

## Primitive Idempotents of the Hyperalgebra for the $r$ -th Frobenius kernel of $\mathrm{SL}(2, k)$

Yutaka Yoshii

Communicated by D. A. Timashev

**Abstract.** In this paper we construct primitive idempotents of the hyperalgebra for the  $r$ -th Frobenius kernel of the algebraic group  $\mathrm{SL}(2, k)$ .

*Mathematics Subject Classification 2010:* 16S30, 17B45, 20G05.

*Key Words and Phrases:* Primitive idempotents, hyperalgebras, algebraic groups, Frobenius kernels.

### 1. Introduction

Let  $k$  be an algebraically closed field of characteristic  $p > 0$ . Let  $G$  be a connected, simply connected and semisimple algebraic group over  $k$  which is split over the finite field  $\mathbb{F}_p$  of order  $p$ .

The representation theory of  $G$  is closely related to that of the  $r$ -th Frobenius kernel  $G_r$ . For example, all simple modules for  $G_r$  can be lifted to some simple modules for  $G$ . In addition, the projective indecomposable modules (PIMs) for  $G_r$  can be lifted to some modules for  $G$  if  $p$  is not too small. So it is important to construct PIMs for  $G_r$  in order to know the structure of some important  $G$ -modules.

On the other hand, the representation theory of  $G$  can be identified with the locally finite representation theory of the corresponding (infinite-dimensional)  $k$ -algebra  $\mathcal{U}$  which is called the hyperalgebra of  $G$ , and the representation theory of  $G_r$  can be identified with that of the corresponding finite-dimensional hyperalgebra  $\mathcal{U}_r$ . If we have a decomposition of the unity  $1 \in \mathcal{U}_r$  into a sum of pairwise orthogonal primitive idempotents, we can construct the PIMs for  $\mathcal{U}_r$ . Unfortunately, it seems that such a decomposition where each primitive idempotent is explicitly described is not known except when  $G$  is of type  $A_1$  (i.e.  $G = \mathrm{SL}(2, k)$ ) and  $r = 1$ , in this case the decomposition is given in Seligman's paper [Sel03].

In this paper we shall generalize Seligman's result. More concretely, when  $G = \mathrm{SL}(2, k)$ , we construct pairwise orthogonal primitive idempotents whose sum is the unity 1 explicitly in  $\mathcal{U}_r$  for an arbitrary positive integer  $r$ .

The main result is given in Section 5. In Section 4 we first construct the primitive idempotents in  $\mathcal{U}_1$  using Seligman’s method. Next, in Section 5 we construct primitive idempotents in  $\mathcal{U}_r$  for  $r \geq 2$  using the primitive idempotents in  $\mathcal{U}_1$  given in the previous section. There we use a linear map constructed in [GK11], which ‘splits’ the Frobenius map on  $\mathcal{U}$ . Finally we also determine the PIMs for  $\mathcal{U}_r$  which the idempotents generate. For convenience, this result will be given more generally for a larger algebra  $\mathcal{U}_{r,r'}$  ( $r' > r$ ) in Theorem 5.8.

### 2. Preliminaries

From now on, let  $G = \mathrm{SL}_2(k)$ . Let

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

be the standard basis in the simple complex Lie algebra  $\mathfrak{g}_{\mathbb{C}} = \mathfrak{sl}_2(\mathbb{C})$ . We define a subring  $\mathcal{U}_{\mathbb{Z}}$  of the universal enveloping algebra  $\mathcal{U}_{\mathbb{C}}$  of  $\mathfrak{g}_{\mathbb{C}}$  generated by  $X^{(m)} = X^m/m!$  and  $Y^{(m)} = Y^m/m!$  with  $m \in \mathbb{Z}_{\geq 0}$ . For  $z = H$  or  $-H$  in  $\mathcal{U}_{\mathbb{Z}}$ , set

$$\binom{z+c}{m} = \frac{(z+c)(z+c-1)\cdots(z+c-m+1)}{m!}$$

for  $c \in \mathbb{Z}$  and  $m \in \mathbb{Z}_{\geq 0}$ , which also lies in  $\mathcal{U}_{\mathbb{Z}}$ . Then the elements

$$Y^{(m)} \binom{H}{n} X^{(m')}$$

with  $m, m', n \in \mathbb{Z}_{\geq 0}$  form a  $\mathbb{Z}$ -basis of  $\mathcal{U}_{\mathbb{Z}}$ . The  $k$ -algebra  $\mathcal{U}_{\mathbb{Z}} \otimes_{\mathbb{Z}} k$  is denoted by  $\mathcal{U}$  and called the hyperalgebra of  $G$ , which is equipped with a structure of Hopf algebra over  $k$ . We use the same notation for the images in  $\mathcal{U}$  of the elements in  $\mathcal{U}_{\mathbb{Z}}$ . In the following propositions we shall give some well-known formulas, which are repeatedly used to carry out calculations in  $\mathcal{U}$  (for example, see [Gro12, §3], [GK15, §4], [Hab80, §5], [Hum72, §26], [Jan03, I. ch. 7]).

**Proposition 2.1.** *For  $m, n \in \mathbb{Z}_{\geq 0}$  and  $s, t \in \mathbb{Z}$ , the following holds in  $\mathcal{U}$ :*

- (i)  $X^{(m)}Y^{(n)} = \sum_{i=0}^{\min(m,n)} Y^{(n-i)} \binom{H-m-n+2i}{i} X^{(m-i)},$   
 $Y^{(m)}X^{(n)} = \sum_{i=0}^{\min(m,n)} X^{(n-i)} \binom{-H-m-n+2i}{i} Y^{(m-i)},$
- (ii)  $\binom{H+s}{m} X^{(n)} = X^{(n)} \binom{H+s+2n}{m}, \quad \binom{H+s}{m} Y^{(n)} = Y^{(n)} \binom{H+s-2n}{m},$
- (iii)  $X^{(m)}X^{(n)} = \binom{m+n}{n} X^{(m+n)}, \quad Y^{(m)}Y^{(n)} = \binom{m+n}{n} Y^{(m+n)},$
- (iv)  $\binom{H}{m} \binom{H}{n} = \sum_{i=0}^{\min(m,n)} \binom{n+m-i}{m} \binom{m}{i} \binom{H}{n+m-i},$
- (v)  $\binom{H+s+t}{m} = \sum_{i=0}^m \binom{s}{m-i} \binom{H+t}{i}.$

**Proposition 2.2.** *Let  $m, m', n, n' \in \mathbb{Z}$  with  $n' \geq 0$  and  $0 \leq m, n \leq p - 1$ . Then*

$$\binom{m + m'p}{n + n'p} \equiv \binom{m}{n} \binom{m'}{n'} \pmod{p}.$$

Let

$$\text{Fr} : G \longrightarrow G, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a^p & b^p \\ c^p & d^p \end{pmatrix}$$

be the geometric Frobenius map. This map induces the  $k$ -algebra endomorphism  $\text{Fr} : \mathcal{U} \rightarrow \mathcal{U}$  which is defined by

$$\text{Fr}(X^{(m)}) = \begin{cases} X^{(m/p)} & \text{if } p \mid m, \\ 0 & \text{if } p \nmid m \end{cases} \quad \text{and} \quad \text{Fr}(Y^{(m)}) = \begin{cases} Y^{(m/p)} & \text{if } p \mid m, \\ 0 & \text{if } p \nmid m \end{cases}.$$

Then we also have

$$\text{Fr} \left( \binom{H}{m} \right) = \begin{cases} \binom{H}{m/p} & \text{if } p \mid m, \\ 0 & \text{if } p \nmid m \end{cases}.$$

Let  $\mathcal{U}^+$  (resp.  $\mathcal{U}^-$ ) be the subalgebra of  $\mathcal{U}$  generated by  $X^{(p^i)}$  (resp.  $Y^{(p^i)}$ ) with  $i \in \mathbb{Z}_{\geq 0}$ , and let  $\mathcal{U}^0$  be the subalgebra of  $\mathcal{U}$  generated by  $\binom{H}{p^i}$  with  $i \in \mathbb{Z}_{\geq 0}$ . The elements  $Y^{(m)} \binom{H}{n} X^{(m')}$  with  $m, m', n \in \mathbb{Z}_{\geq 0}$  form a  $k$ -basis of  $\mathcal{U}$  and we have a triangular decomposition  $\mathcal{U} = \mathcal{U}^- \mathcal{U}^0 \mathcal{U}^+$ . We say that an element  $z \in \mathcal{U}$  has degree  $d$  if it is a  $k$ -linear combination of the elements  $Y^{(m)} \binom{H}{n} X^{(m')}$  with  $m, m', n \in \mathbb{Z}_{\geq 0}$  and  $m' - m = d$ . For a positive integer  $r \in \mathbb{Z}_{>0}$ , let  $\mathcal{U}_r$  be the subalgebra of  $\mathcal{U}$  generated by  $X^{(p^i)}$  and  $Y^{(p^i)}$  with  $0 \leq i \leq r - 1$ . This is a finite-dimensional algebra of dimension  $p^{3r}$  which has  $Y^{(m)} \binom{H}{n} X^{(m')}$  with  $0 \leq m, m', n \leq p^r - 1$  as a basis, and it can be identified with the hyperalgebra of the  $r$ -th Frobenius kernel  $G_r = \text{Ker}(\text{Fr}^r)$  of  $G$ . Let  $\mathcal{U}_r^+$  (resp.  $\mathcal{U}_r^-$ ) be the subalgebra of  $\mathcal{U}$  generated by  $X^{(p^i)}$  (resp.  $Y^{(p^i)}$ ) with  $0 \leq i \leq r - 1$ , and  $\mathcal{U}_r^0$  the subalgebra of  $\mathcal{U}$  generated by  $\binom{H}{p^i}$  with  $0 \leq i \leq r - 1$ . Then we define four subalgebras  $\mathcal{U}^{\geq 0}, \mathcal{U}^{\leq 0}, \mathcal{U}_r^{\geq 0}$  and  $\mathcal{U}_r^{\leq 0}$  as

$$\mathcal{U}^{\geq 0} = \mathcal{U}^0 \mathcal{U}^+, \quad \mathcal{U}^{\leq 0} = \mathcal{U}^- \mathcal{U}^0, \quad \mathcal{U}_r^{\geq 0} = \mathcal{U}_r^0 \mathcal{U}_r^+ \quad \text{and} \quad \mathcal{U}_r^{\leq 0} = \mathcal{U}_r^- \mathcal{U}_r^0.$$

In dealing with the subalgebra  $\mathcal{U}_r$  it is often convenient to consider the larger subalgebras  $\tilde{\mathcal{U}}_r = \mathcal{U}_r^- \mathcal{U}^0 \mathcal{U}_r^+$  generated by  $X^{(p^i)}, Y^{(p^i)}$  and  $\binom{H}{p^l}$  with  $0 \leq i \leq r - 1$  and  $l \in \mathbb{Z}_{\geq 0}$ , and  $\mathcal{U}_{r,r'} = \mathcal{U}_r^- \mathcal{U}_r^0 \mathcal{U}_r^+$  generated by  $X^{(p^i)}, Y^{(p^i)}$  and  $\binom{H}{p^l}$  with  $0 \leq i \leq r - 1$  and  $0 \leq l \leq r' - 1$  for  $r' > r$ . Then the elements  $Y^{(m)} \binom{H}{n} X^{(m')}$  with  $0 \leq m, m' \leq p^r - 1$  and  $n \in \mathbb{Z}_{\geq 0}$  (resp.  $0 \leq n \leq p^{r'} - 1$ ) form a  $k$ -basis of  $\tilde{\mathcal{U}}_r$  (resp.  $\mathcal{U}_{r,r'}$ ).

Consider the  $k$ -linear map  $\text{Fr}' : \mathcal{U} \rightarrow \mathcal{U}$  defined by

$$Y^{(m)} \binom{H}{n} X^{(m')} \mapsto Y^{(mp)} \binom{H}{np} X^{(m'p)}.$$

Clearly we have  $\text{Fr} \circ \text{Fr}' = \text{id}_{\mathcal{U}}$ . Let  $\text{Fr}'^+$  (resp.  $\text{Fr}'^-, \text{Fr}'^0, \text{Fr}'^{\geq 0}, \text{Fr}'^{\leq 0}$ ) be the restriction of  $\text{Fr}'$  to  $\mathcal{U}^+$  (resp.  $\mathcal{U}^-, \mathcal{U}^0, \mathcal{U}^{\geq 0}, \mathcal{U}^{\leq 0}$ ). These five restriction maps are homomorphisms of  $k$ -algebras, whereas  $\text{Fr}'$  is not (see [GK11, 1.2]).

In this paper, the symbol  $\otimes$  is assumed to mean a tensor product over  $k$ .

**Proposition 2.3.** For  $n, n' \in \mathbb{Z}_{>0}$  with  $n' > n$ , the multiplication map

$$\mathcal{U}_n \otimes \text{Fr}^n(\mathcal{U}_{n'-n}) \rightarrow \mathcal{U}_{n'}$$

is a  $k$ -linear isomorphism.

**Proof.** The linearity is clear. Since both the  $k$ -vector spaces  $\mathcal{U}_n \otimes \text{Fr}^n(\mathcal{U}_{n'-n})$  and  $\mathcal{U}_{n'}$  have dimension  $p^{3n'}$ , it is enough to show that the map is injective. Let  $z$  be a nonzero element of  $\mathcal{U}_n \otimes \text{Fr}^n(\mathcal{U}_{n'-n})$ . Note that

$$Y^{(m_1)} \binom{H}{n_1} X^{(m'_1)} \otimes Y^{(m_2 p^n)} \binom{H}{n_2 p^n} X^{(m'_2 p^n)}$$

with  $0 \leq m_1, n_1, m'_1 \leq p^n - 1$  and  $0 \leq m_2, n_2, m'_2 \leq p^{n'-n} - 1$  form a  $k$ -basis of  $\mathcal{U}_n \otimes \text{Fr}^n(\mathcal{U}_{n'-n})$ . Moreover, by using the formulas in Propositions 2.1 and 2.2 we easily see that such a basis vector is mapped to

$$Y^{(m_1)} \binom{H}{n_1} X^{(m'_1)} Y^{(m_2 p^n)} \binom{H}{n_2 p^n} X^{(m'_2 p^n)} = Y^{(m_1+m_2 p^n)} \binom{H}{n_1+n_2 p^n} X^{(m'_1+m'_2 p^n)} + u,$$

where  $u$  is a  $k$ -linear combination of some basis vectors of the form  $Y^{(m_3)} \binom{H}{n_3} X^{(m'_3)}$  with  $0 \leq m_3, n_3, m'_3 \leq p^{n'} - 1$  and  $m_3+n_3+m'_3 < m_1+n_1+m'_1+(m_2+n_2+m'_2)p^n$ . Therefore, if we take a 6-tuple

$$(m_1, n_1, m'_1, m_2, n_2, m'_2) \text{ where } m_1+n_1+m'_1+(m_2+n_2+m'_2)p^n$$

is the largest integer with the coefficient of  $Y^{(m_1)} \binom{H}{n_1} X^{(m'_1)} \otimes Y^{(m_2 p^n)} \binom{H}{n_2 p^n} X^{(m'_2 p^n)}$  in the expression of  $z$  as a  $k$ -linear combination of the basis vectors of the vector space  $\mathcal{U}_n \otimes \text{Fr}^n(\mathcal{U}_{n'-n})$  being nonzero, then the coefficient of

$$Y^{(m_1+m_2 p^n)} \binom{H}{n_1+n_2 p^n} X^{(m'_1+m'_2 p^n)}$$

in the expression of the image of  $z$  as a  $k$ -linear combination of the basis vectors of  $\mathcal{U}_{n'}$  is also nonzero. This shows that the multiplication map is injective, and the proposition follows. ■

**Remark.** These multiplication maps  $\mathcal{U}_n \otimes \text{Fr}^n(\mathcal{U}_{n'-n}) \rightarrow \mathcal{U}_{n'}$  ( $n' > n > 0$ ) induce the multiplication maps  $\mathcal{U}_n \otimes \text{Fr}^n(\mathcal{U}) \rightarrow \mathcal{U}$  and  $\bigotimes_{i \geq 0} \text{Fr}^i(\mathcal{U}_1) \rightarrow \mathcal{U}$  (for the natural ordering of  $\mathbb{Z}_{\geq 0}$ ), all of which are  $k$ -linear isomorphisms.

