ELSEVIER
Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra 320 (2008) 1599–1625
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

q-Deformed necklace rings and q-Möbius function ☆

Young-Tak Oh

Department of Mathematics, Sogang University, Seoul 121-742, Republic of Korea

Received 16 October 2007
Available online 17 June 2008
Communicated by Michel Broué

Abstract

We introduce a q-deformation of the classical Möbius function and investigate its properties in connection with q-deformed truncated necklace rings. Also, we study the strictly natural isomorphism of q-deformed necklace rings.

Keywords: Möbius function; Cyclotomic identity; Necklace ring; Restricted Lie p-algebra

1. Introduction

The necklace ring was first introduced by Metropolis and Rota [8] to explain the structure of the ring of big Witt vectors due to Cartier [2]. It has close connections to various areas such as combinatorics, group theory and ring theory. For example, it can be realized as the Burnside–Grothendieck ring of almost finite cyclic sets over $\mathbb{Z}$ and turns out to be isomorphic to the ring of big Witt vectors over rings satisfying suitable conditions. For more details, see [3,4,8,11,12].

Recently, it has been shown that truncated necklace rings have a q-deformation when q varies over the set of integers (see [12]). Let $\mathbb{N}$ be the set of positive integers. Also, we let N be a nonempty subset with the property that if $n \in N$, then every divisor of N is also contained in N. We then say that N is a *truncation set*. Given a commutative ring A and an integer q, the *q-deformed N-truncated necklace ring over A* is given by $\mathbf{Nr}_N^q(A)$. Here, $\mathbf{Nr}_N^q$ represents a unique covariant functor from the category of commutative rings to itself characterized by the following conditions:

☆ This research was supported by KRF Grant #2007-314-C00005.
E-mail address: ytoh@sogang.ac.kr.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2008.05.016

(1) As a set, it is A^N.
(2) For any ring homomorphism $f: A \to B$, the map $\mathbf{Nr}_N^q(f): \mathbf{x} \mapsto (f(x_n))_{n\in N}$ is a ring homomorphism.
(3) The map,

$$\varphi_N^q : \mathbf{Nr}_N^q(A) \to \mathrm{gh}_N(A), \qquad \mathbf{x} \mapsto \left(\sum_{d|n} dq^{\frac{n}{d}-1} x_d\right)_{n\in N},$$

is a ring homomorphism. Here, $\mathrm{gh}_N(A)$, called the *ghost ring over* A, is just A^N with addition and multiplication defined componentwise.

Given q and r, we say that $\mathbf{Nr}_N^q$ is *strictly-isomorphic* to $\mathbf{Nr}_N^r$ if there exists a natural isomorphism, $\mathfrak{n}_q^r : \mathbf{Nr}_N^q \to \mathbf{Nr}_N^r$ satisfying $\varphi_N^q = \varphi_N^r \circ \mathfrak{n}_q^r$. In this case, $\mathfrak{n}_q^r$ is called a *strict natural isomorphism*. It was shown in [12] that $\mathbf{Nr}_N^q$ is classified up to strict natural isomorphism by the set of prime divisors of q contained in N. However, the explicit form of the strict isomorphism has not been provided there. This was the initial motivation of this paper. We will provide it in Section 2. $\mathbf{Nr}_N^q$ also has a very natural functorial property. To be more precise, if M and N are truncation sets with $M \cap N = \{1\}$, then there exists a functorial isomorphism

$$\mathbf{Nr}_N^q \circ \mathbf{Nr}_M^q \cong \mathbf{Nr}_{MN}^q \tag{1.1}$$

satisfying a suitable condition. This result was published in [12, Theorem 25], but we found that there is a gap in the final step of the original proof since $\mathbf{Nr}_N^q(\mathbb{Z})$ is no longer a binomial ring. This led us to reprove Eq. (1.1). We expect that this method is also applicable to the q-deformed Witt–Burnside ring and the Burnside–Grothendieck ring of a profinite group (refer to [10]).

From an aspect of combinatorics, q-necklace rings are closely related to q-Möbius functions. The natural transformation φ_N^q, when $N = \mathbb{N}$, is given by the left multiplication by an $\mathbb{N} \times \mathbb{N}$ matrix λ_q defined by

$$\lambda_q(i,j) = \begin{cases} jq^{\frac{i}{j}-1} & \text{if } j \mid i, \\ 0 & \text{otherwise.} \end{cases}$$

Motivated by this fact, we introduce a q-deformation of the classical Möbius function, which can be defined as follows: Let q be an indeterminate and let ζ_q be an $\mathbb{N} \times \mathbb{N}$ matrix given by

$$\zeta_q(i,j) = \begin{cases} q^{\frac{i}{j}-1} & \text{if } j \mid i, \\ 0 & \text{otherwise.} \end{cases}$$

Since ζ_q is lower triangular with 1 on the diagonal, there exists its inverse, say μ_q. Letting $\mu_q(n)$ be $\mu_q(n,1)$ for all $n \in \mathbb{N}$, it recovers the classical Möbius function when $q = 1$. In Section 3, we derive a relation between the q-Möbius function and the classical Möbius function utilizing the *q-necklace polynomial*

$$M^q(x,n) = \frac{1}{n}\sum_{d|n} \mu_q\left(\frac{n}{d}\right) q^{d-1} x^d$$

and the *q-cyclotomic identity*

$$\frac{1}{1-qxt}=\prod_{n\geqslant 1}\left(\frac{1}{1-qt^n}\right)^{M^q(x,n)}.$$

In contrast with the classical Möbius function, μ_q is no longer multiplicative except the case $q=1,0,-1$. Instead it has the following type of pseudo-multiplicative property which can be deduced from Eq. (1.1) (see Section 5):

For positive integers m, n which are relatively prime, we have

$$\mu_q(mn)=\sum_{d|m,e|n} f_{d,e}(q)\mu_q(d)\mu_q(e),$$

where $f_{d,e}(q)\in\mathbb{Q}[q]$ are subject to the conditions:

(1) $f_{m,n}(q)=1$,
(2) $f_{d,e}(q)$ *are numerical polynomials in q, that is, it takes integer values at every integer argument, and*
(3) $q(q^2-1)$ *divides* $f_{d,e}(q)$ *unless* $de=mn$.

Finally, we remark that μ_q has deep connections to the Möbius function due to Petrogradsky [13] which appeared in the context of restricted Lie p-algebras. This will be studied extensively in connection with necklace rings in Section 4.

2. The explicit form of strict natural isomorphism

This section provides the explicit form of the strict natural isomorphism between $\mathbf{Nr}_N^q$ and $\mathbf{Nr}_N^r$ when q,r have the same set of prime divisors in N. To begin with, we deal with the case $N=\mathbb{N}$.[1] Assume that q,r be indeterminates. Let us introduce an $\mathbb{N}\times\mathbb{N}$ matrix λ_q defined by

$$\lambda_q(i,j)=\begin{cases} jq^{\frac{i}{j}-1} & \text{if } j\mid i,\\ 0 & \text{otherwise.}\end{cases}$$

Since φ^q (respectively φ^r) represents the left multiplication by λ_q (respectively λ_r), $\mathfrak{n}_q^r(A)$ should be defined by the left multiplication by $(\lambda_r)^{-1}\lambda_q$ in case $A=\mathbb{Q}[q,r]$. It is not difficult to show that each entry of $(\lambda_r)^{-1}\lambda_q$ is contained in $\mathbb{Q}[q,r]$.

Lemma 2.1. *(See [12].) Suppose that q ranges over the set of integers. Then $\mathbf{Nr}_N^q$ is classified up to strict natural isomorphism by the set of prime divisors of q contained in N. The set of prime divisors of* 0 *is assumed to be the set of all primes in* $\mathbb{N}$.

[1] In this case, the suffix N will be omitted.

The proof of Lemma 2.1 shows that every entry of $(\lambda_r)^{-1}\lambda_q$ takes integer values if and only if the set of prime divisors of q contained in N coincides with that of r. In this case, $(\lambda_r)^{-1}\lambda_q$ can be defined over arbitrary commutative rings since $\mathbb{Z}$ is a universal object in the category of commutative rings. For the computation of the explicit form of the isomorphism, we need the following generalization of necklace polynomials.

