Saitama Math. J.
Vol. 29 (2012), 55–64

The image membership algorithm for twisted derivations in modular invariant theory

Ryuji Tanimoto

(*Received 7 July, 2012; Revised 30 August, 2012; Accepted 4 September, 2012*)

Abstract

Let k be a field of positive characteristic p, let $k[x]$ be the polynomial ring in n variables over k, and let σ be a k-algebra automorphism of $k[x]$ whose order is p. We define the twisted derivation $D_\sigma : k[x] \to k[x]$ by $D_\sigma(a) := \sigma(a) - a$ for all $a \in k[x]$. We give an algorithm to determine whether or not a given polynomial of $k[x]$ belongs to the image $D_\sigma(k[x])$ of D_σ.

1. Introduction

Let k be a field of positive characteristic p and let A be a k-domain. We denote by $\mathrm{Aut}_k(A)$ the group of all k-algebra automorphisms of A. The multipication of the group $\mathrm{Aut}_k(A)$ is defined by the composition of automorphisms. Let σ be an element of $\mathrm{Aut}_k(A)$ whose order is p. Associating with the automorphism σ, we can define a k-linear transformation $D_\sigma : A \to A$ as $D_\sigma(a) := \sigma(a) - a$ for all $a \in A$. The k-linear transformation D_σ has the following two properties:

(1) $D_\sigma(a \cdot b) = D_\sigma(a) \cdot \sigma(b) + a \cdot D_\sigma(b)$ for all $a, b \in A$.

(2) $D_\sigma^p = 0$.

We say that D_σ is a *twisted derivation* associated to σ. For each $1 \leq i \leq p-1$, we define the *kernel* $A^{D_\sigma^i}$ of D_σ^i as

$$A^{D_\sigma^i} := \{a \in A \mid D_\sigma^i(a) = 0\},$$

and define the *image* $D_\sigma^i(A)$ of D_σ^i as

$$D_\sigma^i(A) := \{D_\sigma^i(a) \in A \mid a \in A\}.$$

For simplicity, we express $A^{D_\sigma^1}$ as A^{D_σ} and express $D_\sigma^1(A)$ as $D_\sigma(A)$. Then A^{D_σ} is a k-subalgebra of A, each $A^{D_\sigma^i}$ is an A^{D_σ}-module, and each $D_\sigma^i(A)$ is an A^{D_σ}-module. We assume that the following conditions (i) and (ii) are satisfied

2010 Mathematics Subject Classification. Primary 13A50; Secondary 20J06
Key words and phrases. twisted derivations, modular invariant theory
Partially supported by Grant-in-Aid for Young Scientists (B) (No. 22740009) from JSPS.

(especially when $A = k[x_1, \ldots, x_n]$ is a polynomial ring in n variables over k, the following conditions (i) and (ii) are satisfied):

(i) The kernel A^{D_σ} is a Noetherian ring.

(ii) The A^{D_σ}-module A is finite as an A^{D_σ}-module.

Then the kernel $A^{D_\sigma^i}$ and the image $D_\sigma^i(A)$ are finite as A^{D_σ}-modules for all $1 \leq i \leq p-1$. We have the inclusion $D_\sigma^{p-i}(A) \subset A^{D_\sigma^i}$ for all $1 \leq i \leq p-1$. It is an interesting problem to construct a generating set of the A^{D_σ}-module

$$A^{D_\sigma^i}/D_\sigma^{p-i}(A)$$

for each $1 \leq i \leq p-1$. We explain the reason why the problem is interesting in connection with modular invariant theory. We know that the kernel A^{D_σ} of D_σ coincides with the invariant ring $A^{\langle\sigma\rangle}$ of the cyclic group $\langle\sigma\rangle$ generated by σ, and the image $D_\sigma^{p-1}(A)$ of D_σ^{p-1} coincides with the image $\mathrm{Tr}^G(A)$ of the transfer Tr^G, where the transfer $\mathrm{Tr}^G : A \to A$ is defined by $\mathrm{Tr}^G(a) := \sum_{i=0}^{p-1} \sigma^i(a)$ for all $a \in A$. The i-th cohomology $H^i(\langle\sigma\rangle, A)$ of the cyclic group $\langle\sigma\rangle$ with coefficients in A has the following expression (see [2, Page 6]):

