Some commutation formulas and linear isomorphisms for the hyperalgebra of a simple algebraic group

吉井　豊 **(Yutaka Yoshii)**

茨城大学 **(Ibaraki University)**

September 16, 2024

Table of Contents

§1 Preliminaries

$\mathfrak{g}_{\mathbb{C}}$: simple complex Lie algebra with root system Φ

Φ^+(resp. Φ^-): set of all positive (resp. negative) roots

$\Delta := \{\alpha_1, \ldots, \alpha_l\}$: set of all simple roots

$\{e_\alpha, h_i \mid \alpha \in \Phi,\ 1 \leq i \leq l\}$: Chavalley basis of $\mathfrak{g}_{\mathbb{C}}$ with $h_i := [e_{\alpha_i}, e_{-\alpha_i}]$

$h_\alpha := [e_\alpha, e_{-\alpha}]$ for $\alpha \in \Phi$

$\mathcal{U}_{\mathbb{C}}$: universal enveloping algebra of $\mathfrak{g}_{\mathbb{C}}$

Set $e_\alpha^{(n)} := e_\alpha^n/n!$ and $\binom{h_\alpha + c}{n} := \prod_{j=1}^n (h_\alpha + c - j + 1)/n!$
$(\alpha \in \Phi, n \in \mathbb{Z}_{\geq 0}, c \in \mathbb{Z})$.

$\mathbb{F}_p (= \mathbb{Z}/p\mathbb{Z})$: prime field of p elements

G: simply connected and simple algebraic group defined over $\mathbb{F}_p$ with root system Φ

T: maximal split torus of G

$W := N_G(T)/T$: Weyl group

$X(T) := \mathrm{Hom}(T, \overline{\mathbb{F}}_p^{\times})$: character group

$\mathbb{E} := \mathbb{R} \otimes_{\mathbb{Z}} X(T)$: euclidean space

$\langle \cdot, \cdot \rangle$: W-invariant inner product on $\mathbb{E}$

$\beta^{\vee} = 2\beta/\langle \beta, \beta \rangle$: coroot of $\beta \in \Phi$

For $\beta \in \Phi$ ($\subseteq X(T)$), let $s_\beta \in W$ be the reflection with respect to β:

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

$s_i := s_{\alpha_i}$: simple reflection ($1 \leq i \leq l$)

Then

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

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 $l(w)$.

w_0: unique longest element of W (then $l(w_0) = |\Phi^+|$)

$\mathcal{U}_{\mathbb{Z}}$: subring of $\mathcal{U}_{\mathbb{C}}$ generated by all $e_\alpha^{(m)}$ $(\alpha \in \Phi,\ m \geq 0)$

$\mathcal{U} := \mathcal{U}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{F}_p$: hyperalgebra corresponding to G

We use the same symbols for images in $\mathcal{U}$ of the elements of $\mathcal{U}_{\mathbb{Z}}$ (for example, $e_\alpha^{(m)}$, $\binom{h_\alpha + c}{n}$, ...).

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

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

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

$\mathcal{U}^0 := \langle \binom{h_i}{n} \mid 1 \leq i \leq l, n \geq 0 \rangle_{\mathbb{F}_p\text{-alg.}}$ $(\subset \mathcal{U})$

r: fixed positive integer

$$\mathcal{U}_r := \langle e_\alpha^{(m)} \mid \alpha \in \Phi, 0 \leq m \leq p^r - 1 \rangle_{\mathbb{F}_p\text{-alg.}}$$

$$\mathcal{U}_r^+ := \mathcal{U}^+ \cap \mathcal{U}_r = \langle e_\alpha^{(m)} \mid \alpha \in \Phi^+, 0 \leq m \leq p^r - 1 \rangle_{\mathbb{F}_p\text{-alg.}}$$

$$\mathcal{U}_r^- := \mathcal{U}^- \cap \mathcal{U}_r = \langle e_\alpha^{(m)} \mid \alpha \in \Phi^-, 0 \leq m \leq p^r - 1 \rangle_{\mathbb{F}_p\text{-alg.}}$$

$$\mathcal{U}_r^0 := \mathcal{U}^0 \cap \mathcal{U}_r = \langle \binom{h_i}{n} \mid 1 \leq i \leq l,\ 0 \leq n \leq p^r - 1 \rangle_{\mathbb{F}_p\text{-alg.}}$$