Definition 2.2. Suppose that x, q are indeterminates. For each positive integer n, we define $M^q(x,n) \in \mathbb{Q}[x,q]$ recursively via the following relations:

$$\sum_{d|n} dM^q(x,d)q^{\frac{n}{d}-1} = q^{n-1}x^n, \quad \forall n \geqslant 1.$$

When $q = 1$, $M^q(x,n)$ is called a *necklace polynomial* since it counts primitive necklaces of length n out of x-letters. Similarly, $M^q(x,n)$ has a very natural combinatorial meaning. It counts *primitive q-necklaces* of length n out of x-letters, which was due to Lenart [7]. In this sense, $M^q(x,n)$ will be called a *q-necklace polynomial*. Put

$$B = \{nM^q(x,n)\colon n \geqslant 1\} \quad \text{and} \quad B' = \{q^{n-1}x^n\colon n \geqslant 1\}.$$

Since B and B' are $\mathbb{Q}(q)$-basis of the polynomial ring $x\mathbb{Q}(q)[x]$, ζ_q is nothing but the transition matrix from B to B' and μ_q the transition matrix from B' to B. It is easy to show that

$$(\lambda_q)^{-1}(n,d) = \frac{1}{n}\mu_q(n,d)$$

and

$$M^q(x,n) = \frac{1}{n}\sum_{d|n}\mu_q(n,d)q^{d-1}x^d. \tag{2.1}$$

For convenience, we will use the notation

$$A_n = qM^q(rx,n), \qquad B_n = rM^r(qx,n), \quad \forall n \geqslant 1.$$

Since

$$\sum_{d|n} dA_d q^{\frac{n}{d}-1} = \sum_{d|n} dB_d r^{\frac{n}{d}-1} = (qrx)^n, \quad \forall n \geqslant 1, \tag{2.2}$$

we have

$$\varphi^q(A_1, A_2, \ldots) = \varphi^r(B_1, B_2, \ldots).$$

We can rewrite this equation as

$$(B_1, B_2, \ldots)^t = (\lambda_r)^{-1}\lambda_q(A_1, A_2, \ldots)^t.$$

Here, the superscript t denotes the transpose of a matrix. Set

$$C = \{A_n\colon\ n \geqslant 1\}, \qquad C' = \{B_n\colon\ n \geqslant 1\}.$$

Note that C and C' are $\mathbb{Q}(q,r)$-bases of $x\mathbb{Q}(q,r)[x]$ and $(\lambda_r)^{-1}\lambda_q$ denotes the transition matrix from C to C'. Denote by $g_{i,j}(q,r)$ the (i,j)th entry of $(\lambda_r)^{-1}\lambda_q$. Then, for each positive integer n, it holds

$$B_n = \sum_{d|n} g_{n,d}(q,r) A_d, \quad n \geqslant 1.$$

Theorem 2.3. *Under the above notation, the followings hold*:

(a) *For each positive integer n and a divisor d of n,*

$$g_{n,d}(q,r) = \frac{r}{q} M^r\left(\frac{q}{r}, \frac{n}{d}\right).$$

Moreover, if q, r are integers with the same set of prime divisors, then

$$g_{n,d}(q,r) \in \mathbb{Z}$$

for every $n \geqslant 1$ and $d \mid n$.

(b) *Assume that q, r are integers with the same set of prime divisors. Then $\mathfrak{n}_q^r$ is given by the left multiplication by the transition matrix from C to C' whose entries are given as follows*:

$$\mathfrak{n}_q^r(i,j) = \begin{cases} \dfrac{r}{q} M^r\left(\dfrac{q}{r}, \dfrac{i}{j}\right) & \text{if } j \mid i, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. (a) From [11, Section 3.2] it follows that if q, r have the same set of prime divisors, then $g_{n,d}(q,r)$ are numerical polynomials in q and r taking integer values for all integer arguments. Now, let us now find the explicit form of $g_{n,d}(q,r)$ with $d \mid n$. To this end, transform Eq. (2.2) into

$$-(B_n - A_n) = \frac{1}{n} \sum_{\substack{e|n \\ e \neq n}} e\bigl(B_e r^{\frac{n}{e}-1} - A_e q^{\frac{n}{e}-1}\bigr), \quad n \geqslant 1. \tag{2.3}$$

It is straightforward that $g_{n,n}(q,r) = 1$. Now, assume that $d < n$. Comparing the coefficient of A_d on both sides of Eq. (2.3) yields

$$-n g_{n,d}(q,r) = \sum_{\substack{d|e|n \\ d<e}} e r^{\frac{n}{e}-1} g_{e,d}(q,r) - d q^{\frac{n}{d}-1}.$$

Put $n = n'd$ and $e = d'd$. Also, we put

$$G_{n'} = g_{n'd,d}(q,r).$$

Then the above equation is simplified to

$$\sum_{d'|n'} d' r^{\frac{n'}{d'}-1} G_{d'} = q^{n'-1}. \tag{2.4}$$

Observe that the left-hand side of Eq. (2.4) coincides with the n'th component of $\varphi^r(G_1, G_2, \ldots)$ and the n'th component of

$$\frac{r}{q}\varphi^r\left(M^r\left(\frac{q}{r}, 1\right), M^r\left(\frac{q}{r}, 2\right), \ldots\right)$$

is given by $q^{n'-1}$. Since φ^q is a ring isomorphism over a $\mathbb{Q}$-algebra, it follows that

$$G_{n'} = \frac{r}{q} M^r\left(\frac{q}{r}, n'\right), \quad n' \geqslant 1.$$

Therefore we can conclude

$$g_{n,d} = G_{\frac{n}{d}} = \frac{r}{q} M^r\left(\frac{q}{r}, \frac{n}{d}\right).$$

This completes the proof.

(b) It follows from (a). □

In some special cases, $(\lambda_r)^{-1}\lambda_q$ can be computed so easily. Here are such examples.

Example 2.4.

(a) Let $r = -q$. Utilizing

$$M^{-q}(-1, n) = \begin{cases} -1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is odd and } n \neq 1, \end{cases}$$

we obtain

$$g_{n,d} = \begin{cases} 1 & \text{if } d = n, \\ -M^{-q}\left(-1, \frac{n}{d}\right) & \text{if } \frac{n}{d} \text{ is even, and } d \mid n,\ d \neq n, \\ 0 & \text{otherwise.} \end{cases}$$

(b) Let $q = 1$ and $r = -1$. Combining (a) with the fact

$$M^{-1}(-1, n) = \begin{cases} -1 & \text{if } n = 2^k \text{ with } k \geqslant 0, \\ 0 & \text{otherwise,} \end{cases} \tag{2.5}$$

we obtain

$$g_{n,d}(1, -1) = \begin{cases} 1 & \text{if } d = n, \\ 1 & \text{if } n \text{ is even, and } \frac{n}{d} = 2^k \text{ with } k \geqslant 0, \\ 0 & \text{otherwise.} \end{cases}$$

(c) Let $q=-1$ and $r=1$. From

$$M(-1,n)=\begin{cases}-1 & \text{if } n=1,\\ 1 & \text{if } n=2,\\ 0 & \text{otherwise,}\end{cases} \tag{2.6}$$

we obtain

$$g_{n,d}(-1,1)=\begin{cases}-1 & \text{if } d=n,\\ 1 & \text{if } 2d=n,\\ 0 & \text{otherwise.}\end{cases}$$

By the restriction of index from $\mathbb{N}$ to N we can establish an analogous result for truncated q-necklace rings.

Corollary 2.5. *Assume that q, r are integers with the same set of prime divisors in N. Then the strict natural isomorphism $\mathfrak{n}_q^r : \mathbf{Nr}_N^q \to \mathbf{Nr}_N^r$ is given by the left multiplication by an $N\times N$-matrix whose entries are given as follows*:

$$\mathfrak{n}_q^r(i,j)=\begin{cases}\dfrac{r}{q}M^r\left(\dfrac{q}{r},\dfrac{i}{j}\right) & \textit{if } j\mid i,\\ 0 & \textit{otherwise.}\end{cases}$$

3. q-Möbius function and q-necklace polynomial

The classical Möbius function, $\mu:\mathbb{N}\to\mathbb{N}$, is given by

$$\mu(n)=\begin{cases}1 & \text{if } n=1,\\ (-1)^{\omega(n)} & \text{if } n \text{ is square free and } n>1,\\ 0 & \text{otherwise.}\end{cases}$$

Here, $\omega(n)$ denotes the number of distinct prime divisors of n. It can be better understood in the context of matrices. Let ζ be an $\mathbb{N}\times\mathbb{N}$ matrix defined by

$$\zeta(i,j)=\begin{cases}1 & \text{if } j\mid i,\\ 0 & \text{otherwise.}\end{cases}$$

Note that ζ is lower triangular with 1 on the diagonal. By abuse of notation we denote by μ the inverse of ζ, and let $f,g:\mathbb{N}\to\mathbb{Q}$ be functions satisfying

$$f(n)=\sum_{d\mid n} g(d),\quad n\geqslant 1,$$

equivalently

$$\begin{pmatrix}\vdots\\ f(n)\\ \vdots\end{pmatrix}_{n\geqslant 1}=\zeta\begin{pmatrix}\vdots\\ g(n)\\ \vdots\end{pmatrix}_{n\geqslant 1}.$$

The Möbius inversion formula is then nothing but the relation

$$\mu(i,j)=\begin{cases}\mu\left(\frac{i}{j}\right) & \text{if } j\mid i,\\ 0 & \text{otherwise.}\end{cases}$$

Let q be an indeterminate. As in Introduction, μ_q denotes the inverse of ζ_q. Note that the relation $\mu_q\zeta_q=\delta$ is equivalent to

$$\begin{aligned}&\mu_q(i,i)=1, \quad \text{for all } i\geqslant 1,\\ &\mu_q(i,j)=-\sum_{\substack{j|k|i\\ j<k}} q^{\frac{k}{j}-1}\mu_q(i,k), \quad \forall j<i.\end{aligned} \tag{3.1}$$

