Geometry & Topology Monographs 11 (2007) 107–140

Mùi invariants and Milnor operations

MASAKI KAMEKO
MAMORU MIMURA

We describe Mùi invariants in terms of Milnor operations and give a simple proof for Mùi's theorem on rings of invariants of polynomial tensor exterior algebras with respect to the action of finite general linear groups. Moreover, we compute some rings of invariants of Weyl groups of maximal non-toral elementary abelian p–subgroups of exceptional Lie groups.

55R40; 55S10

1 Introduction

Let p be a fixed odd prime, q the power of p and $\mathbb{F}_q$ the finite field of q elements. Let

$$P_n = \mathbb{F}_q[x_1, \dots, x_n]$$

be the polynomial algebra in n variables $x_1, \dots, x_n$ over the finite field $\mathbb{F}_q$. Let

$$E_n^r = \Lambda^r(dx_1, \dots, dx_n)$$

be the r^{th} component of the exterior algebra of $dx_1, \dots, dx_n$ over the finite field $\mathbb{F}_q$ and let

$$E_n = \bigoplus_{r=0}^{n} E_n^r$$

be the exterior algebra of $dx_1, \dots, dx_n$ over $\mathbb{F}_q$. Let

$$P_n \otimes E_n$$

be the polynomial tensor exterior algebra in n variables $x_1, \dots, x_n$ over the finite field $\mathbb{F}_q$. The general linear group $GL_n(\mathbb{F}_q)$ and the special linear group $SL_n(\mathbb{F}_q)$ act on both the polynomial algebra P_n and the polynomial tensor exterior algebra $P_n \otimes E_n$. In [4], the ring of invariants of the polynomial algebra is determined by Dickson. In [7], Mùi determined the ring of invariants of the polynomial tensor exterior algebra and described the invariants in terms of determinants.

Published: 14 November 2007 DOI: 10.2140/gtm.2007.11.107

In the first half of this paper, we describe the invariants in terms of Milnor operations and give a simpler proof for Mùi's theorem. With the notation in Section 2, we may state Mùi's theorems.

Theorem 1.1 (Mùi) *The ring of invariants of the polynomial tensor exterior algebra $P_n \otimes E_n$ with respect to the action of the special linear group $SL_n(\mathbb{F}_q)$ is a free ${P_n}^{SL_n(\mathbb{F}_q)}$–module with the basis $\{1, Q_I dx_1 \dots dx_n\}$, where I ranges over A'_n.*

Theorem 1.2 (Mùi) *The ring of invariants of the polynomial tensor exterior algebra $P_n \otimes E_n$ with respect to the action of the general linear group $GL_n(\mathbb{F}_q)$ is a free ${P_n}^{GL_n(\mathbb{F}_q)}$–module with the basis $\{1, e_n^{q-2} Q_I dx_1 \dots dx_n\}$, where I ranges over A'_n.*

The invariant $Q_{i_1} \dots Q_{i_{n-r}} dx_1 \dots dx_n$ in Theorem 1.1 and Theorem 1.2 above is, up to sign, the same as the Mùi invariant $[r\colon i_1, \dots, i_{n-r}]$ in [7]. The first half of this paper has some overlap with M C Crabb's work [3]. However, our point of view on Mùi invariants seems to be different from his.

The second half of this paper is a sequel to the authors' work in [6] on the invariant theory of Weyl groups of maximal non-toral elementary abelian p–subgroup A of simply connected exceptional Lie groups. For p odd prime, up to conjugation, there are only 6 of them, for $p = 3$, $A = E^3_{F_4}$, $E^4_{3E_6}$, $E^4_{2E_7}$, $E^{5a}_{E_8}$, $E^{5b}_{E_8}$ and for $p = 5$, $A = E^3_{E_8}$. They and their Weyl groups are described by Andersen et al [1]. We computed the polynomial part of the invariants of Weyl groups except for the case $p = 3$, $A = E^{5b}_{E_8}$ as described by the authors [6]. In this paper, we compute rings of invariants of polynomial tensor exterior algebras with respect to the action of Weyl groups except for the case $p = 3$, $A = E^{5b}_{E_8}$.

In Section 2, we set up the notation used in the above theorems. In Section 3, we prove Theorem 1.1 and Theorem 1.2. In Section 4, we state Theorem 4.2 and using this theorem, we compute rings of invariants of Weyl groups of maximal non-toral elementary abelian p–subgroups of simply connected exceptional Lie groups. In Section 5, we prepare for the proof of Theorem 4.1 and Theorem 4.2. In Section 6, we prove Theorem 4.1. In Section 7, we prove Theorem 4.2. In Appendix A, we prove that the invariant $Q_{i_1} \dots Q_{i_{n-r}} dx_1 \dots dx_n$ in Theorem 1.1 and Theorem 1.2 above is, up to sign, equal to the Mùi invariant $[r\colon i_1, \dots, i_{n-r}]$.

We thank N Yagita for informing us that a similar description of Mùi invariants to the above form is also known to him.

2 Preliminaries

Let K_n be the field of fractions of P_n. For a finite set $\{y_1, \ldots, y_r\}$, we denote by $\mathbb{F}_q\{y_1, \ldots, y_r\}$ the $\mathbb{F}_q$–vector space spanned by $\{y_1, \ldots, y_r\}$. Let $GL_n(\mathbb{F}_q)$ be the set of $n \times n$ invertible matrices with coefficients in $\mathbb{F}_q$. We denote by $M_{m,n}(\mathbb{F}_q)$ the set of $m \times n$ matrices with coefficients in $\mathbb{F}_q$. In this paper, we consider the contragredient action of the finite general linear group, that is, for $g \in GL_n(\mathbb{F}_q)$, we define the action of g on $P_n \otimes E_n$ by

$$gx_i = \sum_{j=1}^{n} a_{i,j}(g^{-1})x_j, \quad gdx_i = \sum_{j=1}^{n} a_{i,j}(g^{-1})dx_j,$$

for $i = 1, \ldots, n$ and

$$g(x \cdot y) = g(x) \cdot g(y),$$

for x, y in $P_n \otimes E_n$, where $a_{i,j}(g^{-1})$ is the entry (i, j) in the matrix g^{-1}. For x_i, dx_i in the polynomial tensor exterior algebra $P_n \otimes E_n$, we define cohomological degrees of x_i, dx_i by $\deg x_i = 2$, $\deg dx_i = 1$ for $i = 1, \ldots, n$ and we consider $P_n \otimes E_n$ as a graded $\mathbb{F}_q$–algebra.

Now, we recall Milnor operations Q_j for $j = 0, 1, \ldots$. The exterior algebra

$$\Lambda(Q_0, Q_1, Q_2, \ldots)$$

over $\mathbb{F}_q$, generated by Milnor operations, acts on the polynomial tensor exterior algebra $P_n \otimes E_n$ as follows; the Milnor operation Q_j is a P_n–linear derivation

$$Q_j \colon P_n \otimes E_n^r \to P_n \otimes E_n^{r-1}$$

defined by the Cartan formula

$$Q_j(xy) = (Q_j x) \cdot y + (-1)^{\deg x} x \cdot (Q_j y)$$

for x, y in $P_n \otimes E_n$ and the unstable conditions

$$Q_j dx_i = x_i^{q^j},$$
$$Q_j x_i = 0,$$

for $i = 1, \ldots, n$, $j \geq 0$. Thus, the action of Milnor operations Q_j commutes with the action of the finite general linear group $GL_n(\mathbb{F}_q)$.

It is also clear that the action of Q_j on P_n trivially extends to the quotient field K_n and we may regard Q_j as a K_n–linear homomorphism

$$Q_j \colon K_n \otimes E_n^r \to K_n \otimes E_n^{r-1}.$$

We set up additional notations for handling Milnor operations.

Definition 2.1 For a positive integer n, we denote by S_n the set

$$\{0, 1, \ldots, n-1\}.$$

Let A_n be the set of subsets of S_n. We denote by $A_{n,r}$ the subset of A_n consisting of

$$I = \{i_1, \ldots, i_r\}$$

such that

$$0 \leq i_1 < \cdots < i_r < n.$$

We write Q_I for

$$Q_{i_1} \ldots Q_{i_r}.$$

We consider $A_{n,0}$ as the set of empty set $\{\varnothing\}$ and define $Q_\varnothing$ to be 1. It is also convenient for us to define A'_n to be the union of $A_{n,r}$, where r ranges from 0 to $n-1$.

Definition 2.2 Let I, J be elements of A_n. We define $\mathrm{sign}(I,J)$ as follows. If $I \cap J \neq \varnothing$, then $\mathrm{sign}(I,J) = 0$. If $I \cap J = \varnothing$ and $I \cup J = \{k_1, \ldots, k_{r+s}\}$, then $\mathrm{sign}(I,J)$ is the sign of the permutation

$$\begin{pmatrix} i_1, & \ldots, & i_r, & j_1, & \ldots, & j_s \\ k_1, & \ldots, & k_r, & k_{r+1}, & \ldots, & k_{r+s} \end{pmatrix},$$

where $I = \{i_1, \ldots, i_r\}$, $J = \{j_1, \ldots, j_s\}$, $i_1 < \cdots < i_r$, $j_1 < \cdots < j_s$ and $k_1 < \cdots < k_{r+s}$.

The following proposition is immediate from the definition above.

Proposition 2.3 *For I, J in A_n, we have*

$$Q_I Q_J = \mathrm{sign}(I,J) Q_K = (-1)^{rs} \mathrm{sign}(J,I) Q_K,$$

where $K = I \cup J$.

Finally, using Milnor operations in place of determinants, we describe Dickson invariants. We follow the notation of Wilkerson's paper [9]. Let $\Delta_n(X)$, $f_n(X)$ be polynomials of X over P_n of homogeneous degree q^n defined respectively by

$$\begin{aligned}\Delta_n(X) &= (-1)^n Q_0 \dots Q_n dx_1 \dots dx_n dX \\ &= \sum_{i=0}^{n} (-1)^{n-i} (Q_0 \dots \widehat{Q}_i \dots Q_n dx_1 \dots dx_n) X^{q^i}, \\ f_n(X) &= \prod_{x \in \mathbb{F}_q\{x_1,\dots,x_n\}} (X+x),\end{aligned}$$

where the cohomological degrees of dX, X are 1, 2, and $Q_i dX = X^{q^i}$, $Q_i X = 0$, respectively.

Proposition 2.4 *The polynomial $\Delta_n(X)$ is divisible by the polynomial $f_n(X)$ and*

$$e_n(x_1,\dots,x_n) f_n(X) = \Delta_n(X),$$

where $e_n(x_1,\dots,x_n) = Q_0 \dots Q_{n-1} dx_1 \dots dx_n \neq 0$.

Proof On the one hand, both $\Delta_n(X)$ and $f_n(X)$ have all $x \in \mathbb{F}_q\{x_1,\dots,x_n\}$ as roots. On the other hand, the coefficient of X^{q^n} in $\Delta_n(X)$ is

$$e_n(x_1,\dots,x_n) = Q_0 \dots Q_{n-1} dx_1 \dots dx_n$$

and $f_n(X)$ is monic. Since both $\Delta_n(X)$ and $f_n(X)$ have the same homogeneous degree q^n as polynomials of X, we have the required equality. □

Thus, we have the following proposition.

