第61卷第1期 数学学报中文版 Vol.61, No.1
2018年1月 ACTA MATHEMATICA SINICA, CHINESE SERIES Jan., 2018

文章编号: 0583-1431(2018)01-0059-08 **文献标识码:** A

Verlinde 模性范畴上的 Casimir 数及其应用

王志华

泰州学院数理学院 泰州 225300
南京大学数学系 南京 210009
E-mail: mailzhihua@126.com

李立斌

扬州大学数学科学学院 扬州 225002
E-mail: lbli@yzu.edu.cn

摘　要　本文计算了秩为 $n+1$ 的一类特殊的 Verlinde 模性范畴 $\mathscr{C}$ 的 Casimir 数, 计算结果表明该 Casimir 数为 $2n+4$. 作为应用, 由 Higman 定理知域 K 上的 Grothendieck 代数 $\mathrm{Gr}(\mathscr{C})\otimes_{\mathbb{Z}} K$ 是半单代数当且仅当 $2n+4$ 在域 K 中不为零. 这也给出了第二类型 $n+1$ 次 Dickson 多项式 $E_{n+1}(X)$ 在 $K[X]$ 中无重因式的一个等价刻画. 如果 $2n+4$ 在域 K 中为零, 借助于 Dickson 多项式的有关因式分解定理, 本文完全给出了 Grothendieck 代数 $\mathrm{Gr}(\mathscr{C})\otimes_{\mathbb{Z}} K$ 的 Jacobson 根.

关键词　Grothendieck 环; Verlinde 模性范畴; Casimir 数; Jacobson 根; Dickson 多项式
MR(2010) 主题分类　16W10
中图分类　O153.3

The Casimir Number of a Verlinde Modular Category and Its Applications

Zhi Hua WANG

Department of Mathematical Sciences, Taizhou College, Taizhou 225300, *P. R. China*
Department of Mathematics, Nanjing University, Nanjing 210009, *P. R. China*
E-mail: *mailzhihua@126.com*

Li Bin LI

School of Mathematical Science, Yangzhou University,
Yangzhou 225002, *P. R. China*
E-mail: *lbli@yzu.edu.cn*

Abstract　In this paper the Casimir number of a special kind of Verlinde modular category $\mathscr{C}$ of rank $n+1$ is calculated to be $2n+4$. As an application it follows from Higman's theorem that the Grothendieck algebra $\mathrm{Gr}(\mathscr{C})\otimes_{\mathbb{Z}} K$ over a field K is

收稿日期: 2017-01-18; 接受日期: 2017-03-30
基金项目: 国家自然科学基金资助项目 (11471282); 中国博士后科学基金资助项目 (2017M610316)

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 $\mathrm{Gr}(\mathscr{C})\otimes_{\mathbb{Z}} K$ explicitly.

Keywords Grothendieck ring; Verlinde modular category; Casimir number; Jacobson radical; Dickson polynomial
MR(2010) Subject Classification 16W10
Chinese Library Classification O153.3

1 引言

设 R 为整数环 $\mathbb{Z}$ 上的 Frobenius 代数. R 的 Casimir 理想与整数环 $\mathbb{Z}$ 的交为 $\mathbb{Z}$ 的主理想, 从而可以由一个非负整数生成. 该非负整数称为 Frobenius 代数 R 的 Casimir 数. Casimir 数可以用来描述域 K 上的 Frobenius 代数 $R\otimes_{\mathbb{Z}} K$ 的半单性: $R\otimes_{\mathbb{Z}} K$ 是半单代数当且仅当 R 上的 Casimir 数在域 K 中不为零 (见文 Higman 定理 [1, 定理 1] 或 [2, 命题 6]).

众所周知, fusion 范畴 $\mathscr{C}$ 的 Grothendieck 环 $\mathrm{Gr}(\mathscr{C})$ 为整数环 $\mathbb{Z}$ 上的 Frobenius 代数. 因此人们可以利用 Grothendieck 环 $\mathrm{Gr}(\mathscr{C})$ 的 Casimir 数来判定 Grothendieck 代数 $\mathrm{Gr}(\mathscr{C})\otimes_{\mathbb{Z}} K$ 的半单性. 这种方法已经被用来判定 fusion 范畴 $\mathscr{C}=\mathrm{Re}\,p(H)$ 的 Grothendieck 代数的半单性, 其中 H 为可裂半单 Hopf 代数 (见文 [2, 命题 22]).