Definition 3.1. Let q be an indeterminate. The q-Möbius function, denoted by μ_q, is defined to be the function

$$\mu_q:\mathbb{N}\to\mathbb{Z}[q], \qquad n\mapsto\mu_q(n,1), \quad \forall n\geqslant 1.$$

From Eq. (3.1) it follows that $\mu_q(i,j)=\mu_q(i',j')$ if $i/j=i'/j'$. Thus, we have

$$\mu_q(n)=\mu_q(nk,k), \quad \forall k\in\mathbb{N}.$$

Applying this result to Eq. (3.1) again yields

$$\begin{aligned}&\mu_q(1)=1,\\ &\mu_q(n)=-\sum_{\substack{d|n\\ d\neq 1}} q^{d-1}\mu_q\left(\frac{n}{d}\right), \quad \forall n>1.\end{aligned}$$

As in the classical case (more precisely, $q=1$), q-necklace polynomials due to Eq. (2.1) play a crucial role in the study of q-Möbius function. By the definition of μ_q, it is straightforward that

$$M^q(x,n)=\frac{1}{n}\sum_{d|n}\mu_q\left(\frac{n}{d}\right)q^{d-1}x^d.$$

If $q=1$, we will omit the superscript q in $M^q(x,n)$ and μ_q. The following theorem shows the relation between the q-Möbius function and the classical Möbius function.

Theorem 3.2. *Let $n\in\mathbb{N}$.*

(a) *If n has the prime factorization $p_1^{n_1}p_2^{n-2}\cdots p_k^{n^k}$ with $n_i\geqslant 1$ $(1\leqslant i\leqslant k)$, then*

$$\begin{aligned}\mu_q(n)&=q\sum_{d|n} dM^q\left(\frac{1}{q},d\right)\mu\left(\frac{n}{d}\right)\\ &=qn\sum_{d|p_1\cdots p_k}\frac{(-1)^{\omega(d)}}{d}M^q\left(\frac{1}{q},\frac{n}{d}\right).\end{aligned} \tag{3.2}$$

Here, $\omega(1)$ is assumed to be 0.

(b) *For every $n \in \mathbb{N}$ we have*

$$\mu(n) = \frac{1}{q}\sum_{d|n} dM(q,d)\mu_q\left(\frac{n}{d}\right). \tag{3.3}$$

Proof. Since (b) can be proved in the exactly same way as (a), we will prove only (a). Replace r and q by q and 1, respectively. Then, Theorem 2.3 yields

$$qM^q(x,n) = q\sum_{d|n} M^q\left(\frac{1}{q},\frac{n}{d}\right)M(qx,d), \quad \forall n \geqslant 1. \tag{3.4}$$

Let d be a divisor of n. Comparing the coefficient of x in both sides of Eq. (3.4) yields the equality

$$\frac{q}{n}\mu_q(n,1) = q\sum_{d|n} M^q\left(\frac{1}{q},\frac{n}{d}\right)\frac{1}{d}\mu(d,1)q.$$

Replacing $\mu_q(n,1)$ and $\mu(d,1)$ by $\mu_q(n)$ and $\mu(d)$, respectively, gives the first equality. The second equality follows from the definition of μ. □

Example 3.3.

(a) Put $q=-1$ and $n=2^k n'$ with n' odd. From Eqs. (2.5) and (3.2) we have

$$\mu_{-1}(n) = \begin{cases} \mu(n) & \text{if } k=0, \\ 2^{k-1}\mu(n') & \text{if } k\geqslant 1. \end{cases} \tag{3.5}$$

It is easily seen that μ_{-1} is multiplicative, i.e.,

$$\mu_{-1}(mn) = \mu_{-1}(m)\mu_{-1}(n)$$

in case where m and n are relatively prime. Nevertheless, this is not the case in general. For example, if p, p' are distinct primes, then $\mu_q(pp') = -q^{pp'-1} + 2q^{p+p'-2}$, but $\mu_q(p)\mu_q(p') = q^{p+p'-2}$. This can be verified by Corollary 3.2. Indeed, μ_q is multiplicative only in case where $q=1,-1,0$.

(b) Substitute -1 for q in Eq. (3.3). Then, by Eq. (2.6) we come to have

$$\mu(n) = \begin{cases} \mu_{-1}(n) & \text{if } n \text{ is odd}, \\ \mu_{-1}(n) - 2\mu_{-1}\left(\frac{n}{2}\right) & \text{otherwise}. \end{cases} \tag{3.6}$$

Next, we investigate the properties of q-necklace polynomials when $q=-1$ in detail. It is well known that the necklace polynomial has deep connection with the celebrated cyclotomic identity,

$$\frac{1}{1-xt} = \prod_{n\geqslant 1}\left(\frac{1}{1-t^n}\right)^{M(x,n)},$$

which was due to Gauss [5]. Here, if we replace negative sign in the denominators by positive sign, then we obtain a dual version of the cyclotomic identity such as

$$1 + xt = \prod_{n \geqslant 1} \left(1 + t^n\right)^{N(x,n)}. \tag{3.7}$$

This identity was first introduced in [1,6], and has been called the *cocyclotomic identity*. It is well known that the exponent $N(x, n)$ is given by

$$N(x,n) = \begin{cases} M(x,n) & \text{if } n \text{ is odd,} \\ -\sum_{k \geqslant 0} M\left(-x, \frac{n}{2^k}\right) & \text{if } n \text{ is even.} \end{cases}$$

Conventionally, we assume that $M(x, n)$ is zero for non-integral values n. More simply, we can write

$$N(x,n) = -\sum_{k \geqslant 0} M\left(-x, \frac{n}{2^k}\right) \tag{3.8}$$

since $M(x, n) = -M(-x, n)$ if n is odd. The cocyclotomic identity can be understood more naturally in the context of the q-cyclotomic identity which was first introduced in [11]. The explicit form of the q-cyclotomic identity looks as follows:

$$\frac{1}{1 - qxt} = \prod_{n \geqslant 1} \left(\frac{1}{1 - qt^n}\right)^{M^q(x,n)}. \tag{3.9}$$

Plugging $q = -1$ into Eqs. (3.7) and (3.9) gives rise to the formula

$$N(x,n) = M^{-1}(x,n), \quad n \geqslant 1. \tag{3.10}$$

Assume that n is even, say $n = 2^k n'$ where $k \geqslant 1$ and n' is odd. In [1], it was shown that

$$N(x,n) = -\sum_{i=1}^{k} M\left(x, 2^i n'\right),$$

which implies

$$\sum_{i=1}^{k} M\left(x, 2^i n'\right) = \sum_{i \geqslant 0} M\left(-x, \frac{n}{2^i}\right).$$

Now, we will provide a relation between $M(x, n)$ and $M(-x, n)$. To this end, we will compute the transition matrix from $\{M(x, n): n \geqslant 1\}$ to $\{M(-x, n): n \geqslant 1\}$. More generally, put

$$D = \left\{M^q(x,n): n \geqslant 1\right\}, \qquad D' = \left\{M^q(-x,n): n \geqslant 1\right\}.$$

It is easy to show that D and D' are $\mathbb{Q}(q)$-bases of $x\mathbb{Q}(q)[x]$.

Proposition 3.4.

(a) *For every* $n \geqslant 1$, $M^q(-x,n)$ *is given as follows*:

$$\begin{cases} -M^q(x,n) & \text{if } n \text{ is odd,} \\ M^q(x,n) + \sum_{\substack{d \mid n \\ d \text{ is odd}}} M^q\left(q, \frac{n}{2d}\right) M^q(x,d) & \text{if } n \text{ is even.} \end{cases} \tag{3.11}$$

(b) *The transition matrix* Q *from* D *to* D' *is given as follows*:

$$Q(i,j) = \begin{cases} -1 & \text{if } i = j \text{ is odd,} \\ 1 & \text{if } i = j \text{ is even,} \\ M^q\left(q, \frac{i}{2j}\right) & \text{if } i \text{ is even and } j \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}$$

(c) $Q = Q^{-1}$.

Proof. (a) This can be proven in a similar way as in Theorem 2.3.

(b) It follows from (a).

(c) The transition matrix from D' to D can be obtained by switching x and $-x$ into each other in Eq. (3.11). One can observe that this matrix is also given by Q. This forces Q be equal to Q^{-1}. □

In particular, if $q = 1$, we can establish the following formula.

Corollary 3.5. *For every positive integer* n

$$M(-x,n) = \begin{cases} -M(x,n) & \text{if } n \text{ is odd,} \\ M(x,n) & \text{if } 4 \mid n, \\ M(x,n) + M\left(x, \frac{n}{2}\right) & \text{if } 2 \mid n, \text{ but } 4 \nmid n. \end{cases}$$

Finally we close this section by remarking that Eq. (3.9) gives rise to a general cyclotomic identity

$$\prod_{n \geqslant 1} \left(\frac{1}{1 - qt^n}\right)^{M^q(rx,n)} = \prod_{n \geqslant 1} \left(\frac{1}{1 - rt^n}\right)^{M^r(qx,n)},$$

where q, r, x, t are indeterminates.