Proposition 2.5 *We may express $f_n(X)$ as follows:*

$$f_n(X) = \sum_{i=0}^{n} (-1)^{n-i} c_{n,i}(x_1,\dots,x_n) X^{q^i},$$

where

$$Q_0 \dots \widehat{Q}_i \dots Q_n dx_1 \dots dx_n = e_n(x_1,\dots,x_n) c_{n,i}(x_1,\dots,x_n)$$

and $c_{n,n}(x_1,\dots,x_n) = 1$.

The above proposition defines Dickson invariants $c_{n,i}(x_1,\dots,x_n)$ for $i = 0,\dots,n-1$. When it is convenient and if there is no risk of confusion, we write e_n, $c_{n,i}$ for $e_n(x_1,\dots,x_n)$, $c_{n,i}(x_1,\dots,x_n)$, respectively.

Proposition 2.6 *There holds*

$$c_{n,0}(x_1,\dots,x_n)=e_n(x_1,\dots,x_n)^{q-1}.$$

Proof It is clear that

$$(Q_{i_1}\dots Q_{i_n}dx_1\dots dx_n)^q=Q_{i_1+1}\dots Q_{i_n+1}dx_1\dots dx_n$$

and so

$$e_n(x_1,\dots,x_n)^q=e_n(x_1,\dots,x_n)c_{n,0}(x_1,\dots,x_n).$$ □

From the above definitions of $c_{n,i}(x_1,\dots,x_n)$ and $e_n(x_1,\dots,x_n)$ and from the fact that, for $g\in GL_n(\mathbb{F}_q)$,

$$g\,dx_1\dots dx_n=\det(g^{-1})dx_1\dots dx_n,$$

it follows that

$$ge_n(x_1,\dots,x_n)=\det(g^{-1})e_n(x_1,\dots,x_n)$$

and that

$$gc_{n,i}(x_1,\dots,x_n)=c_{n,i}(x_1,\dots,x_n).$$

Thus, it is clear that ${P_n}^{SL_n(\mathbb{F}_q)}$ contains e_n and $c_{n,1},\dots,c_{n,n-1}$ and that ${P_n}^{GL_n(\mathbb{F}_q)}$ contains $c_{n,0},\dots,c_{n,n-1}$. Indeed, the following results are well-known. For proofs, we refer the reader to Benson [2], Smith [8] and Wilkerson [9].

Theorem 2.7 (Dickson) *The ring of invariants ${P_n}^{SL_n(\mathbb{F}_q)}$ is a polynomial algebra generated by $c_{n,1},\dots,c_{n,n-1}$ and e_n.*

Theorem 2.8 (Dickson) *The ring of invariants ${P_n}^{GL_n(\mathbb{F}_q)}$ is a polynomial algebra generated by $c_{n,0},\dots,c_{n,n-1}$.*

In addition, we need the following proposition.

Proposition 2.9 *Let*

$$\pi\colon \mathbb{F}_q[x_1,\dots,x_n]\to\mathbb{F}_q[x_1,\dots,x_{n-1}]$$

be the obvious projection. Then, we have

$$\pi(e_n(x_1,\dots,x_n))=0$$

and, for $i=1,\dots,n-1$,

$$\pi(c_{n,i}(x_1,\dots,x_n))=c_{n-1,i-1}(x_1,\dots,x_{n-1})^q.$$

Proof It is clear that $e_n(x_1,\dots,x_n)$ is divisible by x_n, so we have

$$\pi(e_n(x_1,\dots,x_n)) = 0.$$

On the one hand, we have

$$\begin{aligned} f_n(X) &= \prod_{\alpha\in\mathbb{F}_q} \prod_{x\in\mathbb{F}_q\{x_1,\dots,x_{n-1}\}} (X+\alpha x_n + x) \\ &= \prod_{\alpha\in\mathbb{F}_q} f_{n-1}(X+\alpha x_n) \\ &= \prod_{\alpha\in\mathbb{F}_q} (f_{n-1}(X)+\alpha f_{n-1}(x_n)) \\ &= f_{n-1}(X)^q - f_{n-1}(X) f_{n-1}(x_n)^{q-1}. \end{aligned}$$

On the other hand, since $f_n(x_n)$ is divisible by x_n, we have

$$\pi(f_n(X)) = f_{n-1}(X)^q.$$

Comparing the coefficients of X^{q^i}, we have, for $i=1,\dots,n-1$,

$$\pi(c_{n,i}(x_1,\dots,x_n)) = c_{n-1,i-1}(x_1,\dots,x_{n-1})^q. \qquad \square$$

3 Proof of Theorem 1.1 and Theorem 1.2

In the case $n=1$, the invariants are obvious. In the case $r=0$, the invariants are calculated by Dickson. So, throughout the rest of this section, we assume $n\geq 2$ and $r>0$. To prove Theorem 1.1 and Theorem 1.2, it suffices to prove the following theorems.

Theorem 3.1 *The submodule $(P_n\otimes E_n^r)^{SL_n(\mathbb{F}_q)}$ is a free ${P_n}^{SL_n(\mathbb{F}_q)}$–module with the basis $\{Q_I dx_1\dots dx_n\}$, where I ranges over $A_{n,n-r}$.*

Theorem 3.2 *The submodule $(P_n\otimes E_n^r)^{GL_n(\mathbb{F}_q)}$ is a free ${P_n}^{GL_n(\mathbb{F}_q)}$–module with the basis $\{e_n^{q-2} Q_I dx_1\dots dx_n\}$, where I ranges over $A_{n,n-r}$.*

To begin with, we prove the following proposition.

Proposition 3.3 *The elements $Q_I dx_1\dots dx_n$ form a basis for $K_n\otimes E_n^r$, where I ranges over $A_{n,n-r}$.*

Proof Firstly, we show the linear independence of $Q_I dx_1 \dots dx_n$. Suppose that

$$a = \sum_{I \in A_{n,n-r}} a_I Q_I dx_1 \dots dx_n,$$

where $a_I \in K_n$. For each $I \in A_{n,n-r}$, let $J = S_n \backslash I$. It is clear that $J \cap I' \neq \emptyset$ if $I' \neq I$ in $A_{n,n-r}$. Hence, we have $\mathrm{sign}(J, I) \neq 0$ and $\mathrm{sign}(J, I') = 0$ for $I' \neq I \in A_{n,n-r}$. By Proposition 2.3, we have

$$Q_J a = \mathrm{sign}(J, I) a_I Q_0 \dots Q_{n-1} dx_1 \dots dx_n = \mathrm{sign}(J, I) a_I e_n.$$

Thus, if $a = 0$, then $a_I = 0$. Therefore, the terms $Q_I dx_1 \dots dx_n$ are linearly independent in $K_n \otimes E_n^r$.

On the other hand, since

$$\dim_{K_n} K_n \otimes E_n^r = \binom{n}{r}$$

is equal to the number of elements in $A_{n,n-r}$, we see, for dimensional reasons, that $Q_I dx_1 \dots dx_n$'s form a basis for $K_n \otimes E_n^r$. □

Lemma 3.4 *Let h_I be polynomials over $\mathbb{F}_q$ in $(n-1)$ variables, where I ranges over $A_{n,n-1}$. Suppose that*

$$a_0 = \sum_{I \in A_{n,n-1}} h_I(c_{n,n-1}, \dots, c_{n,1}) e_n{}^{-1} Q_I dx_1 \dots dx_n$$

is in $P_n \otimes E_n^1$. Then $h_I = 0$ for each $I \in A_{n,n-1}$.

Proof of Theorem 3.1

Suppose that a is an element in $P_n \otimes E_n^r$ and that a is $SL_n(\mathbb{F}_q)$–invariant. By Proposition 3.3, the elements $Q_I dx_1 \dots dx_n$ form a basis for $K_n \otimes E_n^r$. Hence, there exist a_I in K_n such that

$$a = \sum_{I \in A_{n,n-r}} a_I Q_I dx_1 \dots dx_n.$$

For $I \in A_{n,n-r}$, let $J = S_n \backslash I$. Then, $Q_J a$ is in P_n. As in the proof of Proposition 3.3, we have

$$Q_J a = \mathrm{sign}(J, I) a_I e_n.$$

Therefore, there are polynomials $f_{I,k}$ over $\mathbb{F}_q$ in $(n-1)$ variables such that

$$a_I = \sum_{k \geq 0} f_{I,k}(c_{n,n-1}, \dots, c_{n,1}) e_n^{k-1}.$$

Thus, we have

$$a = \sum_{I \in A_{n,n-r}} \sum_{k \geq 0} f_{I,k}(c_{n,n-1}, \dots, c_{n,1}) e_n^{k-1} Q_I \, dx_1 \dots dx_n.$$

It remains to show that $f_{I,0} = 0$ for each $I \in A_{n,n-r}$.

Let

$$a_0 = a - \sum_{I \in A_{n,n-r}} \sum_{k \geq 1} f_{I,k}(c_{n,n-1}, \dots, c_{n,1}) e_n^{k-1} Q_I \, dx_1 \dots dx_n.$$

Then, we have that

$$a_0 = \sum_{I \in A_{n,n-r}} f_{I,0}(c_{n,n-1}, \dots, c_{n,1}) e_n^{-1} Q_I \, dx_1 \dots dx_n$$

and that a_0 is also in $P_n \otimes E_n^r$.

