SOME COMMUTATION FORMULAS AND LINEAR ISOMORPHISMS FOR THE HYPERALGEBRA OF A SIMPLE ALGEBRAIC GROUP

YUTAKA YOSHII

Abstract. In this article, we first present several commutation formulas for root vectors in the hyperalgebra $\mathcal{U}$ corresponding to a simply connected simple algebraic group defined over $\mathbb{F}_p$. Then, we give certain linear isomorphisms in terms of the multiplication in $\mathcal{U}$ and a linear transformation on $\mathcal{U}$ known as the Frobenius splitting.

Key Words: Hyperalgebra, Commutation formula, Linear isomorphism.

2020 *Mathematics Subject Classification*: 14L17, 17B35, 16S30.

1. Introduction

Let $\mathfrak{g}_{\mathbb{C}}$ be a simple complex Lie algebra with root system Φ. Let Φ^+(resp. Φ^-) the set of all positive (resp. negative) roots. Let $\Delta = \{\alpha_1, \ldots, \alpha_l\}$ be a base of Φ. Let $\{e_\alpha, h_i \mid \alpha \in \Phi,\ 1 \leq i \leq l\}$ be a Chavalley basis of $\mathfrak{g}_{\mathbb{C}}$ with $h_i = [e_{\alpha_i}, e_{-\alpha_i}]$. For $\alpha \in \Phi$, set $h_\alpha = [e_\alpha, e_{-\alpha}]$. In the universal enveloping algebra $\mathcal{U}_{\mathbb{C}}$ of $\mathfrak{g}_{\mathbb{C}}$, set $e_\alpha^{(n)} = e_\alpha^n/n!$ and $\binom{h_\alpha+c}{n} = \prod_{j=1}^n (h_\alpha + c - j + 1)/n!$ for $\alpha \in \Phi, n \in \mathbb{Z}_{\geq 0}, c \in \mathbb{Z}$.

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be the field of p elements. Let G be a simply connected and simple algebraic group defined over $\mathbb{F}_p$ with root system Φ and T a maximal split torus of G. Let $W = N_G(T)/T$ be the Weyl group and $X(T) = \mathrm{Hom}(T, \overline{\mathbb{F}}_p^\times)$ the character group of T. In the euclidean space $\mathbb{E} = \mathbb{R} \otimes_{\mathbb{Z}} X(T)$, let $\langle \cdot, \cdot \rangle$ be a W-invariant inner product. For $\beta \in \Phi$ $(\subseteq X(T))$, let $\beta^\vee = 2\beta/\langle \beta, \beta \rangle$ be the coroot of β and $s_\beta \in W$ the reflection with respect to β:

$$s_\beta(\lambda) = \lambda - \langle \lambda, \beta^\vee \rangle \beta \quad (\lambda \in \mathbb{E}).$$

For $\lambda \in \mathbb{E}$, set $||\lambda|| = \sqrt{\langle \lambda, \lambda \rangle}$.

For $1 \leq i \leq l$, we denote the simple reflection s_{α_i} by s_i. Then we have

$$W = \langle s_\alpha \mid \alpha \in \Delta \rangle = \langle s_1, \ldots, s_l \rangle.$$

For $w \in W$ and its reduced expression $w = s_{i_1} \cdots s_{i_t}$, the integer t is called the length of t and denoted by $l(w)$. Let w_0 be the unique longest element of W (then $l(w_0) = |\Phi^+|$). Let $\mathcal{U}_{\mathbb{Z}}$ be the subring of $\mathcal{U}_{\mathbb{C}}$ generated by all $e_\alpha^{(m)}$ with $\alpha \in \Phi$, $m \geq 0$. Then the $\mathbb{F}_p$-algebra $\mathcal{U} = \mathcal{U}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{F}_p$ is called the hyperalgebra corresponding to G. We use the same symbols for images in $\mathcal{U}$ of the elements of $\mathcal{U}_{\mathbb{Z}}$ (for example, $e_\alpha^{(m)}$, $\binom{h_\alpha+c}{n}$, and so on). Then we have $\mathcal{U} = \langle e_\alpha^{(m)} \mid \alpha \in \Phi, m \geq 0 \rangle_{\mathbb{F}_p\text{-alg.}}$. We define $\mathbb{F}_p$-subalgebras $\mathcal{U}^+$, $\mathcal{U}^-$, and $\mathcal{U}^0$ as

$$\mathcal{U}^+ = \langle e_\alpha^{(m)} \mid \alpha \in \Phi^+, m \geq 0 \rangle_{\mathbb{F}_p\text{-alg.}},$$

The detailed version of this paper is [5].