4. Petrogradsky's Möbius function and necklace rings, and its relation with μ_q

In 2003, Petrogradsky [13] introduced a function analogous to the classical Möbius function in the context of restricted Lie p-algebras. It is parametrized by the prime integers p.

Remark 4.1. He denoted the above function by μ_p, but it is completely different from our μ_p. To avoid confusion, we will use $\mu^{(p)}$ to denote Petrogradsky's μ_p throughout this paper.

In this section, we show how $\mu^{(p)}$ appears in the context of necklace rings and how it is related with our q-Möbius function μ_q. We start with introducing isomorphic copies of the classical necklace ring. To do this, for each positive integer r, we introduce the rth *Verschiebung* operators $(r \in \mathbb{N})$

$$V_r : \mathbf{Nr}(A) \to \mathbf{Nr}(A), \qquad (b_n)_{n\in\mathbb{N}} \mapsto (b_{\frac{n}{r}})_{n\geqslant 1}$$

with $b_{\frac{n}{r}} = 0$ if $n/r \notin \mathbb{N}$. Let A be a commutative ring with identity. For each positive integer k we define

$$\theta_k : \mathbf{Nr}(A) \to A^{\mathbb{N}}, \qquad \mathbf{b} \mapsto \sum_{i\geqslant 0} V_{k^i}\mathbf{b}, \qquad \mathbf{b} = (b_n)_{n\geqslant 1}.$$

Proposition 4.2. *θ_k is bijective.*

Proof. Define a map

$$\psi_k : A^{\mathbb{N}} \to \mathbf{Nr}(A), \qquad \mathbf{c} \mapsto \mathbf{c} - V_k\mathbf{c}, \qquad \mathbf{c} = (c_n)_{n\in\mathbb{N}}.$$

Then,

$$\psi_k \circ \theta_k(\mathbf{b}) = \sum_{i\geqslant 0} V_{k^i}\mathbf{b} - \sum_{i\geqslant 1} V_{k^i}\mathbf{b} = \mathbf{b},$$
$$\theta_k \circ \psi_k(\mathbf{c}) = \sum_{i\geqslant 0} V_{k^i}\mathbf{c} - \sum_{i\geqslant 1} V_{k^i}\mathbf{c} = \mathbf{c}.$$

This implies the bijectiveness of θ_k. □

From the above proof it is obvious that the inverse of θ_k is ψ_k. Let us make $A^{\mathbb{N}}$ into a ring via ψ_k. We denote it by $\mathbf{Nr}^{(k)}(A)$. By definition θ_k and ψ_k are ring isomorphisms. Composing ψ_k with φ, we obtain a map

$$\varphi^{(k)} : \mathbf{Nr}^{(k)}(A) \to \mathrm{gh}(A).$$

Proposition 4.3. *As a functor from the category of commutative rings with identity to itself, $\mathbf{Nr}^{(2)}$ coincides with $\mathbf{Nr}^{-1}$.*

Proof. Put $k = 2$. For our purpose it is enough to show that $\theta_2 = \mathfrak{n}_q^r$, where $q = 1$ and $r = -1$. And, to prove this, we have only to show

$$\theta_2\big(M(x,1), M(x,2), \ldots\big) = \mathfrak{n}_q^r\big(M(x,1), M(x,2), \ldots\big). \tag{4.1}$$

The nth component of the left-hand side of Eq. (4.1) is given by

$$\sum_{i\geqslant 0} M\left(x, \frac{n}{2^i}\right),$$

which coincides with $-M^{-1}(-x,n)$ by Eq. (3.10). On the other hand, by Eq. (2.2) we know that the nth component of the right-hand side should is given by $-M^{-1}(-x,n)$, too. This completes the proof. □

Let us investigate $\varphi^{(k)}$ in more detail. For each positive integer k let us introduce the function

$$1_k(n) = \begin{cases} 1 & \text{if } k \nmid n, \\ 1-k & \text{if } k \mid n. \end{cases}$$

We define an $\mathbb{N} \times \mathbb{N}$ matrix $\zeta^{(k)}$ by

$$\zeta^{(k)}(n,d) = \begin{cases} 1_k\left(\frac{n}{d}\right) & \text{if } d \mid n, \\ 0 & \text{otherwise.} \end{cases}$$

With this notation one can see that

$$\varphi^{(k)}(x_1, x_2, \ldots) = \zeta^{(k)} \begin{pmatrix} \vdots \\ nx_n \\ \vdots \end{pmatrix}_{n\geqslant 1}.$$

Note that $\zeta^{(k)}$ is invertible since it is a lower triangular matrix with 1 at the diagonals. Denote by $\mu^{(k)}$ its inverse. From the relation $\mu^{(k)}\zeta^{(k)} = \delta$ it follows that

$$\begin{aligned} &\mu^{(k)}(i,i) = 1, \quad \text{for all } i \geqslant 1, \\ &\mu^{(k)}(i,j) = -\sum_{\substack{j\mid d\mid i \\ j<d}} \mu^{(k)}(i,d)\zeta^{(k)}(d,j), \quad \text{for all } j < i. \end{aligned} \tag{4.2}$$

Exploiting Eq. (4.2) one can show easily that $\mu^{(k)}(i,j) = 0$ unless $j \mid n$, and $\mu^{(k)}(i,j) = \mu^{(k)}(i',j')$ if $i/j = i'/j'$.

Definition 4.4. Let k be a positive integer. For every positive integer n, we define

$$\mu^{(k)} : \mathbb{N} \to \mathbb{N}, \qquad n \mapsto \mu^{(k)}(n,1), \quad \forall n \geqslant 1.$$

By virtue of Eq. (4.2) we have the following recursive form:

$$\mu^{(k)}(1) = 1,$$
$$\mu^{(k)}(n) = -\sum_{\substack{1<d \\ d|n}} \mu^{(k)}\left(\frac{n}{d}\right) 1_k(d), \quad \forall n > 1.$$

Theorem 4.5. *Fix a positive integer k. Then we have*

(a) *For every $n \in \mathbb{N}$ write it as mk^s, where $k \nmid m$. Then*

$$\mu^{(k)}(n) = \begin{cases} \mu(n) & \text{if } s = 0, \\ k^s \mu(m) + k^{s-1}\mu(mk) & \text{otherwise.} \end{cases}$$

(b) *Let $k \in \mathbb{N} - \{1\}$. Then $\mu^{(k)}$ is multiplicative if and only if k is a prime.*

Proof. (a) Consider the element $\mathbf{x} = (x, x^2, x^3, \dots) \in \mathrm{gh}(\mathbb{Q}[x])$. Then the inverse image of $\mathbf{x}$ for φ is given by $(M(x,n))_{n\geqslant 1}$. On the other hand, the inverse image of $\mathbf{x}$ for $\varphi^{(k)}$ is given by $(M^{(k)}(x,n))_{n\geqslant 1}$, where

$$M^{(k)}(x,n) = \frac{1}{n}\sum_{d|n} \mu^{(k)}\left(\frac{n}{d}\right) x^d.$$

Thus,

$$M^{(k)}(x,n) = \sum_{i\geqslant 0} M\left(x, \frac{n}{k^i}\right).$$

Comparing the coefficient of x in the both sides of the above identity gives rise to the formula

$$\frac{1}{n}\mu^{(k)}(n) = \sum_{i\geqslant 0} \frac{k^i}{n}\mu\left(\frac{n}{k^i}\right).$$

If $k \nmid n$, then $\mu^{(k)}(n) = \mu(n)$. If not, write it as mk^s, where $k \nmid m$ and $s \geqslant 1$. Then,

$$\sum_{i\geqslant 0} k^i \mu\left(\frac{n}{k^i}\right) = \sum_{i\geqslant 0} k^i \mu\left(mk^{s-i}\right) = k^s\mu(m) + k^{s-1}\mu(mk).$$

(b) It is not difficult to show "if"-part (see Example 4.6). For the converse, let k be a composite, say k_1k_2 with $(k_1,k_2) = 1$. Then $\mu^{(k)}(k_1k_2) = k$, but

$$\mu^{(k)}(k_1)\mu^{(k)}(k_2) = \mu(k_1)\mu(k_2) = \mu(k).$$

This shows that $\mu^{(k)}$ is not multiplicative. $\square$

Example 4.6. Let k be a prime, say p. Then

$$\mu^{(p)}(n) = \begin{cases} \mu(n) & \text{if } (p,n)=1, \\ \mu(m)\big(p^s - p^{s-1}\big) & \text{if } n = mp^s,\ (p,m)=1,\ s \geqslant 1. \end{cases}$$

So, in view of Eq. (3.5), we can conclude that

$$\mu^{(2)} = \mu_{-1}.$$

5. Pseudo-multiplicative property of μ_q and functorial property of truncated q-necklace rings

Contrary to the classical Möbius function, our q-Möbius function μ_q is no longer multiplicative in general. However, we show that it has a pseudo-multiplicative property, which can be deduced from a functorial isomorphism of q-deformed necklace rings.