For later use, let  $\mathcal{A}$  be the subalgebra of  $\mathcal{U}$  which is generated by  $\mathcal{U}^0$  and the elements  $Y^{(p^i)} X^{(p^i)}$  with  $i \in \mathbb{Z}_{\geq 0}$ .

**Proposition 2.4.** The following holds.

- (i)  $\mathcal{A}$  is commutative.
- (ii)  $\mathcal{A}$  is the centralizer of  $\mathcal{U}^0$  in  $\mathcal{U}$ , consisting of all the elements of degree 0 in  $\mathcal{U}$ .

(iii)  $\mathcal{A}$  is free over  $\mathcal{U}^0$  of basis  $X^{(m)}Y^{(m)}$ ,  $m \in \mathbb{Z}_{\geq 0}$ , and also of basis  $Y^{(m)}X^{(m)}$ ,  $m \in \mathbb{Z}_{\geq 0}$ .

**Proof.** (i) Let  $s, t \in \mathbb{Z}_{\geq 0}$ . Since

$$\begin{aligned} \binom{H}{p^s} Y^{(p^t)} X^{(p^t)} &= Y^{(p^t)} \binom{H - 2p^t}{p^s} X^{(p^t)} \\ &= Y^{(p^t)} \sum_{i=0}^{p^s} \binom{-2p^t}{i} \binom{H}{p^s - i} X^{(p^t)} \\ &= Y^{(p^t)} X^{(p^t)} \sum_{i=0}^{p^s} \binom{-2p^t}{i} \binom{H + 2p^t}{p^s - i} \\ &= Y^{(p^t)} X^{(p^t)} \binom{H}{p^s}, \end{aligned}$$

each  $Y^{(p^t)} X^{(p^t)}$  commutes with all elements of  $\mathcal{U}^0$ . On the other hand, we have

$$\begin{aligned} &Y^{(p^s)} X^{(p^s)} Y^{(p^t)} X^{(p^t)} \\ &= Y^{(p^s)} \sum_{i=0}^{\min(p^s, p^t)} Y^{(p^t-i)} \binom{H - p^s - p^t + 2i}{i} X^{(p^s-i)} X^{(p^t)} \\ &= \sum_{i=0}^{\min(p^s, p^t)} \binom{p^s + p^t - i}{p^s} \binom{p^s + p^t - i}{p^t} Y^{(p^s+p^t-i)} \binom{H - p^s - p^t + 2i}{i} X^{(p^s+p^t-i)}, \end{aligned}$$

which is symmetric with respect to  $p^s$  and  $p^t$ . Therefore,  $Y^{(p^t)} X^{(p^t)}$  also commutes with  $Y^{(p^s)} X^{(p^s)}$ .

(ii) It is easy to see that  $\mathcal{A}$  consists of all the elements of degree 0 in  $\mathcal{U}$ . Let  $C_{\mathcal{U}}(\mathcal{U}^0)$  be the centralizer of  $\mathcal{U}^0$  in  $\mathcal{U}$ . Clearly  $\mathcal{A} \subseteq C_{\mathcal{U}}(\mathcal{U}^0)$ , and we have to show that  $\mathcal{A} \supseteq C_{\mathcal{U}}(\mathcal{U}^0)$ . Let  $z$  be an element of  $C_{\mathcal{U}}(\mathcal{U}^0)$ . Then  $z$  can be written uniquely as

$$z = \sum_{m, m' \in \mathbb{Z}_{\geq 0}} Y^{(m)} z_{(m, m')} X^{(m')}$$

with all  $z_{(m, m')} \in \mathcal{U}^0$ , almost all equal to 0. To show that  $z \in \mathcal{A}$ , it is enough to show that  $z_{(m, m')} = 0$  for each pair  $(m, m')$  with  $m \neq m'$ . For  $s \in \mathbb{Z}$  and  $t \in \mathbb{Z}_{\geq 0}$ , we have

$$\begin{aligned} \binom{H + s}{t} z &= \sum_{m, m' \in \mathbb{Z}_{\geq 0}} Y^{(m)} \binom{H + s - 2m}{t} z_{(m, m')} X^{(m')}, \\ z \binom{H + s}{t} &= \sum_{m, m' \in \mathbb{Z}_{\geq 0}} Y^{(m)} \binom{H + s - 2m'}{t} z_{(m, m')} X^{(m')}. \end{aligned}$$

Since  $\binom{H+s}{t} z = z \binom{H+s}{t}$ , for each pair  $(m, m')$ , we must have

$$\left( \binom{H + s - 2m}{t} - \binom{H + s - 2m'}{t} \right) z_{(m, m')} = 0$$

for any  $s \in \mathbb{Z}$  and  $t \in \mathbb{Z}_{\geq 0}$ . Take unique integers  $c \in \mathbb{Z}_{\geq 0}$  and  $d \in \mathbb{Z}$  such that  $2(m' - m) = p^c d$  and  $p$  does not divide  $d$ . Then if we take  $s = 2m'$  and  $t = p^c$ , we have

$$\begin{aligned} \binom{H + s - 2m}{t} - \binom{H + s - 2m'}{t} &= \binom{H + p^c d}{p^c} - \binom{H}{p^c} \\ &= \sum_{i=0}^{p^c} \binom{p^c d}{i} \binom{H}{p^c - i} - \binom{H}{p^c} \\ &= \binom{H}{p^c} + d - \binom{H}{p^c} = d. \end{aligned}$$

Since  $d \neq 0$  in  $\mathbb{F}_p$ , we must have  $z_{(m,m')} = 0$  and hence  $z \in \mathcal{A}$ .

(iii) It is easy from the fact that  $X^{(m)} \binom{H}{n} Y^{(m)}$  with  $m, n \in \mathbb{Z}_{\geq 0}$  as well as  $Y^{(m)} \binom{H}{n} X^{(m)}$  with  $m, n \in \mathbb{Z}_{\geq 0}$  form a  $k$ -basis of  $\mathcal{A}$ . ■

For  $r, r' \in \mathbb{Z}_{>0}$  with  $r' > r$ , we write  $\mathcal{A}_r$  (resp.  $\tilde{\mathcal{A}}_r, \mathcal{A}_{r,r'}$ ) for the subalgebra of  $\mathcal{U}_r$  (resp.  $\tilde{\mathcal{U}}_r, \mathcal{U}_{r,r'}$ ) generated by  $\mathcal{U}_r^0$  (resp.  $\mathcal{U}^0, \mathcal{U}_{r'}^0$ ) and the elements  $Y^{(p^i)} X^{(p^i)}$  with  $0 \leq i \leq r-1$ . Clearly we have  $\mathcal{A}_r = \mathcal{A} \cap \mathcal{U}_r$ ,  $\tilde{\mathcal{A}}_r = \mathcal{A} \cap \tilde{\mathcal{U}}_r$  and  $\mathcal{A}_{r,r'} = \mathcal{A} \cap \mathcal{U}_{r,r'}$ . We also see that  $\mathcal{A}_r$  (resp.  $\tilde{\mathcal{A}}_r, \mathcal{A}_{r,r'}$ ) is the centralizer of  $\mathcal{U}_r^0$  (resp.  $\mathcal{U}^0, \mathcal{U}_{r'}^0$ ) in  $\mathcal{U}_r$  (resp.  $\tilde{\mathcal{U}}_r, \mathcal{U}_{r,r'}$ ) and is free over  $\mathcal{U}_r^0$  (resp.  $\mathcal{U}^0, \mathcal{U}_{r'}^0$ ) of basis  $X^{(m)} Y^{(m)}$ ,  $0 \leq m \leq p^r - 1$ , and also of basis  $Y^{(m)} X^{(m)}$ ,  $0 \leq m \leq p^r - 1$ .

The following proposition will be used in Section 5.

**Proposition 2.5.** *Let  $n \in \mathbb{Z}_{\geq 0}$ . Then  $X^{(np)}$  and  $Y^{(np)}$  commute with all elements in  $\mathcal{A}_1$ .*

**Proof.** We may assume that  $n > 0$ . Then

$$\begin{aligned} X^{(np)} Y X &= Y X^{(np)} X + (H - np + 1) X^{(np-1)} X \\ &= Y X X^{(np)} \end{aligned}$$

and

$$X^{(np)} H = (H - 2np) X^{(np)} = H X^{(np)}.$$

Similarly we have  $Y X Y^{(np)} = Y^{(np)} Y X$  and  $Y^{(np)} H = H Y^{(np)}$ , as desired. ■

### 3. Representation theory of $\mathcal{U}$

We describe some elementary facts on the representation theory of  $\mathcal{U}$  and some subalgebras.

In this paper, all modules we consider are assumed to be finite-dimensional left modules. The category of finite-dimensional  $\mathcal{U}$ - (resp.  $\mathcal{U}_r$ -) modules is identified with that of finite-dimensional (rational)  $G$ - (resp.  $G_r$ -) modules.

For a nonzero  $\mathcal{U}^0$ -module  $V$  and an integer  $\lambda \in \mathbb{Z}$ , set

$$V_\lambda = \left\{ v \in V \mid \binom{H}{m} v = \binom{\lambda}{m} v, \forall m \in \mathbb{Z}_{\geq 0} \right\}.$$

This is a  $\mathcal{U}^0$ -submodule of  $V$ . If  $V_\lambda \neq 0$ , then we call it the  $\mathcal{U}^0$ -weight space of ( $\mathcal{U}^0$ -) weight  $\lambda$ . A nonzero element of  $V_\lambda$  is called a  $\mathcal{U}^0$ -weight vector of weight  $\lambda$ . Any  $\mathcal{U}$ -module  $M$  can be written as a direct sum of its  $\mathcal{U}^0$ -weight spaces:  $M = \bigoplus_{\lambda \in \mathbb{Z}} M_\lambda$ . For  $\lambda \in \mathbb{Z}$ , let  $k_\lambda$  be a one-dimensional  $\mathcal{U}^0$ -module which is also a  $\mathcal{U}^0$ -weight space of weight  $\lambda$ .

As in the case of  $\mathcal{U}^0$ -modules, we can define a notion of weights for  $\mathcal{U}_r^0$ -modules. For an integer  $\mu \in \mathbb{Z}$ , we consider the subspace  $V_{(r,\mu)}$  of a nonzero  $\mathcal{U}_r^0$ -module  $V$  consisting of the vectors  $v \in V$  which satisfy  $\binom{H}{m}v = \binom{\mu}{m}v$  for all integers  $m$  with  $0 \leq m \leq p^r - 1$ . If  $V_{(r,\mu)} \neq 0$ , then we call it the  $\mathcal{U}_r^0$ -weight space of  $\mathcal{U}_r^0$ -weight  $\mu$ . If  $\nu \equiv \mu \pmod{p^r}$ , then we have  $V_{(r,\nu)} = V_{(r,\mu)}$  since  $\binom{\nu}{m} \equiv \binom{\mu}{m} \pmod{p}$  for all  $m$  with  $0 \leq m \leq p^r - 1$ . Therefore, a  $\mathcal{U}_r^0$ -weight  $\mu \in \mathbb{Z}$  can be regarded as an element of  $\mathbb{Z}/p^r\mathbb{Z}$  and a  $\mathcal{U}_r^0$ -module  $V$  is decomposed as  $V = \bigoplus_{\mu=0}^{p^r-1} V_{(r,\mu)} = \bigoplus_{\mu \in \mathbb{Z}/p^r\mathbb{Z}} V_{(r,\mu)}$ . Moreover, if  $M$  is a  $\mathcal{U}$ -module, then the  $\mathcal{U}_r^0$ -weight space  $M_{(r,\mu)}$  of  $\mathcal{U}_r^0$ -weight  $\mu \in \mathbb{Z}$  is decomposed as  $M_{(r,\mu)} = \bigoplus_{\lambda} M_\lambda$  where  $\lambda$  runs through the integers with  $\lambda \equiv \mu \pmod{p^r}$ .

For a  $\mathcal{U}$ -module  $M$  and  $i \in \mathbb{Z}_{\geq 0}$ , let  $M^{[i]}$  be another  $\mathcal{U}$ -module defined as follows: it is equal to  $M$  as a  $k$ -vector space and the action of  $z \in \mathcal{U}$  on  $M^{[i]}$  is induced by that of  $\text{Fr}^i(z)$  on  $M$ . Therefore, if  $v^{[i]}$  is the corresponding element in  $M^{[i]}$  for  $v \in M$ , then  $zv^{[i]} = (\text{Fr}^i(z)v)^{[i]}$  for  $z \in \mathcal{U}$ . The  $\mathcal{U}$ -module  $M^{[i]}$  is called the  $i$ -th Frobenius twist of  $M$ . If an element  $v \in M$  has  $\mathcal{U}^0$ -weight  $\lambda$ , the corresponding element  $v^{[i]} \in M^{[i]}$  has  $\mathcal{U}^0$ -weight  $\lambda p^i$ . Moreover, if  $i \geq r$ ,  $M^{[i]}$  is isomorphic to a direct sum of  $\dim_k M$  copies of the trivial module  $k$  as a  $\mathcal{U}_r$ -module. If  $M$  and  $M'$  are  $\mathcal{U}$ -modules, the tensor product  $M \otimes M'$  is again a  $\mathcal{U}$ -module via the comultiplication on  $\mathcal{U}$

$$X^{(m)}(v \otimes v') = \sum_{i=0}^m X^{(i)}v \otimes X^{(m-i)}v'$$

and

$$Y^{(m)}(v \otimes v') = \sum_{i=0}^m Y^{(i)}v \otimes Y^{(m-i)}v'$$

for  $m \in \mathbb{Z}_{\geq 0}$ ,  $v \in M$  and  $v' \in M'$ .

