Journal of Algebra **199**, 703–732 (1998)
Article No. JA977203

FORMAL GROUP-THEORETIC GENERALIZATIONS OF THE NECKLACE ALGEBRA, INCLUDING A q-DEFORMATION

CRISTIAN LENART

ABSTRACT. N. Metropolis and G.-C. Rota [*Adv. Math*, **50**, 1983, 95–125] studied the *necklace polynomials*, and were lead to define the *necklace algebra* as a combinatorial model for the classical ring of *Witt vectors* (which corresponds to the multiplicative formal group law $X+Y-XY$). In this paper, we define and study a generalized necklace algebra, which is associated with an arbitrary formal group law F over a torsion free ring A. The map from the ring of Witt vectors associated with F to the necklace algebra is constructed in terms of certain generalizations of the necklace polynomials. We present a combinatorial interpretation for these polynomials in terms of words on a given alphabet. The actions of the *Verschiebung* and *Frobenius* operators, as well as of the *p-typification idempotent* are described and interpreted combinatorially. A q-analogue and other generalizations of the *cyclotomic identity* are also presented. In general, the necklace algebra can only be defined over the rationalization $A \otimes \mathbb{Q}$. Nevertheless, we show that for the family of formal group laws over the integers $F_q(X,Y) = X+Y-qXY$, $q \in \mathbb{Z}$, we can define the corresponding necklace algebras over $\mathbb{Z}$. We classify these algebras, and define isomorphic ring structures on the groups of Witt vectors and the groups of curves associated with the formal group laws F_q. The q-necklace polynomials, which turn out to be *numerical polynomials* in two variables, can be interpreted combinatorially in terms of so-called q-words, and they satisfy an identity generalizing a classical one.

Keywords: necklace algebra, Witt vectors, Verschiebung and Frobenius operators, formal group law.

1. The Classical Necklace Algebra and Ring of Witt Vectors

In [8], Metropolis and Rota studied the properties of the so-called *necklace polynomials*, which are defined for every positive integer n by

$$M(x,n) := \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) x^d \qquad \text{in } \mathbb{Q}[x]\,;$$

as usual, μ denotes the classical Möbius function. For every positive integer m, $M(m,n)$ represents the number of *primitive necklaces* (i.e. asymmetric under rotation) with n colored beads, where the colors are chosen from a set of size m. Hence, $M(x,n)$ are *numerical polynomials* (i.e. they take integer values for integer x).

Metropolis and Rota were lead to define for every torsion free commutative ring A with identity the *necklace algebra* $Nr(A)$ (over A). This algebra is the set A^∞ of infinite sequences of elements of A with componentwise addition, and multiplication defined by

$$(\alpha \cdot \beta)_n := \sum_{[i,j]=n} (i,j)\, \alpha_i\, \beta_j\,; \tag{1.1}$$

here $[i,j]$ and (i,j) denote, as usual, the least common multiple and greatest common divisor of i and j, respectively. Note the convention of writing α for an element $(\alpha_1, \alpha_2, \dots)$ in A^∞; similarly, if h is a map from a set X to A^∞, we write $h(x) = (h_1(x), h_2(x), \dots)$. Following [8], we define a map $M\colon A\mathbb{Q} \to A\mathbb{Q}^\infty$ by $M_n(b) := M(b,n)$, where $A\mathbb{Q}$ is the rationalization $A \otimes \mathbb{Q}$. The algebra $Nr(A)$ has two remarkable operators for every positive integer r, namely the *Verschiebung operator* V_r, and the *Frobenius operator* f_r; the former is defined by

$$\mathrm{V}_{r,n}(\alpha) := \begin{cases} \alpha_i & \text{if } n = ri \\ 0 & \text{otherwise}\,, \end{cases} \tag{1.2}$$

and the latter by

$$\mathrm{f}_{r,n}\, \alpha = \sum_d \frac{d}{n}\, \alpha_d\,, \tag{1.3}$$

where the summation ranges over the set $\{d\ :\ [r,d] = rn\}$. In this setup, the properties of the necklace polynomials proved by Metropolis and Rota can be stated as follows:

$$M(xy) = M(x) \cdot M(y) \qquad \text{in } Nr(\mathbb{Q}[x,y])\,, \tag{1.4}$$

$$M(x^r) = \mathrm{f}_r\, M(x) \qquad \text{in } Nr(\mathbb{Q}[x])\,. \tag{1.5}$$