$$H^i(\langle\sigma\rangle, A) = \begin{cases} A^{D_\sigma} & \text{if} \quad i = 0, \\ A^{D_\sigma^{p-1}}/D_\sigma(A) & \text{if} \quad i \text{ odd}, \\ A^{D_\sigma}/D_\sigma^{p-1}(A) & \text{if} \quad i \text{ even and } i > 0. \end{cases}$$

So, the problem is related to constructing a generating set of the i-th cohomology $H^i(\langle\sigma\rangle, A)$ as an A^{D_σ}-module for $i > 0$. In particular when $p = 3$, constructing a generating set of $H^1(\langle\sigma\rangle, A)$ as an A^{D_σ}-module is related to constructing a generating set of $A^{D_\sigma^2}$ as an A^{D_σ}-module. A generating set of the kernel $A^{D_\sigma^2}$ can be constructed from a generating set of the ideal $D_\sigma(A) \cap A^{D_\sigma}$ of A^{D_σ} since $D_\sigma(A^{D_\sigma^2}) = D_\sigma(A) \cap A^{D_\sigma}$. It seems that the image membership algorithm for the twisted derivation D_σ is useful for guessing a generating set of the ideal $D_\sigma(A) \cap A^{D_\sigma}$.

In this article, we give an algorithm to determine whether or not a given polynomial of $k[x_1, \ldots, x_n]$ belongs to the image $D_\sigma(k[x_1, \ldots, x_n])$. As an application, in particular when $p = 3$ and a cyclic group $\langle\sigma\rangle$ of order three acting linearly and irreducibly on $k[x_1, x_2, x_3]$, we give a generating set of the i-th cohomology $H^i(\langle\sigma\rangle, k[x_1, x_2, x_3])$ of the cyclic group $\langle\sigma\rangle$ with coefficients in $k[x_1, x_2, x_3]$ as a $k[x_1, x_2, x_3]^{D_\sigma}$-module for each $i = 1, 2$.

2. The image membership algorithm

An element a of A is said to be *D_σ-integrable* if there exists an element b of A such that $D_\sigma(b) = a$.

Lemma 1. *Let a be a D_σ-integrable element of A. Then we have $D_\sigma^{p-1}(a) = 0$.*

Proof. Since a is D_σ-integrable, there exists an element b of A such that $D_\sigma(b) = a$. So, we have $D_\sigma^{p-1}(a) = D_\sigma^p(b) = 0$. Q.E.D.

An element s of A is said to be a *slice* of D_σ if $D_\sigma(s) = 1$. For any element a of A and any integer i with $1 \leq i \leq p-1$, we define the symbol $\binom{a}{i}$ as

$$\binom{a}{i} := \begin{cases} 1 & \text{if} \quad i = 0, \\ \dfrac{a(a-1)\cdots(a-(i-1))}{i!} & \text{if} \quad 1 \leq i \leq p-1. \end{cases}$$

Lemma 2. *Let s be a slice of D_σ. Then we have*

$$D_\sigma\left(\binom{-s}{i+1}\right) = -\binom{-s-1}{i}$$

for all $0 \leq i \leq p-2$.