Let  $V_{\mathbb{C}}(\lambda)$  be a simple  $\mathcal{U}_{\mathbb{C}}$ -module with highest weight  $\lambda \in \mathbb{Z}_{\geq 0}$ . For a fixed highest weight vector  $v_\lambda \in V_{\mathbb{C}}(\lambda)$ , the  $\mathcal{U}$ -module  $V(\lambda) = k \otimes_{\mathbb{Z}} (\mathcal{U}_{\mathbb{Z}}v_\lambda)$  is called the Weyl ( $\mathcal{U}$ -) module with highest weight  $\lambda$ . For an element of  $\mathcal{U}_{\mathbb{Z}}v_\lambda$ , we use the same notation for its image in  $V(\lambda)$ . The vectors  $Y^{(i)}v_\lambda$  with  $0 \leq i \leq \lambda$  have weight  $\lambda - 2i$  and form a basis of  $V(\lambda)$ . Each Weyl module  $V(\lambda)$  has a unique maximal submodule, and the quotient  $L(\lambda)$  of  $V(\lambda)$  by the submodule is a simple  $\mathcal{U}$ -module. Then all  $L(\lambda)$  with  $\lambda \in \mathbb{Z}_{\geq 0}$  form the set of non-isomorphic simple  $\mathcal{U}$ -modules. For  $\lambda \in \mathbb{Z}_{\geq 0}$  and its  $p$ -adic expansion  $\lambda = \sum_{i=0}^{n-1} \lambda_i p^i$ , we have by Steinberg's tensor product theorem that

$$L(\lambda) \cong L(\lambda_0) \otimes L(\lambda_1)^{[1]} \otimes \cdots \otimes L(\lambda_{n-1})^{[n-1]}$$

as  $\mathcal{U}$ -modules. For  $i \in \mathbb{Z}_{\geq 0}$ , the simple module  $L(p^i - 1)$  is called the  $i$ -th Steinberg module and often denoted by  $\text{St}_i$ . The trivial  $\mathcal{U}$ -module  $k$  is isomorphic

to  $L(0)$ , and the  $r$ -th Steinberg module  $\text{St}_r$  is projective as a  $\mathcal{U}_r$ -module. If  $0 \leq \lambda \leq p^r - 1$ , then  $L(\lambda)$  is also simple as a  $\mathcal{U}_r$ -module, and any simple  $\mathcal{U}_r$ -module can be obtained in this way. For an integer  $\lambda$  with  $0 \leq \lambda \leq p^r - 1$ , let  $Q_r(\lambda)$  be the projective cover of the simple  $\mathcal{U}_r$ -module  $L(\lambda)$ . It is known that these  $\mathcal{U}_r$ -modules  $Q_r(\lambda)$  can be extended to  $\mathcal{U}$ -modules for any  $r \in \mathbb{Z}_{>0}$  in this situation  $G = \text{SL}_2(k)$  (see [Jan80, 4.5 Corollar] or [Jan03, II. 11.11]). If  $0 \leq \lambda \leq p - 2$ , then  $Q_1(\lambda)$  is a uniserial  $\mathcal{U}$ -module with

$$Q_1(\lambda)/\text{rad}_{\mathcal{U}}Q_1(\lambda) \cong L(\lambda),$$

$$\text{rad}_{\mathcal{U}}Q_1(\lambda)/\text{soc}_{\mathcal{U}}Q_1(\lambda) \cong L(2p - 2 - \lambda)$$

and

$$\text{soc}_{\mathcal{U}}Q_1(\lambda) \cong L(\lambda),$$

whereas  $Q_1(p - 1) = L(p - 1) = \text{St}_1$ . As in the simple  $\mathcal{U}$ -modules, for  $\lambda \in \mathbb{Z}_{\geq 0}$  and its  $p$ -adic expansion  $\lambda = \sum_{i=0}^{n-1} \lambda_i p^i$ , we have

$$Q_n(\lambda) \cong Q_1(\lambda_0) \otimes Q_1(\lambda_1)^{[1]} \otimes \cdots \otimes Q_1(\lambda_{n-1})^{[n-1]}$$

as  $\mathcal{U}$ -modules. The highest  $\mathcal{U}^0$ -weight in  $Q_n(\lambda)$  is  $2p^n - 2 - \lambda$  and the lowest one is  $-2p^n + 2 + \lambda$  (see [Don93, (2.2) Example 1]).

For later use we also consider some modules for  $\tilde{\mathcal{U}}_r$  and  $\mathcal{U}_{r,r'}$  for an integer  $r'$  greater than  $r$ . Let  $\lambda', \lambda'' \in \mathbb{Z}$  be integers with  $0 \leq \lambda' \leq p^r - 1$  and set  $\lambda = \lambda' + \lambda''p^r$ . The simple  $\mathcal{U}$ -module  $L(\lambda')$  is also simple as a  $\mathcal{U}_r$ -module, and then  $\tilde{L}_r(\lambda) = L(\lambda') \otimes k_{\lambda''p^r}$  is a simple  $\tilde{\mathcal{U}}_r$ -module with highest  $\mathcal{U}^0$ -weight  $\lambda$ , where the one-dimensional  $\mathcal{U}^0$ -module  $k_{\lambda''p^r}$  is regarded as a  $\tilde{\mathcal{U}}_r$ -module by the trivial action of  $\mathcal{U}_r$ . Then we see that  $\tilde{L}_r(\lambda) \cong L(\lambda')$  as  $\mathcal{U}_r$ -modules. Similarly, set  $\tilde{Q}_r(\lambda) = Q_r(\lambda') \otimes k_{\lambda''p^r}$  for the above  $\lambda = \lambda' + \lambda''p^r$ . This is the projective cover of the simple  $\tilde{\mathcal{U}}_r$ -module  $\tilde{L}_r(\lambda)$ , and we have  $\tilde{Q}_r(\lambda) \cong Q_r(\lambda')$  as  $\mathcal{U}_r$ -modules. The simple  $\tilde{\mathcal{U}}_r$ -modules  $\tilde{L}_r(\nu)$  with  $\nu \in \mathbb{Z}$  are simple as  $\mathcal{U}_{r,r'}$ -modules, and all simple  $\mathcal{U}_{r,r'}$ -modules can be obtained in this way. Since  $\tilde{L}_r(\nu_1) \cong \tilde{L}_r(\nu_2)$  as  $\mathcal{U}_{r,r'}$ -modules if and only if  $\nu_1 \equiv \nu_2 \pmod{p^{r'}}$ , all non-isomorphic simple  $\mathcal{U}_{r,r'}$ -modules can be written as  $\tilde{L}_r(\nu)$ ,  $0 \leq \nu \leq p^{r'} - 1$ . Then the simple  $\mathcal{U}_{r,r'}$ -module  $\tilde{L}_r(\nu)$  has  $\tilde{Q}_r(\nu)$  as its projective cover.

The following proposition will be used later to determine the PIMs for  $\mathcal{U}_{r,r'}$  (hence for  $\mathcal{U}_r$ ) which the idempotents given there generate.

**Proposition 3.1.** *Let  $r'$  be an integer which is greater than  $r$ . Let  $\lambda$  be an integer with  $0 \leq \lambda \leq p^{r'} - 1$ , and let  $v$  be a  $\mathcal{U}_{r'}^0$ -weight vector of  $\mathcal{U}_r^0$ -weight  $\nu$  with  $0 \leq \nu \leq p^{r'} - 1$  which is also a generator of the projective indecomposable  $\mathcal{U}_{r,r'}$ -module  $\tilde{Q}_r(\lambda)$ . Let  $t$  be the largest integer  $n$  with  $X^{(n)}v \neq 0$  and  $0 \leq n \leq p^r - 1$ . Then if we write  $\lambda = \lambda' + \lambda''p^r$  and  $\nu = \nu' + \nu''p^r$  for some unique integers  $\lambda', \lambda'', \nu', \nu''$  with  $0 \leq \lambda', \nu' \leq p^r - 1$  and  $0 \leq \lambda'', \nu'' \leq p^{r'-r} - 1$ , the following holds:*

- (i)  $t = p^r - 1 - (\lambda' + \nu')/2$  and  $\lambda'' = \nu''$  if  $\nu' + 2t \leq 2p^r - 2$ ,
- (ii)  $t = 3p^r/2 - 1 - (\lambda' + \nu')/2$  and  $\lambda'' = \nu'' + 1$  if  $\nu' + 2t > 2p^r - 2$  and  $\nu'' \neq p^{r'-r} - 1$ ,
- (iii)  $t = 3p^r/2 - 1 - (\lambda' + \nu')/2$  and  $\lambda'' = 0$  if  $\nu' + 2t > 2p^r - 2$  and  $\nu'' = p^{r'-r} - 1$ .

**Proof.** Recall that the highest  $\mathcal{U}^0$ -weight in  $\tilde{Q}_r(\lambda)$  is  $2p^r - 2 - \lambda' + \lambda''p^r$  and the lowest one is  $-2p^r + 2 + \lambda' + \lambda''p^r$  if we extend the  $\mathcal{U}_{r,r'}$ -module  $\tilde{Q}_r(\lambda)$  to a  $\tilde{\mathcal{U}}_r$ -module. Hence  $v$  has the  $\mathcal{U}^0$ -weight space decomposition

$$v = v_{-1} + v_0 + v_1,$$

where  $v_i \in \tilde{Q}_r(\lambda)_{\nu+ip^{r'}}$ . Since  $v$  generates  $\tilde{Q}_r(\lambda)$ ,  $v$  does not lie in  $\text{rad}_{\mathcal{U}_{r,r'}}\tilde{Q}_r(\lambda) = \text{rad}_{\tilde{\mathcal{U}}_r}\tilde{Q}_r(\lambda)$ . Note that  $\tilde{Q}_r(\lambda)/\text{rad}_{\tilde{\mathcal{U}}_r}\tilde{Q}_r(\lambda) \cong \tilde{L}_r(\lambda)$  and that any  $\mathcal{U}^0$ -weight  $\gamma$  of  $\tilde{L}_r(\lambda)$  satisfies  $-\lambda' + \lambda''p^r \leq \gamma \leq \lambda' + \lambda''p^r$ . Since  $\nu + p^{r'}$  is not a  $\mathcal{U}^0$ -weight of  $\tilde{L}_r(\lambda)$ , we have  $v_1 \in \text{rad}_{\tilde{\mathcal{U}}_r}\tilde{Q}_r(\lambda)$ . Therefore, we see that  $v_{-1}$  or  $v_0$  does not lie in  $\text{rad}_{\tilde{\mathcal{U}}_r}\tilde{Q}_r(\lambda)$ .

Suppose that  $v_{-1} \notin \text{rad}_{\tilde{\mathcal{U}}_r}\tilde{Q}_r(\lambda)$ . Then since  $-\lambda' + \lambda''p^r \leq \nu - p^{r'} \leq \lambda' + \lambda''p^r$ , we must have  $\lambda'' = 0$  and  $\nu - p^{r'} \geq -\lambda'$ . Therefore, since

$$\nu \geq p^{r'} - \lambda' > 2(p^r - 1) - \lambda' = 2(p^r - 1) - \lambda' + \lambda''p^r,$$

we have  $v_0 = v_1 = 0$  and  $v = v_{-1}$ . Note that the inequality  $\nu \geq p^{r'} - \lambda'$  also implies  $\nu'' = p^{r'-r} - 1$ . Since  $v \notin \text{rad}_{\tilde{\mathcal{U}}_r}\tilde{Q}_r(\lambda)$ , there exists an element  $z \in \tilde{\mathcal{U}}_r$  such that  $zv$  is a highest  $\mathcal{U}^0$ -weight vector in  $\tilde{Q}_r(\lambda)$  (with  $\mathcal{U}^0$ -weight  $2p^r - 2 - \lambda' + \lambda''p^r$ ). Moreover, since  $v$  has  $\mathcal{U}^0$ -weight  $\nu - p^{r'}$ , the element  $z$  can be taken as a linear combination of some elements of the form

$$Y^{(m_1)}hX^{(m_2)}$$

with  $h \in \mathcal{U}^0$ ,  $0 \leq m_1, m_2 \leq p^r - 1$  and

$$m_2 - m_1 = (2p^r - 2 - \lambda' + \lambda''p^r - (\nu - p^{r'}))/2 = 3p^r/2 - 1 - (\lambda' + \nu')/2.$$

This implies that  $zv$  is proportional to  $X^{(3p^r/2-1-(\lambda'+\nu')/2)}v$  and that  $t = 3p^r/2 - 1 - (\lambda' + \nu')/2$ . In this case we also see that  $\nu' + 2t = 3p^r - 2 - \lambda' > 2p^r - 2$ .

Finally suppose that  $v_0 \notin \text{rad}_{\tilde{\mathcal{U}}_r}\tilde{Q}_r(\lambda)$ . Then  $-\lambda' + \lambda''p^r \leq \nu \leq \lambda' + \lambda''p^r$ . Since  $\nu - p^{r'} < -2(p^r - 1) + \lambda' + \lambda''p^r$  and  $\nu + p^{r'} > 2(p^r - 1) - \lambda' + \lambda''p^r$ , we must have  $v_1 = v_{-1} = 0$  and  $v = v_0$ . Moreover,  $\lambda''$  must be equal to  $\nu''$  or  $\nu'' + 1$  since  $-\lambda' \leq \nu' + (\nu'' - \lambda'')p^r \leq \lambda'$ . As in the last paragraph, we see that  $\lambda'' = \nu''$  if and only if

$$t = (2(p^r - 1) - \lambda' + \lambda''p^r - \nu)/2 = p^r - 1 - (\lambda' + \nu')/2,$$

and in this case we have  $\nu' + 2t = 2p^r - 2 - \lambda' \leq 2p^r - 2$ . Similarly, we see that  $\lambda'' = \nu'' + 1$  if and only if

$$t = (2(p^r - 1) - \lambda' + \lambda''p^r - \nu)/2 = 3p^r/2 - 1 - (\lambda' + \nu')/2,$$

and in this case we have  $\nu'' \neq p^{r'-r} - 1$  and  $\nu' + 2t = 3p^r - 2 - \lambda' > 2p^r - 2$ . Therefore, the proposition is proved. ■

#### 4. Primitive idempotents in $\mathcal{U}_1$

We shall construct primitive idempotents in  $\mathcal{U}_1$ , following Seligman's method [Sel03].

For  $a \in \mathbb{Z}$ , set

$$\mu_a = \binom{H-a-1}{p-1} = \sum_{i=0}^{p-1} \binom{-a-1}{p-1-i} \binom{H}{i} \in \mathcal{U}_1^0.$$

Then  $\mu_a = \mu_b$  if and only if  $a \equiv b \pmod{p}$ . Therefore, the integer  $a$  in the symbol  $\mu_a$  can be regarded as an element of  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ . Then we obtain by Wilson's theorem that

$$\begin{aligned} \mu_a &= \frac{(H-a-1)(H-a-2)\cdots(H-a-p+1)}{(p-1)!} \\ &= -(H-a-1)(H-a-2)\cdots(H-a-p+1) \\ &= - \prod_{\gamma \in \mathbb{F}_p - \{a\}} (H-\gamma). \end{aligned}$$

It is easy to check the following facts (see [GK15, §4]).

**Proposition 4.1.** (i) For  $a \in \mathbb{Z}$ , we have  $H\mu_a = a\mu_a$ . Therefore,  $\mu_a$  is a  $\mathcal{U}_1^0$ -weight vector of weight  $a$  in the  $\mathcal{U}_1^0$ -module  $\mathcal{U}_1^0$ .

(ii) The elements  $\mu_a$  with  $a \in \mathbb{F}_p$  are pairwise orthogonal primitive idempotents in  $\mathcal{U}_1^0$  whose sum is  $1 \in \mathcal{U}_1^0$ .

(iii)  $\mu_a X^{(m)} = X^{(m)} \mu_{a-2m}$  and  $\mu_a Y^{(m)} = Y^{(m)} \mu_{a+2m}$  for  $a \in \mathbb{Z}$  and  $m \in \mathbb{Z}_{\geq 0}$ .

To construct primitive idempotents in  $\mathcal{U}_1$ , we need some lemmas.

**Lemma 4.2.** For  $m \in \mathbb{Z}_{>0}$  and  $a \in \mathbb{F}_p$ , we have

$$\mu_a Y^m X^m = \prod_{i=0}^{m-1} (\mu_a Y X - i(i+a+1))$$

and

$$\mu_a X^m Y^m = \prod_{i=0}^{m-1} (\mu_a X Y - i(i-a+1))$$

in  $\mathcal{U}_1$ .