The algebra $Nr(A)$ is closely related to the ring of *Witt vectors* $W(A)$ (see e.g. [6] pp. 233–234), and the ring of unital formal power series $1 + tA[[t]]$ under *cyclic sum* and *cyclic product* (see [8]). To explain this relation, we introduce the *ghost ring* $Gh(A)$, which is just A^∞ with addition and multiplication defined componentwise. We also define the following maps:

$$\begin{aligned}
T\colon W(A\mathbb{Q}) &\to Nr(A\mathbb{Q})\,, & T(\alpha) &:= \sum_{n\ge 1} \mathrm{V}_n M(\alpha_n)\,,\\
w\colon W(A\mathbb{Q}) &\to Gh(A\mathbb{Q})\,, & w_n(\alpha) &:= \sum_{d|n} d\alpha_d^{n/d}\,,\\
g\colon Nr(A\mathbb{Q}) &\to Gh(A\mathbb{Q})\,, & g_n(\alpha) &:= \sum_{d|n} d\alpha_d\,,\\
c\colon Nr(A\mathbb{Q}) &\to 1 + tA\mathbb{Q}[[t]]\,, & c(\alpha) &:= \prod_{n\ge 1} \left(\frac{1}{1-t^n}\right)^{\alpha_n}\,,\\
E\colon Gh(A\mathbb{Q}) &\to 1 + tA\mathbb{Q}[[t]]\,, & E(\alpha) &:= \exp\left(\sum_{n\ge 1} \frac{\alpha_n}{n} t^n\right)\,.
\end{aligned}$$

Theorem 1.6. *(cf.* [8], [3], [13]*)*

1. *All the above maps are ring isomorphisms, and the following diagram is commutative.*

$$\begin{tikzcd}
W(A\mathbb{Q}) \arrow[r, "T"] \arrow[dr, "w"'] & Nr(A\mathbb{Q}) \arrow[r, "c"] \arrow[d, "g"] & 1+tA\mathbb{Q}[[t]] \\
& Gh(A\mathbb{Q}) \arrow[ur, "E"'] &
\end{tikzcd} \tag{1.7}$$

2. *The image of $W(A)$ in $1+tA\mathbb{Q}[[t]]$ is precisely $1+tA[[t]]$. We also have that $T(W(A))=Nr(A)$ for $A=\mathbb{Z}$, but not in general.*
3. *We have that*

$$(c\circ T)(\alpha)=\prod_{n\geq 1}\frac{1}{1-\alpha_n t^n}\,.$$

The following generalization of the cyclotomic identity *(due to V. Strehl* [12]*) holds:*

$$\prod_{n\geq 1}\left(\frac{1}{1-kt^n}\right)^{M(m,n)}=\prod_{n\geq 1}\left(\frac{1}{1-mt^n}\right)^{M(k,n)}\qquad in\ 1+t\mathbb{Z}[[t]]\,, \tag{1.8}$$

where $k,m\in\mathbb{Z}$.

There is a group-theoretic generalization of the necklace algebra due to Dress and Siebeneicher. They interpreted the necklace algebra $Nr(\mathbb{Z})$ as the *Burnside-Grothendieck ring* of *almost finite cyclic sets* in [3]. They also interpreted the map T in this context, and were lead to a combinatorial interpretation of the ring structure of $W(\mathbb{Z})$. This enabled them to generalize the ring of Witt vectors $W(A)$ in [2], by defining the *Witt-Burnside ring* $W_G(A)$ associated with a profinite group G. There is a corresponding necklace algebra associated with G.

In this paper we propose a different generalization of the necklace algebra. Our starting point is the fact that there are groups of Witt vectors associated with every formal group law (these concepts will be discussed in the next section), the classical case corresponding to the multiplicative formal group law. Hence, it is natural to expect the existence of a necklace algebra associated with a formal group law. We give a rigorous definition of this algebra in the next section, and we also define the corresponding necklace polynomials, Verschiebung and Frobenius operators. We discuss some formulas and combinatorial interpretations concerning the action of these operators, as well as a generalized cyclotomic identity (in §2–4). In §5 we discuss the special case corresponding to the formal group laws $F_q(X,Y)=X+Y-qXY$, $q\in\mathbb{Z}$, which provides a q-deformation of the classical necklace algebra.

I am grateful to Haynes Miller and Mike Hopkins for suggestions concerning formal group laws.

2. Formal Group Laws and Generalizations of Witt Vectors and Necklace Algebras

In this section, we define the necklace algebra associated with a formal group law. We shall see that the classical case corresponds to the multiplicative formal group law.

We start with a brief introduction to formal group laws and Witt vectors associated with them (cf. [4]). A (one-dimensional, commutative) *formal group law* over a ring A is a formal power series $F(X,Y)$ in $A[[X,Y]]$ with the following properties:

1. $F(X,0) = F(0,X) = X$;
2. $F(X,Y) = F(Y,X)$;
3. $F(X,F(Y,Z)) = F(F(X,Y),Z)$.