Theorem 5.1. *For positive integers m, n which are relatively prime, we have*

$$\mu_q(mn) = \sum_{d|m,\, e|n} f_{d,e}(q)\mu_q(d)\mu_q(e),$$

where $f_{d,e}(q) \in \mathbb{Q}[q]$ are subject to the conditions

(1) $f_{m,n}(q) = 1$.
(2) $f_{d,e}(q)$ *are numerical polynomials in q, that is, it takes an integer value at every integer argument.*
(3) $q(q^2-1)$ *divides $f_{d,e}(q)$ unless $de = mn$.*

The proof of Theorem 5.1 will appear in Section 5.2. Note that μ_q is still multiplicative in case where $q = 1, 0, -1$.

5.1. Functorial property of truncated q-necklace rings

To prove the above theorem, we first deal with a functorial property of truncated q-necklace rings. Let M, N be truncation sets, and let $MN := \{mn\colon\ m \in M,\ n \in N\}$. Then MN is also a truncation set. In particular, if $M \cap N = \{1\}$, then $MN \cong M \times N$. Assume that q is any integer. In [12], it was shown that we have isomorphisms of functors,

$$\mathbf{Nr}^q_N \circ \mathbf{Nr}^q_M \cong \mathbf{Nr}^q_{MN},$$

for coprime truncation sets M and N. However, we found that there exists a gap in the final step of the original proof. In this section, we will reprove it in a different way.

Let A be any commutative ring. Applying the functoriality of φ^q_N, we have the commutative diagram

$$\begin{array}{ccc}
\mathbf{Nr}_N^q(\mathbf{Nr}_M^q(A)) & \xrightarrow{\varphi_N^q(\mathbf{Nr}_M^q(A))} & \mathrm{gh}_N(\mathbf{Nr}_M^q(A)) \\
\Big\downarrow{\scriptstyle \mathbf{Nr}_N^q(\varphi_M^q(A))} & & \Big\downarrow{\scriptstyle \varphi_N^q(A)^M} \\
\mathbf{Nr}_N^q(\mathrm{gh}_M(A)) & \xrightarrow{\varphi_N^q(\mathrm{gh}_M(A))} & \mathrm{gh}_N(\mathrm{gh}_M(A)).
\end{array}$$

Now, assume that $M \cap N = \{1\}$. Then $\mathrm{gh}_N \circ \mathrm{gh}_M$ can be identified with gh_{MN}. Under this identification, let us obtain the ring homomorphism

$$\varphi_{M,N}^q(A) : \mathbf{Nr}_N^q\big(\mathbf{Nr}_M^q(A)\big) \to \mathrm{gh}_{MN}(A),$$

which sends $\mathbf{X} = (X_{mn})_{\substack{m\in M\\ n\in N}}$ to $(X_{(m,n)}^q)_{\substack{m\in M\\ n\in N}}$, where

$$X_{(m,n)}^q := \sum_{d|n} dq^{\frac{n}{d}-1}\bigg(\sum_{c|m} cq^{\frac{m}{c}-1}X_{c,d}\bigg).$$

Theorem 5.2. *Let q be any integer, and M, N be truncation sets with $M \cap N = \{1\}$. Then there is a unique functorial isomorphism*

$$\mathfrak{n}_{M,N}^q : \mathbf{Nr}_N^q \circ \mathbf{Nr}_M^q \to \mathbf{Nr}_{MN}^q$$

satisfying $\varphi_{M,N}^q = \varphi_{MN}^q \circ \mathfrak{n}_{M,N}^q$.

Before proving our theorem, we prove a lemma. Given $n \in \mathbb{N}$, the set of all positive integral divisors of n can be made into a poset D_n by defining $i \leqslant j$ in D_n if j is divisible by i. If otherwise stated, we enumerate D_n in the natural order. Let q be an indeterminate, and let m, n be positive integers which are relatively prime. In this case, $D_{mn} = \{cd\colon\ c \mid m,\ d \mid n\}$. From now on, we will fix m, n which are relatively prime. Consider $D_{mn} \times D_{mn}$ matrices $\lambda_q|_{m,n}$, $\lambda_q|_{mn}$ defined by

$$\lambda_q|_{m,n}(ab, cd) = \begin{cases} cdq^{\frac{a}{c}+\frac{b}{d}-2} & \text{if } c \mid a,\, d \mid b, \\ 0 & \text{otherwise} \end{cases}$$

and

$$\lambda_q|_{mn}(ab, cd) = \begin{cases} cdq^{\frac{ab}{cd}-1} & \text{if } c \mid a,\, d \mid b, \\ 0 & \text{otherwise.} \end{cases}$$

It should be remarked that $\lambda_q|_{mn}$ is the matrix from λ_q by restricting the index set from $\mathbb{N}$ to $D(mn)$. Also, $\lambda_q|_{m,n}$ and $\lambda_q|_{mn}$ are lower triangular.

Lemma 5.3. *Let m, n be positive integers which are relatively prime. Then every entry of $(\lambda_q|_{mn})^{-1}\lambda_q|_{m,n}$ has an integral value if q is an integer.*

Proof. Let $\mathbf{X} = (X_{cd})_{\substack{c|m \\ d|n}}$, $\mathbf{Z} = (Z_{cd})_{\substack{c|m \\ d|n}}$, and

$$\lambda_q|_{mn}\mathbf{Z} = \lambda_q|_{m,n}\mathbf{X}.$$

Our claim is equivalent to saying that Z_{ab} is a polynomial in X_{cd}'s with integer coefficients for all $a \mid m$ and $b \mid n$. We will justify our argument by the induction on ab. Note that $Z_{11} = X_{11}$. Put $R = \mathbb{Z}[X_{cd}\colon\ c \mid m,\ d \mid n]$. Applying the induction hypothesis, we can derive that $Z_{cd} \in R$ for all $c \mid a$, $d \mid b$ with $cd < ab$. Now, we will show that $Z_{ab} \in R$. For a prime p dividing ab, we denote by v_p the p-adic discrete valuation on $\mathbb{Q}^\star$ with values in $\mathbb{Z}$, and let $\nu := v_p(ab)$. From $\lambda_q|_{mn}\mathbf{Z} = \lambda_q|_{m,n}\mathbf{X}$

$$\sum_{d|b} dq^{\frac{b}{d}-1}\left(\sum_{c|a} cq^{\frac{a}{c}-1}X_{cd}\right) = \sum_{\substack{c|a \\ d|b}} cdq^{\frac{ab}{cd}-1}Z_{cd}. \tag{5.1}$$

According to the induction hypothesis, we find that $abZ_{ab} \in R$. Hence, since p is an arbitrary prime dividing ab, we are done if we can show that $p^\nu \mid abZ_{ab}$. For simplicity, assume that $p \mid b$. Based on Eq. (5.1) let us proceed the following computation:

$$\begin{aligned}
abZ_{ab} &\equiv \sum_{\substack{c|a,\, d|b \\ v_p(cd)=\nu}} cdq^{\frac{ab}{cd}-1}Z_{cd} \pmod{p^\nu} \\
&= \sum_{c|a,\, d|b} cdq^{\frac{ab}{cd}-1}Z_{cd} - \sum_{c|a,\, d|\frac{b}{p}} cdq^{\frac{ab}{cd}-1}Z_{cd} \\
&= \sum_{d|b} dq^{\frac{b}{d}-1}\left(\sum_{c|a} cq^{\frac{a}{c}-1}X_{cd}\right) - \sum_{c|a,\, d|\frac{b}{p}} cdq^{\frac{ab}{cd}-1}Z_{cd} \\
&\equiv \sum_{d|\frac{b}{p}} dq^{\frac{b}{d}-1}\left(\sum_{c|a} cq^{\frac{a}{c}-1}X_{cd}\right) - \sum_{c|a,\, d|\frac{b}{p}} cdq^{\frac{ab}{cd}-1}Z_{cd} \pmod{p^\nu}.
\end{aligned} \tag{5.2}$$

Set $b = p^\nu b'$ and $d = p^s d'$ with $(p, b') = (p, d') = 1$ and $s < \nu$. In case where p divides q,

$$dq^{\frac{b}{d}-1} \equiv 0 \pmod{p^\nu}$$

since $q^{\frac{b}{d}-1} \equiv 0 \pmod{p^\nu}$. Similarly, $dq^{\frac{ab}{cd}-1} \equiv 0 \pmod{p^\nu}$. Therefore, $abZ_{ab} \equiv 0 \pmod{p^\nu}$. On the other hand, in case where $(p, q) = 1$,

$$dq^{\frac{b}{d}} \equiv dq^{\frac{b}{dp}} \pmod{p^\nu}$$

since $d \equiv 0 \pmod{p^s}$ and $q^{\frac{b}{d}} \equiv q^{\frac{b}{dp}} \pmod{p^{\nu-s}}$. Furthermore, since q is a unit in $\mathbb{Z}/p^\nu\mathbb{Z}$, it follows that

$$dq^{\frac{b}{d}-1} \equiv dq^{\frac{b}{dp}-1} \pmod{p^\nu}.$$

Similarly, we can verify that $dq^{\frac{ab}{cd}-1} \equiv dq^{\frac{ab}{cdp}-1} \pmod{p^\nu}$. Applying this data to Eq. (5.2) yields

$$abZ_{ab} \equiv \sum_{d|\frac{b}{p}} dq^{\frac{b}{dp}-1}\Bigl(\sum_{c|a} cq^{\frac{a}{c}-1}X_{cd}\Bigr) - \sum_{c|a,\, d|\frac{b}{p}} cdq^{\frac{ab}{cdp}-1}Z_{cd} \quad \bigl(\mathrm{mod}\ p^\nu\bigr). \tag{5.3}$$

