THE CENTER OF THE q-WEYL ALGEBRA OVER RINGS WITH TORSION

QUANLIN CHEN

Abstract. We compute the centers of the Weyl algebra, q-Weyl algebra, and the "first q-Weyl algebra" over the quotient of the ring $\mathbb{Z}/p^N\mathbb{Z}[q]$ by some polynomial $P(q)$. Through this, we generalize and "quantize" part of a result by Stewart and Vologodsky on the center of the ring of differential operators on a smooth variety over $\mathbb{Z}/p^n\mathbb{Z}$. We prove that a corresponding Witt vector structure appears for general $P(q)$ and compute the extra terms for special $P(q)$ with particular properties, answering a question by Bezrukavnikov of possible interpolation between two known results.

1. Introduction

1.1. **Background and Motivation.** In noncommutative algebra, the Weyl and q-Weyl algebra are a pair of basic examples of q-deformation, which is a philosophy of understanding an object better after it is deformed or "quantized" via a parameter q.

The Weyl algebra, $W(R)$, is a free algebra generated by a and b over a ring R subject to the relation $ba - ab - 1$; the q-Weyl algebra, $W_q(R)$, on the other hand, is a free algebra generated by a, a^{-1}, b, b^{-1} over a ring R subject to the relation by $ba - qab$, the q-commutation relation. The q-Weyl algebra can be realized as an "exponentiation" and quantization of the Weyl algebra.

The Weyl algebra is also the ring of differential operators over the affine space $\mathbb{A}^1_R$. There gives rise to another natural quantization, the "first q-Weyl algebra," which we obtain by replacing the differential operator by the q-derivative, formally defined by the free algebra over R generated by x, y, x^{-1}, y^{-1} over R and subject to the relation $yx - qxy - 1$.

In [SV13], Stewart and Vologodsky proved a conjecture of Kaledin about the center of the rings of differential operators on smooth varieties over $\mathbb{Z}/p^n\mathbb{Z}$. Their results generalize a classical isomorphism in case $\mathbb{Z}/p\mathbb{Z}$ arising in modular representation theory (see (1.1) in [SV13], or [BMRR08]). They describe the center of these rings of differential operators via the Witt vector construction. Particularly, taking the smooth variety as $\mathbb{A}^1$, we obtain the ring to be the Weyl algebra over $\mathbb{Z}/p^n\mathbb{Z}$ and we deduce that the center is isomorphic to the Witt vector ring over the symmetric algebra generated by two elements $\widetilde{a}, \widetilde{b}$.

The motivation of this paper is to quantize the result in [SV13], taking the first step by investigating the q-deformation of the simplest such ring, the q-Weyl algebra and the first q-Weyl algebra, which quantizes the Weyl algebra.

Date: January 25, 2021.

1.2. **Known Results.** This is not the first attempt to understand the center of the Weyl and q-Weyl algebra. One can easily prove that the center of the Weyl algebra over a torsion-free ring is R itself. And the center of the Weyl algebra over $\mathbb{Z}/p^n\mathbb{Z}$ is implied in [SV13].

As for the q-Weyl algebra, its center over a torsion-free ring is also investigated (see e.g. [GG14]). Especially when q is a l-th root of unity, the center would be freely generated by a^l and b^l. However, the center of the q-Weyl algebra over rings with torsion is largely left as a mystery.

Roman Bezrukavnikov asked the possible interpolation between the two known results. Namely, he asked about the center of the q-Weyl algebra over $\mathbb{Z}/p^N\mathbb{Z}$ where q is a p^n-th root of unity and n is a positive integer. If we obtain the result, it would be the first glance into the possible quantization of [SV13], and it is interesting to see whether the similar Witt vector construction would appear.

1.3. **Our Approach.** The way to formulate Bezrukavnikov's question is to consider the center of the quotient of q-Weyl algebra by an ideal generated by polynomial P with coefficients in a ring $\mathbb{Z}/p^N\mathbb{Z}$. Particularly in the context of choosing q as a p^n-th root of unity, P would be the p^n-th cyclotomic polynomial.

The difficulty is that $\mathbb{Z}/p^N\mathbb{Z}$ is not a domain, when $N \geqslant 2$ (for example, p is a zero divisor). And the p^n cyclotomic polynomial splits completely in $\mathbb{F}_p$ (modulo p) but is not even reducible in $\mathbb{Z}/p^2\mathbb{Z}$.

In this paper, we answer the question of Roman Bezrunikov by completely solving the center ring of $W_q(\mathbb{Z}/p^N\mathbb{Z})/(\Phi_{p^n}(q))$ by Theorem 5.2. On the contrary to the expected Witt vector construction, we find and compute a series of extra terms, which would potentially point out the obstacles in the general quantization.

Extending from Bezrukavnikov's question, we consider the center of

$$W_q(\mathbb{Z}/p^N\mathbb{Z})/P(q)$$

for a general polynomial P. We prove that when monic P is irreducible in $\mathbb{F}_p$ and p is odd, the center preserves the Witt vector structure. This answers the question of quantization for any "algebraic integer" q.

Moreover, we investigate the center of the first Weyl algebra, as another natural quantization of the Weyl algebra. We show that as long as $P(1)$ is not a multiple of p, the center of the first Weyl algebra is isomorphic to the center of the q-Weyl algebra. And there is a natural bijection between their underlying sets (Theorem 6.5).

1.4. **Outline.** We structure the paper as follows.

In §2, we review the basic definitions and structures of the Weyl and q-Weyl algebra, recount a set of elementary number theory facts, and present the Witt vector construction in our context. In §3, we generalize the special case of the result in [SV13] by replacing the Weyl algebra by the generalized Weyl algebra. In §4, we prove the main theorem for odd prime p (Theorem 4.2), solving the center for all "algebraic integer" q and presenting some extensions. In §5, we dedicate to answer Roman Bezrukavnikov's question thoroughly, by solving the center when P is $q^{p^n}-1$ and $\Phi_{p^n}(q)$. In §6, we construct an isomorphism between the first q-Weyl algebra and the Weyl algebra and an additional natural bijection between underlying sets of their centers.

2. Preliminaries

2.1. **Basic Definitions.** In this paper, we focus on $R = \mathbb{Z}/p^N\mathbb{Z}$ as a ring with torsion, where p is a prime and N is a positive integer.

We first recall the definition of the Weyl algebra, q-Weyl algebra, and the first q-Weyl algebra over a ring R.

Definition 2.1. Let q and h be indeterminates. For a ring R we define the *Weyl algebra*, *generalized Weyl algebra*, and *q-Weyl alegbra* over R as

$$W(R) = R\langle a, b\rangle/(ba - ab - 1),$$
$$W^h(R) = R\langle a, b\rangle/(ba - ab - h),$$

and

$$W_q(R) = R\langle a, a^{-1}, b, b^{-1}\rangle/(ba - qab),$$

respectively.

To clarify, there are two different known definitions for the q-Weyl algebra. For the other definition, we call it the first q-Weyl Algebra (as [HL17]), distinguishing it from Definition 2.1.

Definition 2.2. Let q be an indeterminate. For a ring R we define the *first q-Weyl algebra* over R as

$$W_q^{(1)}(R) = R\langle x, x^{-1}, y, y^{-1}\rangle/(yx - qxy - 1).$$

The following well-known result shows that the Weyl algebra (and the first q-Weyl algebra) is essentially the ring of differential operators (and q-derivative) with polynomial coefficients.

Proposition 2.3. *The vector space of all real polynomials $\mathbb{R}[x]$ is*

(a) a faithful representation of $W(\mathbb{R})$, where a acts by multiplication by x and y acts by the differential operator $\frac{\partial}{\partial x}$;

(b) a faithful representation of $W_q^{(1)}(\mathbb{R})$, where a acts by multiplication by x and y acts by the q-differential operator $\left(\frac{d}{dx}\right)_q$.

On the other hand, the q-Weyl algebra can be viewed as the ring of operators of functions f where a sends $f(x)$ to $e^x f(x)$ and b sends $f(x)$ to $f(x + \log q)$. In this sense, the q-Weyl algebra can be seen as an exponentiation and q-deformation of the Weyl algebra.

2.2. **The Structure of the Weyl and q-Weyl algebra.** In this section, we present some basic facts about the Weyl and q-Weyl algebra.

The following well-known proposition provides those algebras a basis (for a proof see, e.g. [EGH$^+$11]).

Proposition 2.4. *A basis for the*

(1) Weyl algebra is $\{a^i b^j | i, j \geqslant 0\}$;

(2) q-Weyl algebra is $\{a^i b^j | i, j \in \mathbb{Z}\}$;

(3) first q-Weyl algebra is $\{x^i y^j | i, j \in \mathbb{Z}\}$.

The following lemma proved that an element is in the center if and only it commutes with both a and b (or x and y). The proof is straightforward, so we omit it.

Lemma 2.5. *We have that*

(a) *an element z is in the center of $W^h(R)$ if and only if it commutes with both a and b.*
(b) *if we replace $W^h(R)$ in (a) by $W_q(R)/P(q)$, the same statement holds true.*
(c) *if we replace $W^h(R)$ in (a) by $W_q^{(1)}(R)/P(q)$ and a, b by x, y, the same statement holds true.*

Proof. (a) If z is in the center, it commutes with every element in the ring, including a and b.

Conversely, suppose that z commutes with both a and b. By Proposition 2.4, every element in $W^h(R)$ can be written in form

$$\sum_{i,j} c_{ij} a^i b^j,$$

where c_{ij} is a polynomial of parameter q, which commutes with every element. We have

$$zc_{ij}a^ib^j = c_{ij}(za)a^{i-1}b^j = c_{i,j}a(za)a^{i-2}b^j = \cdots = c_{i,j}a^i(zb)b^{j-1} = \cdots = c_{ij}a^ib^jz.$$

Thus z commutes with each $c_{ij}a^ib^j$, implying that

$$z\sum_{i,j} c_{ij}a^ib^j = \sum_{i,j} zc_{ij}a^ib^j = \sum_{i,j} c_{ij}a^ib^jz = \left(\sum_{i,j} c_{ij}a^ib^j\right)z.$$

Therefore z commutes with every element; z is in the center.