$$\mathcal{U}^- = \langle e_\alpha^{(m)} \mid \alpha \in \Phi^-, m \geq 0 \rangle_{\mathbb{F}_p\text{-alg.}},$$
$$\mathcal{U}^0 = \left\langle \binom{h_i}{n} \;\middle|\; 1 \leq i \leq l, n \geq 0 \right\rangle_{\mathbb{F}_p\text{-alg.}}.$$

Moreover, for a fixed positive integer r, set

$$\mathcal{U}_r = \langle e_\alpha^{(m)} \mid \alpha \in \Phi, 0 \leq m \leq p^r - 1 \rangle_{\mathbb{F}_p\text{-alg.}},$$
$$\mathcal{U}_r^+ = \mathcal{U}^+ \cap \mathcal{U}_r = \langle e_\alpha^{(m)} \mid \alpha \in \Phi^+, 0 \leq m \leq p^r - 1 \rangle_{\mathbb{F}_p\text{-alg.}},$$
$$\mathcal{U}_r^- = \mathcal{U}^- \cap \mathcal{U}_r = \langle e_\alpha^{(m)} \mid \alpha \in \Phi^-, 0 \leq m \leq p^r - 1 \rangle_{\mathbb{F}_p\text{-alg.}},$$
$$\mathcal{U}_r^0 = \mathcal{U}^0 \cap \mathcal{U}_r = \left\langle \binom{h_i}{n} \;\middle|\; 1 \leq i \leq l,\ 0 \leq n \leq p^r - 1 \right\rangle_{\mathbb{F}_p\text{-alg.}}.$$

Then the multiplication maps

$$\mathcal{U}^- \otimes_{\mathbb{F}_p} \mathcal{U}^0 \otimes_{\mathbb{F}_p} \mathcal{U}^+ \to \mathcal{U}, \quad \mathcal{U}_r^- \otimes_{\mathbb{F}_p} \mathcal{U}_r^0 \otimes_{\mathbb{F}_p} \mathcal{U}_r^+ \to \mathcal{U}_r$$

are $\mathbb{F}_p$-linear isomorphisms (see [3, II 1.12 and Lemma 3.3]).

2. Commutation formulas

Here we describe certain commutation formulas of divided powers $e_\alpha^{(m)}$ (in $\mathcal{U}_\mathbb{Z}$ or $\mathcal{U}$) for $\alpha \in \Phi$ and $m \in \mathbb{Z}_{\geq 0}$.

The following formulas in $\mathcal{U}_\mathbb{Z}$ are well-known.

Proposition 1. *Let $\alpha, \beta \in \Phi$, $c \in \mathbb{Z}$, and $m, n \in \mathbb{Z}_{\geq 0}$. In $\mathcal{U}_\mathbb{Z}$, the following equalities hold.*

(i) $e_\alpha^{(m)} e_\alpha^{(n)} = \binom{m+n}{n} e_\alpha^{(m+n)}$.

(ii) $e_\alpha^{(m)} e_{-\alpha}^{(n)} = \displaystyle\sum_{k=0}^{\min\{m,n\}} e_{-\alpha}^{(n-k)} \binom{h_\alpha - m - n + 2k}{k} e_\alpha^{(m-k)}$.

(iii) $e_\alpha^{(m)} \binom{h_\beta + c}{n} = \binom{h_\beta + c - \langle \alpha, \beta^\vee \rangle m}{n} e_\alpha^{(m)}$.

(iv) $e_\alpha^{(m)} e_\beta^{(n)} = e_\beta^{(n)} e_\alpha^{(m)}$ *if $\alpha + \beta \notin \Phi$ and $\beta \neq -\alpha$.*

(v) $\binom{h_\alpha}{m} \binom{h_\alpha}{n} = \displaystyle\sum_{k=0}^{\min\{m,n\}} \binom{m+n-k}{n} \binom{n}{k} \binom{h_\alpha}{m+n-k}$.

The following formula is also useful for calculation in $\mathcal{U}$.

Proposition 2 (Lucas' Theorem)**.** *Let $m, n \in \mathbb{Z}_{\geq 0}$. Let $m = \sum_{i \geq 0} m_i p^i$ and $n = \sum_{i \geq 0} n_i p^i$ be their p-adic expansions. Then we have*

$$\binom{m}{n} \equiv \prod_{i \geq 0} \binom{m_i}{n_i} \pmod{p}.$$

Consider two roots $\alpha, \beta \in \Phi$ with $\alpha + \beta \in \Phi$. Then $\Phi'(\alpha, \beta) = (\mathbb{Z}\alpha + \mathbb{Z}\beta) \cap \Phi$ forms a root system of type A_2, B_2, or G_2. Let m be a unique integer such that $\beta - m\alpha \in \Phi$ and $\beta - (m+1)\alpha \notin \Phi$. Then there exists $c_{\alpha,\beta} \in \{\pm 1\}$ such that $[e_\alpha, e_\beta] = (m+1)c_{\alpha,\beta}e_{\alpha+\beta}$ in $\mathfrak{g}_{\mathbb{Z}}$. For simplicity, we assume that $||\alpha|| \leq ||\beta||$ and α and β form a base of $\Phi'(\alpha, \beta)$.