对于秩为 $n+1$ 的一类特殊的 Verlinde 模性范畴 $\mathscr{C}$, 本文通过计算 Grothendieck 环 $\mathrm{Gr}(\mathscr{C})$ 上的 Casimir 数来判定 Grothendieck 代数 $\mathrm{Gr}(\mathscr{C})\otimes_{\mathbb{Z}} K$ 的半单性. 计算结果表明 $\mathrm{Gr}(\mathscr{C})$ 的 Casimir 数为 $2n+4$. 因此 $\mathrm{Gr}(\mathscr{C})\otimes_{\mathbb{Z}} K$ 是半单代数当且仅当 $2n+4$ 在域 K 中不为零. 另外, Grothendieck 代数 $\mathrm{Gr}(\mathscr{C})\otimes_{\mathbb{Z}} K$ 与多项式代数的商代数 $K[X]/(E_{n+1}(X))$ 同构, 其中 $E_{n+1}(X)$ 为第二类型的 $n+1$ 次 Dickson 多项式. 而 $K[X]/(E_{n+1}(X))$ 为半单代数当且仅当 $E_{n+1}(X)$ 在 $K[X]$ 中无重因式. 这为我们判定 $E_{n+1}(X)$ 有无重因式提供了一个充分必要条件: $E_{n+1}(X)$ 在 $K[X]$ 中无重因式当且仅当 $2n+4$ 在域 K 中不为零. 这一结果与第二类型的 Dickson 多项式的因式分解定理完全吻合 [3, 4]. 当 $2n+4$ 在域 K 中为零时, 借助于 Dickson 多项式的因式分解定理, 我们完全刻画了 Grothendieck 代数 $\mathrm{Gr}(\mathscr{C})\otimes_{\mathbb{Z}} K$ 的 Jacobson 根.

本文第 2 节简要介绍了整数环 $\mathbb{Z}$ 上的 Frobenius 代数与 Verlinde 模性范畴的一些基本结论; 第 3 节具体计算了一类特殊的 Verlinde 模性范畴上的 Grothendieck 环的 Casimir 数; 第 4 节利用所求 Casimir 数来判定 Verlinde 模性范畴的 Grothendieck 代数的半单性, 当 Grothendieck 代数不是半单代数时, 我们借助于 Dickson 多项式的因式分解定理完全刻画了 Grothendieck 代数的 Jacobson 根.

2 预备知识

本文所有范畴都是定义在代数闭域上, 有关 fusion 范畴的基本概念可见文 [5]. 符号 $\mathbb{Z}$ 与 $\mathbb{C}$ 分别代表整数环与复数域. 先介绍 Frobenius 代数有关结论. 设 R 为 $\mathbb{Z}$- 代数并且作为 $\mathbb{Z}$- 模是秩为 n 的自由模. 如果 R 上被赋予一个结合非退化的双线性型 $(-,-)$, 那么 R 称为 $\mathbb{Z}$ 上的 Frobenius 代数; 如果该双线性型还是对称的, 那么 R 称为 $\mathbb{Z}$ 上的对称代数 [2]. 设 $\{x_i\,|\,1\le i\le n\}$

与 $\{y_i\,|\,1\leq i\leq n\}$ 为 R 的两组 $\mathbb{Z}$- 基并且满足 $(x_i,y_j)=\delta_{ij}$, 其中 δ_{ij} 为 Kronecker 符号, 则集合 $\{x_i,y_i\,|\,1\leq i\leq n\}$ 称为 R 的一组对偶基. 此时 R 中任意元素 a 可以表示为