(b) The proof of this part is exactly the same except for that in the basis provided by Proposition 2.4, the exponents of a and b could be negative. We treat this case specially as follows (let $j = -k$ be negative, where k is a positive integer).

$$zb^{-k} = b^{-1}(bz)b^{-k} = b^{-1}zb^{-k+1} = b^{-2}(bz)b^{-k+2} = b^{-2}zb^{-k+2} = \cdots = b^{-k}z.$$

For the same reason z commutes with a^i for negative integer i so z commutes with all $c_{ij}a^ib^j$. The rest is the same as (a)

(c) The proof of this part is exactly the same as (b). □

From now on, in the expressions like $c_{ij}a^ib^j$ and $z_{ij}a^ib^j$, c_{ij} and z_{ij} would be polynomials of the parameter q. In this way we can more conveniently denote the elements of the algebra by its basis.

So now we only need to find all the element that commutes with both a and b to compute the center. The following lemma explains how the multiplication by a and b works in those algebras.

Lemma 2.6. *We have*

(a) *in $W^h(R)$,*

$$\left(\sum_{i,j\in\mathbb{Z}_{\geqslant 0}} c_{ij}a^ib^j\right)a = \sum_{i,j\in\mathbb{Z}_{\geqslant 0}} c_{ij}a^{i+1}b^j + \sum_{i,j\in\mathbb{Z}_{\geqslant 0}} jhc_{ij}a^ib^{j-1}$$

and

$$b\left(\sum_{i,j\in\mathbb{Z}_{\geqslant 0}} c_{ij}a^ib^j\right) = \sum_{i,j\in\mathbb{Z}_{\geqslant 0}} c_{ij}a^ib^{j+1} + \sum_{i,j\in\mathbb{Z}_{\geqslant 0}} jhc_{ij}a^{i-1}b^j$$

(b) in $W_q(R)/P(q)$,

$$\left(\sum_{i,j\in\mathbb{Z}} c_{ij}a^ib^j\right)a = \sum_{i,j\in\mathbb{Z}} c_{ij}q^ja^{i+1}b^j$$

and

$$b\left(\sum_{i,j\in\mathbb{Z}} c_{ij}a^ib^j\right) = \sum_{i,j\in\mathbb{Z}} q^ic_{ij}a^ib^{j+1}.$$

(c) in $W_q^{(1)}(R)/P(q)$,

$$\left(\sum_{i,j\in\mathbb{Z}} c_{ij}a^ib^j\right)a = \sum_{i,j\in\mathbb{Z}} q^jc_{ij}a^{i+1}b^j + \sum_{i,j\in\mathbb{Z}} \frac{q^{j+1}-1}{q-1}c_{i+1j+1}a^{i+1}b^j$$

and

$$b\left(\sum_{i,j\in\mathbb{Z}} c_{ij}a^ib^j\right) = \sum_{i,j\in\mathbb{Z}} q^ic_{ij}a^ib^{j+1} + \sum_{i,j\in\mathbb{Z}} \frac{q^{i+1}-1}{q-1}c_{i+1j+1}a^ib^{j+1}.$$

Proof. (a) Symmetrically, we only need to prove the first equality. Induct on j to prove that

$$c_{ij}a^ib^ja = c_{ij}a^{i+1}b^j + jhc_{ij}a^ib^{j-1},$$

and clearly this implies the result via direct summation.

The base case is trivial since $a^ia = aa^i$.

For general cases, we have

$$\begin{aligned} c_{ij}a^ib^ja &= c_{ij}a^ib^{j-1}(ab+h) \\ &= hc_{ij}a^ib^{j-1} + (c_{ij}a^ib^{j-1}a)b \\ &= hc_{ij}a^ib^{j-1} + h(j-1)c_{ij}a^ib^{j-2}b + c_{i,j}a^{i+1}b^j \\ &= c_{ij}a^{i+1}b^j + jhc_{ij}a^ib^{j-1}, \end{aligned}$$

by the inductive assumption. As desired.

(b) For the same reason as (a), we only need to prove that

$$c_{ij}a^ib^ja = q^jc_{ij}a^{i+1}b^j.$$

In fact

$$\begin{aligned} c_{ij}a^ib^ja &= c_{ij}a^ib^{j-1}qab \\ &= qc_{ij}a^ib^{j-1}ab \\ &= q^2c_{ij}a^ib^{j-2}ab^2 \\ &= \cdots \\ &= q^jc_{ij}a^{i+1}b^j. \end{aligned}$$

As desired.

(c) For the same reason as (a), we only need to show

$$c_{ij}a^ib^ja = q^jc_{ij}a^{i+1}b^j + \frac{q^j-1}{q-1}c_{ij}a^ib^{j-1}.$$

In fact

$$\begin{aligned} c_{ij}a^ib^ja &= c_{ij}a^ib^{j-1}(qab+1) \\ &= qc_{ij}a^ib^{j-1}ab + c_{ij}a^ib^{j-1} \\ &= q^2c_{ij}a^ib^{j-2}ab^2 + (1+q)c_{ij}a^ib^{j-1} \\ &= \cdots \\ &= q^jc_{ij}a^{i+1}b^j + (1+q+\cdots+q^{j-1})c_{ij}a^ib^{j-1}, \end{aligned}$$

as desired. □

2.3. **Elementary Number-theoretical Setup.** In this section, we set up some elementary facts that will be helpful for future usage.

First, we extend the notion of the p-valuation to polynomials and matrices.

Definition 2.7. For a prime p we define the p-valuation of

(1) an integer entry square matrix M, $\nu_p(M)$, to be the greatest integer k such that p^k divides all the entries of M.
(2) a polynomial $\mathcal{P} \in \mathbb{Z}[x]$, $\nu_p(\mathcal{P})$, to be the greatest integer k such that p^k divides all the coefficients of $\mathcal{P}$.
(3) a polynomial $\mathcal{P} \in \mathbb{Z}/p^N\mathbb{Z}[x]$, $\nu_p(\mathcal{P})$, to be the greatest integer $k \leqslant N$ such that p^k divides all the coefficients of $\mathcal{P}$.

Afterwards, whenever we talk about the p-valuation of an object in $\mathbb{Z}/p^N\mathbb{Z}$, we assume that this value will not be greater than N.

We then review the well-known Kummer's Theorem.

Theorem 2.8 (Kummer)**.** *For p prime, let $n, m_1, m_2, \cdots, m_k$ be non-negative integers such that $n = \sum_{i=1}^k m_i$. Then the p-valuation of $\binom{n}{m_1, m_2, \ldots, m_k}$ is the number of carriers when $m_1, m_2, \ldots, m_k$ are added in base p. Namely,*

$$\nu_p\binom{n}{m_1, m_2, \ldots, m_k} = \frac{1}{p-1}\left(\sum_{i=1}^k S_p(m_i) - S_p(n)\right).$$

where $S_p(s)$ denotes the sum of digits when the integer s is written in base p.

Then we consider various properties about the factorization in $\mathbb{Z}/p^N\mathbb{Z}[x]$. We start by the well-known Gauss Lemma and Bézout's Theorem.

Lemma 2.9 (Gauss)**.** *If polynomial $P_1, P_2 \in \mathbb{Z}[x]$ are both primitive, then P_1P_2 is also primitive.*

Theorem 2.10 (Bézout)**.** *If $Q_1, \ldots, Q_k$ are polynomials in $\mathbb{F}_p[q]$ such that their greatest common divisor is 1. Then there exists polynomials $B_1, \ldots, B_k$ such that $\sum_{i=1}^k Q_iB_i = 1$ in $\mathbb{F}_p[q]$.*

Note that if polynomial H is defined in $\mathbb{Z}/p^N\mathbb{Z}[q]$, then it can also be naturally defined in $\mathbb{Z}/p^n\mathbb{Z}[q]$ where $n \leqslant N$ by modulo p^n. Similarly, if H is defined in $\mathbb{Z}[q]$, then it can be naturally defined in $\mathbb{Z}/p^n\mathbb{Z}[q]$ for any n. For the sake of convenience, we may write polynomial H in $\mathbb{Z}/p^n\mathbb{Z}$, which means to consider it in $\mathbb{Z}/p^n\mathbb{Z}[q]$.

Now we prove the following proposition to explain what a "multiple" or a "divisor" means in $\mathbb{Z}/p^N\mathbb{Z}[q]$.

Proposition 2.11. *Let n be a positive integer, $H \in \mathbb{Z}[q]$ be an irreducible polynomial modulo p. If polynomials $P_1, P_2 \in \mathbb{Z}[q]$ satisfy that H divides P_1P_2 in $\mathbb{Z}/p^n\mathbb{Z}[q]$, then there exists a non-negative integer $k \leqslant n$ such that H divides P_1 in $\mathbb{Z}/p^k\mathbb{Z}[q]$ and H divides P_2 in $\mathbb{Z}/p^{n-k}\mathbb{Z}[q]$.*

Proof. Induct on n. When $n = 1$, this is true since $\mathbb{F}[q]$ is a UFD. For the general cases, modulo p then we have that H divides P_1P_2 in $\mathbb{F}_p[q]$. Since H is a prime in $\mathbb{F}_p[q]$, H divides either P_1 or P_2 in $\mathbb{F}_p[q]$. Without loss of generality, we may write $P_1 = KH + pL$ in $\mathbb{Z}/p^N\mathbb{Z}$. Thus $P_1P_2 = H(KP_2) + p(LP_2)$ is multiple of H in $\mathbb{Z}/p^N\mathbb{Z}$ if and only if LP_2 is a multiple of H in $\mathbb{Z}/p^{N-1}\mathbb{Z}$. By the inductive assumption, there exists k' such that L is a multiple of H in $\mathbb{Z}/p^{k'}\mathbb{Z}$ and P_2 is a multiple of H in $\mathbb{Z}/p^{N-k'-1}\mathbb{Z}$. Thus we may write $L = HK' + p^{k'}L'$, and we have $P_1 = (K + pK')H + p^{k'+1}L'$ so P_1 is a multiple of H in $\mathbb{Z}/p^{k'+1}\mathbb{Z}$. Choosing $k = k' + 1$, we get the desired result. Induction is completed. □

Now we are ready to prove the following proposition, explaining how strong is the notion of "coprime" is in $\mathbb{Z}/p^N\mathbb{Z}$. This result would be useful in the proof of Theorem 4.18.