Then we have $\mathcal{U} = \mathcal{U}^-\mathcal{U}^0\mathcal{U}^+$ and $\mathcal{U}_r = \mathcal{U}_r^-\mathcal{U}_r^0\mathcal{U}_r^+$
(i.e. the multiplication maps

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

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

are $\mathbb{F}_p$-linear isomorphisms).

§2 Commutation formulas

Proposition 2.1

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

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

Proposition 2.2 (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 $\alpha, \beta \in \Phi$ with $\alpha + \beta \in \Phi$.

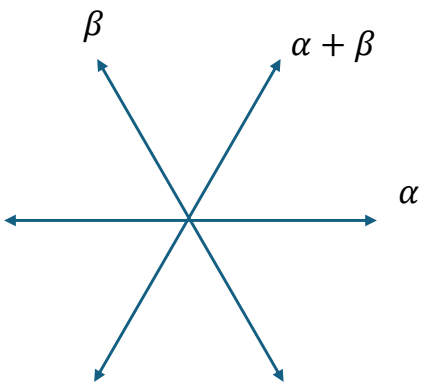
$\Phi'(\alpha, \beta) = (\mathbb{Z}\alpha + \mathbb{Z}\beta) \cap \Phi$ forms a root system of type A_2, B_2, or G_2.

Let m be a unique integer such that $\beta - m\alpha \in \Phi$ and $\beta - (m+1)\alpha \notin \Phi$.

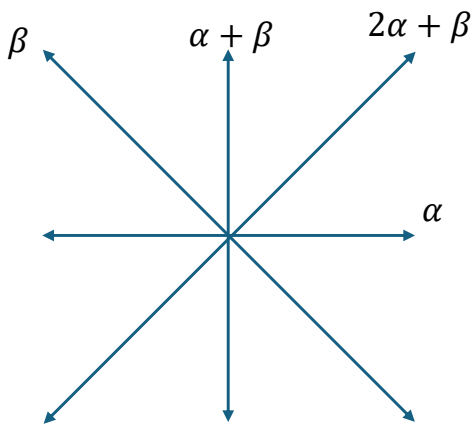
Then there exists $c_{\alpha,\beta} \in \{\pm 1\}$ such that $[e_\alpha, e_\beta] = (m+1)c_{\alpha,\beta}e_{\alpha+\beta}$ in $\mathfrak{g}_{\mathbb{Z}}$.

For simplicity, we assume that $||\alpha|| \leq ||\beta||$ and α and β form a base of $\Phi'(\alpha, \beta)$.

