Journal of Mathematical Research & Exposition
Nov., 2011, Vol. 31, No. 6, pp. 997–1002
DOI:10.3770/j.issn:1000-341X.2011.06.005
Http://jmre.dlut.edu.cn

Modular Vector Invariants of Cyclic Groups Z_2

Ji Zhu NAN*, Hui Fang ZHAO
School of Mathematical Sciences, Dalian University of Technology, Liaoning 116024*, P. R. China*

Abstract Let G be the finite cyclic group Z_2 and V be a vector space of dimension $2n$ with basis $x_1,\dots,x_n,y_1,\dots,y_n$ over the field F with characteristic 2. If σ denotes a generator of G, we may assume that $\sigma(x_i)=ay_i$, $\sigma(y_i)=a^{-1}x_i$, where $a\in F^*$. In this paper, we describe the explicit generator of the ring of modular vector invariants of $F[V]^G$. We prove that

$$F[V]^G=F[l_i=x_i+ay_i, q_i=x_iy_i, 1\le i\le n, M_I=X_I+a^{|I|}Y_I],$$

where $I\subseteq A_n=\{1,2,\dots,n\}$, $2\le |I|\le n$.

Keywords finite cyclic group; invariant ring; modular vector invariants.

Document code A
MR(2010) Subject Classification 13A50
Chinese Library Classification O152

1. Introduction

Let G be a finite group, V be a finite dimensional vector space over a field F and $G\le GL(V)$. Let $F[V]$ be the symmetric algebra of V^*, the dual of V. If we choose a basis, $x_1,\dots,x_n$, for V^*, then we can identify $F[V]$ with the polynomial ring $F[x_1,\dots,x_n]$. The action of G on V induces an action on V^* which extends to an action by algebra automorphisms on the symmetric algebra $F[V]$. Specifically, for $g\in G$, $f\in F[V]$ and $v\in V$, $(g\cdot f)(v)=f(g^{-1}\cdot v)$. The ring of invariants of G is the subring of $F[V]$ given by

$$F[V]^G:=\{f\in F[V]\mid g\cdot f=f \ \text{ for all } \ g\in G\}.$$

If G is a finite group and $|G|$ is not invertible in F, then we say the representation of G on V is modular. If $|G|$ is invertible in F, then V is called a non-modular representation. In the non-modular representation case, Noether [1, 2] proved that the ring of invariants of G is generated by polynomials of degree less than or equal to $|G|$. The result does not hold for modular representation. In particular, the case of "vector invariants" is difficult over finite fields [3, 4]. Next we explain what is meant by this term [5].

Let $\sigma: G\to GL(n;F)$ be a faithful representation of a finite group. Set $\sigma_1=\sigma$ and define

$$\sigma_2: G\to GL(2n;F),$$

Received May 7, 2010; Accepted October 3, 2010
Supported by the National Natural Science Foundation of China (Grant No. 10771023).
* Corresponding author
E-mail address: jznan@163.com (J. Z. NAN); zhf3002@163.com (H. F. ZHAO)

afforded by the block matrices

$$\sigma_2(g) = \begin{pmatrix} \sigma_1 & 0 \\ 0 & \sigma_1 \end{pmatrix}.$$

Iteratively we define

$$\begin{aligned} \sigma_k : & G \to \mathrm{GL}(kn; F), \\ & g \mapsto \mathrm{diag}(\sigma_1(g), \ldots, \sigma_1(g)). \end{aligned}$$

Then σ_k is the k-fold vector representation of σ. The corresponding ring of invariants is called the ring of vector invariants.

For the rest of the paper, let F denote a field with characteristic 2, and let

$$x_1, \ldots, x_n, y_1, \ldots, y_n$$

denote commuting indeterminates. Define the representation

$$\sigma : Z_2 \to \mathrm{GL}(2; F)$$

afforded by the matrices

$$\begin{pmatrix} 0 & a \\ a^{-1} & 0 \end{pmatrix},$$

where $a \in F^*$. For a positive integer n, let $\sigma_n : Z_2 \to \mathrm{GL}(2n; F)$ be the n-fold direct sum $\sigma \oplus \cdots \oplus \sigma$.