Proposition 2.12. *Let $H_1, H_2 \in \mathbb{Z}/p^N\mathbb{Z}[x]$ satisfying that they are coprime and H_1 is irreducible in $\mathbb{F}_p$. If a polynomial $Q \in \mathbb{Z}/p^N\mathbb{Z}[x]$ is divisible by both H_1 and H_2, then Q is divisible by H_1H_2.*

Proof. Since H_1 divides Q in $\mathbb{Z}/p^N\mathbb{Z}$, we may write $Q = H_1Q'$. Considering that H_2 divides $H_1Q' = Q$ in $\mathbb{Z}/p^N\mathbb{Z}$, by Proposition 2.11, there exists a integer k such that H_2 divides H_1 in $\mathbb{Z}/p^k\mathbb{Z}$ and H_2 divides Q' in $\mathbb{Z}/p^{N-k}\mathbb{Z}$. If $k \geqslant 1$, then H_2 must divide H_1 in $\mathbb{F}_p$, which never happens for two coprime polynomials in $\mathbb{F}_p$. Contradiction. So $k = 0$, thus H_2 divides Q' in $\mathbb{Z}/p^N\mathbb{Z}$. We may write $Q' = H_2Q''$. Thus $Q = H_1H_2Q''$ in $\mathbb{Z}/p^N\mathbb{Z}$, so Q is divisible by H_1H_2. □

2.4. **Witt Vector Ring.** Implied by [SV13], the center ring construction of the Weyl algebra can be characterized by Witt vectors. In this subsection, we interpret the Witt vectors construction in our context and build a connection between it to the centers of the Weyl algebra family, which would be discussed later.

Definition 2.13. Fix a prime p and a non-negative integer n, a Witt vector over a commutative ring R is a vector $(r_0, r_1, r_2, \ldots, r_n)$ with components in R. Define the "ghost component map" from R^{n+1} to R as

$$w_{p^n} : (r_0, r_1, r_2, \ldots, r_n) \mapsto \sum_{i=0}^{n} p^i r_i^{p^{n-i}}.$$

The Witt vector ring, $\mathbb{W}_n(R)$, is the ring with the underlying set of all the Witt vectors over R and addition and multiplication preserving the addition and multiplication of the ghost components in R.

To build a connection between the Witt vector ring and our objects of study, we need the following result.

Proposition 2.14. *For non-negative integer k, we have*

$$\sum_{i=0}^{k} p^i \mathbb{Z}/p^N\mathbb{Z}[\widetilde{a}^{p^{k-i}}, \widetilde{a}^{-p^{k-i}}, \widetilde{b}^{p^{k-i}}, \widetilde{b}^{-p^{k-i}}][q] \simeq \mathbb{W}_k(\mathbb{Z}/p^N\mathbb{Z}[\widetilde{a}, \widetilde{a}^{-1}, \widetilde{b}, \widetilde{b}^{-1}])[q]$$

and

$$\sum_{i=0}^{k} p^i\mathbb{Z}/p^N\mathbb{Z}[\widetilde{a}^{p^{k-i}},\widetilde{b}^{p^{k-i}}][q] \simeq \mathbb{W}_k(\mathbb{Z}/p^N\mathbb{Z}[\widetilde{a},\widetilde{b}])[q].$$

Remark that for subrings $R_1,\dots,R_k$ of R^*, $\sum_{i=1}^{k} R_i$ denotes $R_1+R_2+\cdots+R_k$ as a subring of R^*. In this paper, the ring R^* is taken as either $\mathbb{Z}/p^N\mathbb{Z}[\widetilde{a},\widetilde{b},\widetilde{a}^{-1},\widetilde{b}^{-1}]$ or $\mathbb{Z}/p^N\mathbb{Z}[\widetilde{a},\widetilde{b},\widetilde{a}^{-1},\widetilde{b}^{-1}]/P(q)$ for some polynomial P.

The isomorphism map is exactly the ghost component map. The proof is straightforward calculation, involving Theorem 2.8.

Proof. We show they have the same underlying set and this suffice since they have the same multiplication and addition as in R.

An element x is in the left hand side ring if and only if it is in form of

$$x=\sum_{i,j\in\mathbb{Z}} p^{k-\nu_p(\gcd(i,j))}x_{ij}a^ib^j,$$

where $x_{ij}\in\mathbb{Z}/p^N\mathbb{Z}[q]$. In fact

$$p^{n-\nu_p(\gcd(i,j))}x_{ij}a^ib^j=x_{ij}w_{p^n}(0,\dots,a^{\frac{i}{p^{\nu_p(\gcd(i,j))}}}b^{\frac{j}{p^{\nu_p(\gcd(i,j))}}},\dots,0),$$

where every term in the Witt vector is 0 except for the $\nu_p(\gcd(i,j))$-th term, Thus $p^{n-\nu_p(\gcd(i,j))}x_{ij}a^ib^j$ is in the ghost component ring adjoint q, which is the right hand side. So the ring on the left-hand side is a subring of the ring on the right hand side.

Conversely, we show that the ring on the right hand side is a subring of ring on the left. We only need to prove that

$$Yw_{p^n}(0,\dots,y,\dots,0)$$

is in the ring on the left, where $Y\in\mathbb{Z}/p^N\mathbb{Z}[q]$, $y\in\mathbb{Z}/p^N\mathbb{Z}[a,b]$ and every term in the Witt vector is 0 except for the i-th term. This is sufficient because

$$w_{p^n}(v_0,v_1,\dots,v_n)=\sum_{i=0}^{n} w_{p^n}(0,\dots,0,v_i,0,\dots,0),$$

thus all the elements in the ghost component ring is generated by elements in form of $w_{p^n}(0,\dots,0,v_i,0,\dots,0)$. We then write

$$y=\sum_{j,k} y_{jk}a^jb^k,$$

and

$$\begin{aligned}Yw_{p^n}(0,\dots,y,\dots,0)&=Yp^iy^{p^{n-i}}\\&=Yp^i\left(\sum_{j,k}y_{jk}a^jb^k\right)^{p^{n-i}}\\&=Yp^i\sum_{\sum_{j,k}s_{jk}=p^{n-i}}\binom{p^{n-i}}{\{s_{jk}\}}\prod_{j,k}(y_{jk}a^jb^k)^{s_{jk}}.\end{aligned}$$

By $\binom{p^{n-i}}{\{s_{jk}\}}$ we mean the multinomial coefficients:

$$\frac{p^{n-i}!}{\prod_{j,k} s_{jk}!}.$$

By Theorem 2.8, for $0 \leqslant v \leqslant n-i$, $\binom{p^{n-i}}{\{s_{jk}\}}$ is a multiple of p^v unless all s_{jk} is divisible by $p^{n-i-v+1}$; otherwise, there exists a $s_{j'k'}$ with a non-zero digit on the right of the left-most $(n-i-v+1)$-th digit in its base p expression, thus when all the s_{jk} are added together, there will a carrier in every digit since the left-most $(n-i-v+1)$-th term; there are v of such carriers in total, so the multinomial coefficient is a multiple of p^v, contradiction.

Fix a sequence of $\{s_{jk}\}$, we prove that

$$p^i \binom{p^{n-i}}{\{s_{jk}\}} \prod_{j,k} (y_{jk} a^j b^k)^{s_{jk}}$$

is in the left-hand side ring, thus the summation of all the possible sequences of $\{s_{jk}\}$ is still in the left-hand side ring. Suppose that l is the greatest positive integer such that p^l divides all the s_{jk}. Then by the argument above, p^{n-i-l} divides $\binom{p^{n-i}}{\{s_{jk}\}}$. So

$$p^i \binom{p^{n-i}}{\{s_{jk}\}} \prod_{j,k} (y_{jk} a^j b^k)^{s_{jk}} = p^{n-l} \left(\prod_{j,k} (y_{jk} a^j b^k)^{s_{jk}/p^l} \right)^{p^l} \frac{\binom{p^{n-i}}{\{s_{jk}\}}}{p^{n-i-l}},$$

which is in left-hand side ring since the coefficient is a multiple of p^{n-l} and the mutiplicities of a and b are both multiples of p^l.

Thus the rings on the left and right are the isomorphic, as desired. □

3. The Center of the Weyl Algebra

In this section, we generalize partially the result in [SV13] by considering the generalized Weyl algebra instead of the Weyl algebra. We take h as a polynomial of q so that this fits better into the context of this paper. And h could possibly be a zero divisor. The following result shows that the center of such generalized Weyl algebra preserves the Witt vector construction.

Theorem 3.1. *Let $h \in \mathbb{Z}/p^N\mathbb{Z}[q]$ be a polynomial of q. Then*

$$Z(W^h(R)) \simeq \mathbb{W}_{N-\nu_p(h)} \left(R[\widetilde{a}, \widetilde{b}] \right) [q].$$

In the rest of this section, we prove this result.

3.1. Basic Lemmas.

We need first two simple results regarding the p-valuation of polynomials in $\mathbb{Z}/p^N\mathbb{Z}$.

Proposition 3.2. *We have*

(a) for polynomials $P_1, P_2 \in \mathbb{Z}[x]$,

$$\nu_p(P_1) + \nu_p(P_2) = \nu_p(P_1 P_2);$$

(b) for polynomials $P_1, P_2 \in \mathbb{Z}/p^N\mathbb{Z}[x]$,

$$\min(N, \nu_p(P_1) + \nu_p(P_2)) = \nu_p(P_1 P_2).$$

Proof. (a) Let d_1 be the greatest positive integer that divides P_1 and d_2 be the greatest positive integer that divides P_2, and denote $P_1 = dP_1'$ and $P_2 = d_2P_2'$. Then clearly $\nu_p(P_1) = \nu_p(d_1)+\nu_p(P_1') = \nu_p(d_1)$ since P_1' is primitive (otherwise d won't be the greatest). Similarly $\nu_p(P_2) = \nu_p(d_2)$. On the other hand, $P_1P_2 = d_1d_2(P_1'P_2')$, by Lemma 2.9, $\nu_p(P_1P_2) = \nu_p(d_1d_2) + \nu_p(P_1'P_2') = \nu_p(d_1d_2) = \nu_p(d_1) + \nu_p(d_2)$, as desired.