For $J \in A_{n,r-1}$, the element $Q_J a_0$ is in $P_n \otimes E_n^1$. By Proposition 2.3, we have

$$Q_J a_0 = \sum_{K \in A_{n,n-1}, I = K \setminus J, I \in A_{n,n-r}} \operatorname{sign}(J, I) f_{I,0}(c_{n,n-1}, \dots, c_{n,1}) Q_K \, dx_1 \dots dx_n.$$

Hence, by Lemma 3.4, we have $\operatorname{sign}(J, I) f_{I,0} = 0$. For each I in $A_{n,n-r}$, there exists $J \in A_{n,r-1}$ such that $\operatorname{sign}(J, I) \neq 0$. Therefore, we have $f_{I,0} = 0$ for each I. This completes the proof. □

Proof of Theorem 3.2 As in the proof of Theorem 3.1, if $a \in P_n \otimes E_n^r$ is $GL_n(\mathbb{F}_q)$–invariant, the element a can be expressed in the form

$$a = \sum_{I \in A_{n,n-r}} \sum_{k \geq 1} f_{I,k}(c_{n,n-1}, \dots, c_{n,1}) e_n^{k-1} Q_I \, dx_1 \dots dx_n.$$

For $g \in GL_n(\mathbb{F}_q)$, we have

$$ga = \sum_{I \in A_{n,n-r}} \sum_{k \geq 1} \det(g^{-1})^k f_{I,k}(c_{n,n-1}, \dots, c_{n,1}) e_n^{k-1} Q_I \, dx_1 \dots dx_n.$$

Therefore, a is $GL_n(\mathbb{F}_q)$–invariant if and only if $f_{I,k} = 0$ for $k \not\equiv 0$ modulo $q-1$. Hence, we have

$$a = \sum_{I \in A_{n,n-r}} \sum_{m \geq 0} f_{I,m(q-1)+(q-1)}(c_{n,n-1}, \dots, c_{n,1}) e_n^{m(q-1)} e_n^{q-2} Q_I \, dx_1 \dots dx_n.$$

Since $e_n^{q-1} = c_{n,0}$, we may write

$$a = \sum_{I \in A_{n,n-r}} f'_I(c_{n,n-1}, \dots, c_{n,1}, c_{n,0}) e_n^{q-2} Q_I \, dx_1 \dots dx_n,$$

where

$$f_I'(c_{n,n-1},\dots,c_{n,0}) = \sum_{m\geq 0} f_{I,m(q-1)+(q-1)}(c_{n,n-1},\dots,c_{n,1}){c_{n,0}}^m.$$

This completes the proof. □

Proof of Lemma 3.4 For the sake of notational simplicity, let $I_i = S_n\backslash\{i\}$ and we write h_i for h_{I_i}. Since a is in $P_n \otimes E_n^1$, there are $\varphi_1,\dots,\varphi_n$ in P_n such that

$$a_0 = \varphi_1 dx_1 + \cdots + \varphi_n dx_n.$$

The coefficient φ_n of dx_n is given by

$$\begin{aligned}&\sum_{i=0}^{n-1} h_i(c_{n,n-1},\dots,c_{n,1})e_n^{-1}Q_{I_i}dx_1\dots dx_{n-1}\\ &= \left\{\sum_{i=0}^{n-1} h_i(c_{n,n-1},\dots,c_{n,1})c_{n-1,i}\right\} e_n^{-1}e_{n-1}.\end{aligned}$$

Hence, we have

$$\left\{\sum_{i=0}^{n-1} h_i(c_{n,n-1},\dots,c_{n,1})c_{n-1,i}\right\} e_{n-1} = e_n\varphi_n.$$

By Proposition 2.9, the obvious projection

$$\pi\colon \mathbb{F}_q[x_1,\dots,x_n] \to \mathbb{F}_q[x_1,\dots,x_{n-1}]$$

maps e_n, $c_{n,i}$ to 0, $c_{n-1,i-1}^q$, respectively. So, we have

$$\sum_{i=0}^{n-1} h_i(c_{n-1,n-2}^q,\dots,c_{n-1,0}^q)c_{n-1,i} = 0.$$

Since $c_{n-1,i}$ $(i=0,\dots,n-2)$ are algebraically independent in $\mathbb{F}_q[x_1,\dots,x_{n-1}]$ and since $c_{n-1,n-1}=1$, writing y_i for $c_{n-1,i}$, we have the following equation:

(1) $$h_{n-1}(y_{n-2}^q,\dots,y_0^q) + \sum_{i=0}^{n-2} h_i(y_{n-2}^q,\dots,y_0^q)y_i = 0.$$

Applying partial derivatives $\partial/\partial y_i$, we have

(2) $$h_i(y_{n-2}^q,\dots,y_0^q) = 0$$

for $i=0,\dots,n-2$. Hence, $h_i(y_{n-2}^q,\dots,y_0^q)=0$ for $i=0,\dots,n-2$. Substituting these to the previous equation (1), we also have $h_{n-1}(y_{n-2}^q,\dots,y_0^q)=0$. Since we deal with polynomials over the finite field $\mathbb{F}_q$, we have

$$h_i(y_{n-2}^q,\dots,y_0^q)=h_i(y_{n-2},\dots,y_0)^q$$

for $i=0,\dots,n-1$. Therefore, we have $h_i(y_{n-2},\dots,y_0)=0$ for $i=0,\dots,n-1$. Since $y_0,\dots,y_{n-2}$ are algebraically independent, we have

$$h_i=0$$

as polynomials over $\mathbb{F}_q$ in $(n-1)$ variables for $i=0,\dots,n-1$. □

4 Invariants of some Weyl groups

In this section, we consider the invariant theory of polynomial tensor exterior algebras. In what follows, we assume that $n\geq 2$. To state Theorem 4.2, which is our main theorem on the invariant theory, we need some notation. Let

$$P_{n-1}=\mathbb{F}_q[x_2,\dots,x_n]$$

be the subalgebra of P_n generated by $x_2,\dots,x_n$ and let E_{n-1} be the subalgebra of E_n generated by $dx_2,\dots,dx_n$. Let G_1 be a subgroup of $SL_{n-1}(\mathbb{F}_q)$ which acts on P_{n-1} and $P_{n-1}\otimes E_{n-1}$ both. Let G be a subgroup of $SL_n(\mathbb{F}_q)$ consisting of the following matrices:

$$\left(\begin{array}{c|c} 1 & m \\ \hline 0 & g_1 \end{array}\right),$$

where $g_1\in G_1$ and $m\in M_{1,n-1}(\mathbb{F}_q)$. Obviously the group G acts on P_n and $P_n\otimes E_n$. Finally, let

$$\mathcal{O}_{n-1}(x_i)=\prod_{x\in\mathbb{F}_q\{x_2,\dots,x_n\}}(x_i+x).$$

Theorem 4.1 *Suppose that the ring of invariants $P_{n-1}^{G_1}$ is a polynomial algebra generated by homogeneous polynomials $f_2,\dots,f_n$ in $(n-1)$ variables $x_2,\dots,x_n$. Then, the ring of invariants P_n^G is also a polynomial algebra generated by*

$$\mathcal{O}_{n-1}(x_1),f_2,\dots,f_n.$$

This theorem is a particular case of a theorem of Kameko and Mimura [6, Theorem 2.5]. We use this theorem to compute the polynomial part of invariants P_n^G which appear in our main theorem, Theorem 4.2. So, Theorem 4.2 below works effectively together with Theorem 4.1.

Theorem 4.2 *Suppose that the ring of invariants $P_{n-1}^{G_1}$ is a polynomial algebra generated by homogeneous polynomials $f_2, \dots, f_n$ in $(n-1)$ variables $x_2, \dots, x_n$ and suppose that the ring of invariants $(P_{n-1} \otimes E_{n-1})^{G_1}$ is a free $P_{n-1}^{G_1}$–module with a basis $\{v_i\}$, where $i = 1, \dots, 2^{n-1}$. Then, the ring of invariants $(P_n \otimes E_n)^G$ is a free P_n^G–module with the basis $\{v_i, Q_I dx_1 \dots dx_n\}$, where $i = 1, \dots, 2^{n-1}$ and I ranges over A_{n-1}.*

We prove Theorem 4.1 and Theorem 4.2 in Section 5, Section 6 and Section 7.

As an application of Theorem 4.1 and Theorem 4.2, we compute rings of invariants of the mod–p cohomology of the classifying spaces of maximal non-toral elementary abelian p–subgroups of simply connected exceptional Lie groups with respect to the Weyl group action.

It is well-known that for an odd prime p, a simply connected exceptional Lie group G does not have non-toral elementary abelian p–subgroups except for the cases $p = 5$, $G = E_8$, and $p = 3$, $G = F_4,\ E_6,\ E_7,\ E_8$ (see [1] and [5]). Andersen, Grodal, Møller and Viruel [1] described the Weyl groups of maximal non-toral elementary abelian p–subgroups as well as their action on the underlying elementary abelian p–subgroup explicitly for $p = 3$, $G = E_6,\ E_7,\ E_8$. Up to conjugate, there are only 6 maximal non-toral elementary abelian p–subgroups of simply connected exceptional Lie groups. For $p = 5$, $G = E_8$ and for $p = 3$, $G = F_4,\ E_6,\ E_7$, there is one maximal non-toral elementary abelian p–subgroup for each G. We call them $E^3_{E_8}$, $E^3_{F_4}$, $E^4_{3E_6}$, $E^4_{2E_7}$, following the notation in [1]. For $p = 3$, $G = E_8$, there are two maximal non-toral elementary abelian p–subgroups, say $E^{5a}_{E_8}$ and $E^{5b}_{E_8}$, where the superscript indicates the rank of elementary abelian p–subgroup. For a detailed account on non-toral elementary abelian p–subgroups, we refer the reader to Andersen et al [1, Section 8], and its references.

Let A be an elementary abelian p–subgroup of a compact Lie group G. Suppose that A is of rank n. We denote by $W(A)$ the Weyl group of A. Choosing a basis, say $\{a_i\}$, for A, we consider the Weyl group $W(A)$ as a subgroup of the finite general linear group $GL_n(\mathbb{F}_p)$. We write H^*BA for the mod–p cohomology of the classifying space BA. The Hurewicz homomorphism $h\colon A = \pi_1(BA) \to H_1(BA; \mathbb{F}_p)$ is an isomorphism. We denote by $\{dt_i\}$ the dual basis of $\{h(a_i)\}$, so that dt_i is the dual of $h(a_i)$ with respect to the basis $\{h(a_i)\}$ of $H_1(BA; \mathbb{F}_p)$ for $i = 1, \dots, n$. Let $\beta\colon H^1BA \to H^2BA$ be the Bockstein homomorphism. Then, the mod–p cohomology of BA is a polynomial tensor exterior algebra

$$H^*BA = \mathbb{F}_p[t_1, \dots, t_n] \otimes \Lambda(dt_1, \dots, dt_n),$$

where $\deg t_i = 2$, $\deg dt_i = 1$ and $t_i = \beta(dt_i)$ for $i = 1, \ldots, n$. We denote by $\Gamma H^* BA$ the polynomial part of $H^* BA$, that is,

$$\Gamma H^* BA = \mathbb{F}_p[t_1, \ldots, t_n].$$

The action of the Weyl group $W(A)$ on $A = \pi_1(BA)$, given by

$$g a_i = \sum_j a_{j,i}(g) a_j,$$

where $\{a_i\}$ is the fixed basis of A, induces the action of $W(A)$ on $H^* BA$, which is given by

$$g t_i = \sum_j a_{i,j}(g^{-1}) t_j, \quad g dt_i = \sum_j a_{i,j}(g^{-1}) dt_j,$$

for $i = 1, \ldots, n$.

Now, we compute

$$(H^* BA)^{W(A)}$$

for $A = E^3_{E_8}$, $E^3_{F_4}$, $E^4_{3E_6}$, $E^4_{2E_7}$, $E^{5a}_{E_8}$ using Theorem 1.1, Theorem 4.1 and Theorem 4.2.