In this paper, we prove that the ring of vector invariants $F[x_1, \ldots, x_n, y_1, \ldots, y_n]^{Z_2}$ is generated by

$$\{l_i = x_i + ay_i, q_i = x_i y_i, 1 \le i \le n, M_I = X_I + a^{|I|} Y_I, I \subseteq A_n, 2 \le |I| \le n\},$$

where $A_n = \{1, 2, \ldots, n\}$, $I \subseteq A_n$, and

$$M_I = X_I + a^{|I|} Y_I = x_{i_1} x_{i_2} \cdots x_{i_{|I|}} + a^{|I|} y_{i_1} y_{i_2} \cdots y_{i_{|I|}}.$$

For example, $M_{12} = x_1 x_2 + a^2 y_1 y_2$. If $I = \{i\}$, then $M_I = l_i$, for $1 \le i \le n$.

2. The structure of invariant ring $F[x_1, \ldots, x_k, y_1, \ldots, y_k]^{Z_2}$

We begin with the simplest case.

Example 1 For $\sigma_2 : Z_2 \to \mathrm{GL}(4, F)$, it is easy to verify that $\{l_i = x_i + ay_i, q_i = x_i y_i, i = 1, 2\}$ is a set of invariants. Especially, the quadratic form $x_1 x_2 + a^2 y_1 y_2$ is also an invariant. So

$$F[x_1, x_2, y_1, y_2]^{Z_2} \supseteq F[l_i = x_i + ay_i, q_i = x_i y_i, i = 1, 2, M_{12} = x_1 x_2 + a^2 y_1 y_2].$$

In fact, other invariant quadratic forms,

$$x_1 y_2 + y_1 x_2 = a^{-1}(l_1 l_2 - M_{12})$$

and

$$x_i^2 + a^2 y_i^2 = (l_i)^2 - 2aq_i, \quad i = 1, 2$$

are all in $F[l_i = x_i + ay_i, q_i = x_i y_i, i = 1, 2, M_{12} = x_1 x_2 + a^2 y_1 y_2]$.

Example 2 Consider $\sigma_3 : Z_2 \to \mathrm{GL}(6, F)$. It is obvious that

$$\begin{aligned} &F[l_i = x_i + ay_i, q_i = x_iy_i, i = 1, 2, 3, M_{ij} = x_ix_j + a^2y_iy_j, 1 \leq i < j \leq 3] \\ &\quad \subseteq F[x_1, x_2, x_3, y_1, y_2, y_3]^{Z_2}. \end{aligned}$$

Similarly to Example 1, other invariant quadratic forms $x_iy_j + y_ix_j$ $(1 \leq i < j \leq 3)$ and $x_i^2 + a^2y_i^2$ $(i = 1, 2, 3)$ can be generated by these invariants.

Unfortunately, for cubic invariant polynomials, analogously to the example given by Neusel in [6], we find that there is a relation between the invariants, i.e.,

$$l_1M_{23} + l_2M_{13} + l_3M_{12} = l_1l_2l_3 + 2(x_1x_2x_3 + a^3y_1y_2y_3). \tag{1}$$

It follows that in the case of characteristic 2 the cubic form $x_1x_2x_3 + a^3y_1y_2y_3$ is not in

$$F[l_i = x_i + ay_i, q_i = x_iy_i, i = 1, 2, 3, M_{ij} = x_ix_j + a^2y_iy_j, 1 \leq i < j \leq 3].$$

Therefore the algebra of invariants $F[x_1, x_2, x_3, y_1, y_2, y_3]^{Z_2}$ contains an indecomposable cubic form $x_1x_2x_3 + a^3y_1y_2y_3$.