(b) View P_1, P_2 as polynomials in $\mathbb{Z}[x]$ naturally (although there are different possible polynomials they can take, just choose one of them). Clearly the p-valuation of P_i in $\mathbb{Z}/p^N\mathbb{Z}[x]$ is the minimum of $\nu_p(P_i)$ in $\mathbb{Z}[x]$ and N. Apply (a), the result is obvious. □

This result's direct corollary is as follows.

Corollary 3.3. *Polynomials $P_1, \cdots, P_k \in \mathbb{Z}/p^N\mathbb{Z}[x]$, then $\prod_{i=1}^k P_i = 0$ if and only if $\sum_{i=1}^k \nu_p(P_i) \geqslant N$.*

Proof. Apply Proposition 3.2 repeatedly, we know

$$\min\left(N, \sum_{i=1}^k \nu_p(P_i)\right) = \nu_p(0) = N.$$

Thus $\sum_{i=1}^k \nu_p(P_i) \geqslant N$, as desired. □

3.2. **Proof of Theorem 3.1.** Now we proceed with the proof of the Theorem 3.1.

By Proposition 2.14, we only need to show that

$$Z(W^h(R)/P(q)) \simeq \sum_{i=0}^{N-\nu_p(h)} p^i\mathbb{Z}/p^N\mathbb{Z}[\widetilde{a}^{p^{N-\nu_p(h)-i}}, \widetilde{b}^{p^{N-\nu_p(h)-i}}][q].$$

The isomorphism map is

$$\phi : \sum_{i,j} z_{ij}a^ib^j \mapsto \sum_{i,j} z_{ij}\widetilde{a}^i\widetilde{b}^j.$$

Step 1. we first show that ϕ is a bijection.

By Lemma 2.5, z is in the center of $W^h(R)$ if and only if it commutes with both a and b. By Proposition 2.4, we may write z as

$$z = \sum_{i,j\in\mathbb{Z}_{\geqslant 0}} z_{ij}a^ib^j.$$

We have

$$az = \sum_{i,j\in\mathbb{Z}_{\geqslant 0}} z_{ij}a^{i+1}b^j$$

and, by Lemma 2.6,

$$za = \sum_{i,j\in\mathbb{Z}_{\geqslant 0}} z_{ij}a^{i+1}b^j + \sum_{i,j\in\mathbb{Z}_{\geqslant 0}} jhz_{ij}a^ib^{j-1}.$$

So z commutes with a is equivalent to

$$\sum_{i,j\in\mathbb{Z}_{\geqslant 0}} jhz_{ij}a^ib^{j-1} = 0.$$

By Proposition 2.4, this is zero if and only if $jhz_{ij} = 0$ for all i, j.

By Corollary 3.3, we know that $\nu_p(z_{ij}) + \nu_p(j) \geqslant N - \nu_p(h)$. Symmetrically, $\nu_p(z_{ij}) + \nu_p(i) \geqslant N - \nu_p(h)$. Thus z is in the center if and only if z_{ij} is a multiple of $p^{N-\nu_p(h)-\min(\nu_p(i),\nu_p(j))}$ for every pair of i, j. This implies that z is in the center if and only if

$$\phi(z) \in \sum_{i=1}^{N-\nu_p(h)} p^i \mathbb{Z}/p^N\mathbb{Z}[\widetilde{a}^{p^{N-\nu_p(h)-i}}, \widetilde{b}^{p^{N-\nu_p(h)-i}}][q].$$

So ϕ is a well-defined map and so is

$$\phi^{-1} : \sum_{i,j} z_{ij}\widetilde{a}^i\widetilde{b}^j \mapsto \sum_{i,j} z_{ij}a^ib^j.$$

Therefore ϕ is a bijection.

Step 2. we then show that ϕ preserves the addition, multiplication, and multiplicative identity. By definition $\phi(1) = 1$ and

$$\phi\left(\sum_{i,j} z_{ij}a^ib^j\right) + \phi\left(\sum_{i,j} z'_{ij}a^ib^j\right) = \sum_{i,j}(z_{ij} + z'_{ij})\widetilde{a}^i\widetilde{b}^j = \phi\left(\sum_{i,j}(z_{ij} + z'_{ij})a^ib^j\right).$$

Additionally, note that

$$z_{ij}a^ib^j z'_{kl}a^kb^l = z_{ij}z'_{kl}a^{i+k}b^{j+l}$$

since $z'_{kl}a^k$ is in the center, thus commutes with b^j. So

$$\begin{aligned}
\phi\left(\sum_{i,j} z_{ij}a^ib^j\right) \cdot \phi\left(\sum_{i,j} z'_{ij}a^ib^j\right) &= \left(\sum_{i,j} z_{ij}\widetilde{a}^i\widetilde{b}^j\right) \cdot \left(\sum_{i,j} z'_{ij}\widetilde{a}^i\widetilde{b}^j\right) \\
&= \sum_{i,j,k,l} z_{ij}z'_{kl}\widetilde{a}^{i+k}\widetilde{b}^{j+l} \\
&= \phi\left(\sum_{i,j,k,l} z_{ij}z'_{kl}a^{i+k}b^{j+l}\right) \\
&= \phi\left(\sum_{i,j,k,l} z_{ij}a^ib^j z'_{kl}a^kb^l\right) \\
&= \phi\left(\left(\sum_{i,j} z_{ij}a^ib^j\right) \cdot \left(\sum_{i,j} z'_{ij}a^ib^j\right)\right)
\end{aligned}$$

Thus ϕ is indeed an isomorphism.

4. General Polynomials

In this section we consider the center of the q-Weyl algebra, where q is a root of some polynomial and p is a odd prime. Namely, we consider the center of $W_q(\mathbb{Z}/p^N\mathbb{Z})/P(q)$ where P is a integer coefficient polynomial.

The main theorem can be formulated as Theorem 4.2, which requires some additional definitions.

Definition 4.1. For a polynomial $P \in \mathbb{Z}[q]$. Define $M(P)$ to be the smallest positive integer such that $q^{M(P)} - 1$ is divisible by P in $\mathbb{F}_p[q]$. And define $l(P)$ to be the greatest positive integer such that $q^{M(P)} - 1$ is divided by P in $\mathbb{Z}/p^{l(P)}\mathbb{Z}$.

Theorem 4.2. *When monic $P \in \mathbb{Z}/p^N\mathbb{Z}[q]$ is irreducible in $\mathbb{F}_p$, we have*

$$Z(W_q(R)/P(q)) \simeq \mathbb{W}_{N-l(P)}(R[\widetilde{a}^{M(P)}, \widetilde{a}^{-M(P)}, \widetilde{b}^{M(P)}, \widetilde{b}^{-M(P)}])[q]/P(q).$$

We use the rest of this section to prove this theorem. In subsection 4.1, we rephrase the question into a problem about the factorization in $R[q]$. In subsection 4.2, we present some lemmas for preparation. In subsection 4.3, we present the complete proof.

4.1. **Rephrase the problem.** First, we shall rephrase the problem by the following Theorem 4.3.

Define $W_q(R)^{(i)}$ the free algebra generated by a^i and b^i over ring $R = \mathbb{Z}/p^N\mathbb{Z}$ subject to relation $ba = qab$.

Theorem 4.3. *The center of $W_q(\mathbb{Z}/p^N\mathbb{Z})/P(q)$ is*

$$\sum_{i=0}^{\infty} S_{P,p^N,i} W_q(R)^{(i)}[q],$$

where $S_{P,p^N,i}$ is the set consisting of all the polynomials H such that P divides $H(x^i - 1)$ in $\mathbb{Z}/p^N\mathbb{Z}[q]$ and $S_{P,p^N,i}W_q(R)^{(i)}[q] := \sum_{H \in S_{P,p^N,i}} HW_q(R)^{(i)}[q]$.

After this theorem is established, we only need to consider sets $S_{P,p^N,i}$ to find the center, avoiding all the computations in non-commutative rings.

To prove this theorem, we start by proving a lemma, which will also be used in the future.

Lemma 4.4. *In $\mathbb{Z}/p^N\mathbb{Z}[q]$, for positive integers α and β, the ideal generated by $q^\alpha - 1$ and $q^\beta - 1$ is the principal ideal generated by $q^{\gcd(\alpha,\beta)} - 1$. Namely,*

$$(q^\alpha - 1, q^\beta - 1) = (q^{\gcd(\alpha,\beta)} - 1).$$

Proof. By Bezout's theorem, there exists $k, l \in \mathbb{Z}$ such that $k\alpha - l\beta = \gcd(\alpha, \beta)$; denote the greatest common divisor by d. Let I be the ideal generated by $q^\alpha - 1$ and $q^\beta - 1$. Since $q^\alpha - 1 \in I$, we have $q^{k\alpha} - 1 \in I$; similarly $q^{l\beta} - 1 \in I$, then $q^{l\beta+d} - q^d \in I$. So $q^{k\alpha} - 1 - (q^{l\beta+1} - q^d) = q^d - 1 \in I$. So $(q^d - 1) \subset I$. On the other hand, $q^d - 1 | q^\alpha - 1$ and $q^\beta - 1$ (in $\mathbb{Z}[q]$), so $I \subset (q^d - 1)$. Thus $I = (q^d - 1)$. □

Corollary 4.5. *We have*

$$S_{P,p^n,i} \cap S_{P,p^n,j} = S_{P,p^n,\gcd(i,j)}.$$

Proof. Polynomial $H \in S_{P,p^n,i} \cap S_{P,p^n,j}$ if and only if P divides both $H(q^i - 1)$ and $H(q^j - 1)$, which is equivalent to

$$P \in (H(q^i - 1), H(q^j - 1)).$$

By Lemma 4.4, we have

$$\begin{aligned}(H(q^i - 1), H(q^j - 1)) &= (H(q))(q^i - 1, q^j - 1) \\ &= (H(q))(q^{\gcd(i,j)} - 1) \\ &= (H(q)(q^{\gcd(i,j)} - 1)).\end{aligned}$$