Proof. We know from the definition of D_σ that

$$D_\sigma\left(\binom{-s}{i+1}\right) = \sigma\left(\frac{(-s)(-s-1)\cdots(-s-i)}{(i+1)!}\right) - \frac{(-s)(-s-1)\cdots(-s-i)}{(i+1)!}.$$

Since s is a slice of D_σ, we have $\sigma(s) = s+1$ and thereby have

$$\sigma\left(\frac{(-s)(-s-1)\cdots(-s-i)}{(i+1)!}\right) = \frac{(-s-1)(-s-2)\cdots(-s-(i+1))}{(i+1)!}.$$

Now we have

$$\begin{aligned} D_\sigma\left(\binom{-s}{i+1}\right) &= \frac{(-s-1)\cdots(-s-i)}{(i+1)!} \cdot (-s-(i+1)-(-s)) \\ &= -\frac{(-s-1)\cdots(-s-i)}{i!} \\ &= -\binom{-s-1}{i}. \end{aligned}$$

Q.E.D.

Lemma 3. *Let s be a slice of D_σ. Then, for any element a of A satisfying the condition $D_\sigma^{p-1}(a) = 0$, we have the equality*

$$D_\sigma\left(-\sum_{i=0}^{p-2} D_\sigma^i(a) \cdot \binom{-s}{i+1}\right) = a.$$

PROOF. Since D_σ is a twisted derivation associated to σ, we have

$$\begin{aligned}
&D_\sigma\left(-\sum_{i=0}^{p-2} D_\sigma^i(a)\cdot\binom{-s}{i+1}\right)\\
&= -\sum_{i=0}^{p-2}\left(D_\sigma^{i+1}(a)\cdot\sigma\left(\binom{-s}{i+1}\right)+D_\sigma^i(a)\cdot D_\sigma\left(\binom{-s}{i+1}\right)\right).
\end{aligned}$$

The right hand side of the above equality can be calculated by Lemma 2 and the condition $D_\sigma^{p-1}(a)=0$, as follows:

$$\begin{aligned}
&-\sum_{i=0}^{p-2}\left(D_\sigma^{i+1}(a)\cdot\binom{-s-1}{i+1}-D_\sigma^i(a)\cdot\binom{-s-1}{i}\right)\\
&= -\sum_{i=0}^{p-2} D_\sigma^{i+1}(a)\cdot\binom{-s-1}{i+1}+\sum_{i=0}^{p-2} D_\sigma^i(a)\cdot\binom{-s-1}{i}\\
&= -\sum_{i=0}^{p-3} D_\sigma^{i+1}(a)\cdot\binom{-s-1}{i+1}+\sum_{i=0}^{p-2} D_\sigma^i(a)\cdot\binom{-s-1}{i}\\
&= -\sum_{i=0}^{p-3} D_\sigma^{i+1}(a)\cdot\binom{-s-1}{i+1}+\sum_{i=1}^{p-2} D_\sigma^i(a)\cdot\binom{-s-1}{i}+a\\
&= a.
\end{aligned}$$

Thus we have the desired equlity. Q.E.D.

From now on, we assume that A is the polynomial ring $k[x] := k[x_1,\dots,x_n]$ in n variables over k. Now, σ is a k-automorphism of $k[x]$ of order p.

Since $k[x]\neq k[x]^{D_\sigma}$, there exists a polynomial $\alpha\in k[x]$ not belonging to $k[x]^{D_\sigma}$. So, $D_\sigma^m(\alpha)\neq 0$ and $D_\sigma^{m+1}(\alpha)=0$ for some $1\leq m\leq p-1$. Let $d := D_\sigma^m(\alpha)\in k[x]$ and let $s := D_\sigma^{m-1}(\alpha)/d\in k[x][1/d]$. We can naturally extend the automorphism σ of $k[x]$ to an automorphism $\widetilde{\sigma}$ of $k[x][1/d]$. The order of $\widetilde{\sigma}$ is p and the element s of $k[x][1/d]$ is a slice of $D_{\widetilde{\sigma}}$.