Suppose that $\Phi'(\alpha, \beta)$ is of type A_2. Then $||\beta|| = ||\alpha||$ and

$$\Phi'(\alpha, \beta) = \{\pm\alpha, \pm\beta, \pm(\alpha + \beta)\}.$$

If we write $[e_\alpha, e_\beta] = c_{\alpha,\beta}e_{\alpha+\beta}$ in $\mathfrak{g}_{\mathbb{Z}}$ for some $c_{\alpha,\beta} \in \{\pm 1\}$, then

$$e_\alpha^{(a)} e_\beta^{(b)} = \sum_{\substack{t_1+t_2=b,\\ t_2+t_3=a}} c_{\alpha,\beta}^{t_2} e_\beta^{(t_1)} e_{\alpha+\beta}^{(t_2)} e_\alpha^{(t_3)},$$

$$e_\beta^{(b)} e_\alpha^{(a)} = \sum_{\substack{t_1+t_2=a,\\ t_2+t_3=b}} (-c_{\alpha,\beta})^{t_2} e_\alpha^{(t_1)} e_{\alpha+\beta}^{(t_2)} e_\beta^{(t_3)}$$

in $\mathcal{U}_{\mathbb{Z}}$ for $a, b \in \mathbb{Z}_{\geq 0}$.

Suppose that $\Phi'(\alpha, \beta)$ is of type B_2. Then $||\beta|| = \sqrt{2}||\alpha||$ and

$$\Phi'(\alpha, \beta) = \{\pm\alpha, \pm\beta, \pm(\alpha + \beta), \pm(2\alpha + \beta)\}.$$

If we write $[e_\alpha, e_\beta] = c_{\alpha,\beta}e_{\alpha+\beta}$ and $[e_\alpha, e_{\alpha+\beta}] = 2c_{\alpha,\alpha+\beta}e_{2\alpha+\beta}$ in $\mathfrak{g}_{\mathbb{Z}}$ for some $c_{\alpha,\beta}, c_{\alpha,\alpha+\beta} \in \{\pm 1\}$, then

$$e_\alpha^{(a)} e_\beta^{(b)} = \sum_{\substack{t_1+t_2+t_3=b,\\ t_2+2t_3+t_4=a}} c_{\alpha,\beta}^{t_2} (c_{\alpha,\beta}c_{\alpha,\alpha+\beta})^{t_3} e_\beta^{(t_1)} e_{\alpha+\beta}^{(t_2)} e_{2\alpha+\beta}^{(t_3)} e_\alpha^{(t_4)},$$

$$e_\beta^{(b)} e_\alpha^{(a)} = \sum_{\substack{t_1+2t_2+t_3=a,\\ t_2+t_3+t_4=b}} (-c_{\alpha,\beta})^{t_3} (c_{\alpha,\beta}c_{\alpha,\alpha+\beta})^{t_2} e_\alpha^{(t_1)} e_{2\alpha+\beta}^{(t_2)} e_{\alpha+\beta}^{(t_3)} e_\beta^{(t_4)},$$

$$e_\alpha^{(a)} e_{\alpha+\beta}^{(b)} = \sum_{\substack{t_1+t_2=b,\\ t_2+t_3=a}} (2c_{\alpha,\alpha+\beta})^{t_2} e_{\alpha+\beta}^{(t_1)} e_{2\alpha+\beta}^{(t_2)} e_\alpha^{(t_3)},$$

$$e_{\alpha+\beta}^{(b)} e_\alpha^{(a)} = \sum_{\substack{t_1+t_2=a,\\ t_2+t_3=b}} (-2c_{\alpha,\alpha+\beta})^{t_2} e_\alpha^{(t_1)} e_{2\alpha+\beta}^{(t_2)} e_{\alpha+\beta}^{(t_3)}$$

in $\mathcal{U}_{\mathbb{Z}}$ for $a, b \in \mathbb{Z}_{\geq 0}$.