Due to $\zeta_{mn}\mathbf{Z} = \zeta_{m,n}\mathbf{X}$ we have

$$\sum_{d|\frac{b}{p}} dq^{\frac{b}{dp}-1}\Bigl(\sum_{c|a} cq^{\frac{a}{c}-1}X_{cd}\Bigr) = \sum_{c|a,\, d|\frac{b}{p}} cdq^{\frac{ab}{cdp}-1}Z_{cd} \quad \bigl(\mathrm{mod}\ p^\nu\bigr),$$

which implies that the right-hand side of Eq. (5.3) is zero. This completes the proof. □

Proof of Theorem 5.2. Note that $\mathbf{Nr}_N^q \circ \mathbf{Nr}_M^q$, $\mathbf{Nr}_{MN}^q$, and gh_{MN} are represented by the polynomial ring

$$R := \mathbb{Z}[X_{mn}\colon\ m \in M,\ n \in N]$$

with variables X_{mn}. Set $\mathbf{X} = (X_{mn})_{\substack{m\in M\\ n\in N}}$. By Yoneda's Lemma, a functorial map

$$\mathfrak{n}_{M,N}^q : \mathbf{Nr}_N^q \circ \mathbf{Nr}_M^q \to \mathbf{Nr}_{MN}^q$$

satisfying $\varphi_{M,N}^q = \varphi_{MN}^q \circ \mathfrak{n}_{M,N}^q$ corresponds to an element

$$\mathbf{Z} = (Z_{mn})_{\substack{m\in M\\ n\in N}} \in \mathbf{Nr}_{MN}^q(R),$$

where $\varphi_{M,N}^q(\mathbf{X}) = \varphi_{MN}^q(\mathbf{Z})$. Now, the uniqueness of $\mathfrak{n}_{M,N}^q$ is obvious since such a $\mathbf{Z}$ is uniquely determined if exists. Furthermore, $\mathfrak{n}_{M,N}^q$ is an isomorphism if and only if

$$R = \mathbb{Z}[Z_{mn}\colon\ m \in M,\ n \in N]. \tag{5.4}$$

It follows from

$$Z_{mn} - X_{mn} \in \mathbb{Q}[X_{cd}\colon\ c \mid m,\ d \mid n,\ \text{and } cd < mn],$$

and Lemma 5.3. So, we are done. □

Remark 5.4. When $q = 1, 0, -1$, then $\lambda_q|_{m,n} = \lambda_q|_{mn}$. In this case, $\mathfrak{n}_{M,N}^q$ turns out to be the identity transformation.

5.2. Proof of Theorem 5.1

Now, we are ready to show that Theorem 5.2 yields a pseudo-multiplicative property of μ_q where $q \in \mathbb{Z}$. From now on, all q-necklace rings are supposed to be defined over a $\mathbb{Q}$-algebra. Assume that m, n are positive integers which are relatively prime. Let M (respectively N) be the set of all divisors of m (respectively n). For simplicity of notation, we let

$$\mathbf{X}_d = \begin{pmatrix} \vdots \\ X_{cd} \\ \vdots \end{pmatrix}_{d \in N} \quad \text{and} \quad \mathbf{Y}_d = \begin{pmatrix} \vdots \\ Y_{cd} \\ \vdots \end{pmatrix}_{d \in N}$$

for every $d \in N$. In addition, we let $\lambda_q|_{M,N}$, $\lambda_q|_{MN}$, $\lambda_q|_M$, $\lambda_q|_N$ denote matrices representing $\varphi^q_{M,N}$, φ^q_{MN}, φ^q_M, φ^q_N, respectively. Since

$$\lambda_q|_{M,N} \begin{pmatrix} \vdots \\ \mathbf{X}_d \\ \vdots \end{pmatrix}_{d \in N} = \begin{pmatrix} \vdots \\ \mathbf{Y}_d \\ \vdots \end{pmatrix}_{d \in N}$$

is equivalent to

$$\lambda_q|_N \begin{pmatrix} \vdots \\ \lambda_q|_M \mathbf{X}_d \\ \vdots \end{pmatrix}_{d \in N} = \begin{pmatrix} \vdots \\ \mathbf{Y}_d \\ \vdots \end{pmatrix}_{d \in N},$$

we obtain

$$\begin{pmatrix} \vdots \\ \lambda_q|_M \mathbf{X}_d \\ \vdots \end{pmatrix}_{d \in N} = (\lambda_q|_N)^{-1} \begin{pmatrix} \vdots \\ \mathbf{Y}_d \\ \vdots \end{pmatrix}_{d \in N}.$$

Comparing the nth component in both sides of the above equality gives rise to

$$\lambda_q|_M \mathbf{X}_n = \sum_{d|n} (\lambda_q|_N)^{-1}(n,d)\mathbf{Y}_d.$$

Equivalently,

$$\mathbf{X}_n = (\lambda_q|_M)^{-1}\left(\sum_{d|n} (\lambda_q|_N)^{-1}(n,d)\mathbf{Y}_d\right).$$

Thus, the mth entry of $\mathbf{X}_n$ is given by

$$X_{mn} = \sum_{\substack{c|m \\ d|n}} (\lambda_q|_M)^{-1}(m,c)(\lambda_q|_N)^{-1}(n,d)Y_{cd}. \tag{5.5}$$

On the other hand, from the commutativity relation $\varphi^q_{M,N} = \varphi^q_{MN} \circ \mathfrak{n}^q_{M,N}$ it follows that

$$\mathfrak{n}^q_{M,N} \begin{pmatrix} \vdots \\ \mathbf{X}_d \\ \vdots \end{pmatrix}_{d \in N} = (\lambda_q|_{MN})^{-1} \begin{pmatrix} \vdots \\ Y_{cd} \\ \vdots \end{pmatrix}_{c \in M, d \in N}. \tag{5.6}$$

Combining Theorem 5.2 with Eq. (5.5) we can show that the (m,n)th component of the left-hand side of Eq. (5.6) is given by

$$\sum_{d|m,\, e|n} g_{d,e}(q) \sum_{\substack{i|d \\ j|e}} (\lambda_q|_M)^{-1}(d,i)(\lambda_q|_N)^{-1}(e,j) Y_{ij}, \tag{5.7}$$

for some polynomials $g_{d,e}(q) \in \mathbb{Q}[q]$ taking integral values for all integer arguments. Obviously it coincides with that of the right-hand side of Eq. (5.6), i.e.,

$$\sum_{\substack{c|m \\ d|n}} (\lambda_q|_{MN})^{-1}(mn, cd) Y_{cd}. \tag{5.8}$$

Compare the coefficient of $Y_{1,1}$ of Eq. (5.7) with that of Eq. (5.8) to deduce

$$\sum_{d|m, e|n} g_{d,e}(q)(\lambda_q|_M)^{-1}(d,1)(\lambda_q|_N)^{-1}(e,1) = (\lambda_q|_{MN})^{-1}(mn,1). \tag{5.9}$$

By applying the formulae

$$(\lambda_q|_M)^{-1}(d,1) = \frac{1}{d}\mu^q(d),$$
$$(\lambda_q|_N)^{-1}(e,1) = \frac{1}{e}\mu^q(e),$$
$$(\lambda_q|_{MN})^{-1}(mn,1) = \frac{1}{mn}\mu^q(mn)$$

to Eq. (5.9), we can deduce

$$\mu_q(mn) = \sum_{d|m,\, e|n} \frac{mn}{de} g_{d,e}(q)\mu_q(d)\mu_q(e). \tag{5.10}$$

Letting $f_{d,e}(q)$ be $\frac{mn}{de} g_{d,e}(q)$, it satisfies

(1) $f_{m,n}(q) = 1$, and
(2) $f_{d,e}(q)$ are numerical polynomials in q, that is, it takes an integer value at every integer argument.