Lemma 1 *Let $A_n = \{1, 2, \ldots, n\}$, $I \subseteq A_n$, and $M_I = X_I + a^{|I|}Y_I$. Then we have*

$$\sum_{|I|=1, I\subseteq A_n}^{[\frac{n}{2}]} M_IM_{A_n\setminus I} = l_1l_2\cdots l_n + (2^{n-1} - 2)(x_1x_2\cdots x_n + a^ny_1y_2\cdots y_n).$$

Proof This equation can be easily verified. □

For example, for $n = 4$, we have

$$\begin{aligned} \sum_{|I|=1, I\subseteq A_n}^{[\frac{n}{2}]} M_IM_{A_n\setminus I} &= l_1M_{234} + l_2M_{134} + l_3M_{124} + l_4M_{123} + M_{12}M_{34} + M_{13}M_{24} + M_{14}M_{23} \\ &= l_1l_2l_3l_4 + 6(x_1x_2x_3x_4 + a^4y_1y_2y_3y_4). \end{aligned}$$

Theorem 1 *The algebra of invariants $F[x_1, \ldots, x_n, y_1, \ldots, y_n]^{Z_2}$ contains an indecomposable form of degree n for $n \geq 3$.*

Proof We show that by induction on n. For $n = 3$, it is obvious by Example 2. Assume that the conclusion is true for $n = k - 1$. By the hypothesis, suppose that we have got a formula similar to (1),

$$f_{12\cdots(k-1)} = c_1l_1l_2\cdots l_{k-1} + c_2(x_1x_2\cdots x_{k-1} + a^{k-1}y_1y_2\cdots y_{k-1}), \tag{2}$$

where $f_{12\cdots(k-1)}$ is the sum of the product of $l_{i_1}l_{i_2}\cdots l_{i_{|I|}}$ and $M_{A_{k-1}\setminus I}$ for $I \subset A_{k-1}$, and c_1, c_2 are two constants. Iteratively, for $n = k$, we also have

$$f_{1\cdots(k-2)k} = c_1l_1\cdots l_{k-2}l_k + c_2(x_1\cdots x_{k-2}x_k + a^{k-1}y_1\cdots y_{k-2}y_k), \tag{3}$$

$$\cdots$$

$$f_{23\cdots k} = c_1l_2l_3\cdots l_k + c_2(x_2x_3\cdots x_k + a^{k-1}y_2y_3\cdots y_k). \tag{4}$$

Multiplying both sides of the above equality (2) by l_k, equality (3) by $l_{k-1}, \ldots$, equality (4) by l_1, and summing up both sides of these equalities, we have

$$\begin{aligned} &f_{12\cdots(k-1)}l_k + f_{1\cdots(k-2)k}l_{k-1} + \cdots + f_{23\cdots k}l_1 \\ &\quad = (kc_1)l_1l_2\cdots l_k + c_2(l_1M_{23\cdots k} + l_2M_{13\cdots k} + \cdots + l_kM_{12\cdots k-1}). \end{aligned}$$

Then summing up both sides of the above equality by

$$(c_2+1)\sum_{|I|=2}^{[\frac{k}{2}]} M_I M_{A_k\setminus I} + (l_1M_{23\cdots k} + l_2M_{13\cdots k} + \cdots + l_kM_{12\cdots k-1}),$$

by Lemma 1 we obtain

$$\begin{aligned} &f_{12\cdots(k-1)}l_k + f_{1\cdots(k-2)k}l_{k-1} + \cdots + f_{23\cdots k}l_1 + (c_2+1)\sum_{|I|=2}^{[\frac{k}{2}]} M_I M_{A_k\setminus I} + \\ &\quad (l_1M_{23\cdots k} + l_2M_{13\cdots k} + \cdots + l_kM_{12\cdots k-1}) \\ &= (kc_1)l_1l_2\cdots l_k + (c_2+1)\sum_{|I|=1}^{[\frac{k}{2}]} M_I M_{A_k\setminus I} \\ &= (kc_1+c_2+1)l_1l_2\cdots l_k + (c_2+1)(2^{k-1}-2)(x_1x_2\cdots x_k + a^{k-1}y_1y_2\cdots y_k), \end{aligned}$$

where $(c_2+1)(2^{k-1}-2)$ is even. Therefore, in the case of characteristic 2 the algebra of invariants $F[x_1, \ldots, x_k, y_1, \ldots, y_k]^{Z_2}$ contains an indecomposable form of degree k, namely

$$x_1x_2\cdots x_k + a^k y_1y_2\cdots y_k,$$

and the result follows. □

Theorem 2 *For $\sigma_n : Z_2 \to \mathrm{GL}(2n, F)$, $n \geq 2$, the invariants of degree m (≥ 1) can be generated by*

$$\{l_i = x_i + ay_i, 1 \leq i \leq n, q_i = x_iy_i, 1 \leq i \leq n, M_I = X_I + a^{|I|}Y_I, I \subseteq A_n, 2 \leq |I| \leq n\}.$$