Suppose that $\Phi'(\alpha, \beta)$ is of type G_2. Then $||\beta|| = \sqrt{3}||\alpha||$ and

$$\Phi'(\alpha, \beta) = \{\pm\alpha, \pm\beta, \pm(\alpha + \beta), \pm(2\alpha + \beta), \pm(3\alpha + \beta), \pm(3\alpha + 2\beta)\}.$$

If we write

$$[e_\alpha, e_\beta] = c_{\alpha,\beta}e_{\alpha+\beta}, \quad [e_\alpha, e_{\alpha+\beta}] = 2c_{\alpha,\alpha+\beta}e_{2\alpha+\beta},$$
$$[e_\alpha, e_{2\alpha+\beta}] = 3c_{\alpha,2\alpha+\beta}e_{3\alpha+\beta}, \quad [e_{2\alpha+\beta}, e_{\alpha+\beta}] = 3c_{2\alpha+\beta,\alpha+\beta}e_{3\alpha+2\beta}$$

in $\mathfrak{g}_{\mathbb{Z}}$ for some $c_{\alpha,\beta}, c_{\alpha,\alpha+\beta}, c_{\alpha,2\alpha+\beta}, c_{2\alpha+\beta,\alpha+\beta} \in \{\pm 1\}$. Then we have

$$[e_{3\alpha+\beta}, e_\beta] = -c_{\alpha,\beta}c_{\alpha,2\alpha+\beta}c_{2\alpha+\beta,\alpha+\beta}e_{3\alpha+2\beta}$$

in $\mathfrak{g}_{\mathbb{Z}}$ and

$$e_{\alpha}^{(a)}e_{\beta}^{(b)} = \sum_{\substack{t_1+t_2+2t_3+t_4+t_5=b,\\ t_2+3t_3+2t_4+3t_5+t_6=a}} d_1(t_2,t_3,t_4,t_5)e_{\beta}^{(t_1)}e_{\alpha+\beta}^{(t_2)}e_{3\alpha+2\beta}^{(t_3)}e_{2\alpha+\beta}^{(t_4)}e_{3\alpha+\beta}^{(t_5)}e_{\alpha}^{(t_6)},$$

$$e_{\beta}^{(b)}e_{\alpha}^{(a)} = \sum_{\substack{t_1+3t_2+2t_3+3t_4+t_5=a,\\ t_2+t_3+2t_4+t_5+t_6=b}} d_2(t_2,t_3,t_4,t_5)e_{\alpha}^{(t_1)}e_{3\alpha+\beta}^{(t_2)}e_{2\alpha+\beta}^{(t_3)}e_{3\alpha+2\beta}^{(t_4)}e_{\alpha+\beta}^{(t_5)}e_{\beta}^{(t_6)},$$

$$e_{\alpha}^{(a)}e_{\alpha+\beta}^{(b)} = \sum_{\substack{t_1+2t_2+t_3+t_4=b,\\ t_2+t_3+2t_4+t_5=a}} d_3(t_2,t_3,t_4)e_{\alpha+\beta}^{(t_1)}e_{3\alpha+2\beta}^{(t_2)}e_{2\alpha+\beta}^{(t_3)}e_{3\alpha+\beta}^{(t_4)}e_{\alpha}^{(t_5)},$$

$$e_{\alpha+\beta}^{(b)}e_{\alpha}^{(a)} = \sum_{\substack{t_1+2t_2+t_3+t_4=a,\\ t_2+t_3+2t_4+t_5=b}} d_4(t_2,t_3,t_4)e_{\alpha}^{(t_1)}e_{3\alpha+\beta}^{(t_2)}e_{2\alpha+\beta}^{(t_3)}e_{3\alpha+2\beta}^{(t_4)}e_{\alpha+\beta}^{(t_5)},$$

$$e_{\alpha}^{(a)}e_{2\alpha+\beta}^{(b)} = \sum_{\substack{t_1+t_2=b,\\ t_2+t_3=a}} (3c_{\alpha,2\alpha+\beta})^{t_2}e_{2\alpha+\beta}^{(t_1)}e_{3\alpha+\beta}^{(t_2)}e_{\alpha}^{(t_3)},$$

$$e_{2\alpha+\beta}^{(b)}e_{\alpha}^{(a)} = \sum_{\substack{t_1+t_2=a,\\ t_2+t_3=b}} (-3c_{\alpha,2\alpha+\beta})^{t_2}e_{\alpha}^{(t_1)}e_{3\alpha+\beta}^{(t_2)}e_{2\alpha+\beta}^{(t_3)},$$

$$e_{2\alpha+\beta}^{(a)}e_{\alpha+\beta}^{(b)} = \sum_{\substack{t_1+t_2=b,\\ t_2+t_3=a}} (3c_{2\alpha+\beta,\alpha+\beta})^{t_2}e_{\alpha+\beta}^{(t_1)}e_{3\alpha+2\beta}^{(t_2)}e_{2\alpha+\beta}^{(t_3)},$$

$$e_{\alpha+\beta}^{(b)}e_{2\alpha+\beta}^{(a)} = \sum_{\substack{t_1+t_2=a,\\ t_2+t_3=b}} (-3c_{2\alpha+\beta,\alpha+\beta})^{t_2}e_{2\alpha+\beta}^{(t_1)}e_{3\alpha+2\beta}^{(t_2)}e_{\alpha+\beta}^{(t_3)},$$