Thus $H \in S_{P,p^n,i} \cap S_{P,p^n,j}$ is equivalent to that P divides $H(q)(q^{\gcd(i,j)} - 1)$, which is equivalent to $H \in S_{P,p^n,\gcd(i,j)}$. So $S_{P,p^n,i} \cap S_{P,p^n,j} = S_{P,p^n,\gcd(i,j)}$. □

Now we are ready to prove Theorem 4.3

The Proof of Theorem 4.3. By Lemma 2.5, z is in the center ring of $W_q(\mathbb{Z}/p^N\mathbb{Z})/P(q)$ if and only if it commutes with both a and b. By Proposition 2.4, we may write

$$z = \sum_{i\in\mathbb{Z}_{\geqslant 0}, j\in\mathbb{Z}} z_{ij}a^i b^j.$$

By Lemma 2.6,

$$az = \sum_{i\in\mathbb{Z}_{\geqslant 0}, j\in\mathbb{Z}} z_{ij}a^{i+1} b^j$$

and

$$za = \sum_{i\in\mathbb{Z}_{\geqslant 0}, j\in\mathbb{Z}} q^j z_{ij}a^{i+1} b^j.$$

Thus z commutes with a if and only if

$$\sum_{i\in\mathbb{Z}_{\geqslant 0}, j\in\mathbb{Z}} (q^j - 1) z_{ij}a^{i+1} b^j = 0.$$

By Proposition 2.4, the equation above holds if and only if $(q^j - 1)z_{ij} = 0$ in ring $\mathbb{Z}/p^N\mathbb{Z}[q]/P(q)$. Thus it is equivalent to that $P(q)$ divides $(q^j - 1)z_{ij}$ in $\mathbb{Z}/p^N\mathbb{Z}[q]$, equivalent to $z_{ij} \in S_{P,p^n,j}$.

Symmetrically, z commutes with b if and only if $z_{ij} \in S_{P,p^n,i}$. So z is in the center if and only if $z_{ij} \in S_{P,p^n,i} \cap S_{P,p^n,j} = S_{P,p^n,\gcd(i,j)}$, by Corollary 4.5. In other word, the center ring is

$$\sum_{i=0}^{\infty} S_{P,p^N,i} W_q(R)^{(i)}[q],$$

as desired. □

4.2. **Preparations.** We build a system to investigate the structure of $S_{P,p^n,i}$ by importing a series of notions.

4.2.1. *The notion of d_n.*

Theorem 4.6. *Let P be monic and irreducible modulo p. Let $1 \leqslant d_i \leqslant N$ be the largest integer from 0 to N such that P divides $q^i - 1$ in $\mathbb{Z}/p^{d_i}\mathbb{Z}[q]$. Then*

$$Z(W_q(R)/P(q)) = \sum_{i=0}^{\infty} p^{N-d_i} W_q(R)^{(i)}[q].$$

By Theorem 4.3, it is sufficient to show that $S_{P,p^N,i} = \left(p^{N-d_i}\right)$ to prove this theorem.

We start by an easy lemma.

Lemma 4.7. *When P is monic and irreducible in $\mathbb{F}_p$. We can write $q^i - 1 = PK + L$ for some $K, L \in \mathbb{Z}[q]$ with $\deg L < \deg P$. Then $d_i = \nu_p(L)$.*

Proof. Apply the Euclidean division to $q^i - 1$ and P, we may write $q^i - 1 = PK + L$ where L's degree is less than that of P. Now we only need to prove $d_i = \nu_p(L)$.

Consider that $q^i - 1 = PK + p^{\nu_p(L)} \cdot (L/p^{\nu_p(L)}) \equiv PK \pmod{p^{\nu_p(L)}}$. So $d_i \geqslant \nu_p(L)$.

Denote $L' = L/p^{\nu_p(L)}$, then L' does no divide p, equivalent to $L' \neq 0$ in $\mathbb{F}_p$.

If P divides $q^i - 1$ in $\mathbb{Z}/p^{\nu_p(L)+1}\mathbb{Z}$, P divides $L = p^{\nu_p(L)}L'$ in $\mathbb{Z}/p^{\nu_p(L)+1}\mathbb{Z}$. We may write $PK' = p^{\nu_p(L)}L'$ in $\mathbb{Z}/p^{\nu_p(L)+1}\mathbb{Z}$. By Proposition 3.2, $\nu_p(P) + \nu_p(K') \geqslant \nu_p(L)$. Since P is monic, $\nu_p(P) = 0$, so $\nu_p(K') \geqslant \nu_p(L)$. We may write $K' =$

$p^{\nu_p(L)}K''$, then $p^{\nu_p(L)}PK'' = p^{\nu_p(L)}L'$ in $\mathbb{Z}/p^{\nu_p(L)+1}\mathbb{Z}$, implying $PK'' = L'$ in $\mathbb{F}_p$. Since P is a monic prime polynomial and divides L', and L' has degree less than that of P, we must have $L' = 0$ in $\mathbb{F}_p$, contradicting that L' is not divided by p. So P doesn't divide $q^i - 1$ in $\mathbb{Z}/p^{\nu_p(L)+1}\mathbb{Z}$. So $d_i < \nu_p(L) + 1$.

So $d_i = \nu_p(L)$, as desired. □

Now we are ready to prove Theorem 4.6.

Proof of Theorem 4.6. Consider an element $z_i \in S_{P,p^n,i}$, then $z_i(q^i-1)$ is a multiple of $P(q)$. We may remove any multiple of P from z_i, the result remains the same (because we are considering in a ring where $P(q) = 0$). Since P is monic, we may assume that $\deg z_i < \deg P$.

It's sufficient to prove that this is equivalent to that p^{N-d_i} divides z_i. By Lemma 4.7, we may write $q^i - 1 = P(q)K(q) + L(q)$ and $d_i = \nu_p(L)$. Then we know that $z_iL(q)$ is a multiple of $P(q)$. By Proposition 2.11, there exits k such that P divides z_i in $\mathbb{Z}/p^k\mathbb{Z}$ and P divides L in $\mathbb{Z}/p^{N-k}\mathbb{Z}$. By the definition of d_i, we know that $N-k$ can and can only take integer values that no greater than d_i. Thus $z_i \in S_{P,p^N,i}$ is equivalent to that z_i is a multiple of P in $\mathbb{Z}/p^{N-d_i}\mathbb{Z}$. By Lemma 4.7, since $\deg z_i < \deg P$, this is equivalent to $\nu_p(z_i) \geqslant N - d_i$, meaning p^{N-d_i} divides z_i, as desired. □

4.2.2. *The notion of δ and its properties.* Now we introduce δ with various properties to help us better understand d_n.

Definition 4.8. Define $K_i = \{k \in \mathbb{Z}_+ | d_k \geqslant i\}$. Let $\delta_{p,P}(i)$ be the smallest element in K_i. Call $\delta_{p,P}(i)$ the i-th generator of p and P.

The following Proposition 4.10 completely solves the value of d_n by the generators. To prove it, we need a basic lemma.

Lemma 4.9. *If $k_1, k_2 \in K_i$, then $\gcd(k_1, k_2) \in K_i$.*

Proof. If $k_1, k_2 \in K_i$, then P divides both $q^{k_1} - 1$ and $q^{k_2} - 1$ in $\mathbb{Z}/p^i\mathbb{Z}[q]$. Thus

$$P \in (q^{k_1} - 1, q^{k_2} - 1) = (q^{\gcd(k_1,k_2)} - 1),$$

by Lemma 4.4. Thus P divides $q^{\gcd(k_1,k_2)}-1$ in $\mathbb{Z}/p^i\mathbb{Z}[q]$, implying $\gcd(k_1, k_2) \in K_i$, as desired. □

Now we are ready to introduce the main result of the generators.

Proposition 4.10. *For a positive integer i, K_i consists of exactly all the multiples of the i-th generator.*

Proof. Since $q^i - 1$ divides $q^{si} - 1$ for all positive integer s, all the multiples of the i-th generator is in K_i.

If there exists $k' \in K_i$ which is not a multiple of $\delta_{p,P}(i)$, by Lemma 4.9, $\gcd(k', \delta_{p,P}(i)) \in K_i$ which is smaller than $\delta_{p,P}(i)$. contradiction.

So the multiples of the i-th generator are all the elements, as desired. □

Corollary 4.11. *For any $1 \leqslant i \leqslant j \leqslant N$, $\delta_{p,P}(j)$ is a multiple of $\delta_{p,P}(i)$.*

It's obvious by definition that $M(P)$ and $l(P)$ are non-negative integers such that $M(P) = \delta_{p,P}(1) = \cdots = \delta_{p,P}(l(P))$ while $\delta_{p,P}(l(P) + 1) \neq M(P)$.

In the following discussion, for the sake of simplicity, $M(P)$ and $l(P)$ will be written as M and l, since P is fixed.

The key claim for the proof of Theorem 4.2 is as follows.

When p is an odd prime, for non-negative integer k, we have $\delta_{p,P}(l+k) = Mp^k$.

Consider the ring $\mathbb{R}[q]/P(q)$ as a $\deg P$ dimensional vector space, and the multiplication by q acts as a linear operator, denoted $\mathcal{M}(q)$. We may choose $\{1, q, \ldots, q^{\deg P-1}\}$ as a basis and clearly $\mathcal{M}(q)$ acts as a $\deg P$ by $\deg P$ square matrix with integer entries. Now we prove the generalized "LTE Lemma" for $\mathcal{M}(q)$ as follows.

Lemma 4.12. *For any $p > 2$, let k and i be positive integers such that $\nu_p(\mathcal{M}(q)^k - 1) \geqslant 1$, then*

$$\nu_p(\mathcal{M}(q)^{p^i k} - 1) = \nu_p(\mathcal{M}(q)^k - 1) + i.$$

Proof. Denote $v = \nu_p(\mathcal{M}(q)^k - 1)$ and $\mathcal{M}(q)^k - 1 = p^v \mathcal{M}'$. Then $\mathcal{M}'$ is not a multiple of p.