Proof Since the action of G on $F[V]$ sends monomials to monomials, $F[V]^{Z_2}$ has an F-basis consisting of orbit sums of monomials [7]. If $X^AY^B \in F[V]$ is a monomial, where $A = \{a_1, a_2, \ldots, a_n\}$, $B = \{b_1, b_2, \ldots, b_n\}$, then the orbit sum of its Z_2-orbit is

$$S(X^AY^B) = \begin{cases} X^AY^B + a^{\sum(a_i-b_i)}X^AY^B, & \text{if } A \neq B, \\ X^CY^C, & \text{if } A = B = C, \end{cases}$$

where $C = \{c_1, c_2, \ldots, c_n\}$. Obviously, $X^CY^C = \prod(x_iy_i)^{c_i}$. It suffices to show that

$$X^AY^B + a^{\sum(a_i-b_i)}Y^AX^B \in F[l_i, q_i, 1 \leq i \leq n, M_I, I \subseteq A_n, 2 \leq |I| \leq n].$$

Let

$$\begin{aligned} &X^AY^B + a^{\sum(a_i-b_i)}Y^AX^B \\ &\quad = x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}y_1^{b_1}y_2^{b_2}\cdots y_n^{b_n} + a^{\sum(a_i-b_i)}y_1^{a_1}y_2^{a_2}\cdots y_n^{a_n}x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}, \end{aligned}$$

where $\sum_{i=1}^n(a_i+b_i) = m$. We give the proof by induction on m. $m = 1$ is trivial. Suppose the conclusion is true for positive integer less than m. Denote $I = \{i \mid a_i \neq 0, 1 \leq i \leq n\}$, $J = \{j \mid b_j \neq 0, 1 \leq j \leq n\}$. There are several cases to consider.

(a) $I \cap J \neq \phi$, i.e., there is at least an i such that $a_i \neq 0$, $b_i \neq 0$. Suppose $a_i \geq b_i$, then

$$\begin{aligned} X^A Y^B + a^{\sum(a_i-b_i)} Y^A X^B =& (x_i y_i)^{b_i} (x_1^{a_1} \cdots x_{i-1}^{a_{i-1}} x_i^{a_i-b_i} \cdots x_n^{a_n} y_1^{b_1} \cdots y_{i-1}^{b_{i-1}} y_{i+1}^{b_{i+1}} \cdots y_n^{b_n} + \\ & a^{\sum(a_i-b_i)} y_1^{a_1} \cdots y_{i-1}^{a_{i-1}} y_i^{a_i-b_i} \cdots y_n^{a_n} x_1^{b_1} \cdots x_{i-1}^{b_{i-1}} x_{i+1}^{b_{i+1}} \cdots x_n^{b_n}). \end{aligned}$$

(b) $I \neq \phi$, $J \neq \phi$, but $I \cap J = \phi$. For example, $I = \{1\}$, $J = \{2\}$, suppose $a_1 \geq b_2$. If $a_1 = b_2 = 1$, then $x_1 y_2 + y_1 x_2 = l_1 l_2 - M_{12}$. So we may assume $a_1 \geq 2$, then we have

$$\begin{aligned} x_1^{a_1} y_2^{b_2} + a^{a_1-b_2} y_1^{a_1} x_2^{b_2} =& (x_1 + a y_1)(x_1^{a_1-1} y_2^{b_2} + a^{a_1-b_2-1} y_1^{a_1-1} x_2^{b_2}) - \\ & (x_1 y_1)(a x_1^{a_1-2} y_2^{b_2} + a^{a_1-b_2-1} y_1^{a_1-2} x_2^{b_2}). \end{aligned}$$