$$e_{3\alpha+\beta}^{(a)}e_{\beta}^{(b)} = \sum_{\substack{t_1+t_2=b,\\ t_2+t_3=a}} (-c_{\alpha,\beta}c_{\alpha,2\alpha+\beta}c_{2\alpha+\beta,\alpha+\beta})^{t_2}e_{\beta}^{(t_1)}e_{3\alpha+2\beta}^{(t_2)}e_{3\alpha+\beta}^{(t_3)},$$

$$e_{\beta}^{(b)}e_{3\alpha+\beta}^{(a)} = \sum_{\substack{t_1+t_2=a,\\ t_2+t_3=b}} (c_{\alpha,\beta}c_{\alpha,2\alpha+\beta}c_{2\alpha+\beta,\alpha+\beta})^{t_2}e_{3\alpha+\beta}^{(t_1)}e_{3\alpha+2\beta}^{(t_2)}e_{\beta}^{(t_3)}$$

in $\mathcal{U}_{\mathbb{Z}}$ for $a, b \in \mathbb{Z}_{\geq 0}$, where

$$d_1(t_2,t_3,t_4,t_5) = c_{\alpha,\beta}^{t_2}(c_{\alpha,\beta}c_{\alpha,\alpha+\beta})^{t_4}(c_{\alpha,\beta}c_{\alpha,\alpha+\beta}c_{\alpha,2\alpha+\beta})^{t_5}(c_{\alpha,\alpha+\beta}c_{2\alpha+\beta,\alpha+\beta})^{t_3},$$

$$d_2(t_2,t_3,t_4,t_5) = (-c_{\alpha,\beta})^{t_5}(c_{\alpha,\beta}c_{\alpha,\alpha+\beta})^{t_3}(-c_{\alpha,\beta}c_{\alpha,\alpha+\beta}c_{\alpha,2\alpha+\beta})^{t_2}(c_{\alpha,\alpha+\beta}c_{2\alpha+\beta,\alpha+\beta})^{t_4},$$

$$d_3(t_2,t_3,t_4) = (2c_{\alpha,\alpha+\beta})^{t_3}(3c_{\alpha,\alpha+\beta}c_{\alpha,2\alpha+\beta})^{t_4}(3c_{\alpha,\alpha+\beta}c_{2\alpha+\beta,\alpha+\beta})^{t_2},$$

$$d_4(t_2,t_3,t_4) = (-2c_{\alpha,\alpha+\beta})^{t_3}(3c_{\alpha,\alpha+\beta}c_{\alpha,2\alpha+\beta})^{t_2}(3c_{\alpha,\alpha+\beta}c_{2\alpha+\beta,\alpha+\beta})^{t_4}.$$

The above formulas are useful to show the following fact.

Proposition 3 ([5, Proposition 3.3]). *Let $\alpha \in \Phi$, $n \in \mathbb{Z}_{\geq 0}$, $r \in \mathbb{Z}_{>0}$, and $z \in \mathcal{U}_r$. Then the element*

$$\sum_{i=0}^{n} (-1)^i e_{\alpha}^{((n-i)p^r)} z e_{\alpha}^{(ip^r)}$$

of $\mathcal{U}$ lies in $\mathcal{U}_r$.

Consider a reduced expression $w_0 = s_{i_1} s_{i_2} \cdots s_{i_\nu}$ of the longest element w_0. If we set

$$\beta_1 = \alpha_{i_1}, \beta_2 = s_{i_1}(\alpha_{i_2}), \ldots, \beta_\nu = s_{i_1} \ldots s_{i_{\nu-1}}(\alpha_{i_\nu}),$$

then we have $\Phi^+ = \{\beta_1, \beta_2, \ldots, \beta_\nu\}$ (see [2, 5.6 Exercise 1]). The monomials

$$e_{\beta_1}^{(a_1)} e_{\beta_2}^{(a_2)} \cdots e_{\beta_\nu}^{(a_\nu)}$$

with $a_i \in \mathbb{Z}_{\geq 0}$ for $1 \leq i \leq \nu$ form a $\mathbb{Z}$-basis of $\mathcal{U}_{\mathbb{Z}}^+$ and an $\mathbb{F}_p$-basis of $\mathcal{U}^+$.