Clearly we only need to prove case $i = 1$, and then the result follows immediately from induction. It's sufficient to prove that

$$\nu_p(\mathcal{M}(q)^{pk} - 1) = v + 1.$$

In fact,

$$\begin{aligned}\mathcal{M}(q)^{pk} - 1 &= (p^v\mathcal{M}' + 1)^p - 1 \\ &= \sum_{j=1}^{p} \binom{p}{j} p^{vj} (\mathcal{M}')^j \\ &= p^{v+1}\mathcal{M}' + \sum_{j=2}^{p} \binom{p}{j} p^{vj} (\mathcal{M}')^j.\end{aligned}$$

Since $\nu_p(p^{v+1}\mathcal{M}') = v + 1$, now we only need to prove that $\nu_p\left(\binom{p}{j} p^{vj}(\mathcal{M}')^j\right) > v + 1$ when $j \geqslant 2$. When $j = 2$, since p is odd, $\nu_p\left(\binom{p}{j}\right) \geqslant 1$ by Theorem 2.8, thus

$$\nu_p\left(\binom{p}{2} p^{2v} (\mathcal{M}')^2\right) \geqslant 1 + 2v > v + 1.$$

When $j \geqslant 3$, we have

$$\nu_p\left(\binom{p}{j} p^{jv} (\mathcal{M}')^j\right) \geqslant jv \geqslant 3v > v + 1.$$

Therefore

$$\nu_p(\mathcal{M}(q)^{pk} - 1) = v + 1,$$

as desired. □

Proof of Lemma 4.2.2. We prove by induction on k.

For the base case, by the definition of l and M, we know that P divides $x^M - 1$ in $\mathbb{Z}/p^l\mathbb{Z}$ but not in $\mathbb{Z}/p^{l+1}\mathbb{Z}$. By Lemma 4.7, this implies that the remainder of $q^M - 1$ divided by P has p-valuation l. In other word, $\nu_p(\mathcal{M}(q)^M - 1) = l$ in $\mathbb{Z}[q]$. Apply Lemma 4.12, $\nu_p(\mathcal{M}(q)^{pM} - 1) = l + 1$, and $\mathcal{M}(q)^{pM} - 1$ acts as the multiplication by $q^{pM} - 1$, and in particular, acts as the multiplication by the remainder L of $q^{pM} - 1$ divided by P in $\mathbb{Z}[q]/P(q)$. Thus the remainder must be a mutltiple of p^{l+1}, by Lemma 4.7. So $pM \in K_{l+1}$, implying that pM is a multiple of $\delta_{p,P}(l+1)$, by Proposition 4.10. By Corollary 4.11, $\delta_{p,P}(l+1)$ is a multiple of M and doesn't equal to M; since it's also a divisor of pM, it has to be pM.

For the general cases, the process is essentially the same. By Lemma 4.12, $\nu_p(\mathcal{M}(q)^{p^k M}-1)=l+k$, thus $p^kM\in K_{l+k}$. So the $(l+k)$-th generator is a divisor of p^kM and a multiple of the $(l+k-1)$-th divisor, $p^{k-1}M$, by inductive assumption. Since $\nu_p(\mathcal{M}(q)^{p^{k-1}M}-1)=l+k-1$, $p^{k-1}M$ is not in K_{l+k}; thus the $(l+k)$-th generator can only be p^kM. Induction is completed. □

Now we have enough knowledge to explain the value of d_n even further as follows.

Theorem 4.13. *If n is not a multiple of M, then $d_n=0$; if n is a multiple of M, then $d_n=\nu_p(n/M)+l$.*

Proof. When n is not a multiple of M, then $n\notin K_1$ since n is not a multiple of $\delta_{p,P}(1)$, by Proposition 4.10. So $d_n<1$, thus $d_n=0$.

When n is a multiple of M, suppose that $v=\nu_p(n/M)$. Then M is a multiple of $p^vM=\delta_{p,P}(l+v)$ and M is not a multiple of $p^{v+1}M=\delta_{p,P}(l+v)$, by Lemma 4.2.2. Thus n is in K_{l+v} but not K_{l+v+1}, by Proposition 4.10. So $l+v\leqslant d_n<l+v+1$, implying that $d_n=l+v$. □

Now the value of d_n is completely described, we may prove Theorem 4.2.

4.3. Proof of Theorem 4.2.

Proof of Theorem 4.2. By Proposition 2.14, we only need to show that

$$Z(W_q(R)/P(q))\simeq\sum_{i=1}^{N-l}p^iR[\widetilde{a}^{Mp^{N-l-i}},\widetilde{a}^{-Mp^{N-l-i}},\widetilde{b}^{Mp^{N-l-i}},\widetilde{b}^{-Mp^{N-l-i}}][q].$$

The isomorphism map is

$$\phi:\sum_{i,j}z_{ij}a^ib^j\mapsto\sum_{i,j}z_{ij}\widetilde{a}^i\widetilde{b}^j.$$

Step 1. We first show that ϕ is a bijection.

By Theorem 4.13, when i is not a multiple of M, $d_i=0$, and thus the ring

$$p^{N-d_i}W_q(R)^{(i)}[q]=p^NW_q(R)^{(i)}[q]$$

is 0 as a subring of $\mathbb{Z}/p^N\mathbb{Z}[a,b][q]$.

On the other hand, when i is a multiple of M, suppose that $i=Mp^vi'$ where i' is coprime to p. Then ring

$$p^{N-d_i}W_q(R)^{(i)}[q]=p^{N-v-l}W_q(R)^{(p^vMi')}[q]$$

is apparently a subring of

$$p^{N-v-l}W_q(R)^{(p^vM)}[q]=p^{N-d_{\delta_{p,P}}(p^vM)}W_q(R)^{(p^vM)}[q].$$

By Theorem 4.6, we have

$$\begin{aligned}\sum_{i=0}^{\infty}p^{N-d_i}W_q(R)^{(i)}[q]&=\left(\sum_{M\nmid i}p^{N-d_i}W_q(R)^{(i)}[q]\right)+\left(\sum_{M\mid i}p^{N-d_i}W_q(R)^{(i)}[q]\right)\\&=0+\sum_{v=1}^{N-l}\sum_{i,\ \text{where }\nu_p(i/M)=v}p^{N-d_i}W_q(R)^{(i)}[q]\\&=\sum_{v=1}^{N-l}p^{N-l-v}W_q(R)^{(p^vM)}[q].\end{aligned}$$

For the same reason as the proof of 3.1 and Proposition 2.14, ϕ is a bijection from

$$\sum_{v=0}^{N-l} p^{N-l-v} W_q(R)^{(Mp^v)}[q]$$

to

$$\sum_{i=1}^{N-l} p^i \mathbb{Z}/p^N\mathbb{Z}[\widetilde{a}^{Mp^{N-l-i}}, \widetilde{a}^{-Mp^{N-l-i}}, \widetilde{b}^{Mp^{N-l-i}}, \widetilde{b}^{-Mp^{N-l-i}}][q].$$

Step 2. we then show that ϕ preserves addition, multiplication, and multiplicative identity.

Following the same procedure as the proof of Theorem 3.1, we only need to show that

$$z_{ij}a^ib^j z'_{kl}a^kb^l = z_{ij}z'_{kl}a^{i+k}b^{j+l},$$

when $\sum z_{ij}a^ib^j$ and $\sum z'_{ij}a^ib^j$ are in the center, which implies z'_{kl} is a multiple of p^{N-d_k}. This means that $z'_{kl}a^k$ is in the center, so

$$z_{ij}a^ib^j z'_{kl}a^kb^l = z_{ij}a^ib^j z'_{kl}a^kb^l = z_{ij}a^i z'_{kl}a^kb^jb^l = z_{ij}z'_{kl}a^{i+k}b^{j+l}.$$

Combine both steps, we proved that ϕ is an isomorphism. $\square$

4.3.1. *Postscipt.* We would like to remark some properties about $M(P)$.

Proposition 4.14. *$M(P)$ is a divisor of $p^{\deg P} - 1$.*

Proof. $M(P)$ is by definition the smallest k such that P divides $x^k - 1$ in $\mathbb{F}_p$. Consider the field extension $\mathbb{F}_p(\zeta)$ where ζ is a root of P. Then k is the order of ζ in $\mathbb{F}_p(\zeta)$. Then $\mathbb{F}_p(\zeta) \simeq \mathbb{F}_p[x]/P(x)$ as a multiplicative group is a subgroup of K with underlying set

$$\left\{a_0 + a_1\zeta + \cdots + a_{\deg P-1}\zeta^{\deg P-1} | (a_0, \ldots, a_{\deg P-1} \in \mathbb{F}_p^{\deg P} \backslash \{0\}\right\}$$

and canonical multiplication, with order $p^{\deg P} - 1$. Thus the cardinality of $\mathbb{F}_p(\zeta)$ is a divisor of $p^{\deg P} - 1$, and the order of ζ is a divisor of $\mathbb{F}_p(\zeta)$. So k is a divisor of $p^{\deg P} - 1$. $\square$

This is a direct result from the Galois theory in finite field. Its simple corollary is as follows.

Corollary 4.15. *$M(P)$ is never a multiple of p, as long as P is not a constant.*

4.4. **When P has no double root.** When P has no double root, we may also compute the center $W_q(R)/P(q)$. However, the Witt vector construction is not found here. The proof uses Proposition 2.12.

Lemma 4.16. *When P has no double root in $\mathbb{F}_p$, we may write $P = \prod_{i=1}^k P_i \pmod{p^N}$ where $P_i \in \mathbb{Z}/p^N\mathbb{Z}$ are distinct irreducible polynomials modulo p.*

Proof. Induct on k. When $k = 1$, the result is obvious since $\mathbb{F}_p$ is a unique factorization domain and P has no double roots, so all the prime factors of P are irreducible and distinct.

