcal{G}(\mathcal{C})/p\mathcal{G}(\mathcal{C}))$  of  $\mathcal{G}(\mathcal{C})/p\mathcal{G}(\mathcal{C})$  is nilpotent [21, Proposition IV.7]. The canonical ring epimorphism  $\pi : \mathcal{G}(\mathcal{C}) \rightarrow \mathcal{G}(\mathcal{C})/p\mathcal{G}(\mathcal{C})$  yields that  $\pi(J(\mathcal{G}(\mathcal{C}))) \subseteq J(\mathcal{G}(\mathcal{C})/p\mathcal{G}(\mathcal{C}))$ , so  $\pi(J(\mathcal{G}(\mathcal{C})))$  is nilpotent. Thus, there exists a positive integer  $n$  such that  $(J(\mathcal{G}(\mathcal{C})))^n$  is contained in the kernel of  $\pi$ , namely,  $(J(\mathcal{G}(\mathcal{C})))^n \subseteq p\mathcal{G}(\mathcal{C})$ .

(2) If the prime  $p$  satisfies  $p \nmid m$ , then  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{F}_p$  is Jacobson semisimple by Theorem 3.7. In this case,  $\pi(J(\mathcal{G}(\mathcal{C}))) \subseteq J(\mathcal{G}(\mathcal{C})/p\mathcal{G}(\mathcal{C})) = 0$ . This implies that  $J(\mathcal{G}(\mathcal{C})) \subseteq p\mathcal{G}(\mathcal{C})$ . □

**THEOREM 3.11.** *The Green ring  $\mathcal{G}(\mathcal{C})$  is Jacobson semisimple if and only if the Casimir number of  $\mathcal{C}$  is not zero.*

*Proof.* Assume that the Jacobson radical  $J(\mathcal{G}(\mathcal{C}))$  of  $\mathcal{G}(\mathcal{C})$  is zero. Consider the finite dimensional algebra  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q}$  over  $\mathbb{Q}$ . We first show that the Jacobson radical  $J(\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q})$  of  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q}$  is zero. For any  $x \in J(\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q})$ , there exists a

nonzero integer  $n$  such that  $nx \in \mathcal{G}(\mathcal{C}) \cap J(\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q})$ . For any  $y, z \in \mathcal{G}(\mathcal{C})$ , we have  $y(nx)z \in \mathcal{G}(\mathcal{C}) \cap J(\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q})$ . Since  $J(\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q})$  is nilpotent,  $1 - y(nx)z$  is invertible in  $\mathcal{G}(\mathcal{C})$ . This means that  $nx \in J(\mathcal{G}(\mathcal{C})) = 0$ , and hence  $x = 0$ . Now  $J(\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q}) = 0$  and the algebra  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} \mathbb{Q}$  is Jacobson semisimple, it follows from Theorem 3.7 that the Casimir number of  $\mathcal{C}$  is not zero in  $\mathbb{Q}$ , so it is a nonzero integer. Conversely, if the Casimir number of  $\mathcal{C}$  is  $m \neq 0$ , then the set  $\Omega$  consisting of all primes  $p$  such that  $p \nmid m$  is an infinite set. For any  $x \in J(\mathcal{G}(\mathcal{C}))$ , we may write  $x = d \sum_{[X] \in \text{ind}(\mathcal{C})} \lambda_{[X]} [X]$ , where  $d \in \mathbb{Z}$  and all integer coefficients  $\lambda_{[X]}$  are coprime. By Lemma 3.10 (2) we have  $J(\mathcal{G}(\mathcal{C})) \subseteq p\mathcal{G}(\mathcal{C})$  for all  $p \in \Omega$ . It follows that  $p \mid d$  for all  $p \in \Omega$ . Thus,  $d = 0$ , and hence  $x = 0$ . □

If the Green ring  $\mathcal{G}(\mathcal{C})$  is commutative, then the Jacobson radical of  $\mathcal{G}(\mathcal{C})$  is the set of all nilpotent elements of  $\mathcal{G}(\mathcal{C})$ . As a consequence, Theorem 3.11 gives a characterization of a commutative Green ring without nonzero nilpotent elements. In particular, if  $\mathcal{C}$  is a representation category of a finite group of finite representation type, then the Green ring  $\mathcal{G}(\mathcal{C})$  is commutative. In this case, the Green ring  $\mathcal{G}(\mathcal{C})$  has no nonzero nilpotent elements if and only if the Casimir number of  $\mathcal{C}$  is not zero.