Furthermore, when $q = 1, 0, -1$, $\mathfrak{n}^q_{M,N}$ is the identity transformation (refer to Remark 5.4). In this case, it holds

$$\mu_q(mn) = \mu_q(m)\mu_q(n).$$

This implies that $q(q^2 - 1)$ divides $f_{d,e}(q)$ unless $de = mn$. So, we are done. □

Remark 5.5. Assume that $m, n > 1$, $(m, n) = 1$. Choose distinct primes p, p' such that $p \mid m$, $p' \mid n$. We have already shown that $1, 0, -1$ are common roots of $f_{d,e}(q)$'s for $d \mid m$, $e \mid n$, $de < mn$. On the other hand, one can show

$$Z_{mn} = X_{mn} + 0X_{\frac{m}{p}p'} + 0X_{m\frac{n}{p'}} + \frac{q^{p+p'-2}(1 - q^{(p-1)(p'-1)})}{pp'} X_{\frac{m}{p}\frac{n}{p'}} + \cdots,$$

and which implies

$$f_{\frac{m}{p},\frac{n}{p'}}(q) = q^{p+p'-2}\bigl(1 - q^{(p-1)(p'-1)}\bigr) \quad \text{and} \quad f_{\frac{m}{p},n}(q) = f_{m,\frac{n}{p'}}(q) = 0, \ldots.$$

Hence, we can conclude that the common roots are exactly 1, 0, −1. This implies that μ_q is multiplicative if and only if $q = 1, 0, -1$.

5.3. Multiplicativity of $\mu^{(p)}$ and truncated aperiodic rings

In Section 4 we remarked that $\mu^{(p)}$ is multiplicative for every prime p. In this section, we show very briefly that it can be connected to a functorial property of certain truncated rings. In [14], Varadarajan and Wehrhahn introduced the notion of *the aperiodic ring* and investigated its properties and relations with the ring of Witt vectors over a torsion-free ring. The aperiodic ring $\mathrm{Ap}(A)$ over a commutative ring A with identity can be characterized by the following properties:

(Ap1) As a set, it is $A^{\mathbb{N}}$.
(Ap2) For any ring homomorphism $f : A \to B$, the map $\mathrm{Ap}(f) : \mathbf{a} \mapsto (f(a_n))_{n\geqslant 1}$ is a ring homomorphism for $\mathbf{a} = (a_n)_{n\geqslant 1} \in \mathrm{Ap}(A)$.
(Ap3) The maps $\eta_m : \mathrm{Ap}(A) \to A$ defined by

$$\mathbf{a} \mapsto \sum_{d\mid m} a_d \quad \text{for } \mathbf{a} = (a_n)_{n\geqslant 1}$$

are ring homomorphisms.

Given a truncation set N and a positive integer k, we define $\mathrm{Ap}^{(k)}_N$ by a unique covariant functor from the category of commutative rings with identity into itself characterized by the following conditions:

(1) As a set, $\mathrm{Ap}^{(k)}_N(A)$ equals A^N.
(2) For any ring homomorphism $f : A \to B$, the map $\mathrm{Ap}^{(k)}_N(f) : (X_n)_{n\in N} \mapsto (f(X_n))_{n\in N}$ is a ring homomorphism.

(3) The map

$$\eta_N^{(k)} : \mathrm{Ap}_N^{(k)}(A) \to \mathrm{gh}_N(A), \qquad (X_n)_{n\in N} \mapsto \left(\sum_{d|n} \zeta_N^{(k)}(n,d) X_d^{\frac{n}{d}}\right)_{n\in N}$$

is a ring homomorphism. Here, $\zeta_N^{(k)}$ denotes the matrix induced from $\zeta^{(k)}$ by the restriction of index from $\mathbb{N}$ to N.

Given truncation sets M, N with $M \cap N = \{1\}$, we let $\varphi_{M,N}^{(k)} : \mathrm{Ap}_N^{(k)} \circ \mathrm{Ap}_M^{(k)} \to \mathrm{gh}_{MN}$ be the natural transformation such that for any commutative ring A with identity

$$\eta_{M,N}^{(k)}(A) : \mathrm{Ap}_N^{(k)}\big(\mathrm{Ap}_M^{(k)}(A)\big) \to \mathrm{gh}_N\big(\mathrm{gh}_M(A)\big)$$

sends $\mathbf{X} = (X_{mn})_{\substack{m\in M\\ n\in N}}$ to $(X_{(m,n)}^{(k)})_{\substack{m\in M\\ n\in N}}$, where

$$X_{(m,n)}^{(k)} = \sum_{d|n} \zeta_N^{(k)}(n,d)\left(\sum_{c|m} \zeta_M^{(k)}(m,c) X_{c,d}\right).$$

Since $M \cap N = \{1\}$ we can naturally identify $\mathrm{gh}_N(\mathrm{gh}_M(A))$ with $\mathrm{gh}_{MN}(A)$.

Proposition 5.6. *Let $p = 1$ or a prime, and let M, N be truncation sets with $M \cap N = \{1\}$. Then, there is a unique functorial isomorphism*

$$\mathfrak{n}_{M,N}^{(p)} : \mathrm{Ap}_N^{(p)} \circ \mathrm{Ap}_M^{(p)} \to \mathrm{Ap}_{MN}^{(p)}$$

satisfying $\eta_{M,N}^{(p)} = \eta_{MN}^{(p)} \circ \mathfrak{n}_{M,N}^{(p)}$.

Proof. Let

$$R = \mathbb{Z}[X_{m,n}\colon\ m, n \geqslant 1],$$

and let $\mathbf{X} = (X_{m,n})_{m,n\geqslant 1}$. We also let

$$\mathbf{Z} = (Z_{m,n})_{m,n\geqslant 1} := \big(\eta_{MN}^{(p)}\big)^{-1}\big(\eta_{M,N}^{(p)}(\mathbf{X})\big) \in \mathrm{Ap}_{MN}^{(p)}(\mathbb{Q}\otimes R).$$

For our purpose it suffices to show that $\mathbf{Z} \in \mathrm{Ap}_{MN}^{(p)}(R)$. We will show that

$$Z_{m,n} = X_{m,n}$$

for all $m, n \geqslant 1$. But, this is obvious since

$$\zeta^{(p)}(n,d)\zeta^{(p)}(m,c) = \zeta^{(p)}(mn,cd)$$

for c, d, m, n with $c \mid m$, $d \mid n$, and $(m,n) = 1$. □

With the above theorem, one can derive the multiplicativity of $\mu^{(p)}$ by following the way identical to the proof of Theorem 5.1.

6. More on the natural transformation $\mathfrak{n}_q^r$

6.1. $\mathfrak{n}_q^r$ and q-deformed Grothendieck's formal power series ring

In 1956, Grothendieck introduced a functor Λ by endowing a ring structure on the set

$$1 + A[\![t]\!]^+ = \left\{ 1 + \sum_{n=1}^{\infty} a_n t^n \colon a_n \in A,\ \forall n \geqslant 1 \right\}.$$

As a set, $\Lambda(A)$ is the same as $1 + A[\![t]\!]^+$. To explain its ring structure let us introduce indeterminates $x_1, x_2, \ldots; y_1, y_2, \ldots$. And then, we define s_i (respectively σ_j) to be the symmetric functions in variables $x_1, x_2, \ldots$ (respectively $y_1, y_2, \ldots$), that is,

$$\bigl(1 + s_1 t + s_2 t^2 + \cdots\bigr) = \prod_{i \geqslant 1} \frac{1}{1 - x_i t},$$

$$\bigl(1 + \sigma_1 t + \sigma_2 t^2 + \cdots\bigr) = \prod_{i \geqslant 1} \frac{1}{1 - y_i t}.$$

Set $P_n(s_1, \ldots, s_n; \sigma_1, \ldots, \sigma_n)$ to be the coefficient of t^n in

$$\prod_{i,j} \frac{1}{1 - x_i y_j t}.$$

Then, the ring structure on $\Lambda(A)$[2] is given by the following rules:

(1) $\oplus$: Addition is just multiplication of power series.
(2) $\star$: Multiplication is given by

$$\Bigl(1 + \sum a_n t^n\Bigr) \star \Bigl(1 + \sum b_n t^n\Bigr) = 1 + \sum P_n(a_1, \ldots, a_n; b_1, \ldots, b_n) t^n.$$

We now, if possible, define a symmetric map

$$s_t : \mathbf{Nr}(A) \to \Lambda(A), \qquad (b_1, b_2, \ldots) \mapsto \prod_{n \geqslant 1} \left(\frac{1}{1 - t^n} \right)^{b_n}.$$

From [9] it follows that s_t is a ring isomorphism if A has structure of a binomial ring. Here, a binomial ring means a special λ-ring whose all Adams operations are identity, that is $\Psi^n = 1$ for all $n \geqslant 1$. Furthermore, in that case, the diagram

[2] Indeed, $\Lambda(A)$ has even more structure called *special λ-ring*. For more information refer to [9,12].

$$\begin{array}{ccc} \mathbf{Nr}(A) & \xrightarrow{s_t} & \Lambda(A) \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle \frac{d}{dt}\log} \\ \mathrm{gh}(A) & \xrightarrow{\iota} & A[\![t]\!] \end{array}$$

commutes. Here,

$$\iota(d_1, d_2, \ldots) = \sum_{n \geqslant 1} d_n t^{n-1}.$$

Let A be a commutative ring with 1 and assume that $q \cdot 1$ is invertible in A. Consider the map

$$\beta^q : \Lambda(A) \to 1 + A[\![t]\!]^+, \qquad f(t) \mapsto f(t)^q.$$

It is easy to show that β^q is bijective. We define $\Lambda^q(A)$ by the ring whose underlying set is $1 + A[\![t]\!]^+$ and whose ring operations are transported from $\Lambda(A)$ via the map β^q.