We know that the invariant ring $k[x]^{\langle\sigma\rangle}$ is finitely generated as a k-algebra. So, let $f_1,\dots,f_r$ be a generating set of $k[x]^{D_\sigma}$ as a k-algebra, i.e., $k[x]^{D_\sigma}=k[f_1,\dots,f_r]$. Let $k[x,y] := k[x_1,\dots,x_n,y_1,\dots,y_r]$ be the polynomial ring in $n+r$ variables over k. Let I be the ideal

$$I := (y_1-f_1,\dots,y_r-f_r,d^{p-1})$$

of $k[x,y]$. Let $\prec$ be a term order of $k[x,y]$ satisfying $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}\succ y_j$ for all $i_1,i_2,\dots,i_n\geq 0$ excluding the case where $i_1=i_2=\cdots=i_n=0$ and for all $1\leq j\leq r$. Let G be a Gröbner basis of I with respect to the term order $\prec$. For any polynomial f of $k[x]$, we denote by f_* the normal form of f with respect to the Gröbner basis G.

Theorem 4. *Let $k[x], \sigma, d, s, k[x, y], \prec, G$ be as above. Let a be a polynomial of $k[x]$. Let b' and β be the elements of $k[x][1/d]$ defined by*

$$\begin{cases} b' := -\displaystyle\sum_{i=0}^{p-2} D_\sigma^i(a) \cdot \binom{-s}{i+1}, \\ \beta := d^{p-1}b'. \end{cases}$$

Then the following assertions (1), (2) and (3) hold true:

(1) *The element β of $k[x][1/d]$ belongs to $k[x]$.*

(2) *The following conditions (i) and (ii) are equivalent:*
 (i) *The polynomial a of $k[x]$ is D_σ-integrable.*
 (ii) *The equality $D_\sigma^{p-1}(a) = 0$ holds true, and the normal form β_* of β with respect to G belongs to $k[y]$, where $k[y] := k[y_1, \ldots, y_r]$ is the polynomial ring in r variables over k.*

(3) *If the equivalent conditions (i) and (ii) in assertion (2) are satisfied, then $b := (\beta - \beta_*(f_1, \ldots, f_r))/d^{p-1} \in k[x]$ and $D_\sigma(b) = a$.*

Proof. Assertion (1) is clear from the definition of β.

We prove (i) $\Longrightarrow$ (ii) in assertioin (2). We have only to show the latter statement of (ii) in assertion (2) (see Lemma 1). There exists an element b of A such that $D_\sigma(b) = a$. We know from Lemma 3 that

$$D_\sigma(\beta - d^{p-1}b) = D_\sigma(d^{p-1}b' - d^{p-1}b) = d^{p-1}D_{\widetilde{\sigma}}(b') - d^{p-1}D_\sigma(b) = 0.$$

So, we have

$$\beta - d^{p-1}b = h(f_1, \ldots, f_r)$$

for some $h(y_1, \ldots, y_r) \in k[y]$. Since $d^{p-1} \in I$ and $y_1 - f_1, \ldots, y_r - f_r \in I$, we have

$$\beta - h(y_1, \ldots, y_r) \in I.$$

Thus we have $\beta_* - h(y_1, \ldots, y_r)_* = 0$, which implies $\beta_* \in k[y]$ by the condition of the term order $\prec$.

We prove (ii) $\Longrightarrow$ (i) in assertion (2). Since β reduces to β_* with respspect to G, we have

$$\beta = \sum_{i=1}^{r} c_i(y_i - f_i) + c'd^{p-1} + \beta_*$$

for some polynomials $c_1, \ldots, c_r, c' \in k[x, y]$. Substituting f_i for y_i for all $1 \leq i \leq r$, we have

$$\beta = c'(x, f_1, \ldots, f_r)d^{p-1} + \beta_*(f_1, \ldots, f_r).$$

Differentiating this equality with D_σ, we have $D_\sigma(\beta) = D_\sigma(c'(x, f_1, \ldots, f_r))d^{p-1}$. Since $\beta = d^{p-1}b'$, we have

$$D_{\tilde{\sigma}}(b') = D_\sigma(c'(x, f_1, \ldots, f_r)).$$

Note that $D_{\tilde{\sigma}}(b') = a$. In fact, since $D_{\tilde{\sigma}}$ has a slice s and $D_{\tilde{\sigma}}^{p-1}(a)(= D_\sigma^{p-1}(a)) = 0$, we know form Lemma 3 that $D_{\tilde{\sigma}}(b') = a$. Thus, we have

$$D_\sigma(c'(x, f_1, \ldots, f_r)) = a,$$

which implies that a is D_σ-integrable.