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

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

$$\mathbb{k}G \cong \mathbb{k}[X]/(X^p - 1) \cong \mathbb{k}[X]/(X - 1)^p,$$

where the latter is a commutative Nakayama local algebra over  $\mathbb{k}$ . Let  $M_i = \mathbb{k}[X]/(X - 1)^i$  for  $i = 1, \dots, p$ . Then  $\{M_1, M_2, \dots, M_p\}$  is a complete set of indecomposable  $\mathbb{k}G$ -modules up to isomorphism [1, 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  $\mathbb{k}G$ -module.

We follow from [1, ChV, Section 4] and present almost split sequences of  $\mathbb{k}G$ -modules as follows. The almost split sequence ending with the trivial module  $M_1$  is

$$0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_1 \rightarrow 0,$$

and the almost split sequence ending with  $M_i$  is

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

Note that the sequence

$$0 \rightarrow M_i \rightarrow M_2 \otimes M_i \rightarrow M_i \rightarrow 0$$

is also an almost split sequence ending with  $M_i$  for  $1 \leq i < p$  (see [1, 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  $\mathcal{G}(\mathcal{C})$  for  $\mathcal{C} = \text{Rep}(\mathbb{k}G)$ . The product  $[M_i][M_j]$  in  $\mathcal{G}(\mathcal{C})$  can be described as follows.

LEMMA 4.1. *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 [23, Proposition 4.2] for a similar result. □

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

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

We have

$$\mathcal{G}(\mathcal{C}) \cong \mathbb{Z}[X_2, \dots, X_p]/I,$$

where the isomorphism is given by  $[M_i] \mapsto \overline{X_i}$  for  $i = 2, 3, \dots, p$  (see [1, ChV, Proposition 4.11]). Actually, the Green ring  $\mathcal{G}(\mathcal{C})$  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:

$$E_0(X) = 1, E_1(X) = X, \text{ and } E_{i+1}(X) = XE_i(X) - E_{i-1}(X) \text{ for } i \geq 1. \tag{6}$$

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

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

for  $n \geq 0$  (see e.g. [8, equation (1.2)]).

PROPOSITION 4.2. *We have  $\mathcal{G}(\mathcal{C}) \cong \mathbb{Z}[X]/((X - 2)E_{p-1}(X))$ .*

*Proof.* Consider the following ring epimorphism  $\psi$  from  $\mathbb{Z}[X_2, \dots, X_p]$  to  $\mathbb{Z}[X]/((X - 2)E_{p-1}(X))$  given by  $g(X_2, \dots, X_p) \mapsto g(E_1(X), \dots, E_{p-1}(X))$ . By (6) we have  $\psi(I) = 0$ . This induces a ring epimorphism  $\overline{\psi}$  from  $\mathbb{Z}[X_2, \dots, X_p]/I$  to  $\mathbb{Z}[X]/((X - 2)E_{p-1}(X))$  such that the following diagram is commutative:

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

where  $\pi$  is the canonical ring epimorphism. Define another ring morphism  $\varphi$  from  $\mathbb{Z}[X]$  to  $\mathbb{Z}[X_2, \dots, X_p]/I$  by  $\varphi(f(X)) = f(\overline{X_2})$ . By induction on  $i$  one is able to check that  $\overline{E_{i-1}(X_2)} = \overline{X_i}$  holds in  $\mathbb{Z}[X_2, \dots, X_p]/I$  for  $i = 2, 3, \dots, p$ . Thus,  $\varphi$  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  $\varphi$  induces a ring epimorphism  $\bar{\varphi}$  from  $\mathbb{Z}[X]/((X - 2)E_{p-1}(X))$  to  $\mathbb{Z}[X_2, \dots, X_p]/I$  such that the following diagram is commutative:

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

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

The almost split sequences of  $\mathbb{k}G$ -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  $\delta_{[M]}$  in Section 3, 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  $\delta_{[M_i]} = \delta_{[M_i]}[M_i]$  for  $1 \leq i < p$  and  $\delta_{[M_i]}[M_p] = 0$ . 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  $\mathcal{G}(\mathcal{C})$ :