Proposition 4 ([4, Proposition 3.2])**.** *Suppose that $\nu > 1$. For $a, b \in \mathbb{Z}_{>0}$ and $j, k \in \mathbb{Z}$ with $1 \leq j < k \leq \nu$, the element $e_{\beta_k}^{(a)} e_{\beta_j}^{(b)} - e_{\beta_j}^{(b)} e_{\beta_k}^{(a)}$ in $\mathcal{U}_{\mathbb{Z}}$ is a $\mathbb{Z}$-linear combination of monomials of the form $e_{\beta_j}^{(a_j)} \cdots e_{\beta_k}^{(a_k)}$ satisfying the following:*

- *$a_j < b$ and $a_k < a$.*
- *$\sum_{i=j}^{k-1} a_i \leq b$ and $\sum_{i=j+1}^{k} a_i \leq a$.*

Set $\mathcal{N}_r = \{0, 1, \ldots, p^r - 1\}$. Using Proposition 4, we can prove the following:

Proposition 5 ([5, Proposition 3.5])**.** *Let j, k be integers satisfying $1 \leq j \leq k \leq \nu$. Let $r \in \mathbb{Z}_{>0}$. Then the following hold.*

(i) *A $\mathbb{Z}$-span of the monomials $e_{\beta_j}^{(a_j)} \cdots e_{\beta_k}^{(a_k)}$ with $(a_j, \ldots, a_k) \in (\mathbb{Z}_{\geq 0})^{k-j+1}$ forms a subring of $\mathcal{U}_{\mathbb{Z}}^+$.*

(ii) *An $\mathbb{F}_p$-span of the monomials $e_{\beta_j}^{(a_j)} \cdots e_{\beta_k}^{(a_k)}$ with $(a_j, \ldots, a_k) \in (\mathbb{Z}_{\geq 0})^{k-j+1}$ forms an $\mathbb{F}_p$-subalgebra of $\mathcal{U}^+$.*

(iii) *An $\mathbb{F}_p$-span of the monomials $e_{\beta_j}^{(a_j)} \cdots e_{\beta_k}^{(a_k)}$ with $a_i \in \mathcal{N}_r$ for $j \leq i \leq k$ forms an $\mathbb{F}_p$-subalgebra of $\mathcal{U}_r^+$.*

(iv) *Let $e_{\beta_j}^{(a_j)} \cdots e_{\beta_k}^{(a_k)}$ be a fixed monomial of $\mathcal{U}$ satisfying $a_i \in \mathcal{N}_r$ for each i with $j \leq i \leq k$. Let $c \in \mathbb{Z}_{>0}$. Then the following hold.*

- *If $k \neq \nu$, then the element*

$$e_{\beta_{k+1}}^{(c)} e_{\beta_j}^{(a_j)} \cdots e_{\beta_k}^{(a_k)} - e_{\beta_j}^{(a_j)} \cdots e_{\beta_k}^{(a_k)} e_{\beta_{k+1}}^{(c)}$$

in $\mathcal{U}$ is an $\mathbb{F}_p$-linear combination of monomials of the form $e_{\beta_j}^{(b_j)} \cdots e_{\beta_k}^{(b_k)} e_{\beta_{k+1}}^{(b_{k+1})}$ satisfying $b_{k+1} < c$ and $b_i \in \mathcal{N}_r$ for $j \leq i \leq k$.

- *If $j \neq 1$, then the element*

$$e_{\beta_j}^{(a_j)} \cdots e_{\beta_k}^{(a_k)} e_{\beta_{j-1}}^{(c)} - e_{\beta_{j-1}}^{(c)} e_{\beta_j}^{(a_j)} \cdots e_{\beta_k}^{(a_k)}$$

in $\mathcal{U}$ is an $\mathbb{F}_p$-linear combination of monomials of the form $e_{\beta_{j-1}}^{(b_{j-1})} e_{\beta_j}^{(b_j)} \cdots e_{\beta_k}^{(b_k)}$ satisfying $b_{j-1} < c$ and $b_i \in \mathcal{N}_r$ for $j \leq i \leq k$.

3. Linear isomorphisms

Let $\mathrm{Fr}:\mathcal{U}\to\mathcal{U}$ be an $\mathbb{F}_p$-algebra endomorphism defined by

$$e_\alpha^{(n)} \mapsto \begin{cases} e_\alpha^{(n/p)} & \text{if } p \mid n, \\ 0 & \text{if } p \nmid n \end{cases}$$

for $\alpha \in \Phi$. Then we have

$$\mathrm{Fr}\left(\binom{h_i}{n}\right) = \begin{cases} \binom{h_i}{n/p} & \text{if } p \mid n, \\ 0 & \text{if } p \nmid n \end{cases}$$

for $1 \le i \le l$. Let

$$\mathrm{Fr}'^{+}:\mathcal{U}^+\to\mathcal{U}^+,\quad \mathrm{Fr}'^{-}:\mathcal{U}^-\to\mathcal{U}^-,\quad \mathrm{Fr}'^{0}:\mathcal{U}^0\to\mathcal{U}^0$$

be $\mathbb{F}_p$-algebra homomorphisms defined by

$$\mathrm{Fr}'^{+}(e_{\alpha_i}^{(n)}) = e_{\alpha_i}^{(np)},\quad \mathrm{Fr}'^{-}(e_{-\alpha_i}^{(n)}) = e_{-\alpha_i}^{(np)},\quad \mathrm{Fr}'^{0}\left(\binom{h_i}{n}\right) = \binom{h_i}{np}$$