We prove assertion (3). Assume that the condition (ii) in assertion (2) is satisfied. We have already shown that

$$\begin{cases} D_\sigma(c'(x, f_1, \ldots, f_r)) & = & a, \\ c'(x, f_1, \ldots, f_r) & = & \dfrac{\beta - \beta_*(f_1, \ldots, f_r)}{d^{p-1}}. \end{cases}$$

Hence, we have $b \in k[x]$ and $D_\sigma(b) = a$. Q.E.D.

3. An application

Assume that the characteristic of k is three, assume that A is the polynomial ring $k[x] := k[x_1, x_2, x_3]$ in three variables over k, and assume that the k-algebra automorphism σ of $k[x]$ is defined by

$$\sigma(x_i) := \begin{cases} x_1 & \text{if} \quad i = 1, \\ x_i + x_{i-1} & \text{if} \quad i > 1. \end{cases}$$

Clearly, the order of σ is three. The kernel $k[x]^{D_\sigma}$ of the twisted derivation D_σ is generated as a k-algebra by the following four polynomials f_1, f_2, f_3, f_4 (see [1]):

$$\begin{aligned} f_1 &:= x_1, \\ f_2 &:= x_1x_2 + 2x_2^2 + 2x_1x_3, \\ f_3 &:= 2x_1^2x_2 + x_2^3, \\ f_4 &:= x_1x_2x_3 + 2x_2^2x_3 + x_1x_3^2 + x_3^3. \end{aligned}$$

As an application of the image membership algorithm, we can find a generating set of the i-th cohomology $H^i(\langle\sigma\rangle, k[x])$ of the cyclic group $\langle\sigma\rangle$ with coefficients in $k[x]$ for each $i = 1, 2$. Recall that the cohomology $H^i(\langle\sigma\rangle, k[x])$ has the following expression:

$$H^i(\langle\sigma\rangle, k[x]) = \begin{cases} k[x]^{D_\sigma} & \text{if} \quad i=0, \\ k[x]^{D_\sigma^2}/D_\sigma(k[x]) & \text{if} \quad i=1, \\ k[x]^{D_\sigma}/D_\sigma^2(k[x]) & \text{if} \quad i=2. \end{cases}$$

So, we construct a generating set of the $k[x]^{D_\sigma}$-module $k[x]^{D_\sigma^2}$, a generating set of the $k[x]^{D_\sigma}$-module $D_\sigma(k[x])$, and a generating set of the $k[x]^{D_\sigma}$-module $D_\sigma^2(k[x])$.

Theorem 5. (1) *We have*

$$k[x]^{D_\sigma^2} = k[x]^{D_\sigma} + k[x]^{D_\sigma} \cdot g_1 + k[x]^{D_\sigma} \cdot g_2 + k[x]^{D_\sigma} \cdot g_3,$$

where the polynomials g_1, g_2, g_3 *are defined by*

$$\begin{aligned} g_1 &:= x_2, \\ g_2 &:= 2x_1x_2 + x_2^2 + 2x_2x_3, \\ g_3 &:= x_1x_2^2 + 2x_2^3 + 2x_1x_2x_3 + x_2^2x_3 + 2x_1x_3^2. \end{aligned}$$