Proposition 4.3 *For the above elementary abelian p–subgroup A, the ring of invariants $(H^* BA)^{W(A)}$ is given as follows:*

(1) *For $p = 5$, $G = E_8$, $A = E^3_{E_8}$, $(H^* BA)^{W(A)}$ is given by*

$$\mathbb{F}_5[x_{62}, x_{200}, x_{240}] \otimes \mathbb{F}_5\{1, Q_I u_3\},$$

where $x_{62} = e_3(t_1, t_2, t_3)$, $x_{200} = c_{3,2}(t_1, t_2, t_3)$, $x_{240} = c_{3,1}(t_1, t_2, t_3)$, $u_3 = dt_1 dt_2 dt_3$ and I ranges over A'_3;

(2) *For $p = 3$, $G = F_4$, $A = E^3_{F_4}$, $(H^* BA)^{W(A)}$ is given by*

$$\mathbb{F}_3[x_{26}, x_{36}, x_{48}] \otimes \mathbb{F}_3\{1, Q_I u_3\},$$

where $x_{26} = e_3(t_1, t_2, t_3)$, $x_{36} = c_{3,2}(t_1, t_2, t_3)$, $x_{48} = c_{3,1}(t_1, t_2, t_3)$, $u_3 = dt_1 dt_2 dt_3$ and I ranges over A'_3;

(3) *For $p = 3$, $G = E_6$, $A = E^4_{3E_6}$, $(H^* BA)^{W(A)}$ is given by*

$$\mathbb{F}_3[x_{26}, x_{36}, x_{48}, x_{54}] \otimes \mathbb{F}_3\{1, Q_I u_3, Q_J u_4\},$$

where $x_{26} = e_3(t_2, t_3, t_4)$, $x_{36} = c_{3,2}(t_2, t_3, t_4)$, $x_{48} = c_{3,1}(t_2, t_3, t_4)$,

$$x_{54} = \prod_{t \in \mathbb{F}_3\{t_2, t_3, t_4\}} (t_1 + t),$$

$u_3 = dt_2 dt_3 dt_4$, $u_4 = dt_1 dt_2 dt_3 dt_4$, I ranges over A'_3 and J ranges over A_3;

(4) *For* $p=3$, $G=E_7$, $A=E^4_{2E_7}$, $(H^*BA)^{W(A)}$ *is given by*

$$\mathbb{F}_3[x_{26},x_{36},x_{48},x_{108}]\otimes\mathbb{F}_3\{1,Q_Iu_3,x_{54}Q_Ju_4\},$$

where $x_{26}=e_3(t_2,t_3,t_4)$, $x_{36}=c_{3,2}(t_2,t_3,t_4)$, $x_{48}=c_{3,1}(t_2,t_3,t_4)$, $x_{108}=x_{54}^2$,

$$x_{54}=\prod_{t\in\mathbb{F}_3\{t_2,t_3,t_4\}}(t_1+t),$$

$u_3=dt_2dt_3dt_4$, $u_4=dt_1dt_2dt_3dt_4$, I *ranges over* A_3' *and* J *ranges over* A_3;

(5) *For* $p=3$, $G=E_8$, $A=E^{5a}_{E_8}$, $(H^*BA)^{W(A)}$ *is given by*

$$\mathbb{F}_3[x_4,x_{26},x_{36},x_{48},x_{324}]\otimes\mathbb{F}_3\{1,Q_Iu_3,x_2u_1,(Q_Iu_3)x_2u_1,x_2x_{162}Q_Ju_5\},$$

where $x_4=x_2^2$, $x_{26}=e_3(t_2,t_3,t_4)$, $x_{36}=c_{3,2}(t_2,t_3,t_4)$, $x_{48}=c_{3,1}(t_2,t_3,t_4)$, $x_{324}=x_{162}^2$, $x_2=t_5$,

$$x_{162}=\prod_{t\in\mathbb{F}_3\{t_2,t_3,t_4,t_5\}}(t_1+t),$$

$u_1=dt_5$, $u_3=dt_2dt_3dt_4$, $u_5=dt_1dt_2dt_3dt_4dt_5$, I *ranges over* A_3' *and* J *ranges over* A_4,

where the subscripts of u *and* x *indicate their cohomological degrees.*

Proof (1), (2) In the case $p=5$, $G=E_8$, $A=E^3_{E_8}$ and in the case $p=3$, $G=F_4$, $A=E^3_{F_4}$, the Weyl group is $SL_3(\mathbb{F}_p)$. Therefore, it is the case of Mùi invariants and it is immediate from Theorem 1.1.

(3) In the case $p=3$, $G=E_6$, $A=E^4_{E_6}$, the Weyl group $W(A)$ is the subgroup of $SL_4(\mathbb{F}_3)$ consisting of the following matrices:

$$\left(\begin{array}{c|c}1 & m\\ \hline 0 & g_1\end{array}\right),$$

where $m\in M_{1,3}(\mathbb{F}_3)$, $g_1\in SL_3(\mathbb{F}_3)$. The result is immediate from Theorem 1.1, Theorem 4.1 and Theorem 4.2.

(4) In the case $p=3$, $G=E_7$, the Weyl group $W(A)$ is the subgroup of $GL_4(\mathbb{F}_3)$ consisting of the following matrices:

$$\left(\begin{array}{c|c}\varepsilon_1 & m\\ \hline 0 & g_1\end{array}\right),$$

where $\varepsilon_1 \in \mathbb{F}_3^\times = \{1,2\}$, $m \in M_{1,3}(\mathbb{F}_3)$, $g_1 \in SL_3(\mathbb{F}_3)$. Firstly, we compute the ring of invariants of a subgroup W_0 of $W(A)$. The subgroup W_0 is the subgroup of $W(A)$ consisting of the matrices

$$\left(\begin{array}{c|c} 1 & m \\ \hline 0 & g_1 \end{array}\right),$$

where $m \in M_{1,3}(\mathbb{F}_3)$, $g_1 \in SL_3(\mathbb{F}_3)$. By Theorem 1.1, Theorem 4.1 and Theorem 4.2, we have

$$(H^*BA)^{W_0} = \mathbb{F}_3[x_{26}, x_{36}, x_{48}, x_{54}] \otimes \mathbb{F}_3\{1, Q_I u_3, Q_J u_4\},$$

where I ranges over A_3' and J ranges over A_3. Let

$$R = \mathbb{F}_3[x_{26}, x_{36}, x_{48}, x_{108}],$$

and let

$$M = \mathbb{F}_3\{x_{54}^\delta, x_{54}^\delta Q_I u_3, x_{54}^\delta Q_J u_4\},$$

where $x_{108} = x_{54}^2$, $\delta \in \{0,1\}$, I ranges over A_3' and J ranges over A_3. Then, we have

$$(H^*BA)^{W_0} = R \otimes M.$$

Next, we calculate the ring of invariants $(H^*BA)^{W(A)}$ as a subspace of $(H^*BA)^{W_0}$. Put

$$\alpha = \left(\begin{array}{c|ccc} 2 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

Then, for $x \in R$, we have $\alpha x = x$ and we also have the following direct sum decomposition:

$$M = M_1 \oplus M_2,$$

where $M_i = \{x \in M \,|\, \alpha x = ix\}$ for $i = 1,\ 2$. In particular, we have

$$M_1 = \mathbb{F}_3\{1, Q_I u_3, x_{54} Q_J u_4\}.$$

Since the Weyl group $W(A)$ is generated by W_0 and α, an element x in $R \otimes M$ is $W(A)$–invariant if and only if $\alpha x = x$. Hence, we have

$$(H^*BA)^{W(A)} = R \otimes M_1.$$

(5) In the case $p=3$, $G=E_8$, $A=E^{5a}_{E_8}$, the Weyl group $W(A)$ is the subgroup of $GL_5(\mathbb{F}_3)$ consisting of the following matrices:

$$\left(\begin{array}{c|c|c} \varepsilon_1 & m_0 & m_1 \\ \hline 0 & g_1 & 0 \\ \hline 0 & 0 & \varepsilon_2 \end{array}\right),$$

where $\varepsilon_1,\ \varepsilon_2 \in \mathbb{F}_3^\times=\{1,2\}$, $m_0 \in M_{1,3}(\mathbb{F}_3)$, $m_1 \in M_{1,1}(\mathbb{F}_3)$, $g_1 \in SL_3(\mathbb{F}_3)$. We consider the subgroup W_0 of $W(A)$ consisting of the following matrices:

$$\left(\begin{array}{c|c|c} 1 & m_0 & m_1 \\ \hline 0 & g_1 & 0 \\ \hline 0 & 0 & 1 \end{array}\right),$$

where $g_1\in SL_3(\mathbb{F}_3)$, $m_0\in M_{1,3}(\mathbb{F}_3)$, $m_1\in M_{1,1}(\mathbb{F}_3)$. By Theorem 4.1 and Theorem 4.2, we have

$$(H^*BA)^{W_0}=\mathbb{F}_3[x_2,x_{26},x_{36},x_{48},x_{162}]\otimes\mathbb{F}_3\{1,Q_Iu_3,u_1,(Q_Iu_3)u_1,Q_Ju_5\},$$

where I ranges over A_3' and J ranges over A_4. Let

$$R=\mathbb{F}_3[x_4,x_{26},x_{36},x_{48},x_{324}],$$

and let

$$M=\mathbb{F}_3\{x_2^{\delta_1}x_{162}^{\delta_2},x_2^{\delta_1}x_{162}^{\delta_2}Q_Iu_3,x_2^{\delta_1}x_{162}^{\delta_2}u_1,x_2^{\delta_1}x_{162}^{\delta_2}(Q_Iu_3)u_1,x_2^{\delta_1}x_{162}^{\delta_2}Q_Ju_5\},$$

where $\delta_1,\ \delta_2\in\{0,1\}$, I ranges over A_3' and J ranges over A_4. Consider matrices

$$\alpha=\left(\begin{array}{c|ccc|c} 2&0&0&0&0\\ \hline 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ \hline 0&0&0&0&1 \end{array}\right),\quad \beta=\left(\begin{array}{c|ccc|c} 1&0&0&0&0\\ \hline 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ \hline 0&0&0&0&2 \end{array}\right).$$

Then, we have $\alpha x=x$ and $\beta x=x$ for $x\in R$. Furthermore, it is also clear that we have the following direct sum decomposition:

$$M=M_{1,1}\oplus M_{1,2}\oplus M_{2,1}\oplus M_{2,2},$$

where

$$M_{i,j}=\{x\in M\,|\,\alpha x=ix,\beta x=jx\}.$$

In particular, we have

$$M_{1,1}=\mathbb{F}_3\{1,x_2u_1,Q_Iu_3,x_2(Q_Iu_3)u_1,x_2x_{162}Q_Ju_5\}.$$

Since $W(A)$ is generated by W_0 and α, β in the above, $x \in (H^*BA)^{W_0}$ is $W(A)$–invariant if and only if $\alpha x = \beta x = x$. Hence, we have

$$(H^*BA)^{W(A)} = R \otimes M_{1,1}. \qquad \square$$

Remark 4.4 Our computation of the ring of invariants of polynomial tensor exterior algebra in Proposition 4.3 is based on the computation of the ring of invariants of polynomial algebra and the assumption that the ring of invariants of polynomial algebra is also a polynomial algebra. In the case $A = E^{5b}_{E_8}$, however, the Weyl group does not satisfy the condition we assume in this section and the ring of invariants of polynomial algebra is no longer a polynomial algebra. Hence, both Theorem 4.1 and Theorem 4.2 do not apply in this case.