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

设 $Z(R)$ 为 R 的中心. 定义 $\mathbb{Z}$- 线性映射

$$c:R\to Z(R),\quad a\mapsto\sum_{i=1}^{n}y_iax_i,$$

该映射称为 R 的 Casimir 算子 (见文 [2, 3.1 节]). 由于对偶基 $\{x_i,y_i\,|\,1\leq i\leq n\}$ 仅仅依赖于双线性型 $(-,-)$ 的选取 (见文 [2, 1.2.2 节]), 因此 Casimir 算子 c 与对偶基 $\{x_i,y_i\,|\,1\leq i\leq n\}$ 的选取无关. R 的单位元 1 在 Casimir 算子 c 下的像 $c(1)$ 称为 R 的 Casimir 元. R 上的不同双线性型给出不同的 Casimir 元, 但是不同 Casimir 元之间彼此相差一个中心可逆元 (见文 [2, 1.2.5 节]). Casimir 算子 c 的像 $\mathrm{Im}c$ 为 $Z(R)$ 的理想, 该理想称为 R 的 Casimir 理想. 由文 [2, 3.2 节] 可知, R 的 Casimir 理想与 R 上双线性型的选取无关. Casimir 理想 $\mathrm{Im}c$ 与 $\mathbb{Z}$ 的交为某一非负整数生成的 $\mathbb{Z}$ 的主理想. 该非负整数称为 R 的 Casimir 数. 显然, R 的 Casimir 数与 R 上双线性型的选取无关.

我们再介绍一些 Verlinde 模性范畴的有关结果. 设 $\mathfrak{g}$ 为复数域 $\mathbb{C}$ 上的单李代数, n 为正整数, $q=\mathrm{e}^{\frac{\pi\mathrm{i}}{n+2}}$. 与偶对 $(\mathfrak{g},q)$ 匹配的 Verlinde 模性范畴 $\mathscr{C}(\mathfrak{g},q)$ 定义为 Lusztig 量子群 $U_q^L(\mathfrak{g})$ 的表示范畴的某种 "半单部分" (见文 [6] 或 [7, 8.12.2 节]). 本文仅仅考虑 $\mathfrak{g}=\mathfrak{sl}_2$ 情形. 我们把 Verlinde 模性范畴 $\mathscr{C}(\mathfrak{sl}_2,q)$ 简记为 $\mathscr{C}_n(q)$. 此时模性范畴 $\mathscr{C}_n(q)$ 中的单对象为 Lusztig 量子群 $\mathfrak{u}_q(\mathfrak{sl}_2)$ 的不可约表示 $X_0,X_1,\ldots,X_n$; 范畴 $\mathscr{C}_n(q)$ 中的张量积结构为 $\mathfrak{u}_q(\mathfrak{sl}_2)$ 的表示范畴中的张量积结构的 "截断", 即 $\mathfrak{u}_q(\mathfrak{sl}_2)$ 表示范畴中的张量积 $X_i\otimes X_j$ 模去所谓 "可除" 部分. 比如当 $n=1$ 时, $\mathscr{C}_1(q)=\mathrm{Vec}_{\mathbb{Z}/2\mathbb{Z}}^{\omega}$, 其中 ω 为 $\mathbb{Z}/2\mathbb{Z}$ 的非平凡 3- 上循环; 当 $n=2$ 时, $\mathscr{C}_2(q)$ 为 Ising 模性范畴 [8].

范畴 $\mathscr{C}_n(q)$ 的 Grothendieck 环 $\mathrm{Gr}(\mathscr{C}_n(q))$ 为文 [7, 例 4.10.6] 所述的截断 Verlinde 环, 其乘法结构为

$$X_iX_j=\sum_{l=\max\{i+j-n,0\}}^{\min\{i,j\}}X_{i+j-2l}. \tag{2.1}$$

在双线性型 $(X_i,X_j)=\delta_{ij}$ 下, 该 Grothendieck 环为 $\mathbb{Z}$ 上的对称 Frobenius 代数. 此时, 偶对 $\{X_i,X_i\,|\,0\leq i\leq n\}$ 构成 $\mathrm{Gr}(\mathscr{C}_n(q))$ 的一组对偶基.