(2) *We have*

$$D_\sigma(k[x]) = k[x]^{D_\sigma} \cdot h_1 + k[x]^{D_\sigma} \cdot h_2 + k[x]^{D_\sigma} \cdot h_3 + k[x]^{D_\sigma} \cdot h_4 + k[x]^{D_\sigma} \cdot h_5,$$

where the polynomials h_1, h_2, h_3, h_4, h_5 *are defined by*

$$\begin{aligned} h_1 &:= D_\sigma(x_2) &&= x_1, \\ h_2 &:= D_\sigma(x_3) &&= x_2, \\ h_3 &:= D_\sigma(x_2x_3) &&= x_1x_2 + x_2^2 + x_1x_3, \\ h_4 &:= D_\sigma(x_3^2) &&= x_2^2 + 2x_2x_3, \\ h_5 &:= D_\sigma(x_2x_3^2) &&= x_1x_2^2 + x_2^3 + 2x_1x_2x_3 + 2x_2^2x_3 + x_1x_3^2. \end{aligned}$$

(3) *We have*

$$D_\sigma^2(k[x]) = k[x]^{D_\sigma} \cdot h_2' + k[x]^{D_\sigma} \cdot h_4' + k[x]^{D_\sigma} \cdot h_5',$$

where the polynomials h_2', h_4', h_5' *are defined by*

$$\begin{aligned} h_2' &:= D_\sigma(h_2) &&= x_1, \\ h_4' &:= D_\sigma(h_4) &&= x_1^2 + x_1x_2 + 2x_2^2 + 2x_1x_3, \\ h_5' &:= D_\sigma(h_5) &&= 2x_1^3 + x_1x_2^2 + 2x_2^3 + x_1^2x_3. \end{aligned}$$

In order to know whether each polynomial f_i $(1 \le i \le 4)$ belongs to the image $D_\sigma(k[x])$ or not, we run the image membership algorithm in Section 1 to each f_i $(1 \le i \le 4)$. Using a computational software program Mathematica 8, we know that all f_i $(1 \le i \le 3)$ are D_σ-integrable, the equalities $D_\sigma(g_i) = f_i$ $(1 \le i \le 3)$ hold true, and f_4 is not D_σ-integrable. We can check by hand that $D_\sigma(g_i) = f_i$ for all $1 \le i \le 3$. We can generalize the non-integrability of f_4 as in the following Lemma.

Lemma 6. *Let $\varphi(t) \in k[t]$ be a non-zero polynomial. Then $\varphi(f_4)$ is not D_σ-integrable.*

Proof. We first consider the case where $\varphi(t)$ is a non-zero element of k. Any non-zero element of k is not D_σ-integrable. So, the polynomial $\varphi(f_4)(= \varphi(t))$ is not D_σ-integrable.

We next consider the case where $\varphi(t)$ is a polynomial of degree ≥ 1 in t. Then $\varphi(f_4) = D_\sigma(g)$ for some polynomial $g \in k[x]$. Among monomials appearing in f_4, the monomial x_3^3 is the unique monomial of highest degree in x_3. So, the monomial x_3^{3m} appears in $\varphi(f_4)$, where m is the degree of $\varphi(t)$ in t. We can write g as

$$g = \sum_{i_1, i_2, i_3 \geq 0} a_{i_1,i_2,i_3} x_1^{i_1} x_2^{i_2} x_3^{i_3}$$

for some $a_{i_1,i_2,i_3} \in k$ where $i_1, i_2, i_3 \geq 0$. Then we have

$$D_\sigma(g) = \sum_{i_1, i_2, i_3 \geq 0} a_{i_1,i_2,i_3} D_\sigma(x_1^{i_1} x_2^{i_2} x_3^{i_3}).$$

Expand $D_\sigma(x_1^{i_1} x_2^{i_2} x_3^{i_3})$ as a polynomial in x_3, as follows:

$$\begin{aligned} D_\sigma(x_1^{i_1} x_2^{i_2} x_3^{i_3}) &= x_i^{i_1}(x_2 + x_1)^{i_2}(x_3 + x_2)^{i_3} - x_1^{i_1} x_2^{i_2} x_3^{i_3} \\ &= x_1^{i_1}(x_2 + x_1)^{i_2} \sum_{j=0}^{i_3} \binom{i_3}{j} x_2^{i_3-j} x_3^j - x_1^{i_1} x_2^{i_2} x_3^{i_3} \\ &= x_1^{i_1}(x_2 + x_1)^{i_2} \sum_{j=0}^{i_3-1} \binom{i_3}{j} x_2^{i_3-j} x_3^j + (x_1^{i_1}(x_2 + x_1)^{i_2} - x_1^{i_1} x_2^{i_2}) x_3^{i_3}. \end{aligned}$$