**Proof.** It is clear when  $m = 1$ , and we may assume  $m \geq 2$ . Then we have

$$\begin{aligned} & \mu_a Y^m X^m \\ &= \mu_a Y^{m-1} Y X^{m-1} X \\ &= \mu_a Y^{m-1} (X^{m-1} Y + (m-1) X^{m-2} (-H - m + 2)) X \\ &= \mu_a Y^{m-1} X^{m-1} Y X + (m-1) \mu_a Y^{m-1} X^{m-1} (-H - m) \\ &= \mu_a Y^{m-1} X^{m-1} Y X + (m-1) \mu_a (-H - m) Y^{m-1} X^{m-1} \\ &= \mu_a Y^{m-1} X^{m-1} Y X + (m-1) (-a - m) \mu_a Y^{m-1} X^{m-1} \\ &= \mu_a Y^{m-1} X^{m-1} (\mu_a Y X - (m-1)(a+m)). \end{aligned}$$

By induction on  $m$ , this is equal to

$$\prod_{i=0}^{m-2} (\mu_a Y X - i(i+a+1)) (\mu_a Y X - (m-1)(a+m)) = \prod_{i=0}^{m-1} (\mu_a Y X - i(i+a+1)).$$

Similarly we can check that  $\mu_a X^m Y^m = \prod_{i=0}^{m-1} (\mu_a X Y - i(i-a+1))$ . ■

If  $p$  is odd, set  $\mathcal{S} = \{i \in \mathbb{F}_p \mid i = 0, 1, \dots, (p-1)/2\}$ . Then we define polynomials  $\varphi_{a,m}(x), \psi(x) \in \mathbb{F}_p[x]$  for  $a \in \mathbb{F}_p$  and  $m \in \mathbb{Z}_{\geq 0}$  as

$$\varphi_{a,0}(x) = 1,$$

$$\varphi_{a,n}(x) = \prod_{i=0}^{n-1} (x - i(i+a+1))$$

if  $n > 0$ , and

$$\psi(x) = \prod_{i \in \mathbb{F}_p} (x - i^2) = x \prod_{i \in \mathcal{S} - \{0\}} (x - i^2)^2.$$

**Lemma 4.3.** *Suppose that  $p$  is odd and let  $a \in \mathbb{F}_p$ . Then the following holds.*

- (i)  $\psi(x + ((a+1)/2)^2) = \varphi_{a,p}(x)$ .
- (ii)  $\varphi_{a,p}(\mu_a Y X) = \varphi_{-a,p}(\mu_a X Y) = 0$ .

**Proof.** (i) Set  $y = x + ((a+1)/2)^2$ . We have

$$\begin{aligned} \varphi_{a,p}(x) &= \prod_{i \in \mathbb{F}_p} (x - i(i+a+1)) \\ &= \prod_{i \in \mathbb{F}_p} (x + ((a+1)/2)^2 - (i + (a+1)/2)^2) \\ &= \prod_{i \in \mathbb{F}_p} (y - (i + (a+1)/2)^2) \\ &= \prod_{i \in \mathbb{F}_p} (y - i^2) \\ &= \psi(y). \end{aligned}$$

(ii) It is immediate from Lemma 4.2 since  $X^p = Y^p = 0$  in  $\mathcal{U}$ . ■

If  $p$  is odd, we define  $(p+1)/2$  polynomials  $\psi_0(x)$  and  $\psi_j(x)$  with  $j \in \mathcal{S} - \{0\}$  as

$$\psi_0(x) = \prod_{i \in \mathbb{F}_p^\times} (x - i^2) = \prod_{i \in \mathcal{S} - \{0\}} (x - i^2)^2$$

and

$$\psi_j(x) = 2x(x + j^2) \prod_{i \in \mathbb{F}_p^\times - \{j, p-j\}} (x - i^2) = 2x(x + j^2) \prod_{i \in \mathcal{S} - \{0, j\}} (x - i^2)^2.$$

**Lemma 4.4.** *Suppose that  $p$  is odd. The following holds in  $\mathbb{F}_p[x]$  ( $\delta_{m,n}$  denotes Kronecker's symbol).*

- (i)  $\sum_{i \in \mathcal{S}} \psi_i(x) = 1$ .
- (ii)  $\psi_m(x)\psi_n(x) \equiv \delta_{m,n}\psi_m(x) \pmod{(\psi(x))}$  for  $m, n \in \mathcal{S}$ .

**Proof.** (i) Set  $\Phi(x) = \sum_{i \in \mathcal{S}} \psi_i(x) - 1$ . Then we have

$$\frac{d\psi_0}{dx} = \sum_{t \in \mathcal{S} - \{0\}} 2(x - t^2) \prod_{i \in \mathcal{S} - \{0, t\}} (x - i^2)^2$$

and

$$\frac{d\psi_j}{dx} = 2(2x + j^2) \prod_{i \in \mathcal{S} - \{0, j\}} (x - i^2)^2 + 2x(x + j^2) \sum_{t \in \mathcal{S} - \{0, j\}} 2(x - t^2) \prod_{i \in \mathcal{S} - \{0, j, t\}} (x - i^2)^2$$

for  $j \in \mathcal{S} - \{0\}$ . Suppose that  $\Phi(x) \neq 0$  in  $\mathbb{F}_p[x]$ . If  $s \in \mathcal{S} - \{0\}$  we have

$$\begin{aligned} \Phi(s^2) &= \sum_{i \in \mathcal{S}} \psi_i(s^2) - 1 \\ &= \psi_s(s^2) - 1 \\ &= 2s^2(s^2 + s^2) \prod_{i \in \mathbb{F}_p^\times - \{s, p-s\}} (s^2 - i^2) - 1 \\ &= 4s^4 \prod_{i \in \mathbb{F}_p^\times - \{s, p-s\}} (s + i)(s - i) - 1 \\ &= 4s^4 \left( \prod_{i \in \mathbb{F}_p^\times - \{s, p-s\}} (s + i) \right) \left( \prod_{j \in \mathbb{F}_p^\times - \{s, p-s\}} (s - j) \right) - 1 \\ &= 4s^4 \left( \frac{1}{2s^2} \prod_{i \in \mathbb{F}_p - \{p-s\}} (s + i) \right) \left( \frac{1}{2s^2} \prod_{j \in \mathbb{F}_p - \{s\}} (s - j) \right) - 1 \\ &= 4s^4 \left( \frac{1}{2s^2} \prod_{i \in \mathbb{F}_p^\times} i \right) \left( \frac{1}{2s^2} \prod_{j \in \mathbb{F}_p^\times} j \right) - 1 \\ &= 4s^4 \cdot \left( -\frac{1}{2s^2} \right)^2 - 1 \\ &= 0, \end{aligned}$$

whereas

$$\Phi(0) = \sum_{i \in \mathcal{S}} \psi_i(0) - 1 = \psi_0(0) - 1 = \prod_{i \in \mathbb{F}_p^\times} (-i^2) - 1 = 1 - 1 = 0.$$

Therefore,  $\Phi(x)$  contains each linear polynomial  $x - s^2$  with  $s \in \mathcal{S}$  as a factor.

We would like to claim that  $\left. \frac{d\psi_j}{dx} \right|_{x=s^2} = 0$  if  $j \in \mathcal{S}$  and  $s \in \mathcal{S} - \{0\}$ . Clearly the equality holds if  $j = 0$  or if  $j \neq 0$  and  $s \neq j$ . So we only have to show that  $\left. \frac{d\psi_j}{dx} \right|_{x=j^2} = 0$  for  $j \in \mathcal{S} - \{0\}$ . If  $j \in \mathcal{S} - \{0\}$ , we have

$$\begin{aligned} \left. \frac{d\psi_j}{dx} \right|_{x=j^2} &= 6j^2 \prod_{i \in \mathcal{S} - \{0, j\}} (j^2 - i^2)^2 + 4j^4 \sum_{t \in \mathcal{S} - \{0, j\}} 2(j^2 - t^2) \prod_{i \in \mathcal{S} - \{0, j, t\}} (j^2 - i^2)^2 \\ &= \left( 6j^2 + 4j^4 \sum_{t \in \mathcal{S} - \{0, j\}} \frac{2}{j^2 - t^2} \right) \prod_{i \in \mathcal{S} - \{0, j\}} (j^2 - i^2)^2. \end{aligned}$$

But since

$$\begin{aligned} &\sum_{t \in \mathcal{S} - \{0, j\}} \frac{2}{j^2 - t^2} \\ &= \frac{1}{2} \sum_{t \in \mathbb{F}_p^\times - \{j, p-j\}} \frac{2}{j^2 - t^2} \\ &= \frac{1}{2j} \sum_{t \in \mathbb{F}_p^\times - \{j, p-j\}} \left( \frac{1}{j-t} + \frac{1}{j+t} \right) \\ &= \frac{1}{2j} \left( \sum_{t \in \mathbb{F}_p - \{j\}} \frac{1}{j-t} - \frac{1}{j} - \frac{1}{2j} + \sum_{t \in \mathbb{F}_p - \{p-j\}} \frac{1}{j+t} - \frac{1}{j} - \frac{1}{2j} \right) \\ &= \frac{1}{2j} \left( 0 - \frac{1}{j} - \frac{1}{2j} + 0 - \frac{1}{j} - \frac{1}{2j} \right) \\ &= -\frac{3}{2j^2}, \end{aligned}$$

we conclude that  $\left. \frac{d\psi_j}{dx} \right|_{x=j^2} = 0$ , and the claim follows. Therefore, we obtain

$\left. \frac{d\Phi}{dx} \right|_{x=s^2} = 0$  for  $s \in \mathcal{S} - \{0\}$  and the polynomial  $\Phi(x)$  has  $x \prod_{i \in \mathcal{S} - \{0\}} (x - i^2)^2$  as a factor. So the degree of the polynomial  $\Phi(x)$  is greater than  $p - 1$ , which is a contradiction. Therefore,  $\Phi(x)$  must be zero and (i) is proved.

(ii) By the definition of  $\psi_i(x)$ , clearly we have  $\psi_m(x)\psi_n(x) \in (\psi(x))$  for  $m \neq n$ . Combining this with (i) the result follows. ■

Set  $\mathcal{P} = \mathbb{F}_p \times \mathcal{S}$  if  $p$  is odd, and  $\mathcal{P} = \{(0, 1/2), (1, 0), (1, 1)\} \subset \mathbb{F}_2 \times (1/2)\mathbb{Z}$  if  $p = 2$ .

If  $p$  is odd, for a pair  $(a, j) \in \mathcal{P}$  we set

$$E(a, j) = \psi_j \left( \mu_a YX + ((a + 1)/2)^2 \right) \cdot \mu_a.$$

This element also can be written as  $E(a, j) = \psi_j \left( \mu_a XY + ((a - 1)/2)^2 \right) \cdot \mu_a$ . If  $p = 2$ , for each pair  $(a, j) \in \mathcal{P}$  we define  $E(a, j)$  as follows:

$$E(0, 1/2) = \mu_0, \quad E(1, 0) = \mu_1 YX = \mu_1 (XY + 1), \quad E(1, 1) = \mu_1 XY = \mu_1 (YX + 1).$$

Clearly all  $E(a, j)$  lie in  $\mathcal{A}_1$ .

**Proposition 4.5.** *For a fixed element  $a \in \mathbb{F}_p$ , the elements  $E(a, j)$  with  $(a, j) \in \mathcal{P}$  are pairwise orthogonal primitive idempotents in  $\mathcal{U}_1$  whose sum is  $\mu_a$ . Thus, all the elements  $E(a, j)$  with  $(a, j) \in \mathcal{P}$  are pairwise orthogonal primitive idempotents in  $\mathcal{U}_1$  whose sum is 1.*

**Proof.** If  $p = 2$ , then the claim but primitivity is clear. Consider the case when  $p$  is odd. Then note that  $\mathcal{P} = \mathbb{F}_p \times \mathcal{S}$ . For a fixed  $a \in \mathbb{F}_p$ , we have by Lemma 4.4 (i) that

$$\sum_{j \in \mathcal{S}} E(a, j) = \left( \sum_{j \in \mathcal{S}} \psi_j \left( \mu_a YX + ((a + 1)/2)^2 \right) \right) \cdot \mu_a = \mu_a.$$

On the other hand, it follows from Lemma 4.4 (ii) and Lemma 4.3 (i) and (ii) that the elements  $E(a, j)$  with  $j \in \mathcal{S}$  are pairwise orthogonal idempotents in  $\mathcal{U}_1$ . Moreover, we also see that

$$\sum_{a \in \mathbb{F}_p} \sum_{j \in \mathcal{S}} E(a, j) = \sum_{a \in \mathbb{F}_p} \mu_a = 1$$

and

$$E(a, j)E(a', j') = \delta_{(a, j), (a', j')} E(a, j)$$

since  $\mu_a \mu_{a'} = \delta_{a, a'} \mu_a$  by Proposition 4.1 (ii).

It remains to show that each idempotent  $E(a, j)$  is primitive when  $p$  is arbitrary. Recall that the non-isomorphic simple  $\mathcal{U}_1$ -modules are  $L(\lambda)$  with  $0 \leq \lambda \leq p - 1$  and that  $\dim_k L(\lambda) = \lambda + 1$ . Hence the number of summands in a decomposition of  $1 \in \mathcal{U}_1$  into pairwise orthogonal primitive idempotents must be

$$1 + 2 + \cdots + p = \frac{p(p + 1)}{2}.$$

On the other hand, the number of all  $E(a, j)$  with  $(a, j) \in \mathcal{P}$  is also equal to  $p(p + 1)/2$ . Therefore, each idempotent  $E(a, j)$  must be primitive (see [CR62, (54.5) Theorem]). ■

If  $p$  is odd and  $(a, j) \in \mathcal{P}$ , we define  $n(a, j)$  as the largest non-negative integer  $n$  satisfying  $\varphi_{a, n}(x) \mid \psi_j \left( x + ((a + 1)/2)^2 \right)$ . (Recall that  $\varphi_{a, 0}(x) = 1$ . Thus  $n(a, j) = 0$  if  $x \nmid \psi_j \left( x + ((a + 1)/2)^2 \right)$ .) If  $p = 2$ , set

$$n(0, 1/2) = 0, \quad n(1, 0) = 1, \quad n(1, 1) = 0.$$

With respect to each pair  $(a, j) \in \mathcal{P}$ , we consider the following four cases, regarding  $a$  and  $j$  as the corresponding integers with  $0 \leq a \leq p - 1$  and  $0 \leq j \leq (p - 1)/2$  if  $p$  is odd:

- (A)  $a$  is even and  $(p - a + 1)/2 \leq j \leq (p - 1)/2$  if  $p$  is odd
- (B)  $a$  is even and  $0 \leq j \leq (p - a - 1)/2$  if  $p$  is odd, or  $(a, j) = (0, 1/2)$  if  $p = 2$
- (C)  $a$  is odd and  $0 \leq j \leq (a - 1)/2$  if  $p$  is odd, or  $(a, j) = (1, 0)$  if  $p = 2$
- (D)  $a$  is odd and  $(a + 1)/2 \leq j \leq (p - 1)/2$  if  $p$  is odd, or  $(a, j) = (1, 1)$  if  $p = 2$

**Lemma 4.6.** *Let  $(a, j) \in \mathcal{P}$ . The following holds.*

- (i) *If  $(a, j)$  satisfies (A), then  $n(a, j) = (p - a - 1)/2 + j$ .*
- (ii) *If  $(a, j)$  satisfies (B), then  $n(a, j) = (p - a - 1)/2 - j$ .*
- (iii) *If  $(a, j)$  satisfies (C), then  $n(a, j) = (2p - a - 1)/2 - j$ .*
- (iv) *If  $(a, j)$  satisfies (D), then  $n(a, j) = j - (a + 1)/2$ .*

*On the right-hand side of each equality,  $a$  and  $j$  are regarded as the corresponding integers with  $0 \leq a \leq p - 1$  and  $0 \leq j \leq (p - 1)/2$  except for  $j$  when  $p = 2$ .*