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

Note that

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

whose  $(i, j)$ -entry is  $\min\{i, j\}$ . By (4) we have

$$[M_i] = \sum_{j=1}^p ([M_i], [M_j])\delta_{[M_j]}^* = \sum_{j=1}^p \dim_{\mathbb{k}} \text{Hom}_{\mathbb{k}G}(M_i, M_j)\delta_{[M_j]}$$

since the dual operator  $*$  on  $\mathcal{G}(\mathcal{C})$  is the identity map. It follows that  $\dim_{\mathbb{k}} \text{Hom}_{\mathbb{k}G}(M_i, M_j) = \min\{i, j\}$ .

**4.2. The Casimir number.** The Casimir operator  $c$  of  $\mathcal{G}(\mathcal{C})$  is given by

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

since  $\mathcal{G}(\mathcal{C})$  is commutative. To determine the Casimir number of  $\mathcal{C}$ , we need to describe the Casimir element  $c(1)$  of  $\mathcal{G}(\mathcal{C})$ .

LEMMA 4.3. *The Casimir element  $c(1) = [M_p] + 2 \sum_{i=1}^p (-1)^{i-1} (p - i)[M_i]$ .*

*Proof.* First, it is straightforward to check (by Lemma 4.1) that

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

Using this equality we have

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

The proof is completed. □

Note that  $\{\delta_{[M_t]} \mid t = 1, 2, \dots, p\}$  and  $\{[M_t] \mid t = 1, 2, \dots, p\}$  form dual bases of  $\mathcal{G}(\mathcal{C})$ . For any  $x \in \mathcal{G}(\mathcal{C})$ ,  $c(x)$  has the form  $c(x) = \sum_{t=1}^p (\delta_{[M_t]}, c(x))[M_t]$  by (4). 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  $1 \leq t \leq p$ .

LEMMA 4.4. *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 we have

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

where the last equality follows from Lemma 4.1 (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,

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

We have completed the proof. □

To describe  $(\delta_{[M_t]}, c(x))$  for  $1 \leq t \leq p-1$ , we need some preparations. The left multiplication by  $[M_t]$  with respect to the basis  $\{[M_1], [M_2], \dots, [M_p]\}$  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:

$$\begin{aligned} \mathbf{M}_t &= \mathbf{E}_{1,t} + \mathbf{E}_{2,t+1} + \mathbf{E}_{3,t+2} + \cdots + \mathbf{E}_{p-t,p-1} \\ &\quad + \mathbf{E}_{2,t-1} + \mathbf{E}_{3,t} + \mathbf{E}_{4,t+1} + \cdots + \mathbf{E}_{p-t+1,p-2} \\ &\quad + \mathbf{E}_{3,t-2} + \mathbf{E}_{4,t-1} + \mathbf{E}_{5,t} + \cdots + \mathbf{E}_{p-t+2,p-3} \\ &\quad + \cdots \\ &\quad + \mathbf{E}_{t,1} + \mathbf{E}_{t+1,2} + \mathbf{E}_{t+2,3} + \cdots + \mathbf{E}_{p-1,p-t} \\ &\quad + t\mathbf{E}_{p,p} + (t-1)\mathbf{E}_{p-1,p} + (t-2)\mathbf{E}_{p-2,p} + \cdots + \mathbf{E}_{p-t+1,p} \\ &= \sum_{s=1}^t \sum_{r=1}^{p-t} \mathbf{E}_{s+r-1,t+r-s} + \sum_{s=1}^t (t+1-s)\mathbf{E}_{p-s+1,p}. \end{aligned} \tag{7}$$

LEMMA 4.5. *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  $1 \leq t \leq p-1$ .