5 $\mathcal{O}_{n-1}(x_i)$ and $\mathcal{D}_{n-1}$

In this section, we collect some facts, which we need in the proof of Theorem 4.1 and Theorem 4.2.

For $i = 1, \dots, n$, the element $\mathcal{O}_{n-1}(x_i)$ in $\mathbb{F}_q[x_1, \dots, x_n]$ is defined to be

$$\mathcal{O}_{n-1}(x_i) = \prod_{x \in \mathbb{F}_q\{x_2,\dots,x_n\}} (x_i + x).$$

We also define $\mathcal{O}_{n-2}(x_i)$ in $\mathbb{F}_q[x_1, \dots, x_{n-1}]$ by

$$\mathcal{O}_{n-2}(x_i) = \prod_{x \in \mathbb{F}_q\{x_2,\dots,x_{n-1}\}} (x_i + x)$$

for $n \geq 3$ and by

$$\mathcal{O}_0(x_i) = x_i$$

for $n = 2$.

Using the same argument as in the proof of Proposition 2.5, we can easily obtain the following proposition.

Proposition 5.1 *For $i = 1, \dots, n$, we may express $\mathcal{O}_{n-1}(x_i)$ and $\mathcal{O}_{n-2}(x_i)$ in terms of Dickson invariants as follows*:

$$\mathcal{O}_{n-1}(x_i) = \sum_{j=0}^{n-1} (-1)^{n-1-j} c_{n-1,j}(x_2, \dots, x_n) {x_i}^{q^j} \qquad \text{for } n \geq 2,$$
$$\mathcal{O}_{n-2}(x_i) = \sum_{j=0}^{n-2} (-1)^{n-2-j} c_{n-2,j}(x_2, \dots, x_{n-1}) {x_i}^{q^j} \quad \text{for } n > 2.$$

We need Proposition 5.2 and Proposition 5.3 below in the proof of Proposition 7.5.

Proposition 5.2 *In $\mathbb{F}_q[x_1,\dots,x_{n-1}]$, we have the following equality:*

$$e_{n-1}(x_1,\dots,x_{n-1}) = \mathcal{O}_{n-2}(x_1)e_{n-2}(x_2,\dots,x_{n-1})$$

for $n \geq 3$, and

$$e_1(x_1) = x_1$$

for $n = 2$.

Proof For $n=2$, the proposition is obvious. For $n \geq 3$, by Proposition 2.4, Proposition 2.5 and Proposition 5.1, we have

$$\begin{aligned}
& e_{n-1}(x_1,\dots,x_{n-1}) \\
= {} & Q_0 \dots Q_{n-2} dx_1 \dots dx_{n-1} \\
= {} & \sum_{j=0}^{n-2} (-1)^{n-2-j} (Q_0 \dots \widehat{Q}_j \dots Q_{n-2} dx_2 \dots dx_{n-1}) x_1^{q^j} \\
= {} & \sum_{j=0}^{n-2} (-1)^{n-2-j} e_{n-2}(x_2,\dots,x_{n-1}) c_{n-2,j}(x_2,\dots,x_{n-1}) x_1^{q^j} \\
= {} & e_{n-2}(x_2,\dots,x_{n-1}) \mathcal{O}_{n-2}(x_1).
\end{aligned}$$

□

Proposition 5.3 *The obvious projection*

$$\pi\colon \mathbb{F}_q[x_1,\dots,x_n] \longrightarrow \mathbb{F}_q[x_1,\dots,x_{n-1}]$$

maps $\mathcal{O}_{n-1}(x_1)$, $e_{n-1}(x_2,\dots,x_n)$ to $\mathcal{O}_{n-2}(x_1)^q$, 0, respectively.

Proof Since $e_{n-1}(x_2,\dots,x_n)$ is divisible by x_n, we have

$$\pi(e_{n-1}(x_2,\dots,x_n)) = 0$$

as in the proof of Proposition 2.9. For $n=2$, the equality

$$\pi(\mathcal{O}_1(x_1)) = \mathcal{O}_0(x_1)^q = x_1^q$$

is obvious. For $n \geq 3$, by Proposition 2.9, we have

$$\pi(c_{n-1,j}(x_2,\dots,x_n)) = c_{n-2,j-1}(x_2,\dots,x_{n-1})^q$$

for $j = 1, \ldots, n-1$. Hence, we have

$$\begin{aligned}\pi(\mathcal{O}_{n-1}(x_1)) &= \pi\left(\sum_{j=0}^{n-1}(-1)^{n-1-j}c_{n-1,j}(x_2,\ldots,x_n)x_1^{q^j}\right)\\ &= \sum_{j=1}^{n-1}(-1)^{n-1-j}c_{n-2,j-1}(x_2,\ldots,x_{n-1})^q x_1^{q^j}\\ &= \mathcal{O}_{n-2}(x_1)^q.\end{aligned}$$

□

For a in $P_n \otimes E_n$, let

$$\mathcal{D}_{n-1}(a) = \sum_{j=0}^{n-1}(-1)^{n-1-j}c_{n-1,j}(x_2,\ldots,x_n)Q_j a.$$

Then, $\mathcal{D}_{n-1}$ induces a P_n–linear homomorphism

$$\mathcal{D}_{n-1}\colon P_n \otimes E_n^r \longrightarrow P_n \otimes E_n^{r-1},$$

which extends naturally to

$$\mathcal{D}_{n-1}\colon K_n \otimes E_n^r \to K_n \otimes E_n^{r-1}.$$

Proposition 5.4 *For $i = 1, \ldots, n$, we have*

$$\mathcal{D}_{n-1}(dx_i) = \mathcal{O}_{n-1}(x_i).$$

In particular, for $i = 2, \ldots, n$, we have $\mathcal{D}_{n-1}(dx_i) = 0$.

Proof By Proposition 5.1, we have

$$\begin{aligned}\mathcal{D}_{n-1}(dx_i) &= \sum_{j=0}^{n-1}(-1)^{n-1-j}c_{n-1,j}(x_2,\ldots,x_n)Q_j dx_i\\ &= \sum_{j=0}^{n-1}(-1)^{n-1-j}c_{n-1,j}(x_2,\ldots,x_n)x_i^{q^j}\\ &= \mathcal{O}_{n-1}(x_i).\end{aligned}$$

On the other hand, by the definition of $\mathcal{O}_{n-1}(x_i)$, we have

$$\mathcal{O}_{n-1}(x_i) = 0$$

for $i = 2, \ldots, n$. Hence, we have $\mathcal{D}_{n-1}(dx_i) = 0$ for $i = 2, \ldots, n$. □

Let g_1 be an element in $GL_{n-1}(\mathbb{F}_q)$. We consider the following matrix

$$\bar{g}_1 = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & g_1 \end{array}\right).$$

We need Proposition 5.5 and Proposition 5.6 below in the proof of Proposition 7.8.

Proposition 5.5 *For g_1 in $GL_{n-1}(\mathbb{F}_q)$, there holds*

$$\mathcal{D}_{n-1}(\bar{g}_1 a) = \bar{g}_1 \mathcal{D}_{n-1}(a).$$

Proof Suppose that

$$a = \sum_{i=1}^{n} a_i dx_i,$$

where $a_i \in K_n$ for $i = 1, \dots, n$. Since

$$\bar{g}_1 dx_1 = dx_1,$$

and since, for $i = 2, \dots, n$,

$$\bar{g}_1 dx_i$$

is in E^1_{n-1}, we have

$$\bar{g}_1 a = (\bar{g}_1 a_1) dx_1 + a'_2 dx_2 + \cdots + a'_n dx_n$$

for some $a'_i \in K_n$ for $i = 2, \dots, n$. Hence, by Proposition 5.4, we have

$$\mathcal{D}_{n-1}(\bar{g}_1 a) = (\bar{g}_1 a_1) \mathcal{O}_{n-1}(x_1).$$

On the other hand, by Proposition 5.4, we have

$$\bar{g}_1 \mathcal{D}_{n-1}(a) = \bar{g}_1 (a_1 \mathcal{O}_{n-1}(x_1)) = (\bar{g}_1 a_1) \mathcal{O}_{n-1}(x_1). \qquad \square$$

Let $\mathbb{P}^{n-2}$ be the projective space

$$(\mathbb{F}_q^{n-1} \backslash \{(0, \dots, 0)\}) / \sim,$$

where $\ell \sim \ell'$ if and only if there is $\alpha \in \mathbb{F}_q^{\times}$ such that $\ell = \alpha \ell'$.

Proposition 5.6 *If $a \in P_n$ is divisible by $\alpha_2 x_2 + \cdots + \alpha_n x_n$ for arbitrary $(\alpha_2, \dots, \alpha_n) \in \mathbb{P}^{n-2}$, then a is divisible by $e_{n-1}(x_2, \dots, x_n)$.*

Proof Since the number of elements in $\mathbb{P}^{n-2}$ is equal to the homogeneous degree $1+q+\cdots+q^{n-2}$ of $e_{n-1}(x_2,\ldots,x_n)$, it suffices to show that $e_{n-1}(x_2,\ldots,x_n)$ is a product of elements of the form $\alpha_2x_2+\cdots+\alpha_nx_n$, where $(\alpha_2,\ldots,\alpha_n)$ ranges over $\mathbb{P}^{n-2}$. It is clear that $e_{n-1}(x_2,\ldots,x_n)$ is divisible by x_n. So, we have

$$e_{n-1}(x_2,\ldots,x_n)=bx_n$$

for some $b\in P_n$. It is also clear that $e_{n-1}(x_2,\ldots,x_n)$ is invariant under the action of $SL_{n-1}(\mathbb{F}_q)$. There is $g_1\in SL_{n-1}(\mathbb{F}_q)$ such that $\alpha_2x_2+\cdots+\alpha_nx_n=\bar{g}_1x_n$. Hence, on the one hand, we have

$$\bar{g}_1e_{n-1}(x_2,\ldots,x_n)=(\bar{g}_1b)(\alpha_2x_2+\cdots+\alpha_nx_n)$$

and, on the other hand, we have

$$\bar{g}_1e_{n-1}(x_2,\ldots,x_n)=e_{n-1}(x_2,\ldots,x_n).$$

Therefore, $e_{n-1}(x_2,\ldots,x_n)$ is divisible by arbitrary $\alpha_2x_2+\cdots+\alpha_nx_n$. This completes the proof. □

6 Proof of Theorem 4.1

In order to prove Theorem 4.1, we recall the strategy to compute rings of invariants given by Wilkerson in [9, Section 3]. It can be stated in the following form.

Theorem 6.1 *Suppose that G is a subgroup of $GL_n(\mathbb{F}_q)$ and G acts on the polynomial algebra $\mathbb{F}_q[x_1,\ldots,x_n]$ in the obvious manner. Let $f_1,\ldots,f_n$ be homogeneous G–invariant polynomials in $\mathbb{F}_q[x_1,\ldots,x_n]$. Let R be the subalgebra of $\mathbb{F}_q[x_1,\ldots,x_n]$ generated by $f_1,\ldots,f_n$. Then, R is a polynomial algebra $\mathbb{F}_q[f_1,\ldots,f_n]$ and the ring of invariants $\mathbb{F}_q[x_1,\ldots,x_n]^G$ is equal to the subalgebra R if and only if $\mathbb{F}_q[x_1,\ldots,x_n]$ is integral over R and* $\deg f_1\ldots\deg f_n=|G|$.