**Proof.** It is clear if  $p = 2$ , so we may assume that  $p$  is odd. We have

$$\prod_{i \in \mathbb{F}_p} (x - i(i + a + 1)) = \left(x + ((a + 1)/2)^2\right) \prod_{m \in \mathcal{S} - \{0\}} \left(x + ((a + 1)/2)^2 - m^2\right)^2$$

since  $\varphi_{a,p}(x) = \psi\left(x + ((a + 1)/2)^2\right)$ . Hence each factor  $x - i(i + a + 1)$  with  $i \in \mathbb{F}_p$  on the left-hand side has the form  $x + ((a + 1)/2)^2 - t^2$  with  $t \in \mathcal{S}$ . Since

$$\begin{aligned} \psi_j\left(x + ((a + 1)/2)^2\right) &= 2\left(x + ((a + 1)/2)^2\right)\left(x + ((a + 1)/2)^2 + j^2\right) \\ &\quad \times \prod_{m \in \mathcal{S} - \{0, j\}} \left(x + ((a + 1)/2)^2 - m^2\right)^2 \end{aligned}$$

if  $j \neq 0$ , whereas

$$\psi_j\left(x + ((a + 1)/2)^2\right) = \prod_{m \in \mathcal{S} - \{0\}} \left(x + ((a + 1)/2)^2 - m^2\right)^2$$

if  $j = 0$ , it is only  $x + ((a + 1)/2)^2 - j^2$  among the linear polynomials  $x + ((a + 1)/2)^2 - t^2$  with  $t \in \mathcal{S}$  that does not appear as a factor of the polynomial  $\psi_j\left(x + ((a + 1)/2)^2\right)$ . Moreover, since

$$x - n(n + a + 1) \mid \psi_j\left(x + ((a + 1)/2)^2\right)$$

for any non-negative integer  $n$  with  $n < n(a, j)$  and since

$$x - n(a, j)(n(a, j) + a + 1) \nmid \psi_j\left(x + ((a + 1)/2)^2\right)$$

by the definition of  $n(a, j)$ , the factor  $x - n(a, j)(n(a, j) + a + 1)$  must be equal to  $x + ((a + 1)/2)^2 - j^2$ . Therefore, we see that  $n(a, j)$  is the smallest non-negative integer  $n$  satisfying  $-n(n + a + 1) = ((a + 1)/2)^2 - j^2$  in  $\mathbb{F}_p$ . Note that this implies  $(n(a, j) + (a + 1)/2)^2 = j^2$  in  $\mathbb{F}_p$  and hence  $n(a, j) = \pm j - (a + 1)/2$  in  $\mathbb{F}_p$ .

Suppose that the pair  $(a, j)$  satisfies the condition (A). Then we see that  $n(a, j) = (p - a - 1)/2 + j$  or  $(3p - a - 1)/2 - j$  since  $n(a, j) \equiv \pm j + (p - a - 1)/2 \pmod{p}$  and  $(p - a + 1)/2 \leq j \leq (p - 1)/2$ . By the minimality of  $n(a, j)$  we obtain  $n(a, j) = (p - a - 1)/2 + j$ .

Suppose that the pair  $(a, j)$  satisfies the condition (B). Then we see that  $n(a, j) = (p - a - 1)/2 - j$  or  $(p - a - 1)/2 + j$  since  $n(a, j) \equiv \pm j + (p - a - 1)/2 \pmod{p}$  and  $0 \leq j \leq (p - a - 1)/2$ . By the minimality of  $n(a, j)$  we obtain  $n(a, j) = (p - a - 1)/2 - j$ .

Suppose that the pair  $(a, j)$  satisfies the condition (C). Then we see that  $n(a, j) = (2p - a - 1)/2 - j$  or  $(2p - a - 1)/2 + j$  since  $n(a, j) \equiv \pm j - (a + 1)/2 \pmod{p}$  and  $0 \leq j \leq (a - 1)/2$ . By the minimality of  $n(a, j)$  we obtain  $n(a, j) = (2p - a - 1)/2 - j$ .

Suppose that the pair  $(a, j)$  satisfies the condition (D). Then we see that  $n(a, j) = j - (a + 1)/2$  or  $(2p - a - 1)/2 - j$  since  $n(a, j) \equiv \pm j - (a + 1)/2 \pmod{p}$  and  $(a + 1)/2 \leq j \leq (p - 1)/2$ . By the minimality of  $n(a, j)$  we obtain  $n(a, j) = j - (a + 1)/2$ .  $\blacksquare$

For a pair  $(a, j) \in \mathcal{P}$ , we set  $\tilde{n}(a, j) = n(-a, j)$  if  $p$  is odd, and

$$\tilde{n}(0, 1/2) = 0, \quad \tilde{n}(1, 0) = 0, \quad \tilde{n}(1, 1) = 1$$

if  $p = 2$ .

**Lemma 4.7.** *Let  $(a, j) \in \mathcal{P}$ . The following holds.*

- (i) *If  $(a, j)$  satisfies (A), then  $\tilde{n}(a, j) = (-p + a - 1)/2 + j$ .*
- (ii) *If  $(a, j)$  satisfies (B), then  $\tilde{n}(a, j) = (p + a - 1)/2 - j$ .*
- (iii) *If  $(a, j)$  satisfies (C), then  $\tilde{n}(a, j) = (a - 1)/2 - j$ .*
- (iv) *If  $(a, j)$  satisfies (D), then  $\tilde{n}(a, j) = j + (a - 1)/2$ .*

*On the right-hand side of each equality,  $a$  and  $j$  are regarded as the corresponding integers with  $0 \leq a \leq p - 1$  and  $0 \leq j \leq (p - 1)/2$  except for  $j$  when  $p = 2$ .*

**Proof.** It is clear if  $p = 2$ , so we may assume that  $p$  is odd. If  $a = 0$ , the lemma holds by Lemma 4.6 (ii) since each  $(0, j) \in \mathcal{P}$  satisfies (B). So we may assume  $a \neq 0$ . Then the element  $-a \in \mathbb{F}_p$  corresponds to  $p - a$  in the set of integers  $\{0, 1, \dots, p - 1\}$ . Set  $a' = p - a$ .

Suppose that the pair  $(a, j)$  satisfies the condition (A). Then  $(a', j)$  satisfies (D) and so we have  $n(-a, j) = n(a', j) = j - (p - a + 1)/2$  by Lemma 4.6 (iv).

Suppose that the pair  $(a, j)$  satisfies the condition (B). Then  $(a', j)$  satisfies (C) and so we have  $n(-a, j) = n(a', j) = (p + a - 1)/2 - j$  by Lemma 4.6 (iii).

Suppose that the pair  $(a, j)$  satisfies the condition (C). Then  $(a', j)$  satisfies (B) and so we have  $n(-a, j) = n(a', j) = (a - 1)/2 - j$  by Lemma 4.6 (ii).

Suppose that the pair  $(a, j)$  satisfies the condition (D). Then  $(a', j)$  satisfies (A) and so we have  $n(-a, j) = n(a', j) = (a - 1)/2 + j$  by Lemma 4.6 (i). ■

**Lemma 4.8.** *Let  $(a, j) \in \mathcal{P}$ . Then the primitive idempotent  $E(a, j)$  can be written as*

$$E(a, j) = \mu_a \sum_{m=n(a,j)}^{p-1} c_m Y^m X^m = \mu_a \sum_{m=\tilde{n}(a,j)}^{p-1} \tilde{c}_m X^m Y^m$$

for some  $c_m, \tilde{c}_m \in \mathbb{F}_p$  with  $c_{n(a,j)} \neq 0$  and  $\tilde{c}_{\tilde{n}(a,j)} \neq 0$ .

**Proof.** It is clear when  $p = 2$ , so we may assume that  $p$  is odd. By the definition of  $n(a, j)$  we can write

$$\psi_j\left(x + \left((a + 1)/2\right)^2\right) = \tau_j\left(x + \left((a + 1)/2\right)^2\right) \cdot \varphi_{a,n(a,j)}(x) \tag{*}$$

for some  $\tau_j(x) \in \mathbb{F}_p[x]$ . Then

$$\begin{aligned} E(a, j) &= \psi_j\left(\mu_a Y X + \left((a + 1)/2\right)^2\right) \cdot \mu_a \\ &= \tau_j\left(\mu_a Y X + \left((a + 1)/2\right)^2\right) \cdot \varphi_{a,n(a,j)}(\mu_a Y X) \cdot \mu_a \\ &= \mu_a Y^{n(a,j)} X^{n(a,j)} \cdot \tau_j\left(\mu_a Y X + \left((a + 1)/2\right)^2\right). \end{aligned}$$

Since

$$\begin{aligned} &\mu_a Y^{n(a,j)} X^{n(a,j)} \cdot \mu_a Y X \\ &= \mu_a Y^{n(a,j)+1} X^{n(a,j)+1} + n(a, j)(n(a, j) + a + 1)\mu_a Y^{n(a,j)} X^{n(a,j)}, \end{aligned}$$

we see that  $E(a, j)$  can be written as  $E(a, j) = \mu_a \sum_{m=n(a,j)}^{p-1} c_m Y^m X^m$  for some  $c_m \in \mathbb{F}_p$  with  $n(a, j) \leq m \leq p - 1$ . Note that  $\tau_j\left(x + \left((a + 1)/2\right)^2\right)$  is a product of some linear polynomials, but  $x - n(a, j)(n(a, j) + a + 1)$  does not appear as a factor of it. Thus we conclude that  $c_{n(a,j)} \neq 0$ , and the first equality in the lemma is proved.

Similarly, we obtain

$$E(a, j) = \mu_a X^{n(-a,j)} Y^{n(-a,j)} \cdot \tau_j\left(\mu_a X Y + \left((a - 1)/2\right)^2\right),$$

using the equality (\*) where  $a$  is replaced by  $-a$ . Then a similar argument in the last paragraph shows the second equality in the lemma. ■

The projective indecomposable  $\mathcal{U}_1$ -module generated by  $E(a, j)$  will be determined in Theorem 5.8 as the result for  $r = 1$  there.

**5. Primitive idempotents in  $\mathcal{U}_r$**

To construct primitive idempotents in  $\mathcal{U}_r$  for  $r \geq 2$  we need the  $k$ -linear map  $\text{Fr}' : \mathcal{U} \rightarrow \mathcal{U}$  which was introduced in Section 2. Recall that the linear map  $\text{Fr}'$  is defined by

$$Y^{(m)} \binom{H}{n} X^{(m')} \mapsto Y^{(mp)} \binom{H}{np} X^{(m'/p)}$$

for  $m, m', n \in \mathbb{Z}_{\geq 0}$ .

First we construct primitive idempotents in  $\mathcal{U}_r^0$ . For  $a \in \mathbb{Z}$ , define an element  $\mu_a^{(r)} \in \mathcal{U}_r^0$  as

$$\mu_a^{(r)} = \binom{H - a - 1}{p^r - 1}.$$

We have  $\mu_a^{(1)} = \mu_a$ , and  $\mu_a^{(r)} = \mu_b^{(r)}$  if and only if  $a \equiv b \pmod{p^r}$ . Then the following holds.

**Proposition 5.1.** (i) *Suppose that  $r \geq 2$ . Then for an integer  $a = a_0 + a'p$  with  $0 \leq a_0 \leq p - 1$  and  $a' \in \mathbb{Z}$ , we have  $\mu_a^{(r)} = \mu_{a_0} \text{Fr}'(\mu_{a'}^{(r-1)})$ . In particular,  $\mu_a^{(r)}$  is a  $\mathcal{U}_r^0$ -weight vector of  $\mathcal{U}_r^0$ -weight  $a$ .*

(ii) *The elements  $\mu_a^{(r)}$  with  $a \in \mathbb{Z}/p^r\mathbb{Z}$  are pairwise orthogonal primitive idempotents in  $\mathcal{U}_r^0$  whose sum is  $1 \in \mathcal{U}_r^0$ .*

(iii)  *$\mu_a^{(r)} X^{(m)} = X^{(m)} \mu_{a-2m}^{(r)}$  and  $\mu_a^{(r)} Y^{(m)} = Y^{(m)} \mu_{a+2m}^{(r)}$  for  $a \in \mathbb{Z}$  and  $m \in \mathbb{Z}_{\geq 0}$ .*

For details, see 4.7 and 4.8 in [GK15] if  $p$  is odd, but the proposition also holds for  $p = 2$ .

If a pair  $(a, j) \in \mathcal{P}$  satisfies (A) or (C), set  $s(a, j) = (p - a + 1)/2$  if  $p$  is odd and  $a$  is even,  $s(a, j) = (p - a)/2$  if  $p$  is odd and  $a$  is odd, and  $s(a, j) = 1$  if  $p = 2$ , regarding  $a$  as the corresponding integer with  $0 \leq a \leq p - 1$ .

The following lemma will be used later.

**Lemma 5.2.** (i) *Let  $a, b \in \mathbb{Z}$  with  $0 \leq a \leq b \leq p - 1$ . Then*

$$\mu_a \text{Fr}'(z_1) \text{Fr}'(z_2) X^b = \mu_a \text{Fr}'(z_1 z_2) X^b$$

for any  $z_1, z_2 \in \mathcal{U}$ .

(ii) *Suppose that a pair  $(a, j) \in \mathcal{P}$  satisfies (A) or (C). Let  $m, n \in \mathbb{Z}_{\geq 0}$  with  $n(a, j) \leq m \leq p - 1$ . Then  $X^{(np)}$  and  $Y^{(np)}$  commute with  $\mu_a Y^m X^{m-s(a,j)}$ , whereas*

$$\mu_a Y^m X^{m-s(a,j)} \binom{H}{np} = \left( \binom{H}{np} + \binom{H}{(n-1)p} \right) \mu_a Y^m X^{m-s(a,j)}$$

if we define  $\binom{H}{t} = 0$  for  $t < 0$ .