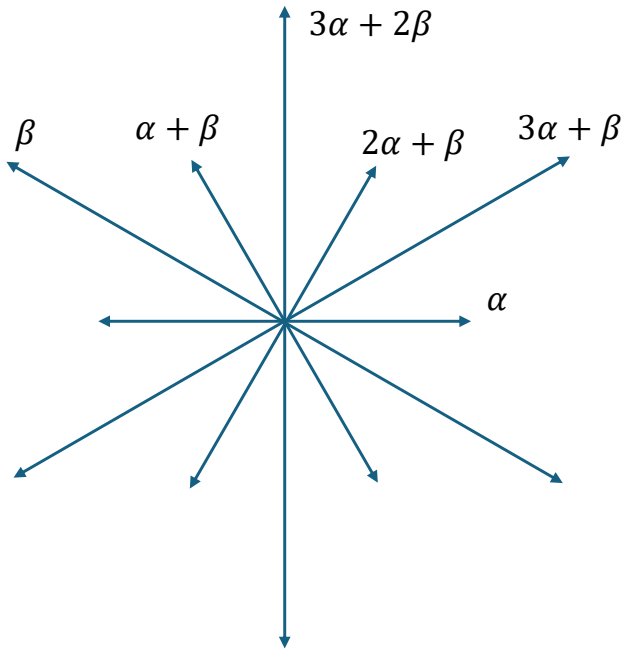
A_2


β
$\alpha+\beta$
α

B_2


β
$\alpha+\beta$
$2\alpha+\beta$
α

G_2


$3\alpha+2\beta$
β
$\alpha+\beta$
$2\alpha+\beta$
$3\alpha+\beta$
α

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

$$||\beta|| = ||\alpha||,$$

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

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

$$e_\alpha^{(a)} e_\beta^{(b)} = \sum_{\substack{t_1+t_2=b,\\ t_2+t_3=a}} c_{\alpha,\beta}^{t_2} e_\beta^{(t_1)} e_{\alpha+\beta}^{(t_2)} e_\alpha^{(t_3)} \quad (a, b \in \mathbb{Z}_{\geq 0})$$

in $\mathcal{U}_\mathbb{Z}$.

Suppose that $\Phi'(\alpha, \beta)$ is of type B_2. Then

$$||\beta|| = \sqrt{2}||\alpha||,$$

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

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

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

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

in $\mathcal{U}_{\mathbb{Z}}$.

Suppose that $\Phi'(\alpha, \beta)$ is of type G_2. Then

$$||\beta|| = \sqrt{3}||\alpha||,$$

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

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

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

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

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

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

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

in $\mathcal{U}_\mathbb{Z}$, where

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

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

w_0: (unique) longest element of W

$w_0 = s_{i_1} s_{i_2} \cdots s_{i_\nu}$: reduced expression ($\nu := l(w_0) = |\Phi^+|$)

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 $\Phi^+ = \{\beta_1, \beta_2, \ldots, \beta_\nu\}$ and 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 2.3 (Y, 2022)

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 2.3, we can prove the following:

Proposition 2.4 (Y, 2025)

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 $\mathcal{U}_r^+$.*

Proposition 2.5 (Y, 2025)

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

$$e_\alpha^{(n)} \mapsto \begin{cases} e_\alpha^{(n/p)} & \text{if } p \mid n, \\ 0 & \text{if } p \nmid n \end{cases} \qquad \left(\text{then } \binom{h_i}{n} \mapsto \begin{cases} \binom{h_i}{n/p} & \text{if } p \mid n, \\ 0 & \text{if } p \nmid n \end{cases} \right)$$

for $\alpha \in \Phi$. 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

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

Then there is a (unique) $\mathbb{F}_p$-linear map $\mathrm{Fr}' : \mathcal{U} \to \mathcal{U}$ defined by

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

Clearly we have $\mathrm{Fr} \circ \mathrm{Fr}' = \mathrm{id}_{\mathcal{U}}$.

Caution! Fr' is not an $\mathbb{F}_p$-algebra homomorphism.

Theorem 3.1 (Y, 2025)

Let $n \in \mathbb{Z}_{>0}$. Then the multiplication on $\mathcal{U}$ induces $\mathbb{F}_p$-linear isomorphisms

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

Theorem 3.2 (Y, 2025)

Let $n \in \mathbb{Z}_{>0}$. Then the multiplication on $\mathcal{U}$ induces $\mathbb{F}_p$-linear isomorphisms

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

Proposition 3.3

Let $n \in \mathbb{Z}_{>0}$. Then the multiplication on $\mathcal{U}$ induces $\mathbb{F}_p$-algebra isomorphisms

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

Outline of proof of Theorem 3.1

For $\mathbf{a} = (a_1, \ldots, a_\nu) \in (\mathbb{Z}_{\geq 0})^\nu$, set

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

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

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

Proposition 3.4

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

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

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

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

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

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

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

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 a $\mathbb{F}_p$-linear isomorphism.


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


Y. Yoshii, *Certain linear isomorphisms for hyperalgebras relative to a Chevalley group*, J. Algebra Appl. (2025), No.2550185.