In the statement of Theorem 6.1, $\deg f$ is the homogeneous degree of f, that is, we define the degree $\deg x_i$ of indeterminate x_i to be 1. For the proof of this theorem, we refer the reader to Smith's book [8, Corollaries 2.3.2 and 5.5.4, and Proposition 5.5.5] and Wilkerson's paper [9, Section 3].

Proof of Theorem 4.1

As we mentioned, in order to prove Theorem 4.1, it suffices to show the following:

(1) homogeneous polynomials $\mathcal{O}_{n-1}(x_1)$, $f_2,\ldots,f_n$ are G–invariant;

(2) indeterminates $x_1, \dots, x_n$ are integral over R;

(3) the product of homogeneous degrees of $\mathcal{O}_{n-1}(x_1)$, $f_2, \dots, f_n$ is equal to the order of G, that is,

$$\deg \mathcal{O}_{n-1}(x_1) \deg f_2 \dots \deg f_n = |G|.$$

By definition, $f_2, \dots, f_n$ are G_1–invariant, and so they are also G–invariant. It follows from Theorem 6.1 that $x_2, \dots, x_n$ are integral over $R_1 = \mathbb{F}_q[f_2, \dots, f_n]$, and so they are integral over R. It is also immediate from Theorem 6.1 that $\deg f_2 \dots \deg f_n = |G_1|$. It is clear from the definition of $\mathcal{O}_{n-1}(x_1)$ that $\deg \mathcal{O}_{n-1} = 2^{n-1}$. Hence, we have

$$\deg \mathcal{O}_{n-1}(x_1) \deg f_2 \dots \deg f_n = 2^{n-1}|G_1| = |G|.$$

So, it remains to show the following:

(1) $\mathcal{O}_{n-1}(x_1)$ is G–invariant and

(2) x_1 is integral over R.

First, we deal with (1). By the definition of $\mathcal{O}_{n-1}(x_1)$, we have that

$$g\mathcal{O}_{n-1}(x_1)$$

is a product of

$$g(x_1 + x) = x_1 + \sum_{j=2}^{n} a_{1,j}(g^{-1})x_j + gx,$$

where x ranges over $\mathbb{F}_q\{x_2, \dots, x_n\}$. As x ranges over $\mathbb{F}_q\{x_2, \dots, x_n\}$, the sum

$$\sum_{j=2}^{n} a_{1,j}(g^{-1})x_j + gx$$

also ranges over $\mathbb{F}_q\{x_2, \dots, x_n\}$. Hence, we have

$$g\mathcal{O}_{n-1}(x_1) = \mathcal{O}_{n-1}(x_1).$$

Next, we deal with (2). By Proposition 5.1, we have

$$\mathcal{O}_{n-1}(X) = X^{q^{n-1}} + \sum_{j=0}^{n-2} (-1)^{n-1-j} c_{n-1,j}(x_2, \dots, x_n) X^{q^j}.$$

Since Dickson invariants $c_{n-1,j}(x_2, \dots, x_n)$ are in $R_1 = \mathbb{F}_2[x_2, \dots, x_n]^{G_1}$, the polynomial

$$\varphi(X) = \mathcal{O}_{n-1}(X) - \mathcal{O}_{n-1}(x_1)$$

is a monic polynomial in $R[X]$. It is clear that

$$\varphi(x_1) = 0.$$

Hence, the indeterminate x_1 is integral over R. This completes the proof. □

7 Proof of Theorem 4.2

Let G_0 be the subgroup of G consisting of the following matrices:

$$\left(\begin{array}{c|c} 1 & m \\ \hline 0 & 1_{n-1} \end{array}\right),$$

where $m \in M_{1,n-1}(\mathbb{F}_q)$, 1_{n-1} is the identity matrix in $GL_{n-1}(\mathbb{F}_q)$. Let B_n be the set of subsets of

$$\{2, \ldots, n\}.$$

Let $B_{n,r}$ be the subset of B_n such that $J \in B_{n,r}$ if and only if

$$J = \{j_1, \ldots, j_r\} \quad \text{and} \quad 1 < j_1 < \cdots < j_r \le n.$$

We write dx_J for

$$dx_{j_1} \ldots dx_{j_r}$$

and we define $dx_\varnothing$ to be 1.

The following proposition is nothing but the particular case of Theorem 4.1 and Theorem 4.2.

Proposition 7.1 *The ring of invariants $P_n^{G_0}$ is given as follows:*

$$P_n^{G_0} = \mathbb{F}_q[\mathcal{O}_{n-1}(x_1), x_2, \ldots, x_n].$$

The ring of invariants $(P_n \otimes E_n)^{G_0}$ is a free $P_n^{G_0}$–module with the basis

$$\{Q_I dx_1 \ldots dx_n, dx_J\},$$

where I ranges over A_{n-1} and J ranges over B_n.

Now, we consider a K_n–basis for $K_n \otimes E_n$.

Proposition 7.2 *The elements*

$$Q_0 \ldots Q_{n-2} dx_1 \ldots dx_n, dx_2, \ldots, dx_n$$

form a K_n–basis for $K_n \otimes E_n^1$.

Proof For dimensional reasons, it suffices to show that the above elements are linearly independent in $K_n \otimes E_n^1$. Suppose that

$$a_1 Q_0 \dots Q_{n-2} dx_1 \dots dx_n + a_2 dx_2 + \dots + a_n dx_n = 0$$

in $K_n \otimes E_n^1$, where $a_1, \dots, a_n$ are in K_n. Then, since

$$Q_0 \dots Q_{n-2} dx_1 \dots dx_n = \sum_{i=1}^{n} (-1)^{n-i} e_{n-1}(x_1, \dots, \widehat{x}_i, \dots, x_n) dx_i,$$

we have

$$\begin{aligned} (-1)^{n-1} a_1 e_{n-1}(\widehat{x}_1, \dots, x_n) &= 0, \\ a_2 + (-1)^{n-2} a_1 e_{n-1}(x_1, \widehat{x}_2, \dots, x_n) &= 0, \\ &\vdots \\ a_n + (-1)^0 a_1 e_{n-1}(x_1, \dots, x_{n-1}, \widehat{x}_n) &= 0. \end{aligned}$$

Thus, solving this linear system, we obtain $a_1 = 0, \dots, a_n = 0$. □

Proposition 7.3 *The elements*

$$Q_I dx_1 \dots dx_n, dx_J$$

form a K_n–basis for $K_n \otimes E_n^r$, where $I \in A_{n-1,n-r}$ and $J \in B_{n,r}$.

Proof Again, for dimensional reasons, it suffices to show that the above elements are linearly independent in $K_n \otimes E_n^r$. Suppose that

$$\sum_{I \in A_{n-1,n-r}} a_I Q_I dx_1 \dots dx_n + \sum_{J \in B_{n,r}} b_J dx_J = 0,$$

where a_I, b_J are in K_n. The linear independence of the terms dx_J is clear. Hence, it remains to show that $a_I = 0$ for each I.

Fix $I \in A_{n-1,n-r}$ and let $K = S_{n-1} \backslash I$. Then, applying Q_K to the both sides of the above equality, we have

$$\operatorname{sign}(K, I) a_I Q_0 \dots Q_{n-2} dx_1 \dots dx_n + \alpha = 0$$

in $K_n \otimes E_n^1$, where α is a linear combination of $dx_2, \dots, dx_n$ over K_n. Hence, by Proposition 7.2, we have $a_I = 0$ for each $I \in A_{n-1,n-r}$. □

Suppose that a is in $P_n \otimes E_n^1$. Then, on the one hand, we may express a as follows:

$$a = \varphi_1 dx_1 + \cdots + \varphi_n dx_n,$$

where $\varphi_1, \ldots, \varphi_n$ are in P_n. On the other hand, by Proposition 7.2, we may express a as follows:

$$a = a_1 Q_0 \ldots Q_{n-2} dx_1 \ldots dx_n + a_2 dx_2 + \cdots + a_n dx_n,$$

where $a_1, \ldots, a_n$ are in K_n. Observe that terms a and φ are unique in the above expressions.

We need to show that $a_1, \ldots, a_n$ are in P_n if a is G_0–invariant.

Proposition 7.4 *There are polynomials a_i' over $\mathbb{F}_q$ in n variables such that*

$$a_i e_{n-1}(x_2, \ldots, x_n) = a_i'(x_1, \ldots, x_n)$$

for $i = 1, \ldots, n$.

Proof For $i = 1$, we apply $\mathcal{D}_{n-1}$ to a. Then, we have

$$\mathcal{D}_{n-1}(a) = \varphi_1 \mathcal{O}_{n-1}(x_1).$$

On the other hand, we have

$$\begin{aligned} \mathcal{D}_{n-1}(a) &= (-1)^{n-1} a_1 Q_0 \ldots Q_{n-1} dx_1 \ldots dx_n \\ &= (-1)^{n-1} a_1 \mathcal{O}_{n-1}(x_1) e_{n-1}(x_2, \ldots, x_n). \end{aligned}$$

Hence, we obtain

$$a_1 = (e_{n-1}(x_2, \ldots, x_n))^{-1} \varphi_1$$

and

$$a_1'(x_1, \ldots, x_n) = \varphi_1.$$

For $i = 2, \ldots, n$, applying $Q_0, \ldots, Q_{n-2}$ to a, we have a linear system

$$\begin{aligned} Q_0 a &= a_2 x_2 + \cdots + a_n x_n, \\ Q_1 a &= a_2 x_2^q + \cdots + a_n x_n^q, \\ &\vdots \\ Q_{n-2} a &= a_2 x_2^{q^{n-2}} + \cdots + a_n x_n^{q^{n-2}}. \end{aligned}$$

Writing this linear system in terms of matrix, we have

$$\begin{pmatrix} Q_0 a \\ Q_1 a \\ \vdots \\ Q_{n-2} a \end{pmatrix} = A \begin{pmatrix} a_2 \\ a_3 \\ \vdots \\ a_n \end{pmatrix},$$

where

$$A = \begin{pmatrix} x_2 & \dots & x_n \\ x_2^q & \dots & x_n^q \\ \vdots & \ddots & \vdots \\ x_2^{q^{n-2}} & \dots & x_n^{q^{n-2}} \end{pmatrix}.$$

It is clear that $\det A = e_{n-1}(x_2, \dots, x_n) \neq 0$. It is also clear that each entry of A is in P_{n-1}. Therefore, for some $\varphi_{i,j}$ in P_{n-1}, we have

$$a_i = e_{n-1}(x_2, \dots, x_n)^{-1} \left(\sum_{j=1}^{n} \varphi_{i,j} Q_j a \right).$$