**Proof.** (i) Without loss of generality we may assume that  $z_j = Y^{(m_j)} \binom{H}{n_j} X^{(m'_j)}$  with  $m_j, m'_j, n_j \in \mathbb{Z}_{\geq 0}$  and  $j \in \{1, 2\}$ . For simplicity we set  $m = m_2$ ,  $m' = m'_1$ ,  $\mathbf{Y} = Y^{(m_1)}$ ,  $\mathbf{X} = X^{(m'_2)}$ ,  $\mathbf{H}_1 = \binom{H}{n_1}$  and  $\mathbf{H}_2 = \binom{H}{n_2}$ . Then we can write  $z_1 = \mathbf{Y}\mathbf{H}_1 X^{(m')}$  and  $z_2 = Y^{(m)}\mathbf{H}_2\mathbf{X}$ . For each  $l \in \mathbb{Z}_{\geq 0}$  there exist  $\mathbf{H}_{1,l}, \mathbf{H}_{2,l} \in \mathcal{U}^0$  such that  $\mathbf{H}_1 Y^{(l)} = Y^{(l)}\mathbf{H}_{1,l}$  and  $X^{(l)}\mathbf{H}_2 = \mathbf{H}_{2,l}X^{(l)}$ . Then we have

$$\begin{aligned} & \mu_a \text{Fr}'(z_1 z_2) X^b \\ &= \mu_a \text{Fr}'(\mathbf{Y}\mathbf{H}_1 X^{(m')} Y^{(m)} \mathbf{H}_2 \mathbf{X}) X^b \\ &= \mu_a \text{Fr}'\left(\mathbf{Y}\mathbf{H}_1 \sum_{i=0}^{\min(m, m')} Y^{(m-i)} \binom{H-m-m'+2i}{i} X^{(m'-i)} \mathbf{H}_2 \mathbf{X}\right) X^b \\ &= \sum_{i=0}^{\min(m, m')} \mu_a \text{Fr}'\left(\mathbf{Y} Y^{(m-i)} \mathbf{H}_{1, m-i} \binom{H-m-m'+2i}{i} \mathbf{H}_{2, m'-i} X^{(m'-i)} \mathbf{X}\right) X^b. \end{aligned}$$

On the other hand, we have

$$\begin{aligned} & \mu_a \text{Fr}'(z_1) \text{Fr}'(z_2) X^b \\ &= \mu_a \text{Fr}'^-(\mathbf{Y}) \text{Fr}'^0(\mathbf{H}_1) \text{Fr}'^+(X^{(m')}) \text{Fr}'^-(Y^{(m)}) \text{Fr}'^0(\mathbf{H}_2) \text{Fr}'^+(\mathbf{X}) X^b \\ &= \mu_a \text{Fr}'^-(\mathbf{Y}) \text{Fr}'^0(\mathbf{H}_1) X^{(m'p)} Y^{(mp)} \text{Fr}'^0(\mathbf{H}_2) \text{Fr}'^+(\mathbf{X}) X^b \\ &= \sum_{i=0}^{\min(mp, m'p)} \text{Fr}'^-(\mathbf{Y}) \text{Fr}'^0(\mathbf{H}_1) \cdot \mu_a Y^{(mp-i)} \binom{H-(m+m')p+2i}{i} \\ & \quad \times X^{(m'p-i)} \text{Fr}'^0(\mathbf{H}_2) \text{Fr}'^+(\mathbf{X}) X^b. \end{aligned}$$

In this sum we consider the  $i$ -th summand. Choose a unique integer  $i'$  satisfying  $i \equiv i' \pmod{p}$  and  $0 \leq i' \leq p-1$ . Then we can write  $i = i' + i''p$  for some  $i'' \in \mathbb{Z}_{\geq 0}$ . Suppose that  $i' \neq 0$ . We have  $\mu_a Y^{(mp-i)} \binom{H-(m+m')p+2i}{i}$

$$\begin{aligned} &= \mu_a \binom{H+(m-m')p}{i} Y^{(mp-i)} \\ &= \mu_a \sum_{l=0}^i \binom{(m-m')p}{l} \binom{H}{i-l} Y^{(mp-i)} \\ &= \mu_a \sum_{l=0}^{i''} \binom{(m-m')p}{lp} \binom{H}{i-lp} Y^{(mp-i)} \\ &= \mu_a \sum_{l=0}^{i''} \binom{(m-m')p}{lp} \binom{H}{i'} \binom{H}{(i''-l)p} Y^{(mp-i)} \\ &= \mu_a \sum_{l=0}^{i''} \binom{(m-m')p}{lp} \binom{a}{i'} \binom{H}{(i''-l)p} Y^{(mp-i)}. \end{aligned}$$

On the other hand, if we choose  $\mathbf{H}_3 \in \mathcal{U}^0$  such that  $X^{(m'p-i)} \text{Fr}'^0(\mathbf{H}_2) = \mathbf{H}_3 X^{(m'p-i)}$ ,

then

$$\begin{aligned} X^{(m'p-i)}\mathrm{Fr}'^0(\mathbf{H}_2)\mathrm{Fr}'^+(\mathbf{X})X^b &= \mathbf{H}_3X^{(m'p-i)}\mathrm{Fr}'^+(\mathbf{X})X^b \\ &= \mathbf{H}_3\mathrm{Fr}'^+(\mathbf{X})X^{(m'p-i)}X^b \\ &= b! \binom{(m' - i'')p + b - i'}{b} \mathbf{H}_3\mathrm{Fr}'^+(\mathbf{X})X^{(m'p-i+b)}. \end{aligned}$$

But either  $a < i'$  or  $b \geq i'$  holds since  $a \leq b$ , and so either  $\mu_a Y^{(mp-i)} \binom{H-(m+m')p+2i}{i}$  or  $X^{(m'p-i)}\mathrm{Fr}'^0(\mathbf{H}_2)\mathrm{Fr}'^+(\mathbf{X})X^b$  must be zero. Therefore, the  $i$ -th summand in the equality of  $\mu_a \mathrm{Fr}'(z_1)\mathrm{Fr}'(z_2)X^b$  is zero if  $p$  does not divide  $i$  and we have

$$\begin{aligned} &\mu_a \mathrm{Fr}'(z_1)\mathrm{Fr}'(z_2)X^b \\ &= \sum_{i=0}^{\min(mp, m'p)} \mathrm{Fr}'^-(\mathbf{Y})\mathrm{Fr}'^0(\mathbf{H}_1) \cdot \mu_a Y^{(mp-i)} \binom{H - (m + m')p + 2i}{i} \\ &\quad \times X^{(m'p-i)}\mathrm{Fr}'^0(\mathbf{H}_2)\mathrm{Fr}'^+(\mathbf{X})X^b \\ &= \sum_{i=0}^{\min(m, m')} \mathrm{Fr}'^-(\mathbf{Y})\mathrm{Fr}'^0(\mathbf{H}_1) \cdot \mu_a Y^{(mp-ip)} \binom{H - (m + m' - 2i)p}{ip} \\ &\quad \times X^{(m'p-ip)}\mathrm{Fr}'^0(\mathbf{H}_2)\mathrm{Fr}'^+(\mathbf{X})X^b. \end{aligned}$$

It is easy to see that

$$\binom{H - (m + m' - 2i)p}{ip} = \mathrm{Fr}'^0 \left( \binom{H - (m + m') + 2i}{i} \right)$$

by using Proposition 2.1 (v). Recall also that the restriction maps  $\mathrm{Fr}'^{\geq 0}, \mathrm{Fr}'^{\leq 0}, \mathrm{Fr}'^0, \mathrm{Fr}'^+$  and  $\mathrm{Fr}'^-$  are homomorphisms of  $k$ -algebras. Therefore, we obtain

$$\begin{aligned} &\mu_a \mathrm{Fr}'(z_1)\mathrm{Fr}'(z_2)X^b \\ &= \sum_{i=0}^{\min(m, m')} \mu_a \mathrm{Fr}'^-(\mathbf{Y})\mathrm{Fr}'^0(\mathbf{H}_1)\mathrm{Fr}'^-(Y^{(m-i)})\mathrm{Fr}'^0 \left( \binom{H - (m + m') + 2i}{i} \right) \\ &\quad \times \mathrm{Fr}'^+(X^{(m'-i)})\mathrm{Fr}'^0(\mathbf{H}_2)\mathrm{Fr}'^+(\mathbf{X})X^b \\ &= \sum_{i=0}^{\min(m, m')} \mu_a \mathrm{Fr}'^{\leq 0} \left( \mathbf{Y}\mathbf{H}_1 Y^{(m-i)} \binom{H - (m + m') + 2i}{i} \right) \mathrm{Fr}'^{\geq 0} (X^{(m'-i)}\mathbf{H}_2\mathbf{X})X^b \\ &= \sum_{i=0}^{\min(m, m')} \mu_a \mathrm{Fr}'^{\leq 0} \left( \mathbf{Y}Y^{(m-i)}\mathbf{H}_{1, m-i} \binom{H - (m + m') + 2i}{i} \right) \\ &\quad \times \mathrm{Fr}'^{\geq 0} (\mathbf{H}_{2, m'-i} X^{(m'-i)}\mathbf{X})X^b \\ &= \sum_{i=0}^{\min(m, m')} \mu_a \mathrm{Fr}'^-(\mathbf{Y}Y^{(m-i)})\mathrm{Fr}'^0 \left( \mathbf{H}_{1, m-i} \binom{H - (m + m') + 2i}{i} \right) \mathrm{Fr}'^0(\mathbf{H}_{2, m'-i}) \\ &\quad \times \mathrm{Fr}'^+(X^{(m'-i)}\mathbf{X})X^b \end{aligned}$$

$$\begin{aligned}
 &= \sum_{i=0}^{\min(m,m')} \mu_a \text{Fr}'^-(\mathbf{Y}Y^{(m-i)})\text{Fr}'^0 \left( \mathbf{H}_{1,m-i} \binom{H - (m + m') + 2i}{i} \mathbf{H}_{2,m'-i} \right) \\
 &\quad \times \text{Fr}'^+(X^{(m'-i)}\mathbf{X})X^b \\
 &= \sum_{i=0}^{\min(m,m')} \mu_a \text{Fr}' \left( \mathbf{Y}Y^{(m-i)} \mathbf{H}_{1,m-i} \binom{H - (m + m') + 2i}{i} \mathbf{H}_{2,m'-i} X^{(m'-i)}\mathbf{X} \right) X^b.
 \end{aligned}$$

The last sum is equal to  $\mu_a \text{Fr}'(z_1 z_2) X^b$ , and (i) is proved.

(ii) It is easy for  $p = 2$ , since  $\mu_a Y^m X^{m-s(a,j)} = \mu_1 Y$  in this situation. So we may assume that  $p$  is odd. Set  $s = s(a, j)$ . It is clear if  $n = 0$ , so we may assume that  $n > 0$ . We have

$$\begin{aligned}
 X^{(np)} \mu_a Y^m X^{m-s} &= \mu_a X^{(np)} Y^m X^{m-s} \\
 &= m! \mu_a \sum_{i=0}^m Y^{(m-i)} \binom{H - np - m + 2i}{i} X^{(np-i)} X^{m-s} \\
 &= m! \mu_a \sum_{i=0}^m \binom{H - np + m}{i} Y^{(m-i)} X^{(np-i)} X^{m-s} \\
 &= m! \mu_a \sum_{i=0}^m \binom{a - np + m}{i} Y^{(m-i)} X^{m-s} X^{(np-i)},
 \end{aligned}$$

where the last equality follows from  $i \leq p - 1$ . Consider a summand for  $i \neq 0$  of this sum. Since  $X^{m-s} X^{(np-i)} = (m-s)! \binom{m-s+np-i}{np-i} X^{(m-s+np-i)}$ , we must have  $i > m - s$  if  $X^{m-s} X^{(np-i)} \neq 0$ . On the other hand, we must have  $a + m - p \geq i$  if  $\binom{a-np+m}{i} \neq 0$  in  $\mathbb{F}_p$  since  $p \leq a + m \leq 2p - 2$ . But the inequalities  $i > m - s$  and  $a + m - p \geq i$  do not hold simultaneously since  $(a + m - p) - (m - s) = a + s - p$  is not positive. Therefore, each summand for  $i \neq 0$  must be zero and we obtain  $X^{(np)} \mu_a Y^m X^{m-s} = \mu_a Y^m X^{m-s} X^{(np)}$ .

In turn, we have

$$\mu_a Y^m X^{m-s} Y^{(np)} = \sum_{i=0}^{m-s} (m-s)! \mu_a Y^m Y^{(np-i)} \binom{H - np - m + s + 2i}{i} X^{(m-s-i)}.$$

However, on the right-hand side, only the summand for  $i = 0$  survives. Indeed, if  $m > s$ , we see that

$$Y^m Y^{(np-i)} = m! \binom{m-i+np}{m} Y^{(m-i+np)} = 0$$

for  $1 \leq i \leq m - s$ , since  $\binom{m-i+np}{m} = 0$  in  $\mathbb{F}_p$ . Therefore, we obtain

$$\begin{aligned}
 \mu_a Y^m X^{m-s} Y^{(np)} &= \mu_a Y^m Y^{(np)} X^{m-s} \\
 &= Y^{(np)} \mu_a Y^m X^{m-s}.
 \end{aligned}$$

Finally, observe that

$$\begin{aligned} \mu_a Y^m X^{m-s} \binom{H}{np} &= \mu_a \binom{H+2s}{np} Y^m X^{m-s} \\ &= \mu_a \sum_{l=0}^{np} \binom{2s}{l} \binom{H}{np-l} Y^m X^{m-s}. \end{aligned}$$

Since  $2s \leq p-1$ , we have

$$\begin{aligned} \mu_a \sum_{l=0}^{np} \binom{2s}{l} \binom{H}{np-l} &= \mu_a \sum_{l=0}^{p-1} \binom{2s}{l} \binom{H}{np-l} \\ &= \mu_a \left( \binom{H}{np} + \sum_{l=1}^{p-1} \binom{2s}{l} \binom{H}{p-l} \binom{H}{(n-1)p} \right) \\ &= \mu_a \left( \binom{H}{np} + \sum_{l=1}^{p-1} \binom{2s}{l} \binom{a}{p-l} \binom{H}{(n-1)p} \right). \end{aligned}$$

But it is easy to see that  $\sum_{l=1}^{p-1} \binom{2s}{l} \binom{a}{p-l} = 1$  in  $\mathbb{F}_p$ , and we obtain

$$\mu_a Y^m X^{m-s} \binom{H}{np} = \left( \binom{H}{np} + \binom{H}{(n-1)p} \right) \mu_a Y^m X^{m-s},$$

the proof is complete. ■

Now we shall construct primitive idempotents in  $\mathcal{U}_r$ . Suppose that  $r \geq 2$ . Recall from Lemma 4.8 that each primitive idempotent  $E(a, j)$  in  $\mathcal{U}_1$  can be written as

$$E(a, j) = \mu_a \sum_{m=n(a,j)}^{p-1} c_m Y^m X^m = \mu_a \sum_{m=\tilde{n}(a,j)}^{p-1} \tilde{c}_m X^m Y^m$$

for some  $c_m, \tilde{c}_m \in \mathbb{F}_p$  with  $c_{n(a,j)} \neq 0$  and  $\tilde{c}_{\tilde{n}(a,j)} \neq 0$ . For each  $z \in \mathcal{U}$ , using the above notation we define an element  $Z(z; (a, j)) \in \mathcal{U}$  as follows.

· If the pair  $(a, j)$  satisfies (A) or (C), then

$$Z(z; (a, j)) = \mu_a \sum_{m=n(a,j)}^{p-1} c_m Y^m X^{m-s(a,j)} \text{Fr}'(z) X^{s(a,j)}.$$

· If the pair  $(a, j)$  satisfies (B) or (D), then

$$Z(z; (a, j)) = \text{Fr}'(z) E(a, j).$$

**Lemma 5.3.** *For a pair  $(a, j) \in \mathcal{P}$  and a nonzero element  $z \in \mathcal{U}$ , there exists a nonzero element  $z' \in \mathcal{U}$  such that  $Z(z; (a, j)) = \text{Fr}'(z') E(a, j) = E(a, j) \text{Fr}'(z')$ . Moreover, if  $z \in \mathcal{A}$ , then  $Z(z; (a, j))$  also lies in  $\mathcal{A}$ .*

**Proof.** Since  $E(a, j) \in \mathcal{A}_1$ , the commutativity of  $\text{Fr}'(z')$  and  $E(a, j)$  follows immediately from Propositions 2.4 (i) and 2.5. So we have to show the first equality in the lemma. There is nothing to do if the pair  $(a, j)$  satisfies (B) or (D). So we may assume that  $(a, j)$  satisfies (A) or (C). Set  $s = s(a, j)$ . It is enough to show the first equality for  $z = Y^{(n_1)} \binom{H}{n_2} X^{(n_3)}$  with  $n_1, n_2, n_3 \in \mathbb{Z}_{\geq 0}$ . By Lemma 5.2 (ii) we have

$$\begin{aligned} & Z\left(Y^{(n_1)} \binom{H}{n_2} X^{(n_3)}; (a, j)\right) \\ &= \mu_a \sum_{m=n(a, j)}^{p-1} c_m Y^m X^{m-s} Y^{(n_1 p)} \binom{H}{n_2 p} X^{(n_3 p)} X^s \\ &= Y^{(n_1 p)} \left( \binom{H}{n_2 p} + \binom{H}{(n_2 - 1)p} \right) X^{(n_3 p)} \mu_a \sum_{m=n(a, j)}^{p-1} c_m Y^m X^m \\ &= \text{Fr}'\left(Y^{(n_1)} \left( \binom{H}{n_2} + \binom{H}{n_2 - 1} \right) X^{(n_3)}\right) E(a, j), \end{aligned}$$

as required. Moreover, if  $Y^{(n_1)} \binom{H}{n_2} X^{(n_3)}$  lies in  $\mathcal{A}$  (i.e.  $n_1 = n_3$ ), clearly  $Y^{(n_1)} \left( \binom{H}{n_2} + \binom{H}{n_2 - 1} \right) X^{(n_3)}$  and  $Z\left(Y^{(n_1)} \binom{H}{n_2} X^{(n_3)}; (a, j)\right)$  also lie in  $\mathcal{A}$ . ■

**Proposition 5.4.** (i) For  $z \in \mathcal{U}$  and  $(a, j) \in \mathcal{P}$ , we have  $E(a, j)Z(z; (a, j)) = Z(z; (a, j)) = Z(z; (a, j))E(a, j)$ .