Grothendieck 环 $\mathrm{Gr}(\mathscr{C}_n(q))$ 作为 $\mathbb{Z}$ 上的 Frobenius 代数, 其 Casimir 算子为

$$c(x)=\sum_{i=0}^{n}X_ixX_i,$$

其中, $x\in\mathrm{Gr}(\mathscr{C}_n(q))$. 注意到 $\mathrm{Gr}(\mathscr{C}_n(q))$ 为交换环, $c(x)=c(1)x$, 其中 $c(1)=\sum_{i=0}^{n}X_i^2$ 为 $\mathrm{Gr}(\mathscr{C}_n(q))$ 的 Casimir 元. 若非负整数 m 满足 $\mathbb{Z}\cap\mathrm{Im}\,c=(m)$, 则 m 为 Grothendieck 环 $\mathrm{Gr}(\mathscr{C}_n(q))$ 的 Casimir 数. 由于 Casimir 数为模性范畴 $\mathscr{C}_n(q)$ 的不变量, 即与 $\mathscr{C}_n(q)$ 张量等价的模性范畴具有相同的 Casimir 数, 因此也把 Grothendieck 环 $\mathrm{Gr}(\mathscr{C}_n(q))$ 的 Casimir 数称为模性范畴 $\mathscr{C}_n(q)$ 的 Casimir 数.

3 Casimir 数

本节计算 Verlinde 模性范畴 $\mathscr{C}_n(q)$ 的 Casimir 数. 首先给出 Casimir 元 $c(1)$ 的具体表达式.

引理 3.1 我们有 $c(1)=\sum_{j=0}^{[\frac{n}{2}]}(n+1-2j)X_{2j}$.

证明 直接计算可得

$$\begin{aligned}
c(1)&=\sum_{j=0}^{[\frac{n}{2}]}X_j^2+\sum_{j=[\frac{n}{2}]+1}^{n}X_j^2\\
&=\sum_{j=0}^{[\frac{n}{2}]}\sum_{l=0}^{j}X_{2j-2l}+\sum_{j=[\frac{n}{2}]+1}^{n}\sum_{l=2j-n}^{j}X_{2j-2l}\quad(\text{见 (2.1)})\\
&=\begin{cases}2(X_0+(X_0+X_2)+\cdots+(X_0+X_2+\cdots+X_{n-2}))\\ +(X_0+X_2+\cdots+X_n), & 2\mid n\\ 2(X_0+(X_0+X_2)+\cdots+(X_0+X_2+\cdots+X_{n-1})), & 2\nmid n\end{cases}\\
&=\sum_{j=0}^{[\frac{n}{2}]}(n+1-2j)X_{2j}.
\end{aligned}$$

证毕.

对于任意 $x\in\mathrm{Gr}(\mathscr{C}_n(q))$, 为了描述 $c(x)$ 的 $\mathbb{Z}$- 线性表达式, 需要做如下准备工作. 左乘变换 X_i 在基 $\{X_0,X_1,\ldots,X_n\}$ 下对应了一个矩阵 $\mathbf{X}_i$, 即

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

记 $\mathbf{E}_{i+1,j+1}$ 为 $n+1$ 阶矩阵单位: $(i+1,j+1)$- 元为 1, 其余元为 0, 则矩阵 $\mathbf{X}_i$ 可以描述如下

$$\begin{aligned}
\mathbf{X}_i&=\mathbf{E}_{1,i+1}+\mathbf{E}_{2,i+2}+\mathbf{E}_{3,i+3}+\cdots+\mathbf{E}_{n-i+1,n+1}\\
&\quad+\mathbf{E}_{2,i}+\mathbf{E}_{3,i+1}+\mathbf{E}_{4,i+2}+\cdots+\mathbf{E}_{n-i+2,n}\\
&\quad+\mathbf{E}_{3,i-1}+\mathbf{E}_{4,i}+\mathbf{E}_{5,i+1}+\cdots+\mathbf{E}_{n-i+3,n-1}+\cdots\\
&\quad+\mathbf{E}_{i+1,1}+\mathbf{E}_{i+2,2}+\mathbf{E}_{i+3,3}+\cdots+\mathbf{E}_{n+1,n-i+1}\\
&=\sum_{s=0}^{i}\sum_{t=0}^{n-i}\mathbf{E}_{s+t+1,i+t-s+1}.
\end{aligned}\tag{3.1}$$

对于任意整数 i, 如果 i 是偶数定义 $\delta(i)=1$; 如果 i 是奇数, 定义 $\delta(i)=0$.