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

$$\begin{aligned} N_{ij}^t &= (\delta_{[M_i]}, [M_j][M_t]) = (\delta_{[M_i]}, [M_t][M_j]) \\ &= (\delta_{[M_i]}, [M_j][M_t]) = (\delta_{[M_j]}, [M_t][M_i]) \\ &= N_{ji}^t. \end{aligned} \tag{8}$$

Consequently, we have

$$\begin{aligned} c(x) &= c(1)x = \left( [M_p] + 2 \sum_{i=1}^p (-1)^{i-1} (p-i)[M_i] \right) \sum_{j=1}^p \lambda_j[M_j] \\ &= \mu_1[M_p] + 2 \sum_{i,j=1}^{p-1} (-1)^{i-1} (p-i) \lambda_j [M_i][M_j] \quad (\text{for some } \mu_1 \in \mathbb{Z}) \\ &= \mu_1[M_p] + 2 \sum_{i,j=1}^{p-1} (-1)^{i-1} (p-i) \lambda_j \sum_{t=1}^p N_{ij}^t[M_t] \\ &= \mu_2[M_p] + 2 \sum_{i,j,t=1}^{p-1} (-1)^{i-1} (p-i) \lambda_j N_{ij}^t[M_t] \quad (\text{for some } \mu_2 \in \mathbb{Z}) \\ &= \mu_2[M_p] + 2 \sum_{i,j,t=1}^{p-1} (-1)^{i-1} (p-i) \lambda_j N_{it}^j[M_t] \quad \text{by (8)}. \end{aligned}$$

Thus,

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

Let  $\widehat{M}_t$  be the submatrix of  $M_t$  obtained by deleting the  $p$ -th column and row. By (7) we have  $\widehat{M}_t = \sum_{s=1}^t \sum_{r=1}^{p-t} E_{s+r-1, t+r-s}$ . The matrix  $\widehat{M}_t$  is symmetric and

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

We are done. □

The Casimir number of  $\mathcal{C}$  can be presented as follows:

**THEOREM 4.6.** *The Casimir number of  $\mathcal{C}$  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  $t = 2, 3, \dots, p$ . However,

$$(\delta_{[M_t]}, c(x)) = 2(p-t) \sum_{i=1}^t (-1)^{t+i} i \lambda_i + 2t \sum_{i=t+1}^{p-1} (-1)^{t+i} (p-i) \lambda_i, \tag{9}$$

for  $t = 2, 3, \dots, p-1$  (see Lemma 4.5), and

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

(see Lemma 4.4). This gives a system of equations with variables  $\lambda_1, \dots, \lambda_p$ . Consider the following equations:

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

Using (9) 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  $\lambda_{p-1} = \lambda_{p-2} = \dots = \lambda_3 = 0$ . 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  $\text{Im } c \cap \mathbb{Z} = (2p^2)$ . □

**4.3. The Jacobson radical.** Since the Casimir number of  $\mathcal{C}$  is  $2p^2 \neq 0$ , the Green ring  $\mathcal{G}(\mathcal{C})$  is Jacobson semisimple. This is exactly a result of J.A. Green [13]. For the Green algebra  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ , it follows from Theorem 3.7 that  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$  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  $\mathcal{G}(\mathcal{C}) \otimes_{\mathbb{Z}} K$ , or equivalently,  $K[X]/((X-2)E_{p-1}(X))$  (see Proposition 4.2) in the cases where  $K$  is of characteristic 2 or  $p$ .

**PROPOSITION 4.7.** *If the characteristic of  $K$  is  $p$ , then the Jacobson radical of  $K[X]/((X-2)E_{p-1}(X))$  is a principal ideal generated by  $X^2 - 4$ .*

*Proof.* We have the decomposition  $E_{p-1}(X) = (X-2)^{\frac{p-1}{2}}(X+2)^{\frac{p-1}{2}}$  in  $K[X]$  [8, 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 4.8. *If the characteristic of  $K$  is 2, then the Jacobson radical of  $K[X]/((X - 2)E_{p-1}(X))$  is a principal ideal generated by*

$$\sum_{i=0}^{\lfloor \frac{p-1}{2} \rfloor} \binom{p-1-i}{i} (-1)^i \overline{X^{\frac{p+1}{2}-i}}.$$

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

$$K[X]/((X - 2)E_{p-1}(X)) \cong K[X]/(XE_{p-1}(X)). \tag{10}$$

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

$$E_{p-1}(X) = \sum_{i=0}^{\lfloor \frac{p-1}{2} \rfloor} \binom{p-1-i}{i} (-1)^i X^{p-1-2i} = (f(X))^2,$$

where

$$f(X) = \sum_{i=0}^{\lfloor \frac{p-1}{2} \rfloor} \binom{p-1-i}{i} (-1)^i X^{\frac{p-1}{2}-i}$$

and it has no multiple factors in  $K[X]$ , see [5, 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.  $\square$

ACKNOWLEDGEMENTS. The authors would like to thank the referees for their careful reading of this paper and for valuable comments. The first author was funded by China Postdoctoral Science Foundation (Grant No. 2017M610316), the second author was funded by the NSF of China (Grant No. 11471282).