(ii) For a pair  $(a, j) \in \mathcal{P}$ , the map  $Z(-; (a, j)) : \mathcal{U} \rightarrow \mathcal{U}$ ,  $z \mapsto Z(z; (a, j))$  induces an injective  $k$ -algebra homomorphism from  $\mathcal{U}$  to  $E(a, j)\mathcal{U}E(a, j)$ .

(iii) Let  $z_1, z_2 \in \mathcal{U}$  and  $(a_1, j_1), (a_2, j_2) \in \mathcal{P}$ . If  $(a_1, j_1) \neq (a_2, j_2)$ , then we have  $Z(z_1; (a_1, j_1))Z(z_2; (a_2, j_2)) = 0$ .

(iv) Let  $u$  be an element of the subalgebra of  $\mathcal{U}$  generated by  $X^{(p^i)}$  and  $Y^{(p^i)}$  with  $i \geq 1$ . Then, for  $z \in \mathcal{U}$ , we have  $uZ(z; (a, j)) = Z(\text{Fr}(u)z; (a, j))$ .

**Proof.** (i) There exists  $z' \in \mathcal{A}$  such that  $Z(z; (a, j)) = \text{Fr}'(z')E(a, j) = E(a, j)\text{Fr}'(z')$  by Lemma 5.3. Since  $E(a, j)$  is an idempotent, the claim follows.

(ii) By (i), clearly all  $Z(z; (a, j))$  lie in  $E(a, j)\mathcal{U}E(a, j)$ . The linearity of the map is also clear and the injectivity follows from Lemma 5.3 and Proposition 2.3. Note also that  $Z(1; (a, j)) = E(a, j)$ . So we only have to show that  $Z(z_1; (a, j))Z(z_2; (a, j)) = Z(z_1 z_2; (a, j))$  for all  $z_1, z_2 \in \mathcal{U}$ . Suppose that the pair

$(a, j)$  satisfies (B) or (D). Then

$$\begin{aligned}
Z(z_1; (a, j))Z(z_2; (a, j)) &= \text{Fr}'(z_1)E(a, j)\text{Fr}'(z_2)E(a, j) \\
&= \text{Fr}'(z_1)\text{Fr}'(z_2)E(a, j) \\
&= \sum_{m=\tilde{n}(a, j)}^{p-1} \tilde{c}_m \mu_a \text{Fr}'(z_1)\text{Fr}'(z_2)X^m Y^m \\
&= \sum_{m=\tilde{n}(a, j)}^{p-1} \tilde{c}_m \mu_a \text{Fr}'(z_1 z_2)X^m Y^m \quad (\text{by Lemma 5.2 (i)}) \\
&= \text{Fr}'(z_1 z_2) \sum_{m=\tilde{n}(a, j)}^{p-1} \tilde{c}_m \mu_a X^m Y^m \\
&= \text{Fr}'(z_1 z_2)E(a, j) \\
&= Z(z_1 z_2; (a, j)).
\end{aligned}$$

Next, suppose that the pair  $(a, j)$  satisfies (A) or (C). Set  $s = s(a, j)$ . Then

$$\begin{aligned}
&Z(z_1; (a, j))Z(z_2; (a, j)) \\
&= \left( \mu_a \sum_{m=n(a, j)}^{p-1} c_m Y^m X^{m-s} \text{Fr}'(z_1) X^s \right) \cdot \left( \mu_a \sum_{m'=n(a, j)}^{p-1} c_{m'} Y^{m'} X^{m'-s} \text{Fr}'(z_2) X^s \right) \\
&= \mu_a \sum_{m=n(a, j)}^{p-1} c_m Y^m X^{m-s} \cdot \mu_{a+2s} \text{Fr}'(z_1) \sum_{m'=n(a, j)}^{p-1} c_{m'} X^s Y^{m'} X^{m'-s} \text{Fr}'(z_2) X^s \\
&= \mu_a \sum_{m=n(a, j)}^{p-1} c_m Y^m X^{m-s} \sum_{m'=n(a, j)}^{p-1} c_{m'} X^s Y^{m'} X^{m'-s} \cdot \mu_{a+2s} \text{Fr}'(z_1) \text{Fr}'(z_2) X^s.
\end{aligned}$$

Note that  $a + 2s = 0$  or  $1$  in  $\mathbb{F}_p$ , and hence that  $\mu_{a+2s} \text{Fr}'(z_1) \text{Fr}'(z_2) X^s = \mu_{a+2s} \text{Fr}'(z_1 z_2) X^s$  by Lemma 5.2 (i). Therefore, the last term in the above equalities is equal to

$$\begin{aligned}
&E(a, j) \sum_{m'=n(a, j)}^{p-1} c_{m'} Y^{m'} X^{m'-s} \cdot \mu_{a+2s} \text{Fr}'(z_1 z_2) X^s \\
&= E(a, j) \cdot \mu_a \sum_{m'=n(a, j)}^{p-1} c_{m'} Y^{m'} X^{m'-s} \text{Fr}'(z_1 z_2) X^s \\
&= E(a, j)Z(z_1 z_2; (a, j)) \\
&= Z(z_1 z_2; (a, j)),
\end{aligned}$$

where the last equality follows from (i), and the claim follows.

(iii) We know that  $E(a_1, j_1)E(a_2, j_2) = 0$  if  $(a_1, j_1) \neq (a_2, j_2)$ . Then the claim easily follows from Lemma 5.3.

(iv) It is enough to show the equality for  $u = X^{(p^i)}$  and  $u = Y^{(p^i)}$  with

$i \geq 1$ . Using Lemma 5.2 we have

$$\begin{aligned}
X^{(p^i)}Z(z; (a, j)) &= \text{Fr}'(X^{(p^{i-1})})\text{Fr}'(z)E(a, j) \\
&= \sum_{m=\tilde{n}(a, j)}^{p-1} \tilde{c}_m \mu_a \text{Fr}'(X^{(p^{i-1})})\text{Fr}'(z)X^m Y^m \\
&= \sum_{m=\tilde{n}(a, j)}^{p-1} \tilde{c}_m \mu_a \text{Fr}'(X^{(p^{i-1})}z)X^m Y^m \\
&= \text{Fr}'(X^{(p^{i-1})}z) \sum_{m=\tilde{n}(a, j)}^{p-1} \tilde{c}_m \mu_a X^m Y^m \\
&= \text{Fr}'(X^{(p^{i-1})}z)E(a, j) \\
&= Z(\text{Fr}(X^{(p^i)}z); (a, j))
\end{aligned}$$

if the pair  $(a, j)$  satisfies (B) or (D), and

$$\begin{aligned}
X^{(p^i)}Z(z; (a, j)) &= X^{(p^i)}\left(\mu_a^2 \sum_{m=n(a, j)}^{p-1} c_m Y^m X^{m-s} \text{Fr}'(z)X^s\right) \\
&= \mu_a^2 \sum_{m=n(a, j)}^{p-1} c_m Y^m X^{m-s} X^{(p^i)}\text{Fr}'(z)X^s \\
&= \mu_a \sum_{m=n(a, j)}^{p-1} c_m Y^m X^{m-s} \mu_{a+2s} \text{Fr}'(X^{(p^{i-1})})\text{Fr}'(z)X^s \\
&= \mu_a \sum_{m=n(a, j)}^{p-1} c_m Y^m X^{m-s} \mu_{a+2s} \text{Fr}'(X^{(p^{i-1})}z)X^s \\
&= \mu_a^2 \sum_{m=n(a, j)}^{p-1} c_m Y^m X^{m-s} \text{Fr}'(X^{(p^{i-1})}z)X^s \\
&= Z(\text{Fr}(X^{(p^i)}z); (a, j))
\end{aligned}$$

if the pair  $(a, j)$  satisfies (A) or (C), where  $s = s(a, j)$ .

Similarly we obtain  $Y^{(p^i)}Z(z; (a, j)) = Z(\text{Fr}(Y^{(p^i)}z); (a, j))$  for  $i \geq 1$ , the proof is complete.  $\blacksquare$

For  $n$  pairs  $(a_i, j_i) \in \mathcal{P}$ ,  $0 \leq i \leq n-1$ , define  $E((a_0, \dots, a_{n-1}), (j_0, \dots, j_{n-1}))$  inductively as

$$E((a_0), (j_0)) = E(a_0, j_0)$$

and

$$E((a_0, \dots, a_{n-1}), (j_0, \dots, j_{n-1})) = Z\left(E((a_1, \dots, a_{n-1}), (j_1, \dots, j_{n-1})); (a_0, j_0)\right)$$

for  $n \geq 2$ . Note that all  $E((a_0, \dots, a_{n-1}), (j_0, \dots, j_{n-1}))$  lie in  $\mathcal{A}_n$ .

**Proposition 5.5.** For  $r$  pairs  $(a_i, j_i) \in \mathcal{P}$ ,  $0 \leq i \leq r - 1$ , the following holds.

(i) We have

$$\mu_{\sum_{i=0}^{r-1} b_i p^i}^{(r)} E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) = E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})),$$

where

$$b_i = \begin{cases} a_i - p & \text{if } (a_i, j_i) \text{ satisfies (A) or (C),} \\ a_i & \text{if } (a_i, j_i) \text{ satisfies (B) or (D) } \end{cases},$$

regarding each  $a_i$  as the corresponding integer with  $0 \leq a_i \leq p - 1$ . In particular,  $E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1}))$  is a  $\mathcal{U}_r^0$ -weight vector of  $\mathcal{U}_r^0$ -weight  $\sum_{i=0}^{r-1} b_i p^i$ .

(ii) Suppose that  $r \geq 2$ . Then

$$\sum_{(a_i, j_i) \in \mathcal{P}, 1 \leq i \leq r-1} E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) = E(a_0, j_0).$$

(iii) The elements  $E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1}))$  with  $(a_i, j_i) \in \mathcal{P}$ ,  $0 \leq i \leq r - 1$  are pairwise orthogonal primitive idempotents in  $\mathcal{U}_r$  whose sum is 1.

**Proof.** We use induction on  $r$ . (i) and (iii) for  $r = 1$  follow immediately from the definition of  $E(a_0, j_0)$  and Proposition 4.5. Suppose that  $r \geq 2$ .

(i) We see that  $\mu_{\sum_{i=0}^{r-1} b_i p^i}^{(r)} E(a, j) = Z(\mu_{\sum_{i=1}^{r-1} b_i p^{i-1}}^{(r-1)}; (a_0, j_0))$ . Indeed, by Proposition 5.1 (i) and (iii) we have

$$\begin{aligned} Z(\mu_{\sum_{i=1}^{r-1} b_i p^{i-1}}^{(r-1)}; (a_0, j_0)) &= \text{Fr}'(\mu_{\sum_{i=1}^{r-1} b_i p^{i-1}}^{(r-1)}) E(a_0, j_0) \\ &= \text{Fr}'(\mu_{\sum_{i=1}^{r-1} b_i p^{i-1}}^{(r-1)}) \mu_{a_0} E(a_0, j_0) \\ &= \mu_{a_0 + \sum_{i=1}^{r-1} b_i p^i}^{(r)} E(a_0, j_0) \\ &= \mu_{\sum_{i=0}^{r-1} b_i p^i}^{(r)} E(a_0, j_0) \end{aligned}$$

if the pair  $(a_0, j_0)$  satisfies (B) or (D), and

$$\begin{aligned} Z(\mu_{\sum_{i=1}^{r-1} b_i p^{i-1}}^{(r-1)}; (a_0, j_0)) &= \mu_{a_0}^2 \sum_{m=n(a_0, j_0)}^{p-1} c_m Y^m X^{m-s} \text{Fr}'(\mu_{\sum_{i=1}^{r-1} b_i p^{i-1}}^{(r-1)}) X^s \\ &= \mu_{a_0} \sum_{m=n(a_0, j_0)}^{p-1} c_m Y^m X^{m-s} \mu_{a_0+2s} \text{Fr}'(\mu_{\sum_{i=1}^{r-1} b_i p^{i-1}}^{(r-1)}) X^s \\ &= \mu_{a_0} \sum_{m=n(a_0, j_0)}^{p-1} c_m Y^m X^{m-s} \mu_{a_0+2s-p+\sum_{i=1}^{r-1} b_i p^i}^{(r)} X^s \\ &= \mu_{a_0-p+\sum_{i=1}^{r-1} b_i p^i}^{(r)} \cdot \mu_{a_0} \sum_{m=n(a_0, j_0)}^{p-1} c_m Y^m X^m \\ &= \mu_{\sum_{i=0}^{r-1} b_i p^i}^{(r)} E(a_0, j_0) \end{aligned}$$

if the pair  $(a_0, j_0)$  satisfies (A) or (C), where  $s = s(a_0, j_0)$ . Then using Proposition 5.4 (i) and (ii) we have

$$\begin{aligned}
& \mu_{\sum_{i=0}^{r-1} b_i p^i}^{(r)} E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) \\
&= \mu_{\sum_{i=0}^{r-1} b_i p^i}^{(r)} Z\left(E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})); (a_0, j_0)\right) \\
&= \mu_{\sum_{i=0}^{r-1} b_i p^i}^{(r)} E(a_0, j_0) Z\left(E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})); (a_0, j_0)\right) \\
&= Z\left(\mu_{\sum_{i=1}^{r-1} b_i p^{i-1}}^{(r-1)}; (a_0, j_0)\right) Z\left(E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})); (a_0, j_0)\right) \\
&= Z\left(\mu_{\sum_{i=1}^{r-1} b_i p^{i-1}}^{(r-1)} E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})); (a_0, j_0)\right).
\end{aligned}$$

By induction, we have

$$\mu_{\sum_{i=1}^{r-1} b_i p^{i-1}}^{(r-1)} E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})) = E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})),$$

and the claim follows.

(ii) By Proposition 5.4 (ii) and induction, we have

$$\begin{aligned}
& \sum_{(a_i, j_i) \in \mathcal{P}, 1 \leq i \leq r-1} E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) \\
&= \sum_{(a_i, j_i) \in \mathcal{P}, 1 \leq i \leq r-1} Z\left(E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})); (a_0, j_0)\right) \\
&= Z\left(\sum_{(a_i, j_i) \in \mathcal{P}, 1 \leq i \leq r-1} E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})); (a_0, j_0)\right) \\
&= Z(1; (a_0, j_0)) \\
&= E(a_0, j_0),
\end{aligned}$$

as desired.