For the general cases, suppose that we can write $P \equiv \prod_{i=1}^k Q_i \pmod{p^{N-1}}$ where Q_i are distinct and irreducible in $\mathbb{F}_p$. Suppose that $T \in \mathbb{Z}[q]$ is a polynomial satisfying

$$P - \prod_{i=1}^k Q_i \equiv p^{N-1}T \pmod{p^N}.$$

Then by Bezout's Theorem, since

$$\gcd_{i=1}^{k}(P/Q_i) = 1$$

in $\mathbb{F}_p$, there exists polynomial $B_1, \ldots, B_k \in \mathbb{Z}[q]$ such that

$$\sum_{i=1}^{k} B_i \frac{P}{Q_i} \equiv 1 \pmod{p}.$$

Now consider (since $N \geqslant 2$, $2N-2 \geqslant N$)

$$\begin{aligned}\prod_{i=1}^{k}(Q_i + p^{N-1}B_iT) &\equiv \prod_{i=1}^{k} Q_i + p^{N-1}\sum_{i=1}^{k} B_iT\frac{P}{Q_i} + p^{2N-2}\Theta \\ &\equiv \prod_{i=1}^{k} Q_i + p^{N-1}T \\ &\equiv P \pmod{p^N},\end{aligned}$$

where Θ is some integer coefficient polynomial of q. Let $Q_i' = Q_i + p^{N-1}B_iT$, we know that $P = \prod_{i=1}^{k} Q_i'$ in $\mathbb{Z}/p^N\mathbb{Z}$, where Q_i are distinct and irreducible modulo p since they are congruent to Q modulo p^{N-1}. Induction is completed. □

Proposition 4.17. *Polynomials $Q_1, Q_2, \ldots, Q_k \in \mathbb{Z}[q]$ are pairwisely distinct and all irreducible in $\mathbb{F}_p[q]$. If Q is divided by Q_i in $\mathbb{Z}/p^N\mathbb{Z}[q]$ for every $1 \leqslant i \leqslant k$, then Q is divided by $\prod_{i=1}^{k} Q_i$ in $\mathbb{Z}/p^N\mathbb{Z}[q]$.*

Proof. Induct on k. When $k = 2$, the result is implied by Proposition 2.12. For general cases, by inductive assumption, we know that both $\prod_{i=1}^{k-1} Q_i$ and Q_k divide P; they are coprime and Q_k is irreducible in $\mathbb{F}_p$. By Proposition 2.12, $Q_k\prod_{i=1}^{k-1} Q_i = \prod_{i=1}^{k} Q_i$ divides P. Induction is completed. □

Theorem 4.18.

$$Z(W_q(\mathbb{Z}/p^N\mathbb{Z})/Q(q)) = \bigcap_{i=1}^{k} \widetilde{Z}(W_q(\mathbb{Z}/p^N\mathbb{Z})/P_i(q)),$$

where $\widetilde{Z}(W_q(\mathbb{Z}/p^N\mathbb{Z})/P_i(q))$ consists of all the elements that are in $Z(W_q(\mathbb{Z}/p^N\mathbb{Z})/P_i(q)$ modulo P_i.

Proof. By Theorem 4.3, the center is isomorphic to

$$\sum_{i=0}^{\infty} S_{P,p^n,i}W_q(R)^{(i)}[q].$$

By definition $S_{P,p^N,i}$ consists of all the polynomial Q' such that P divides $Q'(x^i-1)$, which is equivalent to, by Proposition 4.17, that P_j divides $Q'(x^i-1)$ for all j. Thus $S_{P,p^N,i} = \bigcap_{j=1}^{k} S_{P_i,p^N,i}$. And this implies the result. □

5. Roots of Unity

We dedicate this section to thoroughly answer Roman Bezrukavnikov's question. Namely, the case when q is a p^n-th root of unity. We solve the center of $W_q(\mathbb{Z}/p^N\mathbb{Z})/(q^{p^n}-1)$ for P both being $q^{p^N}-1$ and $\Phi_{p^n}(q)$.

Theorem 5.1. *The center of $W_q(\mathbb{Z}/p^N\mathbb{Z})/(q^{p^n}-1)$ is*

$$\sum_{i=0}^{n}\frac{q^{p^n}-1}{q^{p^i}-1}W_q(R)^{(p^i)}[q].$$

Theorem 5.2. *The center of $W_q(\mathbb{Z}/p^N\mathbb{Z})/(\Phi_{p^n}(q))$ is*

$$\left(\sum_{i=0}^{n-1}p^{N-1}\cdot\frac{\Phi_{p^n}(q)-p}{q^{p^i}-1}W_q(R)^{(p^i)}[q]\right)+W_q(R)^{(p^n)}[q].$$

Proof of Theorem 5.1. Let $P(q)=x^{p^n}-1$.

Consider that $z_{ij}\in S_{p,P,k}$ if and only if

$$(z_{ij}(q^k-1))\in(q^{p^n}-1)$$

as ideals of $\mathbb{Z}/p^N\mathbb{Z}[q]$ for all i,j. By Lemma 4.4, we have

$$(z_{ij}(q^{\gcd(k,p^n)}-1))=(z_{ij}(q^k-1),z_{ij}(q^{p^n}-1))\subset(q^{p^n}-1).$$

Denote $\gcd(k,p^n)=p^t$. Note that $\frac{q^{p^n}-1}{q^{p^t}-1}=1+q^{p^t}+q^{2p^t}+\cdots+q^{p^n-p^t}$ is a monic polynomial. And if $(z_{ij}(q^{\gcd(k,p^n)}-1))\in(q^{p^n}-1)$, we have

$$((z_{ij}-Q(q)(\frac{q^{p^n}-1}{q^{p^t}-1})(q^{p^t}-1))\in(q^{p^n}-1)$$

for any polynomial Q. So we can apply Euclidean division to z_{ij} divided by $\frac{q^{p^n}-1}{q^{p^t}-1}$ and assume that z_{ij} is a polynomial of q with degree less than p^n-p^t. Then $z_{ij}(q^t-1)$ has degree less than p^n. Since it's in $(q^{p^n}-1)$, and $q^{p^n}-1$ is monic, it must be 0. It's easy to see that monic $q^{p^t}-1$ is not a zero divisor, so z_{ij} must be zero. So z_{ij} must be a multiple of $\frac{q^{p^n}-1}{q^{p^t}-1}$.

Conversely, if z_{ij} is a multiple of $\frac{q^{p^n}-1}{q^{p^t}-1}$, $z_{ij}(q^k-1)$ is clearly a multiple of $q^{p^n}-1$. So $S_{p,P,k}$ consists of all the polynomial that is multiple of $\frac{q^{p^n}-1}{q^{\gcd(k,p^n)}-1}$. By Theorem 4.3, the center is

$$\sum_{i=0}^{n}\frac{q^{p^n}-1}{q^{p^i}-1}W_q(R)^{(p^i)}[q],$$

as desired. □

Proof of Theorem 5.2. Let $P=\Phi_{p^n}$. Similar to the proof of Theorem 5.1, We only need to consider z such that

$$(z(q^k-1))\in(\Phi_{p^n}(q))$$

as ideals of $\mathbb{Z}/p^N\mathbb{Z}[q]$. Thus

$$(z(q^k-1),z(q^{p^n}-1))\in(z(q^k-1),z\cdot\Phi_{p^n}(q))\in(\Phi_{p^n}(q)).$$

By Lemma 4.4,

$$(z(q^k-1),z(q^{p^n}-1))=(z)(q^{\gcd(p^n,k)}-1).$$

Denote $\gcd(k, p^n) = p^t$ $(t \leqslant n)$. Then

$$I = (z)(q^{p^t} - 1, \Phi_{p^n}(q)) \in (\Phi_{p^n}(q)).$$

CASE 1. When $t < n$, note that $\frac{\Phi_{p^n}(q)-p}{q^{p^t}-1} \in \mathbb{Z}[q]$. We have

$$p = \Phi_{p^n}(q) - (q^{p^t} - 1) \cdot \frac{\Phi_{p^n}(q) - p}{q^{p^t} - 1} \in (q^{p^t} - 1, \Phi_{p^n}(q)).$$

So

$$(z)(p) \in (\Phi_{p^n}(q)).$$

Now consider z as a polynomial in $\mathbb{Z}[q]$ in a natural way, then we have

$$pz = H_1\Phi_{p^n} + H_2 p^N$$

for some $H_1, H_2 \in \mathbb{Z}[q]$. This implies $p|H_1$; we may write $H_1 = pH_3$, then we have $z = H_3\Phi_{p^n} + H_2 p^{N-1}$, so $z \in (\Phi_{p^n}, p^{N-1})$ as an ideal of $\mathbb{Z}/p^N\mathbb{Z}[q]$. We need to satisfy

$$(z)(q^{p^t} - 1) = \left(H_3\Phi_{p^n} + H_2 p^{N-1}\right)(q^{p^t} - 1) \in (\Phi_{p^n}(q))$$

which is equivalent to

$$(H_2 p^{N-1})(q^{p^t} - 1) = (p^{N-1})(H_2)(q^{p^t} - 1) \in (\Phi_{p^n}(q)).$$

Therefore

$$(H_2)(q^{p^t} - 1) \in (\Phi_{p^n}(q))$$

as ideals of $\mathbb{F}_p[q]$. Since $\mathbb{F}_p[q]$ is a UFD, and $\frac{\Phi_{p^n}(q)-p}{q^{p^t}-1} \cdot (q^{p^t} - 1) = \Phi_{p^n}(q)$ in $\mathbb{F}_p$. We have $H_2 \in \left(\frac{\Phi_{p^n}(q)-p}{q^{p^t}-1}\right)$.

We have

$$z = p^{N-1} H \frac{\Phi_{p^n}(q) - p}{q^{p^t} - 1}$$

in $W_q(\mathbb{Z}/p^N\mathbb{Z})/(\Phi_{p^n}(q))$ for some H.

If conversely z is a multiple of $p^{N-1}\frac{\Phi_{p^n}(q)-p}{q^{p^t}-1}$, simple calculation yields that $z(p^k - 1)$ is a multiple of P.

So $S_{p,P,k}$ consists of all the multiples of $p^{N-1}\frac{\Phi_{p^n}(q)-p}{q^{p^t}-1}$.