Now, for a binomial ring A, consider the map

$$s_t^q : \mathbf{Nr}^q(A) \to \Lambda^q(A), \qquad (b_1, b_2, \ldots) \mapsto \prod_{n \geqslant 1} \left(\frac{1}{1 - qt^n} \right)^{b_n}.$$

Proposition 6.1. *(See [11].) Let q be a non-zero integer. If A is a binomial ring in which $q \cdot 1$ is a unit, then s_t^q is a ring isomorphism. Moreover, the diagram*

$$\begin{array}{ccc} \mathbf{Nr}^q(A) & \xrightarrow{s_t^q} & \Lambda^q(A) \\ {\scriptstyle\varphi^q}\downarrow & & \downarrow{\scriptstyle \frac{d}{dt}\log} \\ \mathrm{gh}(A) & \xrightarrow{\iota_q} & A[\![t]\!] \end{array}$$

commutes. Here,

$$\iota_q(d_1, d_2, \ldots) = q \cdot \sum_{n \geqslant 1} d_n t^{n-1}.$$

Suppose that A is a $\mathbb{Z}[\frac{1}{q}, \frac{1}{r}]$-algebra. Note that it is a binomial ring, and $q \cdot 1$ and $r \cdot 1$ are invertible in A. It is almost straightforward that the map,

$$\iota_q^r : \Lambda^q(A) \to \Lambda^r(A), \qquad f(t) \mapsto f(t)^{\frac{r}{q}},$$

is a ring isomorphism since $\iota_q^r \circ \beta^q = \beta^r$. Letting

$$\gamma_q^r := \left(s_t^r\right)^{-1} \circ \iota_q^r \circ s_t^q,$$

we have the following commutative diagram:

$$\begin{array}{ccc} \mathbf{Nr}^q(A) & \xrightarrow{\gamma_q^r} & \mathbf{Nr}^r(A) \\ {\scriptstyle s_t^q}\downarrow & & \downarrow{\scriptstyle s_t^r} \\ \Lambda^q(A) & \xrightarrow{\iota_q^r} & \Lambda^r(A). \end{array}$$

Letting

$$(y_n)_{n\geqslant 1} = \gamma_q^r\big((x_n)_{n\geqslant 1}\big),$$

it holds

$$\prod_{n\geqslant 1}\left(\frac{1}{1-qt^n}\right)^{\frac{r}{q}x_n} = \prod_{n\geqslant 1}\left(\frac{1}{1-rt^n}\right)^{y_n}.$$

Taking logarithm on both sides and then computing the coefficient of t^n gives rise to the identity

$$\sum_{d|n} d\left(\frac{r}{q}x_d\right)q^{\frac{n}{d}} = \sum_{d|n} dy_d r^{\frac{n}{d}}, \quad \forall n \geqslant 1. \tag{6.1}$$

Canceling q and r out in the both sides of Eq. (6.1), we obtain the relation

$$\varphi^q(x_1, x_2, \ldots) = \varphi^r(y_1, y_2, \ldots),$$

which is equivalent to

$$(y_n)_{n\geqslant 1} = \mathfrak{n}_q^r\big((x_n)_{n\geqslant 1}\big).$$

Thus we can establish the following result.

Theorem 6.2. *Let q and r be non-zero integers. Suppose that A is a $\mathbb{Z}[\frac{1}{q}, \frac{1}{r}]$-algebra. Then, $\mathfrak{n}_q^r = \gamma_q^r$.*

6.2. $\mu^{(p)}$ and restricted free Lie p-algebras

Finally, we investigate the relation between the Möbius function $\mu^{(p)}$ and the denominator identity of a restricted free Lie p-algebra. Note that, for any positive integer k, $s_t \circ \psi_k : \mathbf{Nr}^{(k)}(A) \to \Lambda(A)$ is given by the rule

$$\mathbf{b} \mapsto \prod_{n\geqslant 1}\left(\frac{1-t^{kn}}{1-t^n}\right)^{b_n}.$$

For the definition of s_t see Section 6.1. Set $s_t^{(k)} := s_t \circ \psi_k$. Obviously, $s_t^{(k)}$ is a ring isomorphism and $s_t = s_t^{(k)} \circ \theta_k$, that is,

$$\prod_{n=1}^{\infty}\left(\frac{1}{1-t^n}\right)^{b_n} = \prod_{n=1}^{\infty}\left(\frac{1-t^{kn}}{1-t^n}\right)^{b_n^{(k)}}, \tag{6.2}$$

where $b_n^{(k)} = \sum_{i\geqslant 0} b_{n/k^i}$ with $b_n = 0$ for non-integral values n. In particular, if $k=2$, Eq. (6.2) gives rise to the following formula.

Proposition 6.3. *Set*

$$\prod_{n=1}^{\infty}(1+t^n)^{b_n} = \prod_{n=1}^{\infty}(1-t^n)^{d_n}.$$

Then

(a) $$b_n = -d_n^{(2)},$$

(b) $$d_n = \begin{cases} -b_n & \text{if } n \text{ is odd,} \\ -b_n + b_{\frac{n}{2}} & \text{otherwise.} \end{cases}$$

Proof. Let $k=2$. Then Eq. (6.2) looks like

$$\prod_{n=1}^{\infty}(1-t^n)^{-b_n} = \prod_{n=1}^{\infty}(1+t^n)^{b_n^{(2)}}.$$

This proves our assertion. □

Proposition 6.4. *For $k \in \mathbb{N}$ we have*

$$\frac{1}{1-xt} = \prod_{n\geqslant 1}\left(\frac{1-t^{kn}}{1-t^n}\right)^{M^{(k)}(x,n)}, \tag{6.3}$$

where $M^{(k)}(x,n) = \sum_{i\geqslant 0} M(x, \frac{n}{k^i})$.

Proof. This can be derived by combining the cyclotomic identity with Eq. (6.2). □

We observe that Eq. (6.3) has deep connection with the denominator identity of a restricted free Lie p-algebras. To show this, let p be a prime and $L = L_p(X)$ be the free Lie p-algebra generated by the alphabet $X = \{x_1, \ldots, x_m\}$. It is well known that the dimension of the nth homogeneous component of L equals $M^{(p)}(m,n)$ and its denominator identity is given by

$$\frac{1}{1-mt} = \prod_{n\geqslant 1}\left(\frac{1-t^{pn}}{1-t^n}\right)^{M^{(p)}(m,n)}.$$

One can see that the above identity can be obtained by the substitution of $x = m$ in Eq. (6.3).

Acknowledgment

The author would like to express his sincere gratitude to the referee for his/her valuable advices.

References

[1] H.L. Buchanan, A. Knopfmacher, M.E. Mays, On the cyclotomic identity and related product expansions, Australas. J. Combin. 8 (1993) 233–245.
[2] P. Cartier, Groupes formels associés aux anneaux de Witt generalises, C. R. Acad. Sci. Paris Ser. A–B 265 (1967) A49–A52.
[3] A. Dress, C. Siebeneicher, The Burnside ring of profinite groups and the Witt vectors construction, Adv. Math. 70 (1988) 87–132.
[4] A. Dress, C. Siebeneicher, The Burnside ring of the infinite cyclic group and its relation to the necklace algebra, λ-ring and the Universal ring of the Witt vectors, Adv. Math. 78 (1989) 1–41.
[5] C.F. Gauss, Werke, Band II, Königliche Gesellschaft der Wissenschaften, Göttingen, 1863, pp. 219–222.
[6] G. Labelle, P. Leroux, An extension of the exponential formula in enumerative combinatorics, Electron. J. Combin. 3 (2) (1996) 1–14.
[7] C. Lenart, Formal group-theoretic generalization of the necklace algebra, including a q-deformation, J. Algebra 199 (1998) 703–732.
[8] N. Metropolis, G.-C. Rota, Witt vectors and the algebra of necklaces, Adv. Math. 50 (1983) 95–125.
[9] Y.-T. Oh, Necklace rings and logarithmic functions, Adv. Math. 205 (2) (2006) 434–486.
[10] Y.-T. Oh, q-Deformation of Witt–Burnside rings, Math. Z. 257 (2007) 151–191.
[11] Y.-T. Oh, Classification of the ring of Witt vectors and the necklace ring associated with the formal group law $X + Y - qXY$, J. Algebra 310 (1) (2007) 325–350.
[12] Y.-T. Oh, Nested Witt vectors and their q-deformation, J. Algebra 309 (2) (2007) 683–710.
[13] V.M. Petrogradsky, Witt's formula for restricted Lie algebras, Adv. in Appl. Math. 30 (1–2) (2003) 219–227.
[14] K. Varadarajan, K. Wehrhahn, Aperiodic rings, necklace rings, and Witt vectors, Adv. Math. 81 (1990) 1–29.