命题 3.2 设 $x=\sum_{k=0}^{n}\lambda_kX_k$, 则 $c(x)$ 的线性表达式中 X_i 前面的系数为

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

证明 设 $X_jX_k=\sum_{i=0}^{n}N_{jk}^iX_i$, 则 $N_{jk}^i=(X_jX_k,X_i)=(X_iX_j,X_k)=N_{ij}^k$, 这是因为双线性型 $(-,-)$ 是结合对称的. 由此可得

$$c(x)=c(1)x=\sum_{j,k=0}^{n}(n+1-j)\delta(j)\lambda_kX_jX_k=\sum_{i,j,k=0}^{n}(n+1-j)\delta(j)\lambda_kN_{ij}^kX_i.$$

因此, $c(x)$ 的线性表达式中 X_i 前面的系数为 $\sum_{j,k=0}^{n}(n+1-j)\delta(j)\lambda_k N_{ij}^k$. 进一步, 该系数可以写成以下形式:

$$\begin{aligned}\sum_{j,k=0}^{n}(n+1-j)\delta(j)\lambda_k N_{ij}^k &= (\lambda_0,\lambda_1,\ldots,\lambda_n)\mathbf{X}_i\begin{pmatrix}(n+1)\delta(0)\\ n\delta(1)\\ \vdots\\ \delta(n)\end{pmatrix}\\ &= \sum_{s=0}^{i}\sum_{t=0}^{n-i}(\lambda_0,\lambda_1,\ldots,\lambda_n)\mathbf{E}_{s+t+1,i+t-s+1}\begin{pmatrix}(n+1)\delta(0)\\ n\delta(1)\\ \vdots\\ \delta(n)\end{pmatrix}\\ &= \sum_{s=0}^{i}\sum_{t=0}^{n-i}(n+1-i-t+s)\delta(i+t-s)\lambda_{s+t}. \end{aligned}\tag{3.2}$$

直接计算表明: 如果 $s+t=k\le i$, 那么 (3.2) 式中的系数 λ_k 为 $(n+1-i)(k+1)\delta(i+k)$; 如果 $s+t=k>i$, 那么 (3.2) 式中的系数 λ_k 为 $(i+1)(n-k+1)\delta(i+k)$. 因此 (3.2) 式即为

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

证毕.

本节主要结果表述如下.

定理 3.3　Verlinde 模性范畴 $\mathscr{C}_n(q)$ 的 Casimir 数为 $2n+4$.

证明　设 $x=\sum_{k=0}^{n}\lambda_k X_k$. 根据命题 3.2, $c(x)$ 的线性表达式中 X_i 前面的系数 α_i 为

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

其中 $0\le i\le n$. 如果 $c(x)\in\mathbb{Z}$, 那么 $\alpha_i=0$, 其中 $1\le i\le n$. 考虑以 $\lambda_0,\lambda_1,\ldots,\lambda_n$ 为变量的线性方程组:

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

直接求解可得 $\lambda_n=0$. 类似地, 求解线性方程组

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

并代入 $\lambda_n=0$, 解得 $\lambda_{n-1}=0$. 不断重复上述过程, 解得 $\lambda_n=\lambda_{n-1}=\cdots=\lambda_3=0$. 最后考虑线性方程组

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

代入 $\lambda_n=\lambda_{n-1}=\cdots=\lambda_3=0$, 解得 $\lambda_1=0$, $\lambda_0=-3\lambda_2$. 因此 X_0 前面的系数 α_0 为

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

我们证得 Verlinde 模性范畴 $\mathscr{C}_n(q)$ 的 Casimir 数为 $2n+4$.