CASE 2. When $t = n$. Then k is a multiple of p^n. So $q^k - 1$ is a multiple of $\Phi_{p^n}(q)$. Regardless the value of z, $z\Phi_{p^n}(q)$ is a multiple of P. So $S_{p,P,k}$ consists of all the polynomials.

Combine cases 1 and 2, and Theorem 4.3, we know that the center is

$$\left(\sum_{i=0}^{n-1} p^{N-1} \cdot \frac{\Phi_{p^n}(q) - p}{q^{p^i} - 1} W_q(R)^{(p^i)}[q]\right) + W_q(R)^{(p^n)}[q],$$

as desired. $\square$

6. The First q-Weyl Algebra

We recall the definition of the first q-Weyl algebra.

Definition 6.1. Let the first q-Weyl algebra over a ring R be

$$W_q^{(1)}(R) = R\langle x, y\rangle/(yx - qxy - 1).$$

Now we recall the known homomorphism between the first q-Weyl algebra and Weyl algebra, which is an isomorphism when $P(1)$ is not a multiple of p (see e.g. [HL17]).

Proposition 6.2. *Let $P \in \mathbb{Z}[q]$ be a polynomial such that $P(1) \neq 0$. Then*

$$W_q(R)/P(q) \simeq W_q^{(1)}(R)/P(q).$$

And the isomorphism map is given by

$$f : a \mapsto x, b \mapsto (q-1)xy - 1.$$

Proof. We may do Euclidean division to $P(q)$ by $q-1$ in $\mathbb{Z}[q]$, then we get $P(q) = (q-1)K(q) + L$, where L is a constant. Plug in $q = 1$ we get $L = P(1)$ is not a multiple of p. So L has an inverse, L^{-1}, in $\mathbb{Z}/p^N\mathbb{Z}$. Thus

$$-L^{-1}(q-1)K(q) = 1$$

in $\mathbb{Z}/p^N\mathbb{Z}[q]$. So $q-1$ has an inverse.

We now construct the isomorphism map $f : a \mapsto x, b \mapsto (q-1)xy - 1$. To show that this is a homomorphism, it's sufficient to prove that $f(b)f(a) = qf(a)f(b)$. This is true because

$$\begin{aligned} f(b)f(a) - qf(a)f(b) &= ((q-1)xy + 1)x - qx((q-1)xy + 1) \\ &= (q-1)x(yx) + x - q(q-1)x^2y - qx \\ &= (q-1)\left(x(qxy+1) - qx^2y - x\right) \\ &= 0. \end{aligned}$$

On the other hand, we may define inverse of homomorphisms f as

$$f^{-1} : x \mapsto a, y \mapsto (q-1)^{-1}a^{-1}(b-1).$$

Obviously they are respectively the inverse of f^{-1}. Therefore f_1 and is an isomorphism map between $W_q(R)$ and $W_q^{(1)}(R)$, as desired. □

Corollary 6.3. *For any polynomial P such that $P(1)$ is not a multiple of p, we have*

$$Z(W_q(R)/P(q)) \simeq Z(W_q^{(1)}(R)/P(q)).$$

If P is monic and irreducible modulo p, we have

$$Z(W_q^{(1)}(R)/P(q)) \simeq \mathbb{W}_{N-l(P)}(R[\widetilde{a}^{M(P)}, \widetilde{b}^{M(P)}])[q].$$

6.1. **The center of the first Weyl algebra.** In this section we show that the underlying sets of the first Weyl algebra and the Weyl algebra has a natural bijection

$$\sum_{i,j} z_{ij}x^iy^j \mapsto \sum_{i,j} z_{ij}a^ib^j.$$

Proposition 6.4. *If $P(1)$ is not a multiple of p and $(q-1)Q(q)$ is divided by $P(q)$ in $\mathbb{Z}/p^N\mathbb{Z}$, then P divides Q in $\mathbb{Z}/p^N\mathbb{Z}$.*

Proof. Induct on N. When $N = 1$, since $P(1)$ is not a multiple of p, $P(x)$ is coprime with $x-1$ in $\mathbb{F}_p[q]$. Thus P must divide Q.

For the general cases, we may first do the Euclidean division to Q and P, and then we may assume that $\deg Q < \deg P$. Since P divides Q in $\mathbb{Z}/p^{N-1}\mathbb{Z}[q]$, if Q is non-zero in $\mathbb{Z}/p^{N-1}\mathbb{Z}[q]$, there exists a $Q' \in \mathbb{Z}/p^{N-1}\mathbb{Z}[q]$ such that $Q'P = Q$; look at the leading coefficient and degree, and we obtain a contradiction. Thus Q is a multiple of p^{N-1}. Thus we know that P divides Q/p^{N-1} in $(q-1)\mathbb{Z}/p\mathbb{Z}[q]$. This is reduced to the base case. Induction is completed. □

Theorem 6.5. *When $P(1)$ is not a multiple of p, the map*

$$\phi : \sum_{i,j} z_{ij}x^i y^j \mapsto \sum_{i,j} z_{ij}a^i b^j.$$

is a bijection from

$$Z(W_q^{(1)}(\mathbb{Z}/p^N\mathbb{Z})/P(q)) \to Z(W_q(\mathbb{Z}/p^N\mathbb{Z})/P(q))$$

.

Proof. By Lemma 2.5, z is in the center ring of $W_q^{(1)}(\mathbb{Z}/p^N\mathbb{Z})/P(q)$ if and only if it commutes with both x and y. By Proposition 2.4, we may write

$$z = \sum_{i\in\mathbb{Z}_{\geqslant 0}, j\in\mathbb{Z}} z_{ij}x^i y^j.$$

By Lemma 2.6,

$$xz = \sum_{i\in\mathbb{Z}_{\geqslant 0}, j\in\mathbb{Z}} z_{ij}x^{i+1}y^j$$

and

$$zx = \sum_{i,j\in\mathbb{Z}} \left(q^j z_{ij} + \frac{q^{j+1}-1}{q-1} z_{i+1j+1}\right) x^{i+1}y^j.$$

Thus z commutes with a if and only if

$$\sum_{i,j\in\mathbb{Z}} \left((q^j-1) z_{ij} + \frac{q^{j+1}-1}{q-1} z_{i+1j+1}\right) x^{i+1}y^j = 0.$$

By Proposition 2.4, the equation above holds if and only if

$$(q^j-1) z_{ij} + \frac{q^{j+1}-1}{q-1} z_{i+1j+1} = 0$$

in ring $\mathbb{Z}/p^N\mathbb{Z}[q]/P(q)$ for all i, j. Thus it's equivalent to that $P(q)$ divides $(q^j - 1)z_{ij} + \frac{q^{j+1}-1}{q-1} z_{i+1j+1}$ in $\mathbb{Z}/p^N\mathbb{Z}[q]$.

Now we prove $z_{ij} \in S_{P,p^n,j}$ by induction on j. Denote $\theta_{ij} = \frac{q^j-1}{q-1} z_{ij}$, then $(q-1)\theta_{ij} + \theta_{i+1j+1} = 0$ for all i, j. When $j = -1$, we know $\theta_{i0} = 0$ since $\theta_{i,-1}$ doesn't exist. Base case is done.

For the general cases, the result is immediate since $(q-1)\theta_{i-1j-1} + \theta_{ij} = 0$ and $\theta_{i-1j-1} = 0$. Induction is completed.

Thus $\theta_{ij} = 0$ in $\mathbb{Z}/p^N\mathbb{Z}[q]/P(q)$, so $\frac{q^j-1}{q-1} z_{ij}$ is a multiple of P in $\mathbb{Z}/p^N\mathbb{Z}[q]$. So $(q^j-1)z_{ij}$ is a multiple of P and by definition $z_{ij} \in S_{P,p^n,j}$.

On the other hand, we prove the converse is true. Namely, if $z_{ij} \in S_{P,p^n,j}$, then z is a center. Note that $z_{ij} \in S_{P,p^n,j}$ is equivalent to P dividing $(q^j-1)z_{ij}$ in $\mathbb{Z}/p^N\mathbb{Z}[q]$. By Proposition 6.4, this is equivalent to P dividing θ_{ij}. The rest of the proof above can be reversed without any complication.

So

$$z' = \sum_{i\in\mathbb{Z}_{\geqslant 0}, j\in\mathbb{Z}} z_{ij}x^i y^j \in Z(W_q^{(1)}(\mathbb{Z}/p^N\mathbb{Z})/P(q))$$

if and only if

$$z = \sum_{i \in \mathbb{Z}_{\geqslant 0}, j \in \mathbb{Z}} z_{ij} a^i b^j \in Z(W_q(\mathbb{Z}/p^N\mathbb{Z})/P(q)).$$

So ϕ is indeed a bijection. As desired. □

Acknowledgements

I would like to thank Calder Oakes Morton-Ferguson from MIT for mentorship. I also thank Prof. Roman Bezrukavnikov for suggesting this project and offering helpful advice. Lastly, I thank the PRIMES-USA Program for the research opportunity.

References

[BMRR08] Roman Bezrukavnikov, Ivan Mirković, Dmitriy Rumynin, and Simon Riche. Localization of modules for a semisimple lie algebra in prime characteristic. *Annals of Mathematics*, pages 945–991, 2008. 1

[EGH+11] Pavel I Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, and Elena Yudovina. *Introduction to representation theory*, volume 59. American Mathematical Soc., 2011. 3

[GG14] Murray Gerstenhaber and Anthony Giaquinto. On the cohomology of the weyl algebra, the quantum plane, and the q-weyl algebra. *Journal of Pure and Applied Algebra*, 218(5):879–887, 2014. 2

[HL17] Albert Heinle and Viktor Levandovskyy. Factorization of $\mathbb{Z}$-homogeneous polynomials in the first q-weyl algebra. In *Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory*, pages 455–480. Springer, 2017. 3, 21

[SV13] Allen Stewart and Vadim Vologodsky. On the center of the ring of differential operators on a smooth variety over $\mathbb{Z}/p^n\mathbb{Z}$. *Compositio Mathematica*, 149(1):63–80, 2013. 1, 2, 7, 9