Since $Q_j a$ is in P_n, by letting

$$a_i'(x_1, \dots, x_n) = \sum_{j=1}^{n} \varphi_{i,j} Q_j a,$$

we obtain the required results. □

Proposition 7.5 *Suppose that a is G_0–invariant. Then $a_i'(x_1, \dots, x_n)$ in Proposition 7.4 are also G_0–invariant for $i = 1, \dots, n$.*

Proof For $g \in G_0$, we have

$$g(dx_i) = dx_i$$

for $i = 2, \dots, n$ and, since $G_0 \subset SL_n(\mathbb{F}_q)$, we have

$$g(dx_1 \dots dx_n) = dx_1 \dots dx_n.$$

Since the action of Milnor operations Q_j commutes with the action of the general linear group $GL_n(\mathbb{F}_q)$, we have

$$g(Q_0 \dots Q_{n-2} dx_1 \dots dx_n) = Q_0 \dots Q_{n-2} dx_1 \dots dx_n.$$

Hence, we have

$$ga = (ga_1) Q_0 \dots Q_{n-2} dx_1 \dots dx_n + (ga_2) dx_2 + \dots + (ga_n) dx_n.$$

Thus, if $ga = a$, we have $ga_1 = a_1, \dots, ga_n = a_n$. It is also clear that $e_{n-1}(x_2, \dots, x_n)$ is G_0–invariant. Hence, $a'_i(x_1, \dots, x_n)$ are also G_0–invariant for $i = 1, \dots, n$. □

Proposition 7.6 *Suppose that a is G_0–invariant. Then, $a'_1(x_1, \dots .x_n)$ is divisible by x_n.*

Proof Let us consider the coefficient φ_n of dx_n; we have

$$\varphi_n e_{n-1}(x_2, \dots, x_n) = a'_n(x_1, \dots, x_n) + a'_1(x_1, \dots, x_n) e_{n-1}(x_1, \dots, x_{n-1}).$$

Since $a'_1(x_1, \dots, x_n)$ and $a'_n(x_1, \dots, x_n)$ are G_0–invariant, there are polynomials a''_1, a''_n over $\mathbb{F}_q$ in n variables such that

$$a'_1(x_1, \dots, x_n) = a''_1(\mathcal{O}_{n-1}(x_1), x_2, \dots, x_n),$$
$$a'_n(x_1, \dots, x_n) = a''_n(\mathcal{O}_{n-1}(x_1), x_2, \dots, x_n).$$

Since $\mathcal{O}_{n-1}(x_1), x_2, \dots, x_n$ are algebraically independent, it suffices to show that

$$a''_1(y_1, x_2, \dots, x_{n-1}, 0) = 0$$

for algebraically independent $y_1, x_2, \dots, x_{n-1}$.

Substituting $x_n = 0$, we have the obvious projection

$$\pi\colon \mathbb{F}_q[x_1, \dots, x_n] \to \mathbb{F}_q[x_1, \dots, x_{n-1}].$$

It is clear from Proposition 5.2 and Proposition 5.3 that

$$\begin{aligned}
\pi(e_{n-1}(x_1, \dots, x_{n-1})) &= e_{n-1}(x_1, \dots, x_{n-1}) \\
&= \mathcal{O}_{n-2}(x_1) e_{n-2}(x_2, \dots, x_{n-1}) \quad \text{for } n \geq 3, \\
\pi(e_1(x_1)) &= \mathcal{O}_0(x_1) \quad \text{for } n = 2, \\
\pi(e_{n-1}(x_2, \dots, x_n)) &= 0, \\
\pi(\mathcal{O}_{n-1}(x_1)) &= \mathcal{O}_{n-2}(x_1)^q.
\end{aligned}$$

Hence, for $n \geq 3$, we have

$$0 = a''_n(y^q, x_2, \dots, x_{n-1}, 0) + y a''_1(y^q, x_2, \dots, x_{n-1}, 0) e_{n-2}(x_2, \dots, x_{n-1}),$$

where $y = \mathcal{O}_{n-2}(x_1)$ and $y, x_2, \dots, x_{n-1}$ are algebraically independent. Applying the partial derivative $\partial/\partial y$, we have

$$a''_1(y^q, x_2, \dots, x_{n-1}, 0) e_{n-2}(x_2, \dots, x_{n-1}) = 0.$$

Hence, we have

$$a''_1(y^q, x_2, \dots, x_{n-1}, 0) = 0.$$

Since $y^q, x_2, \dots, x_{n-1}$ are algebraically independent, we have the required result.

For $n=2$, we have
$$0 = a_2''(y^q,0) + y a_1''(y^q,0).$$
Applying the partial derivative $\partial/\partial y$, we have
$$a_1''(y^q,0)=0$$
and the required result. □

Lemma 7.7 *Suppose that $g_1 \in GL_{n-1}(\mathbb{F}_q)$ and that a is G_0–invariant. Then, $\bar{g}_1 a$ is also G_0–invariant.*

Proof Suppose that for each g, there is a $g' \in G_0$ such that $g\bar{g}_1 = \bar{g}_1 g'$. If it is true, then for any G_0–invariant a, we have
$$g\bar{g}_1 a = \bar{g}_1 g' a = g_1 a.$$
Hence, g_1 induces a homomorphism from $P_n^{G_0}$ to $P_n^{G_0}$. So, it suffices to show that for each g in G_0, there is a $g' \in G_0$ such that $gg_1 = g_1 g'$, which is immediate from the following equality:
$$\left(\begin{array}{c|c} 1 & m \\ \hline 0 & 1_{n-1}\end{array}\right)\left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & g_1\end{array}\right) = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & g_1\end{array}\right)\left(\begin{array}{c|c} 1 & mg_1 \\ \hline 0 & 1_{n-1}\end{array}\right),$$
where $m \in M_{1,n-1}(\mathbb{F}_q)$ and 1_{n-1} stands for the identity matrix in $GL_{n-1}(\mathbb{F}_q)$. □

Proposition 7.8 *Suppose that a is G_0–invariant. Then, $a_1,\dots,a_n$ are in P_n.*

Proof Firstly, we verify that a_1 is in P_n. To this end, we prove that the element $a_1'(x_1,\dots,x_n)$ is divisible by $e_{n-1}(x_2,\dots,x_n)$. Let $\ell = \alpha_2 x_2 + \dots + \alpha_n x_n$, where $\alpha_2,\dots,\alpha_n \in \mathbb{F}_q$ and $\ell \neq 0$. By Proposition 5.6, it suffices to show that $a_1'(x_1,\dots,x_n)$ is divisible by ℓ. There is g_1 in $GL_{n-1}(\mathbb{F}_q)$ such that $\bar{g}_1(x_n)=\ell$. Since, by Lemma 7.7, $\bar{g}_1^{-1}a$ is also in $(P_n \otimes E_n^1)^{G_0}$, there is an element f in P_n such that
$$\mathcal{D}_{n-1}(\bar{g}_1^{-1}a) = f x_n \mathcal{O}_{n-1}(x_1).$$
Here we have
$$\mathcal{O}_{n-1}(x_1) a_1'(x_1,\dots,x_n) = \mathcal{D}_{n-1}(a) = \bar{g}_1 \mathcal{D}_{n-1}(\bar{g}_1^{-1}a) = \mathcal{O}_{n-1}(x_1)\bar{g}_1(f)\ell.$$
So we have
$$a_1'(x_1,\dots,x_n) = (\bar{g}_1 f)\ell.$$
Secondly, we verify that a_i are in P_n for $i=2,\dots,n$, which follows from the fact that
$$\varphi_i = a_i + (-1)^{n-i} a_1 e_{n-1}(x_1,\dots,\widehat{x}_i,\dots,x_n).$$ □

Proof of Proposition 7.1

Suppose that a is in $P_n \otimes E_n^r$ and G_0–invariant. By Proposition 7.3, there are a_I, $b_J \in K_n$ such that

$$a = \sum_{I \in A_{n-1,n-r}} a_I Q_I dx_1 \dots dx_n + \sum_{J \in B_{n,r}} b_J dx_J .$$

It suffices to show that a_I, b_J are in P_n.

Firstly, we verify that a_I is in P_n. Choose I and let $K = S_{n-1} \setminus I$. Then, we have

$$Q_K a = \operatorname{sign}(K, I) a_I Q_0 \dots Q_{n-2} dx_1 \dots dx_n + \sum_{J \in B_{n,r}} b_J Q_K dx_J .$$

By Proposition 7.8, $\operatorname{sign}(K, I) a_I$ is in P_n and, by definition, $\operatorname{sign}(K, I) \neq 0$, hence a_I is also in P_n.

Secondly, we prove that b_J is in P_n. Put

$$a' = a - \sum_{I \in A_{n-1,n-r}} a_I Q_I dx_1 \dots dx_n = \sum_{J \in B_{n,r}} b_J dx_J .$$

It is clear that a' is also in $P_n \otimes E_n^r$. Hence, b_J is in P_n. This completes the proof. □

Now, we complete the proof of Theorem 4.2.

Proof of Theorem 4.2

Suppose that a is an element in $P_n \otimes E_n$ and that a is also G–invariant. It suffices to show that a is a linear combination of $\{v_i, Q_I dx_1 \dots, dx_n\}$ over P_n^G. It is clear that a is also G_0–invariant. Hence, by Proposition 7.1, there are a_I, b_J in $P_n^{G_0} = \mathbb{F}_q[\mathcal{O}_{n-1}(x_1), x_2 \dots, x_n]$ such that

$$a = \sum_I a_I Q_I dx_1 \dots dx_n + \sum_J b_J dx_J .$$

Thus, we have

$$a = \sum_I \sum_{k \geq 0} a_{I,k} \mathcal{O}_{n-1}(x_1)^k Q_I dx_1 \dots dx_n + \sum_J \sum_{k \geq 0} b_{J,k} \mathcal{O}_{n-1}(x_1)^k dx_J ,$$

where $a_{I,k}$, $b_{J,k}$ are in $P_{n-1} = \mathbb{F}_q[x_2, \dots, x_n]$. Since, by Theorem 4.1, $g \in G$ acts trivially on $\mathcal{O}_{n-1}(x_1)$, and since $g \in G \subset SL_n(\mathbb{F}_q)$ acts trivially on $Q_I dx_1 \dots dx_n$, we have

$$ga = \sum_{k \geq 0} \sum_I (g a_{I,k}) \mathcal{O}_{n-1}(x_1)^k Q_I dx_1 \dots dx_n + \sum_{k \geq 0} \sum_J (g b_{J,k}) \mathcal{O}_{n-1}(x_1)^k (g dx_J).$$

It is clear that gdx_J is in E_{n-1}. As a P_{n-1}–module, $(P_n \otimes E_n^r)^{G_0}$ is a free P_{n-1}–module with the basis

$$\{\mathcal{O}_{n-1}(x_1)^k dx_J, \mathcal{O}_{n-1}(x_1)^k Q_I dx_1 \dots dx_n\}.$$