(c) $I \neq \phi$, $J = \phi$(or $I = \phi$, $J \neq \phi$). If $a_i = 1$ for all $i \in I$, the case is trivial, for the invariant is just M_I. So without loss of generality we may assume that there exists an i such that $a_i \geq 2$. It follows that

$$\begin{aligned} X^A Y^B + a^{\sum(a_i-b_i)} Y^A X^B =& x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} + a^m y_1^{a_1} y_2^{a_2} \cdots y_n^{a_n} \\ =& (x_i + a y_i)(x_1^{a_1} \cdots x_i^{a_i-1} \cdots x_n^{a_n} + a^{m-1} y_1^{a_1} \cdots y_i^{a_i-1} \cdots y_n^{a_n}) - \\ & (x_i y_i)(a x_1^{a_1} \cdots x_i^{a_i-2} \cdots x_n^{a_n} + a^{m-1} y_1^{a_1} \cdots y_i^{a_i-2} \cdots y_n^{a_n}). \end{aligned}$$

By the hypothesis, we prove that $X^A Y^B + a^{\sum(a_i-b_i)} Y^A X^B$ can be generated by

$$\{l_i = x_i + a y_i, 1 \leq i \leq n, q_i = x_i y_i, 1 \leq i \leq n, M_I = X_I + a^{|I|} Y_I, I \subseteq A_n, 2 \leq |I| \leq n\}. \quad \Box$$

This allows us to obtain the desired result.

Theorem 3 *Let $\sigma_n : Z_2 \to \mathrm{GL}(2n, F)$ be the representation of cyclic group Z_2 over the field F of characteristic 2, where $n \geq 2$. Then the ring of vector invariants*

$$F[x_1, \ldots, x_n, y_1, \ldots, y_n]^{Z_2} = F[l_i, q_i, 1 \leq i \leq n, M_I, I \subseteq A_n, 2 \leq |I| \leq n]. \quad \Box$$

In addition to the algebra of invariants $F[V]^G$, another basic object of study in invariant theory is the algebra of coinvariants.

Definition 1 ([6]) *Let $\rho : G \to \mathrm{GL}(n, F)$ be a representation of a finite group G over the field F. The ring, or algebra, of coinvariants, denoted by $F[V]_G$, is the quotient of $F[V]$ by the ideal generated by the invariant polynomials of positive degree.*

Corollary 1 *The algebra of coinvariants $F[x_1, \ldots, x_n, y_1, \ldots, y_n]_{Z_2} = F[x_1, \ldots, x_n]$.*

Proof From Theorem 3 the result can be easily derived. □

Remark 1 Let $a = 1$. Then the representation of Z_2 is just the permutation representation. For this case we have

$$F[V]^G = F[l_i = x_i + y_i, q_i = x_i y_i, 1 \leq i \leq n, M_I = X_I + Y_I],$$

where $I \subseteq A_n = \{1, 2, \ldots, n\}$, $2 \leq |I| \leq n$. The conclusion coincides with the result of Richman [8].

References

[1] NOETHER E. *Der Endlichkeitssatz der Invarianten endlicher Gruppen* [J]. Math. Ann., 1915, **77**(1): 89–92. (in German)

[2] NOETHER E. *Der endlichkeitssatz der invarianten endlicher linearer Gruppen der characteristik p* [J]. Nachr. Akad. Wiss. Göttingen, 1926, 28–35. (in German)

[3] RICHMAN D R. *On vector invariants over finite fields* [J]. Adv. Math., 1990, **81**(1): 30–65.

[4] CAMPBELL H E A, HUGHES I P. *Vector invariants of $U_2(\mathbf{F}_p)$: a proof of a conjecture of Richman* [J]. Adv. Math., 1997, **126**(1): 1–20.

[5] NEUSEL M D. *Invariant Theory* [M]. American Mathematical Society, Providence, RI, 2007.

[6] NEUSEL M D, SMITH L. *Invariant Theory of Finite Groups* [M]. American Mathematical Society, Providence, RI, 2002.

[7] SMITH L. *Polynomial Invariants of Finite Groups* [M]. A K Peters, Ltd., Wellesley, MA, 1995.

[8] RICHMAN D R. *Explicit generators of the invariants of finite groups* [J]. Adv. Math., 1996, **124**(1): 49–76.