注 3.4 矩阵 $\mathbf{X}_i$ 的极大非负特征值称为 X_i 的 Frobenius–Perron 维数, 记为 $\mathrm{FPdim}(X_i)$. 由文 [7, 习题 4.10.7] 可知

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

其中 $0\leq i\leq n$. Verlinde 模性范畴 $\mathscr{C}_n(q)$ 的 Frobenius–Perron 维数 $\mathrm{FPdim}(\mathscr{C}_n(q))$ 定义为

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

该式揭示了 Verlinde 模性范畴 $\mathscr{C}_n(q)$ 的 Casimir 数 $2n+4$ 与 $\mathscr{C}_n(q)$ 的 Frobenius–Perron 维数之间的关系. 该式也可以从如下角度加以解释: 由定理 3.3 知 $2n+4=c(1)x$, 其中 $x=3-X_2$. 用 FPdim 作用等式两边, 也可以得到 $2n+4=\mathrm{FPdim}(\mathscr{C}_n(q))\mathrm{FPdim}(x)=\mathrm{FPdim}(\mathscr{C}_n(q))(q-q^{-1})^2$.

4 Jacobson 根

由 Higman 定理知, 域 K 上的 Frobenius 代数是半单代数当且仅当 $1\in\mathrm{Im}\,c$ (可见文 [1, 定理 1]). 将 Higman 定理应用于 Grothendieck 代数 $\mathrm{Gr}(\mathscr{C}_n(q))\otimes_{\mathbb{Z}}K$, 得到如下命题:

命题 4.1 Grothendieck 代数 $\mathrm{Gr}(\mathscr{C}_n(q))\otimes_{\mathbb{Z}}K$ 是半单代数当且仅当 Casimir 数 $2n+4$ 在域 K 中不为零.

当 $2n+4$ 在域 K 中为零时, 我们来确定 Grothendieck 代数 $\mathrm{Gr}(\mathscr{C}_n(q))\otimes_{\mathbb{Z}}K$ 的 Jacobson 根. 先要确定 $\mathrm{Gr}(\mathscr{C}_n(q))\otimes_{\mathbb{Z}}K$ 的多项式表达式. 注意到第二类型的 Dickson 多项式可以通过如下递推关系定义:

$$E_0(X)=1,\quad E_1(X)=X,\quad E_{i+1}(X)=XE_i(X)-E_{i-1}(X),\quad \text{其中}\quad i\geq 1. \tag{4.1}$$

根据文 [4, 等式 (1.2)], 第 i 次 Dickson 多项式 $E_i(X)$ 可以展开成如下形式

$$E_i(X)=\sum_{j=0}^{[\frac{i}{2}]}\binom{i-j}{j}(-1)^jX^{i-2j},$$

其中 $[\frac{i}{2}]$ 表示不超过 $\frac{i}{2}$ 的最大整数.

设 $\mathbb{Z}[X]$ 是以 X 为变量的 $\mathbb{Z}$ 上的多项式环, $(E_{n+1}(X))$ 为 $\mathbb{Z}[X]$ 的以 $E_{n+1}(X)$ 为生成子的主理想. $\mathbb{Z}[X]$ 中的多项式 $f(X)$ 在典范同态 $\mathbb{Z}[X]\to\mathbb{Z}[X]/(E_{n+1}(X))$ 下的像记为 $\overline{f(X)}$.

引理 4.2 在 $\mathbb{Z}[X]/(E_{n+1}(X))$ 中, 有

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

其中 $0\leq i,j\leq n$.