(see [1, Proposition 1.1 and Corollaire 1.2]). Then there is a (unique) $\mathbb{F}_p$-linear map $\mathrm{Fr}':\mathcal{U}\to\mathcal{U}$ defined by

$$\boldsymbol{fhe} \mapsto \mathrm{Fr}'^{-}(\boldsymbol{f})\mathrm{Fr}'^{0}(\boldsymbol{h})\mathrm{Fr}'^{+}(\boldsymbol{e}) \quad (\boldsymbol{f}\in\mathcal{U}^-, \boldsymbol{h}\in\mathcal{U}^0, \boldsymbol{e}\in\mathcal{U}^+),$$

which is called the Frobenius splitting on $\mathcal{U}$. Clearly we have $\mathrm{Fr}\circ\mathrm{Fr}' = \mathrm{id}_{\mathcal{U}}$, but Fr' is not an $\mathbb{F}_p$-algebra homomorphism.

Now we are ready to give a main result.

Theorem 6 ([5, Theorems 4.5 and 5.5 and Corollaries 4.6 and 5.6]). *Let $n \in \mathbb{Z}_{>0}$. Then the multiplication on $\mathcal{U}$ induces $\mathbb{F}_p$-linear isomorphisms*

$$\mathcal{U}_r^+ \otimes_{\mathbb{F}_p} \mathrm{Fr}'^r(\mathcal{U}_n^+) \to \mathcal{U}_{r+n}^+,\quad \mathcal{U}_r^+ \otimes_{\mathbb{F}_p} \mathrm{Fr}'^r(\mathcal{U}^+) \to \mathcal{U}^+,$$
$$\mathcal{U}_r^- \otimes_{\mathbb{F}_p} \mathrm{Fr}'^r(\mathcal{U}_n^-) \to \mathcal{U}_{r+n}^-,\quad \mathcal{U}_r^- \otimes_{\mathbb{F}_p} \mathrm{Fr}'^r(\mathcal{U}^-) \to \mathcal{U}^-,$$
$$\mathcal{U}_r \otimes_{\mathbb{F}_p} \mathrm{Fr}'^r(\mathcal{U}_n) \to \mathcal{U}_{r+n},\quad \mathcal{U}_r \otimes_{\mathbb{F}_p} \mathrm{Fr}'^r(\mathcal{U}) \to \mathcal{U}.$$

Unlike $\mathcal{U}^+$, $\mathcal{U}^-$, and $\mathcal{U}$, the algebra $\mathcal{U}^0$ is commutative. Therefore, in this case, an $\mathbb{F}_p$-algebra isomorphism can be obtained, and its proof is easier.

Proposition 7 ([5, Proposition 5.1]). *Let $n \in \mathbb{Z}_{>0}$. Then the multiplication on $\mathcal{U}$ induces $\mathbb{F}_p$-algebra isomorphisms*

$$\mathcal{U}_r^0 \otimes_{\mathbb{F}_p} \mathrm{Fr}'^r(\mathcal{U}_n^0) \to \mathcal{U}_{r+n}^0,\quad \mathcal{U}_r^0 \otimes_{\mathbb{F}_p} \mathrm{Fr}'^r(\mathcal{U}^0) \to \mathcal{U}^0.$$

Now we outline the proof of the first linear isomorphism in Theorem 6.

For $\boldsymbol{a} = (a_1,\dots,a_\nu) \in (\mathbb{Z}_{\ge 0})^\nu$, set

$$\boldsymbol{e}^{(\boldsymbol{a})} = e_{\beta_1}^{(a_1)} e_{\beta_2}^{(a_2)} \cdots e_{\beta_\nu}^{(a_\nu)}.$$

We proceed by induction on n. Suppose that $n = 1$. Since

$$\dim_{\mathbb{F}_p}(\mathcal{U}_r^+ \otimes_{\mathbb{F}_p} \mathrm{Fr}'^r(\mathcal{U}_1^+)) = \dim_{\mathbb{F}_p} \mathcal{U}_{r+1}^+ = p^{(r+1)\nu},$$

it is enough to show that

$$\mathcal{U}_r^+ \otimes_{\mathbb{F}_p} \mathrm{Fr}'^r(\mathcal{U}_1^+) \to \mathcal{U}_{r+1}^+$$

is injective. Consider the elements

$$\boldsymbol{e}^{(\boldsymbol{a})}\mathrm{Fr}'^{r}(\boldsymbol{e}^{(\boldsymbol{b})}) \quad (\boldsymbol{a} \in (\mathcal{N}_r)^\nu, \boldsymbol{b} \in (\mathcal{N}_1)^\nu).$$

We need the following proposition.