### REFERENCES

1. M. Auslander, I. Reiten and S. O. Smalø, *Representation theory of Artin algebras*, vol. 36 (Cambridge Studies in Advanced Mathematics, Cambridge, 1994).
2. B. Bakalov and A. A. Kirillov, *Lectures on tensor categories and modular functors*, vol. 21, (AMS, Providence, 2001).
3. D. J. Benson, The Green ring of a finite group, *J. Algebra* **87** (1984), 290–331.
4. D. J. Benson and J. F. Carlson, Nilpotent elements in the Green ring, *J. Algebra* **104** (1986), 329–350.
5. M. Bhargava and M. E. Zieve, Factoring Dickson polynomials over finite fields, *Finite Fields Appl.* **5**(2) (1999), 103–111.
6. H. Chen, The green ring of drinfeld double  $D(H_4)$ , *Algebras and Representation Theory* **17**(5) (2014), 1457–1483.
7. H. Chen, F. V. Oystaeyen and Y. Zhang, The green rings of taft algebras, *Proc. Amer. Math. Soc.* **142** (2014), 765–775.
8. W. S. Chou, The factorization of Dickson polynomials over finite fields, *Finite Fields Appl.* **3** (1997), 84–96.
9. E. Darpö and M. Herschend, On the representation ring of the polynomial algebra over perfect field, *Math. Z* **265** (2011), 605–615.
10. M. Domokos and T. H. Lenagan, Representation rings of quantum groups, *J. Algebra* **282** (2004), 103–128.

11. P. Etingof, S. Gelaki, D. Nikshych and V. Ostrik, *Tensor categories*, Mathematical Surveys and Monographs, vol. 205 (AMS, Providence, RI, 2015).
12. P. Etingof and V. Ostrik, Finite tensor categories, *Mosc. Math. J.* **4**(3) (2004), 627–654.
13. J. A. Green, A transfer theorem for modular representations, *J. Algebra* **1** (1964), 73–84.
14. J. A. Green, The modular representation algebra of a finite group, *Ill. J. Math.* **6**(4) (1962), 607–619.
15. D. G. Higman, On orders in separable algebras, *Canad. J. Math.* **7** (1955), 509–515.
16. H. Huang, F. V. Oystaeyen, Y. Yang and Y. Zhang, The Green rings of pointed tensor categories of finite type, *J. Pure Appl. Algebra* **218** (2014), 333–342.
17. Y. Li and N. Hu, The Green rings of the 2-rank Taft algebra and its two relatives twisted, *J. Algebra* **410** (2014), 1–35.
18. L. Li and Y. Zhang, The Green rings of the generalized Taft Hopf algebras, *Contemp. Math.* **585** (2013), 275–288.
19. S. Liu, Auslander-Reiten theory in a Krull-Schmidt category, *São Paulo J. Math. Sci.* **4**(3) (2010), 425–472.
20. M. Lorenz, Some applications of Frobenius algebras to Hopf algebras, *Contemp. Math.* **537** (2011), 269–289.
21. B. R. McDonald, *Finite rings with identity*, vol. 28 (Marcel Dekker Incorporated, 1974).
22. C. M. Ringel, *Tame algebras and integral quadratic forms*, Lecture Notes in Mathematics, vol. 1099 (Springer, Berlin Heidelberg, 1984).
23. Z. Wang, L. Li and Y. Zhang, Green rings of pointed rank one Hopf algebras of nilpotent type, *Algebras Represent. Theory* **17**(6) (2014), 1901–1924.
24. Z. Wang, L. Li and Y. Zhang, Green rings of pointed rank one Hopf algebras of non-nilpotent type, *J. Algebra* **449** (2016), 108–137.
25. S. J. Witherspoon, The representation ring of the quantum double of a finite group, *J. Algebra* **179** (1996), 305–329.
26. J. Zemanek, Nilpotent elements in representation rings, *J. Algebra* **19** (1971), 453–469.