证明 方便起见, 当 $s<0$ 时, 设 $E_s(X)=0$. 对 $i+j$ 用数学归纳法证明该引理. 这里仅仅证明 $0\leq i+j\leq n$ 情形, 对 $n\leq i+j\leq 2n$ 的情形类似可以证明. 显然 $i+j=0$ 时等式成立. 对于任意 $1\leq k\leq n-1$, 假设当 $1\leq i+j\leq k$ 时等式成立. 下面证明 $i+j=k+1$ 时等式仍然成立. 注意到 $(i-1)+j\leq k$ 并且 $(i-2)+j\leq k$, 对 $(i-1)+j\leq k$ 以及 $(i-2)+j\leq k$ 利用归纳假设得到:

$$\overline{E_{i-1}(X)E_j(X)}=\sum_{l=\max\{i-1+j-n,0\}}^{\min\{i-1,j\}}\overline{E_{i-1+j-2l}(X)}, \tag{4.2}$$

$$\overline{E_{i-2}(X)E_j(X)} = \sum_{l=\max\{i-2+j-n,0\}}^{\min\{i-2,j\}} \overline{E_{i-2+j-2l}(X)}. \tag{4.3}$$

考虑 $\mathbb{Z}[X]/(E_{n+1}(X))$ 中的乘积 $\overline{XE_{i-1}(X)E_j(X)}$. 一方面, 根据 (4.2) 有

$$\begin{aligned}\overline{XE_{i-1}(X)E_j(X)} &= \overline{X} \sum_{l=\max\{i-1+j-n,0\}}^{\min\{i-1,j\}} \overline{E_{i-1+j-2l}(X)} \\ &= \sum_{l=\max\{i-1+j-n,0\}}^{\min\{i-1,j\}} (\overline{E_{i+j-2l}(X)} + \overline{E_{i-2+j-2l}(X)}) \quad (\text{见 } (4.1)).\end{aligned}$$

另一方面, 根据 (4.3) 有

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

因此

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

对 $i-1<j$, $i-1=j$ 以及 $i-1>j$ 三种情形分别加以讨论, 都能得到

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

证毕.

定理 4.3 Grothendieck 环 $\mathrm{Gr}(\mathscr{C}_n(q))$ 与商环 $\mathbb{Z}[X]/(E_{n+1}(X))$ 同构.

证明 考虑如下 $\mathbb{Z}$- 线性映射

$$\theta: \mathrm{Gr}(\mathscr{C}_n(q)) \to \mathbb{Z}[X]/(E_{n+1}(X)), \quad X_i \mapsto \overline{E_i(X)}, \quad 0 \le i \le n.$$

由引理 4.2 知该映射为环满同态. 下面验证该映射是单射, 设 $\sum_{i=0}^n \lambda_i \overline{E_i(X)} = 0$, 则存在多项式 $f(X) \in \mathbb{Z}[X]$, 使得

$$\sum_{i=0}^n \lambda_i E_i(X) = E_{n+1}(X) f(X).$$

比较等式两边多项式的次数可知 $f(X)=0$, 因此对于任意 $0 \le i \le n$, 都有 $\lambda_i = 0$. 证毕.

Dickson 多项式的因式分解早在文 [3, 4] 中就有研究. 根据定理 4.3, 得到如下 Dickson 多项式 $E_{n+1}(X)$ 在 $K[X]$ 中有无重因式的一个判定. 该判定与文 [3, 4] 中 Dickson 多项式因式分解有关结果完全吻合.

命题 4.4 第二类型的 $n+1$ 次 Dickson 多项式 $E_{n+1}(X)$ 在 $K[X]$ 中无重因式当且仅当 $2n+4$ 在域 K 中不为零.

证明 由定理 4.3 知 $\mathrm{Gr}(\mathscr{C}_n(q)) \otimes_{\mathbb{Z}} K \cong K[X]/(E_{n+1}(X))$. 根据命题 4.1, $2n+4$ 在域 K 中不为零当且仅当 $K[X]/(E_{n+1}(X))$ 为半单代数, 当且仅当 $E_{n+1}(X)$ 在 $K[X]$ 中无重因式. 证毕.

下面考虑 $2n+4$ 在域 K 中为零时, Grothendieck 代数 $\mathrm{Gr}(\mathscr{C}_n(q))\otimes_{\mathbb{Z}} K$ (或多项式的商代数 $K[X]/(E_{n+1}(X)))$ 的 Jacobson 根. 注意到 $K[X]$ 是主理想整环, $K[X]$ 的每一个素理想都是极大理想, 因此 $K[X]/(E_{n+1}(X))$ 的 Jacobson 根是 $E_{n+1}(X)$ 中互不相同的不可约因式的乘积在商代数 $K[X]/(E_{n+1}(X))$ 中生成的主理想.