(iii) If  $(a_0, j_0) \neq (a'_0, j'_0)$ , we have by Proposition 5.4 (iii) that

$$E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) E((a'_0, \dots, a'_{r-1}), (j'_0, \dots, j'_{r-1})) = 0,$$

so we may assume that  $(a_0, j_0) = (a'_0, j'_0)$ . Then

$$\begin{aligned}
& E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) E((a'_0, \dots, a'_{r-1}), (j'_0, \dots, j'_{r-1})) \\
&= Z\left(E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})); (a_0, j_0)\right) \\
&\quad \times Z\left(E((a'_1, \dots, a'_{r-1}), (j'_1, \dots, j'_{r-1})); (a_0, j_0)\right) \\
&= Z\left(E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})) E((a'_1, \dots, a'_{r-1}), (j'_1, \dots, j'_{r-1})); (a_0, j_0)\right)
\end{aligned}$$

by Proposition 5.4 (ii). By induction, this is equal to

$$Z\left(E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})); (a_0, j_0)\right) = E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1}))$$

if  $(a_i, j_i) = (a'_i, j'_i)$  for all  $i$  with  $1 \leq i \leq r - 1$ , and to

$$Z(0; (a_0, j_0)) = 0$$

otherwise. Therefore, we conclude that all  $E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1}))$  are pairwise orthogonal idempotents. The fact that a sum of these idempotents is 1 follows from (ii) and Proposition 4.5. It remains to show that these idempotents are primitive. Consider an integer  $\lambda$  with  $0 \leq \lambda \leq p^r - 1$  and its  $p$ -adic expansion  $\lambda = \sum_{i=0}^{r-1} \lambda_i p^i$ . It follows from Steinberg's tensor product theorem that

$$\dim_k L(\lambda) = \prod_{i=0}^{r-1} \dim_k L(\lambda_i) = \prod_{i=0}^{r-1} (\lambda_i + 1).$$

Therefore, the number of the summands in a decomposition of  $1 \in \mathcal{U}_r$  into pairwise orthogonal primitive idempotents is

$$\begin{aligned} \sum_{\lambda=0}^{p^r-1} \dim_k L(\lambda) &= \sum_{(\lambda_0, \dots, \lambda_{r-1}) \in \{0, 1, \dots, p-1\}^r} (\lambda_0 + 1) \cdots (\lambda_{r-1} + 1) \\ &= \prod_{i=0}^{r-1} \left( \sum_{\lambda_i=0}^{p-1} (\lambda_i + 1) \right) \\ &= \prod_{i=0}^{r-1} (p(p+1)/2) \\ &= (p(p+1)/2)^r. \end{aligned}$$

On the other hand, the number of the elements  $E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1}))$  is  $(p(p+1)/2)^r$  as well. Therefore, these idempotents must be primitive. ■

**Remark.** Note that any idempotent in  $\mathcal{U}$  must have degree 0, namely, it must lie in  $\mathcal{A}$ . Since the subalgebra  $\mathcal{A}$  (hence  $\mathcal{A}_r$ ) is commutative, (iii) gives a unique decomposition of 1 into a sum of primitive idempotents in  $\mathcal{U}_r$  (see [NT89, ch. 1. Theorem 4.6]).

We can also give primitive idempotents in  $\mathcal{U}_{r,r'}$  ( $r' > r$ ).

**Proposition 5.6.** *For  $r' > r$ , the elements*

$$E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) \text{Fr}^{r'}(\mu_{a'}^{(r'-r)})$$

*with  $(a_i, j_i) \in \mathcal{P}$ ,  $0 \leq i \leq r - 1$  and  $0 \leq a' \leq p^{r'-r} - 1$  are pairwise orthogonal primitive idempotents in  $\mathcal{U}_{r,r'}$  whose sum is 1.*

**Proof.** By Proposition 5.5 (iii), all  $E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1}))$  are pairwise orthogonal primitive idempotents in  $\mathcal{A}_r$  whose sum is 1. On the other hand, by Proposition 5.1 (ii), all  $\text{Fr}^{r'}(\mu_{a'}^{(r'-r)})$  (with  $0 \leq a' \leq p^{r'-r} - 1$ ) are pairwise orthogonal primitive idempotents in the  $k$ -algebra  $\text{Fr}^{r'}(\mathcal{U}_{r,-r}^0)$  whose sum is 1.

Note that the multiplication map  $\mathcal{A}_r \otimes \text{Fr}^{r'}(\mathcal{U}_{r',r}^0) \rightarrow \mathcal{A}_{r,r'}$  is not only a  $k$ -linear isomorphism (see Proposition 2.3) but also a  $k$ -algebra isomorphism since  $\mathcal{A}$  is commutative. Therefore, all

$$E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) \text{Fr}^{r'}(\mu_{a'}^{(r'-r)})$$

are pairwise orthogonal primitive idempotents in  $\mathcal{A}_{r,r'}$  whose sum is 1. But these are primitive also in  $\mathcal{U}_{r,r'}$  since any idempotent in  $\mathcal{U}$  lies in  $\mathcal{A}$ . ■

The following lemma is used to determine the PIMs generated by the primitive idempotents.

**Lemma 5.7.** *Let  $(a_i, j_i) \in \mathcal{P}$ ,  $0 \leq i \leq r - 1$ , and let  $t$  is the largest integer  $n$  with  $X^{(n)}E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) \neq 0$  and  $0 \leq n \leq p^r - 1$ . Then  $t = \sum_{i=0}^{r-1} (p - 1 - \tilde{n}(a_i, j_i))p^i$ .*

**Proof.** If  $r = 1$ , the result follows from Lemma 4.8. Suppose that  $r \geq 2$ . We use induction on  $r$ . Let  $n$  be an integer with  $0 \leq n \leq p^r - 1$  and write  $n = n_0 + n'p$  for some integers  $n_0, n'$  with  $0 \leq n_0 \leq p - 1$  and  $0 \leq n' \leq p^{r-1} - 1$ . Then

$$\begin{aligned} X^{(n)}E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) \\ &= X^{(n_0)}X^{(n'p)}Z\left(E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})); (a_0, j_0)\right) \\ &= X^{(n_0)}Z\left(X^{(n')}E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})); (a_0, j_0)\right) \end{aligned}$$

by Proposition 5.4 (iv). By induction the largest integer  $n'$  with

$$X^{(n')}E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})) \neq 0$$

and  $0 \leq n' \leq p^{r-1} - 1$  is  $\sum_{i=1}^{r-1} (p - 1 - \tilde{n}(a_i, j_i))p^{i-1}$ . Then, by Lemma 5.3, there is a nonzero element  $z' \in \mathcal{U}$  such that

$$X^{(n_0)}Z\left(X^{(n')}E((a_1, \dots, a_{r-1}), (j_1, \dots, j_{r-1})); (a_0, j_0)\right) = X^{(n_0)}E(a_0, j_0)\text{Fr}'(z').$$

Hence the largest integer  $n_0$  where this term does not vanish is  $p - 1 - \tilde{n}(a_0, j_0)$  by Lemma 4.8. Thus we obtain

$$\begin{aligned} t &= (p - 1 - \tilde{n}(a_0, j_0)) + p \sum_{i=1}^{r-1} (p - 1 - \tilde{n}(a_i, j_i))p^{i-1} \\ &= \sum_{i=0}^{r-1} (p - 1 - \tilde{n}(a_i, j_i))p^i, \end{aligned}$$

and the lemma follows. ■

Now we describe the main result.

**Theorem 5.8.** For  $0 \leq i \leq r - 1$ , let  $(a_i, j_i) \in \mathcal{P}$ , and set

$$\beta_i = \begin{cases} p - 2j_i - 1 & \text{if } (a_i, j_i) \text{ satisfies (B) or (C),} \\ 2j_i - 1 & \text{if } (a_i, j_i) \text{ satisfies (A) or (D)} \end{cases}$$

and

$$b_i = \begin{cases} a_i - p & \text{if } (a_i, j_i) \text{ satisfies (A) or (C),} \\ a_i & \text{if } (a_i, j_i) \text{ satisfies (B) or (D)} \end{cases}$$

regarding  $a_i$  and  $j_i$  as the corresponding integers with  $0 \leq a_i \leq p - 1$  and  $0 \leq j_i \leq (p - 1)/2$  except for  $j_i$  when  $p = 2$ . Moreover, let  $a' \in \mathbb{Z}$  with  $0 \leq a' \leq p^{r'-r} - 1$ . Then the element

$$E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) \text{Fr}^{r'}(\mu_{a'}^{(r'-r)})$$

generates a  $\mathcal{U}_{r,r'}$ -module isomorphic to  $\tilde{Q}_r(\sum_{i=0}^{r-1} \beta_i p^i + a' p^r)$  provided that  $\sum_{i=0}^{r-1} b_i p^i \geq 0$ , and to  $\tilde{Q}_r(\sum_{i=0}^{r-1} \beta_i p^i + (a' + 1)p^r)$  if  $\sum_{i=0}^{r-1} b_i p^i < 0$ . In particular, the element  $E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1}))$  generates a  $\mathcal{U}_r$ -module isomorphic to  $Q_r(\sum_{i=0}^{r-1} \beta_i p^i)$ .

**Proof.** Since  $E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) \text{Fr}^{r'}(\mu_{a'}^{(r'-r)})$  is a primitive idempotent in  $\mathcal{U}_{r,r'}$  by Proposition 5.6, it generates a projective indecomposable  $\mathcal{U}_{r,r'}$ -module isomorphic to  $\tilde{Q}_r(\lambda' + \lambda'' p^r)$  for certain integers  $\lambda'$  and  $\lambda''$  with  $0 \leq \lambda' \leq p^r - 1$  and  $0 \leq \lambda'' \leq p^{r'-r} - 1$ . The element

$$E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) \text{Fr}^{r'}(\mu_{a'}^{(r'-r)})$$

has  $\mathcal{U}_{r'}^0$ -weight  $\sum_{i=0}^{r-1} b_i p^i + a' p^r$  if  $\sum_{i=0}^{r-1} b_i p^i \geq 0$ , and  $\sum_{i=0}^{r-1} b_i p^i + p^r + a' p^r$  if  $\sum_{i=0}^{r-1} b_i p^i < 0$ , since

$$\begin{aligned} & E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) \text{Fr}^{r'}(\mu_{a'}^{(r'-r)}) \\ &= E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) \mu_{\sum_{i=0}^{r-1} b_i p^i}^{(r)} \text{Fr}^{r'}(\mu_{a'}^{(r'-r)}) \\ &= \begin{cases} \mu_{\sum_{i=0}^{r-1} b_i p^i + a' p^r}^{(r)} E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) & \text{if } \sum_{i=0}^{r-1} b_i p^i \geq 0, \\ \mu_{\sum_{i=0}^{r-1} b_i p^i + p^r + a' p^r}^{(r)} E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) & \text{if } \sum_{i=0}^{r-1} b_i p^i < 0 \end{cases} \end{aligned}$$

By Lemma 4.7, we see that

$$\begin{aligned} b_i + 2(p - 1 - \tilde{n}(a_i, j_i)) &= \begin{cases} p - 1 + 2j_i & \text{if } (a_i, j_i) \text{ satisfies (B) or (C),} \\ 2p - 1 - 2j_i & \text{if } (a_i, j_i) \text{ satisfies (A) or (D)} \end{cases} \\ &= 2(p - 1) - \beta_i. \end{aligned}$$

Moreover, by Lemma 5.7, the largest integer  $t$  satisfying  $0 \leq t \leq p^r - 1$  and  $X^{(t)} E((a_0, \dots, a_{r-1}), (j_0, \dots, j_{r-1})) \neq 0$  is  $\sum_{i=0}^{r-1} (p - 1 - \tilde{n}(a_i, j_i)) p^i$ .

Suppose that  $\sum_{i=0}^{r-1} b_i p^i \geq 0$ . Then we have

$$\begin{aligned} \sum_{i=0}^{r-1} b_i p^i + 2t &= \sum_{i=0}^{r-1} (b_i + 2(p - 1 - \tilde{n}(a_i, j_i))) p^i \\ &= \sum_{i=0}^{r-1} (2(p - 1) - \beta_i) p^i \\ &\leq 2p^r - 2, \end{aligned}$$

and hence  $\lambda'' = a'$  and

$$\lambda' = 2p^r - 2 - \left( \sum_{i=0}^{r-1} b_i p^i + 2t \right) = 2p^r - 2 - \sum_{i=0}^{r-1} (2(p - 1) - \beta_i) p^i = \sum_{i=0}^{r-1} \beta_i p^i$$

by Proposition 3.1 (i).

Finally, suppose that  $\sum_{i=0}^{r-1} b_i p^i < 0$ . Then we have

$$\left( \sum_{i=0}^{r-1} b_i p^i + p^r \right) + 2t = \sum_{i=0}^{r-1} (2(p - 1) - \beta_i) p^i + p^r > 2p^r - 2.$$

If  $a' \neq p^{r'-r} - 1$ , then  $\lambda'' = a' + 1$  and

$$\begin{aligned} \lambda' &= 3p^r - 2 - \left( \sum_{i=0}^{r-1} b_i p^i + p^r + 2t \right) \\ &= 3p^r - 2 - \sum_{i=0}^{r-1} (2(p - 1) - \beta_i) p^i - p^r \\ &= \sum_{i=0}^{r-1} \beta_i p^i \end{aligned}$$

by Proposition 3.1 (ii). If  $a' = p^{r'-r} - 1$ , then  $\lambda'' = 0$  and  $\lambda' = \sum_{i=0}^{r-1} \beta_i p^i$  by Proposition 3.1 (iii), but  $\tilde{Q}_r(\sum_{i=0}^{r-1} \beta_i p^i) \cong \tilde{Q}_r(\sum_{i=0}^{r-1} \beta_i p^i + (a' + 1)p^r)$  as  $\mathcal{U}_{r,r'}$ -modules since

$$\sum_{i=0}^{r-1} \beta_i p^i \equiv \sum_{i=0}^{r-1} \beta_i p^i + p^{r'} = \sum_{i=0}^{r-1} \beta_i p^i + (a' + 1)p^r \pmod{p^{r'}}.$$

Thus the first statement is proved. The second statement is clear. ■

**Acknowledgment.** The author would like to thank the referee for carefully reading the first and the second versions of this paper and giving helpful comments.

## References

- [CR62] Curtis, C. W., and I. Reiner, “Representation theory of finite groups and associative algebras”, Wiley-Interscience, New York, 1962.
- [Don93] Donkin, S., *On tilting modules for algebraic groups*, Math. Z. **212** (1993), 39–60.
- [Gro12] Gros, M., *A splitting of the Frobenius morphism on the whole algebra of distributions of  $SL_2$* , Algebr. Represent. Theory **15** (2012), 109–118.
- [GK11] Gros, M., and M. Kaneda, *Contraction par Frobenius de  $G$ -modules*, Ann. Inst. Fourier **61** (2011), 2507–2542.
- [GK15] —, *Un scindage du morphisme de Frobenius quantique*, Ark. Mat. **53** (2015), 271–301.
- [Hab80] Haboush, W. J., *Central differential operators on split semi-simple groups over fields of positive characteristic*, Lect. Notes Math. **795** (1980), 35–85.
- [Hum72] Humphreys, J. E., “Introduction to Lie algebras and representation theory,” Grad. Texts in Math., **9**, Springer, New York, 1972.
- [Jan80] Jantzen, J. C., *Darstellungen halbeinfacher Gruppen und ihrer Frobenius-Kerne*, J. Reine Angew. Math. **317** (1980), 157–199.
- [Jan03] —, “Representations of algebraic groups,” 2nd ed., Math. Surveys Monogr. **107**, Amer. Math. Soc., RI, 2003.
- [NT89] Nagao, H., and Y. Tsushima, “Representations of finite groups,” Academic Press, San Diego, 1989.
- [Sel03] Seligman, G. B., *On idempotents in reduced enveloping algebras*, Trans. Amer. Math. Soc. **355** (2003), 3291–3300.

Yutaka Yoshii  
College of Education  
Ibaraki University  
2-1-1 Bunkyo  
Mito, Ibaraki, 310-8512, Japan  
yutaka.yoshii.6174@vc.ibaraki.ac.jp

Received September 9, 2016  
and in final form March 9, 2017