Proposition 8 ([5, Proposition 4.4]). *For $n \in \mathbb{Z}_{\geq 0}$, set $q_{p,r}(n) = \lfloor n/p^r \rfloor$. Suppose that $\boldsymbol{a} = (a_1, \ldots, a_\nu) \in (\mathcal{N}_r)^\nu$ and that $\boldsymbol{b} = (b_1, \ldots, b_k) \in (\mathcal{N}_1)^k$ with $1 \leq k \leq \nu$. Then we have*

$$\boldsymbol{e}^{(\boldsymbol{a})}\mathrm{Fr}'^{r}\left(\boldsymbol{e}^{(\boldsymbol{b})}\right) = \left(\prod_{i=1}^{k} e_{\beta_i}^{(a_i+p^r b_i)}\right) \prod_{i=k+1}^{\nu} e_{\beta_i}^{(a_i)} + \sum_{\boldsymbol{c}=(c_1,\ldots,c_\nu)} \xi(\boldsymbol{c})\boldsymbol{e}^{(\boldsymbol{c})}$$

in $\mathcal{U}$, where $\xi(\boldsymbol{c}) \in \mathbb{F}_p$ and each $\boldsymbol{c}$ with $\xi(\boldsymbol{c}) \neq 0$ satisfies

$$(q_{p,r}(c_1), \ldots, q_{p,r}(c_k)) \neq (b_1, \ldots, b_k)$$

in $(\mathbb{Z}_{\geq 0})^k$, $q_{p,r}(c_i) \leq b_i$ for $1 \leq i \leq k$, and $q_{p,r}(c_i) = 0$ for $k+1 \leq i \leq \nu$.

Using the proposition, we can show that the elements

$$\boldsymbol{e}^{(\boldsymbol{a})}\mathrm{Fr}'^{r}(\boldsymbol{e}^{(\boldsymbol{b})}) \quad (\boldsymbol{a} \in (\mathcal{N}_r)^\nu, \boldsymbol{b} \in (\mathcal{N}_1)^\nu)$$

are linearly independent over $\mathbb{F}_p$.

Suppose that $n \geq 2$. We obtain the following commutative diagram induced by multiplication:

$$\begin{array}{ccc}
\mathcal{U}_r^+ \otimes_{\mathbb{F}_p} \mathrm{Fr}'^{r}\left(\mathcal{U}_{n-1}^+\right) \otimes_{\mathbb{F}_p} \mathrm{Fr}'^{r+n-1}\left(\mathcal{U}_1^+\right) & \xrightarrow{\sim} & \mathcal{U}_r^+ \otimes_{\mathbb{F}_p} \mathrm{Fr}'^{r}\left(\mathcal{U}_n^+\right) \\
\sim\downarrow & & \downarrow \\
\mathcal{U}_{r+n-1}^+ \otimes_{\mathbb{F}_p} \mathrm{Fr}'^{r+n-1}\left(\mathcal{U}_1^+\right) & \xrightarrow{\sim} & \mathcal{U}_{r+n}^+
\end{array}$$

Here the upper, the lower, and the left maps are $\mathbb{F}_p$-linear isomorphisms. Therefore, the multiplication map

$$\mathcal{U}_r^+ \otimes_{\mathbb{F}_p} \mathrm{Fr}'^{r}\left(\mathcal{U}_n^+\right) \to \mathcal{U}_{r+n}^+$$

is also an $\mathbb{F}_p$-linear isomorphism.

References

[1] M. Gros and M. Kaneda, *Contraction par Frobenius de G-modules*, Ann. Inst. Fourier **61** (2011), 2507–2542.

[2] J. E. Humphreys, *Reflection Groups and Coxeter Group*, Cambridge University Press, Cambridge (1990).

[3] J. C. Jantzen, *Representations of Algebraic Groups*, 2nd ed., Math. Surveys Monogr., vol. 107, Amer. Math. Soc., Rhode Island (2003).

[4] Y. Yoshii, *Some results on certain finite-dimensional subalgebras of the hyperalgebra of a universal Chevalley group*, J. Lie Theory **32** (2022), 899–916.

[5] ———, *Certain linear isomorphisms for hyperalgebras relative to a Chevalley group*, J. Algebra Appl. (2025), No.2550185.

College of Education
Ibaraki University
Mito, Ibaraki 310-8512 JAPAN
E-mail address: yutaka.yoshii.6174@vc.ibaraki.ac.jp