命题 4.5 设域 K 的特征为 $p>2$. 如果 $p\,|\,2n+4$, 记 $n+2=p^r(m+1)$, 其中 $(p,m+1)=1$, 则 $K[X]/(E_{n+1}(X))$ 的 Jacobson 根为 $\overline{E_m(X)(X^2-4)}$ 生成的主理想.

证明 由文 [3, 3 节] 知, Dickson 多项式 $E_{n+1}(X)$ 在 $K[X]$ 中有因式分解

$$E_{n+1}(X)=E_m(X)^{p^r}(X^2-4)^{\frac{p^r-1}{2}},$$

其中 Dickson 多项式 $E_m(X)$ 在 $K[X]$ 中无重因式 (见命题 4.4). 因此 $E_m(X)(X^2-4)$ 为 $E_{n+1}(X)$ 中互不相同的不可约因式的乘积, 从而 $K[X]/(E_{n+1}(X))$ 的 Jacobson 根为 $\overline{E_m(X)(X^2-4)}$ 生成的主理想. 证毕.

设域 K 的特征为 2. 如果 m 为偶数, 由文 [3, 定理 6] 知 $E_m(X)=F_m(X)^2$, 其中

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

为 $K[X]$ 中一些互不相同的不可约因式的乘积.

命题 4.6 设域 K 的特征为 2.

(1) 如果 $n+1$ 为偶数, $K[X]/(E_{n+1}(X))$ 的 Jacobson 根为 $\overline{F_{n+1}(X)}$ 生成的主理想.

(2) 如果 $n+1$ 为奇数, 记 $n+2=2^r(m+1)$, 其中 m 为偶数, 则 $K[X]/(E_{n+1}(X))$ 的 Jacobson 根为 $\overline{XF_m(X)}$ 生成的主理想.

证明 (1) 如果 $n+1$ 为偶数, 那么 $F_{n+1}(X)$ 为 $E_{n+1}(X)$ 中所有互不相同的不可约因式的乘积 (见文 [3, 定理 6]). 因此 $K[X]/(E_{n+1}(X))$ 的 Jacobson 根为 $\overline{F_{n+1}(X)}$ 生成的主理想.

(2) 如果 $n+1$ 为奇数, 记 $n+2=2^r(m+1)$, 其中 $r\geq 1$ 且 m 为偶数. 由文 [3, 3 节] 知

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

因此, $XF_m(X)$ 为 $E_{n+1}(X)$ 中所有互不相同的不可约因式的乘积, $K[X]/(E_{n+1}(X))$ 的 Jacobson 根为 $\overline{XF_m(X)}$ 生成的主理想. 证毕.

参 考 文 献

[1] Higman D. G., On orders in separable algebras, *Canad. J. Math.*, 1955, **7**: 509–515.

[2] Lorenz M., Some applications of Frobenius algebras to Hopf algebras, *Contemp. Math.*, 2011, **537**: 269–289.

[3] Bhargava M., Zieve M. E., Factoring Dickson polynomials over finite fields, *Finite Fields Appl.*, 1999, **5**(2): 103–111.

[4] Chou W. S., The factorization of Dickson polynomials over finite fields, *Finite Fields Appl.*, 1997, **3**: 84–96.

[5] Etingof P., Nikshych D., Ostrik V., On fusion categories, *Annals of Mathematics*, 2005, **162**: 581–642.

[6] Bakalov B., Kirillov A. A., Lectures on Tensor Categories and Modular Functors, University Series Lectures, Vol. **21**, AMS, 2001.

[7] Etingof P., Gelaki S., Nikshych D., Ostrik V., Tensor Categories, Mathematical Surveys and Monographs, **205**, AMS, 2015.

[8] Drinfeld V., Gelaki S., Nikshych D., Ostrik V., On braided fusion categories I, *Selecta Mathematica* (*N. S.*), 2010, **16**: 1–119.