The monomial x_3^{3m} appears in $D_\sigma(x_1^{i_1} x_2^{i_2} x_3^{i_3})$ for some $i_1, i_2, i_3 \geq 0$. So, the monomial x_3^{3m} appears in

$$x_1^{i_1}(x_2 + x_1)^{i_2} \sum_{j=0}^{i_3-1} \binom{i_3}{j} x_2^{i_3-j} x_3^j \qquad \text{for some } 1 \leq j \leq i_3 - 1,$$

or the monomial x_3^{3m} appears in

$$(x_1^{i_1}(x_2 + x_1)^{i_2} - x_1^{i_1} x_2^{i_2}) x_3^{i_3}.$$

In either case, we have $i_1 = i_2 = 0$. So, x_3^{3m} has to appear in $\sum_{j=0}^{i_3-1} \binom{i_3}{j} x_2^{i_3-j} x_3^j$. This is a contradiction. Q.E.D.

We use the following Lemma on proving assertion (1) of Theorem 5.

Lemma 7. *The equality $D_\sigma(k[x]) \cap k[x]^{D_\sigma} = k[x]^{D_\sigma} \cdot f_1 + k[x]^{D_\sigma} \cdot f_2 + k[x]^{D_\sigma} \cdot f_3$ holds true.*

PROOF. Take any element f of $D_\sigma(k[x]) \cap k[x]^{D_\sigma}$. Then f is D_σ-integrable, and $f \in k[f_1, f_2, f_3, f_4]$. We can write f as

$$f = \sum_{i_1, i_2, i_3, i_4 \geq 0} a_{i_i, i_2, i_3, i_4} f_1^{i_1} f_2^{i_2} f_3^{i_3} f_4^{i_4}$$

for some $a_{i_i, i_2, i_3, i_4} \in k$ for all $i_1, i_2, i_3, i_4 \geq 0$. We define polynomials F_1, F_2 by

$$\begin{aligned} F_1 &:= \sum_{i_4 \geq 0} a_{0,0,0,i_4} f_4^{i_4}, \\ F_2 &:= f - F_1. \end{aligned}$$

So, for any polynomial $a_{i_i, i_2, i_3, i_4} f_1^{i_1} f_2^{i_2} f_3^{i_3} f_4^{i_4}$ appearing in F_2, at least one of suffixes i_1, i_2 and i_3 is not zero. Note that F_2 is D_σ-integrable (because f_1, f_2, f_3 are D_σ-integrable and $f_1, f_2, f_3 \in k[x]^{D_\sigma}$). Since f is D_σ-integrable, $F_1 (= f - F_2)$ is also D_σ-integrable. We know from Lemma 6 that $F_1 = 0$, which implies $f = F_2 \in k[x]^{D_\sigma} f_1 + k[x]^{D_\sigma} f_2 + k[x]^{D_\sigma} f_3$. To check the converse inclusion is left to the reader. Q.E.D.

In the following, we give a proof of Theorem 5. First, we prove assertion (1). Take any element f of $k[x]^{D_\sigma^2}$. Then $D_\sigma(f) \in D_\sigma(k[x]) \cap k[x]^{D_\sigma}$. By Lemma 7, we can write f as

$$D_\sigma(f) = \alpha_1 f_1 + \alpha_2 f_2 + \alpha_3 f_3$$

for some $\alpha_1, \alpha_2, \alpha_3 \in k[x]^{D_\sigma}$. Now we have

$$D_\sigma(f) = D_\sigma(\alpha_1 g_1 + \alpha_2 g_2 + \alpha_2 g_3)$$

since $D_\sigma(g_i) = f_i$ for all $1 \leq i \leq 3$. Thus,

$$f - (\alpha_1 g_1 + \alpha_2 g_2 + \alpha_2 g_3) \in k[x]^{D_\sigma}.$$

This implies that f belongs to the right hand side of the desired equlity. To check the converse inclusion is left to the reader.