Hence, we have

$$g(a_{I,k}) = a_{I,k}.$$

Thus, $a_{I,k}$ is in ${P_{n-1}}^{G_1}$ and so a_I is in P_n^G. Put

$$a' = a - \sum_I a_I Q_I dx_1 \dots dx_n.$$

Then, a' is also in the ring of invariants $(P_n \otimes E_n)^G$, and we have

$$a' = \sum_{k \geq 0} \left(\sum_J b_{J,k} dx_J \right) \mathcal{O}_{n-1}(x_1)^k.$$

Hence, $\sum_J b_{J,k} dx_J$ is in the ring of invariants $(P_{n-1} \otimes E_{n-1})^{G_1}$. By the assumption on the ring of invariants $(P_{n-1} \otimes E_{n-1})^{G_1}$, there are polynomials $b_{1,k}, \dots, b_{2^{n-1},k}$ in $P_{n-1}^{G_1}$ such that

$$\sum_J b_{J,k} dx_J = \sum_{i=1}^{2^{n-1}} b_{i,k} v_i.$$

Thus, writing b_i for $\sum_{k \geq 0} b_{i,k} \mathcal{O}_{n-1}(x_1)^k$, we have

$$a = \sum_{i=1}^{2^{n-1}} b_i v_i + \sum_I a_I Q_I dx_1 \dots dx_n,$$

where b_i, a_I are in P_n^G. This completes the proof. □

Appendix A

In [7], Mùi used the determinant of the $k \times k$ matrix $\left(x_j^{q^{i_\ell}}\right)$ whose (ℓ, j) entry is $x_j^{q^{i_\ell}}$ to describe the Dickson invariant $[i_1, \dots, i_k]$. Using these Dickson invariants, he defined the Mùi invariant $[r : i_1, \dots, i_{n-r}]$. In this appendix, we verify in Proposition A.4 that the Mùi invariant

$$Q_{i_1} \dots Q_{i_{n-r}} dx_1 \dots dx_n$$

in this paper is indeed equal to the Mùi invariant $[r : i_1, \dots, i_{n-r}]$, up to sign.

Firstly, we recall the definitions. See [7, Section 2] for the definition of $[i_1, \dots, i_k]$ and and [7, Defintion 4.3] for the definition of $[r : i_1, \dots, i_{n-r}]$.

Definition A.1 The Dickson invariant $[i_1, \dots, i_k](x_1, \dots, x_k) \in \mathbb{F}_q[x_1, \dots, x_k]$ is defined by

$$\sum_\sigma \mathrm{sgn}(\sigma) x_{\sigma(1)}^{q^{i_1}} \dots x_{\sigma(k)}^{q^{i_k}} = \det(x_j^{q^{i_\ell}}),$$

where σ ranges over the set of permutations of $\{1, \dots, k\}$ and $\mathrm{sgn}(\sigma)$ is the sign of the permutation σ.

Definition A.2 The Mùi invariant $[r : i_1, \dots, i_{n-r}] \in P_n \otimes E_n^r$ is defined by

$$[r : i_1, \dots, i_{n-r}] = \sum_J \mathrm{sgn}(\sigma_J) dx_{j_1} \dots dx_{j_r} [i_1, \dots, i_{n-r}](x_{j_{r+1}}, \dots, x_{j_n}),$$

where

$$\sigma_J = \begin{pmatrix} 1, & \dots, & n \\ j_1, & \dots, & j_n \end{pmatrix}$$

ranges over the set of permutations of $\{1, \dots, n\}$ such that $j_1 < \dots < j_r$ and $j_{r+1} < \dots < j_n$. The above σ_J corresponds to the subset $J = \{j_1, \dots, j_r\}$ of order r of $\{1, \dots, n\}$.

Secondly, we prove the following proposition.

Proposition A.3 *There holds*

$$\begin{aligned} [i_1, \dots, i_k](x_1, \dots, x_k) &= Q_{i_k} \dots Q_{i_1} dx_1 \dots dx_k \\ &= (-1)^{k(k-1)/2} Q_{i_1} \dots Q_{i_k} dx_1 \dots dx_k. \end{aligned}$$

Proof We prove the first equality in this proposition by induction on k. Indeed, in the case $k = 1$, the proposition holds. Suppose that $k \geq 2$ and that there holds the equality

$$[i_2, \dots, i_k](x_1, \dots, x_{k-1}) = Q_{i_k} \dots Q_{i_2} dx_1 \dots dx_{k-1}.$$

Using the cofactor expansion (or the Laplace development) of the $k \times k$ matrix $(x_j^{q^{i_\ell}})$ along the first row

$$(x_1^{q^{i_1}}, x_2^{q^{i_1}}, \dots, x_k^{q^{i_1}}),$$

we have

$$\begin{aligned}[i_1,\dots,i_k](x_1,\dots,x_k) &= \sum_{s=1}^{k}(-1)^{s+1}[i_2,\dots,i_k](x_1,\dots,\widehat{x}_s,\dots,x_k)x_s^{q^{i_1}}\\ &= \sum_{s=1}^{k}(-1)^{s+1}(Q_{i_k}\dots Q_{i_2}dx_1\dots\widehat{dx}_s\dots dx_k)x_s^{q^{i_1}}\\ &= Q_{i_k}\dots Q_{i_2}\left(\sum_{s=1}^{k}(-1)^{s+1}x_s^{q^{i_1}}dx_1\dots\widehat{dx}_s\dots dx_k\right)\\ &= Q_{i_k}\dots Q_{i_1}dx_1\dots dx_k.\end{aligned}$$

So, the first equality holds. The second equality is immediate from the fact that

$$Q_{i_k}\dots Q_{i_1} = (-1)^{k(k-1)/2}Q_{i_1}\dots Q_{i_k}. \qquad \square$$

Finally, we state and prove the following proposition.

Proposition A.4 *There holds*

$$\begin{aligned}[r : i_1,\dots,i_{n-r}] &= (-1)^{(n-r)r}Q_{i_{n-r}}\dots Q_{i_1}dx_1\dots dx_n\\ &= (-1)^{(n-r)r+(n-r)(n-r-1)/2}Q_{i_1}\dots Q_{i_{n-r}}dx_1\dots dx_n.\end{aligned}$$

Proof As in the definition of $[r : i_1,\dots,i_{n-r}]$, let σ_J be a permutation of $\{1,\dots,n\}$ with $\sigma_J(1)<\dots<\sigma_J(r)$, $\sigma_J(r+1)<\dots<\sigma_J(n)$ and we denote by j_k the value $\sigma_J(k)$ of σ_J at k. Let $I(J)$ be the ideal of $P_n\otimes E_n$ generated by $dx_{j_{r+1}},\dots,dx_{j_n}$. Let

$$p_J\colon P_n\otimes E_n\to P_n\otimes E_n/I(J)$$

be the projection. It is clear that

$$P_n\otimes E_n^r/((P_n\otimes E_n^r)\cap I(J)) = P_n$$

and for f in $P_n\otimes E_n^r$, we have

$$f = \sum_J p_J(f)dx_{j_1}\dots dx_{j_r}.$$

So, by Proposition A.3, in order to prove the proposition, it suffices to show that

$$p_J(Q_{i_{n-r}}\dots Q_{i_1}dx_1\dots dx_n) = (-1)^{(n-r)r}\operatorname{sgn}(\sigma_J)Q_{i_{n-r}}\dots Q_{i_1}dx_{j_{r+1}}\dots dx_{j_n}.$$

Suppose that

$$\psi(Q_{i_{n-r}}\dots Q_{i_1}) = 1\otimes Q_{i_{n-r}}\dots Q_{i_1}+\sum a\otimes a',$$

where ψ is the coproduct of the Steenrod algebra. We may choose a', so that $a' = Q_{e_1} \dots Q_{e_\ell}$ and $\ell < n-r$. Thus, $a'(dx_{j_{r+1}} \dots dx_{j_n})$ belongs to $I(J)$.

Then, there holds

$$\begin{aligned} & Q_{i_{n-r}} \dots Q_{i_1} dx_1 \dots dx_n \\ = \; & \operatorname{sgn}(\sigma_J) Q_{i_{n-r}} \dots Q_{i_1} dx_{j_1} \dots dx_{j_n} \\ = \; & (-1)^{(n-r)r} \operatorname{sgn}(\sigma_J) dx_{j_1} \dots dx_{j_r} Q_{i_{n-r}} \dots Q_{i_1} dx_{j_{r+1}} \dots dx_{j_n} \\ & + \sum (-1)^{r \deg a'} \operatorname{sgn}(\sigma_J)(a dx_{j_1} \dots dx_{j_r})(a' dx_{j_{r+1}} \dots dx_{j_n}). \end{aligned}$$

Hence, we have

$$p_J(Q_{i_{n-r}} \dots Q_{i_1} dx_1 \dots dx_n) = (-1)^{(n-r)r} \operatorname{sgn}(\sigma_J) Q_{i_{n-r}} \dots Q_{i_1} dx_{j_{r+1}} \dots dx_{j_n}$$

as required. □

References

[1] **K Andersen**, **J Grodal**, **J Møller**, **A Viruel**, *The classification of p–compact groups for p odd* arXiv:math.AT/0302346

[2] **D J Benson**, *Polynomial invariants of finite groups*, London Mathematical Society Lecture Note Series 190, Cambridge University Press, Cambridge (1993) MR1249931

[3] **M C Crabb**, *Dickson–Mùi invariants*, Bull. London Math. Soc. 37 (2005) 846–856 MR2186717

[4] **L E Dickson**, *A fundamental system of invariants of the general modular linear group with a solution of the form problem*, Trans. Amer. Math. Soc. 12 (1911) 75–98 MR1500882

[5] **R L Griess, Jr**, *Elementary abelian p–subgroups of algebraic groups*, Geom. Dedicata 39 (1991) 253–305 MR1123145

[6] **M Kameko**, **M Mimura**, *On the Rothenberg-Steenrod spectral sequence for the* mod 3 *cohomology of the classifying space of the exceptional Lie group E_8*, from: "Proceedings of the Nishida Fest (Kinosaki 2003)", Geometry and Topology Monographs 10, Mathematical Sciences Publishers 209–222

[7] **H Mùi**, *Modular invariant theory and cohomology algebras of symmetric groups*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 22 (1975) 319–369 MR0422451

[8] **L Smith**, *Polynomial invariants of finite groups*, Research Notes in Mathematics 6, A K Peters Ltd., Wellesley, MA (1995) MR1328644

[9] **C Wilkerson**, *A primer on the Dickson invariants*, from: "Proceedings of the Northwestern Homotopy Theory Conference (Evanston, Ill., 1982)", Contemp. Math. 19, Amer. Math. Soc., Providence, RI (1983) 421–434 MR711066A corrected version is available at the Hopf Topology Archive.

Department of Mathematics, Faculty of Regional Science
Toyama University of International Studies, 65-1 Higashikuromaki, Toyama, 930-1292, Japan

Department of Mathematics, Faculty of Science, Okayama University
3-1-1 Tsushima-naka, Okayama, 700-8530, Japan

kameko@tuins.ac.jp, mimura@math.okayama-u.ac.jp

Received: 26 Feb 2005 Revised: 12 Sept 2005