Next, we prove assertion (2). Let $P := k[f_1, f_3, f_4]$ be the k-subalgebra of $k[x]^{D_\sigma}$. We have

$$k[x] = \sum_{0 \leq i \leq 2,\ 0 \leq j \leq 2} P \cdot x_2^i x_3^j$$

since $f_3 = x_2^3 +$ (terms of lower degree in x_2) and $f_4 = x_3^3 +$ (terms of lower degree in x_3). The monomials x_2^2, $x_2^2 x_3$, $x_2^2 x_3^2$ have the following expression:

$$
\begin{aligned}
x_2^2 &= -f_2 + f_1 \cdot x_2 + 2f_1 \cdot x_3, \\
x_2^2 x_3 &= -f_2 \cdot x_3 + f_1 \cdot x_2 x_3 + 2f_1 \cdot x_3^2, \\
x_2^2 x_3^2 &= -f_2 x_3^2 + f_1 x_2 x_3^2 + 2f_1 x_3^3 \\
&= -f_2 x_3^2 + f_1 x_2 x_3^2 + 2f_1(f_4 - f_1 x_2 x_3 - 2x_2^2 x_3 - f_1 x_3^2) \\
&= 2f_1 f_4 - 2f_1^2 \cdot x_2 x_3 + (-f_2 - 2f_1^2) \cdot x_3^2 + f_1 \cdot x_2 x_3^2 - f_1 \cdot x_2^2 x_3.
\end{aligned}
$$

So, the monomials $x_2^2, x_2^2 x_3, x_2^2 x_3^2$ belong to $\sum_{0 \le i \le 1,\ 0 \le j \le 2} k[x]^{D_\sigma} \cdot x_2^i x_3^j$. Now, we have

$$k[x] = \sum_{0 \le i \le 1,\ 0 \le j \le 2} k[x]^{D_\sigma} \cdot x_2^i x_3^j.$$

Differentiating this equality with D_σ, we have

$$D_\sigma(k[x]) = \sum_{i=1}^{5} k[x]^{D_\sigma} \cdot h_i.$$

Finally, we prove assertion (3). We can easily check the following:

$$
\begin{aligned}
D_\sigma(h_1) &= 0, \\
D_\sigma(h_2) &= x_1, \\
D_\sigma(h_3) &= 2x_1^2, \\
D_\sigma(h_4) &= x_1^2 + x_1 x_2 + 2x_2^2 + 2x_1 x_3, \\
D_\sigma(h_5) &= 2x_1^3 + x_1 x_2^2 + 2x_2^3 + x_1^2 x_3.
\end{aligned}
$$

Thus, we have $D_\sigma^2(k[x]) = k[x]^{D_\sigma} \cdot D_\sigma(h_2) + k[x]^{D_\sigma} \cdot D_\sigma(h_4) + k[x]^{D_\sigma} \cdot D_\sigma(h_5)$.

We complete the proof of Theorem 5.

Acknowledgements

The author would like to express his thanks to the referee for careful reading and comments.

References

[1] H. E. A. Eddy Campbell, David L. Wehlau, *Modular Invariant Theory*, Encyclopaedia of Mathematical Sciences 139, Invariant Theory and Algebraic Transformation Groups VIII, Springer-Verlag, Berlin, 2011, xiv+233 pp.

[2] L. Evens, *The cohomology of groups*, Oxford Mathematical Monographs, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1991, xii+159 pp.

Faculty of Education, Shizuoka University,
836 Ohya, Suruga-ku, Shizuoka 422–8529, Japan
e-mail: ertanim@ipc.shizuoka.ac.jp