A *homomorphism* between two formal group laws F and G over A is a formal power series $f(X)$ in $A[[X]]$ with constant term 0 satisfying

$$f(F(X,Y)) = G(f(X), f(Y))\,.$$

If $f(X)$ is invertible, i.e. $f'(0)$ is a unit in A, then this power series is called an *isomorphism*; if $f'(0) = 1$, it is called a *strict isomorphism.* If $F = G$, a homomorphism is called an endomorphism of F, or an automorphism if it is also an isomorphism. The set of endomorphisms of F is closed under addition using F (see (2.5)) and composition, whence it forms a ring. As in the previous section, we assume that A is a torsion free commutative ring with identity. Therefore, the formal group law F has a *logarithm*

$$\log_F(X) = \sum_{n\geq 1} a_n X^n\,, \quad a_1 = 1\,, \quad a_n \in A\mathbb{Q}\,,$$

that is a strict isomorphism from F to the additive formal group law $X + Y$. The compositional inverse of $\log_F(X)$ is denoted by $\exp_F(X)$. Since A is torsion free, a homomorphism between the formal group laws F and G over A is necessarily of the form $\exp_G(b\log_F(X))$ for some $b \in A$; if b is a unit, we have an isomorphism, and if $b = 1$, we have a strict isomorphism.

Let us introduce the following notation:

$$[b]_F(X) := \exp_F(b\,\log_F(X)) \in A\mathbb{Q}[[X]] \qquad \text{for } b \in A\mathbb{Q}\,. \tag{2.1}$$

Note that if n is a positive integer, $[n]_F(X)$ lies in $A[[X]]$, and can be defined inductively by

$$[1]_F(X) = X \quad \text{and} \quad [n]_F(X) = F([n-1]_F(X), X)\,;$$

furthermore, $[-n]_F(X)$ also lies in $A[[X]]$, and can be defined by

$$F([-n]_F(X), [n]_F(X)) = 0\,.$$

If $[b]_F(X)$ has coefficients in A for every b in a certain subalgebra B of A, then F is known as a *formal B-module.* In this case, the map $b \mapsto [b]_F$ is a homomorphism from B to the ring of endomorphisms of F extending the homomorphism $n \mapsto [n]_F$ for $n \in \mathbb{Z}$. Note that any formal group law F over a torsion free ring is a formal $\mathbb{Z}_{(r)}$-module (throughout this work, we use the standard notation $\mathbb{Z}_{(r)}$ for the ring of integers localized at r, that is $\{m/n \in \mathbb{Q} \,:\, (n,r) = 1\}$, and $A_{(r)} := A \otimes \mathbb{Z}_{(r)}$). Indeed, $[n]_F(X) \equiv nX \mod (X^2)$, whence $[n]_F(X)$ has a compositional inverse in $\mathbb{Z}_{(r)}[[X]]$ if n is an integer prime to r; thus F has endomorphisms $[1/n]_F(X)$ and so, for any integer m, endomorphisms $[m/n]_F(X) = [m]_F([1/n]_F(X))$.

We now present some examples of formal group laws which will be used later. For every integer q we consider the formal group law over $\mathbb{Z}$

$$F_q(X,Y) := X + Y - qXY\,, \tag{2.2}$$

with logarithm

$$\log_q(X) = \sum_{n\geq 1} \frac{q^{n-1}}{n} X^n\,. \tag{2.3}$$

Note that we have written $\log_q(X)$ instead of $\log_{F_q}(X)$, for simplicity; the same notational convention will be applied throughout. Also note that $F_0(X,Y)$ and $F_1(X,Y)$ are the additive and multiplicative formal group laws, respectively. We will also refer to the formal group laws

$$P(X,Y) = \frac{X+Y-2XY}{1-XY} \quad \text{and} \quad Q(X,Y) = \frac{X+Y}{1+XY} \tag{2.4}$$

with logarithms

$$\log_P(X) = \frac{X}{1-X} \quad \text{and} \quad \log_Q(X) = \sum_{n\geq 0} \frac{X^{2n+1}}{2n+1}\,.$$

Note that $\log_P(X)$ is a strict isomorphism over the integers from P to the additive formal group law, and that Q gives the addition formula for the hyperbolic tangent. Moreover, it is not difficult to check that $X/(1+X)$ is a strict isomorphism (over the integers) from Q to F_2. There is a universal formal group law F_U, which is defined over the so-called *Lazard ring* L. It is known that $L\mathbb{Q}$ is the $\mathbb{Q}$-polynomial algebra $\mathbb{Q}[m_2, m_3, \ldots]$, where m_i are the coefficients of the logarithm of F_U; furthermore, according to Lazard's theorem, L is a polynomial algebra over the integers in infinitely many variables.

We define the map

$$w^F\colon A\mathbb{Q}^\infty \to Gh(A\mathbb{Q})\,, \qquad w_n^F(\alpha) := \sum_{d|n} a_{n/d}\, \alpha_d^{n/d}\,.$$

The group of Witt vectors $W^F(A\mathbb{Q})$ associated with F has underlying set $A\mathbb{Q}^\infty$, and is defined by insisting that w^F be a group homomorphism. Let $\mathcal{C}(F,A)$ denote the group of curves in the formal group law F, that is the group $tA[[t]]$ with addition specified by

$$\alpha(t) +_F \beta(t) := F(\alpha(t), \beta(t))\,. \tag{2.5}$$

The third condition in the definition of a formal group law allows us to iterate the notation $+_F$, whence it makes sense to denote by $\sum^F(\ )$ the formal sum of the indicated elements. We define the map

$$E^F\colon Gh(A\mathbb{Q}) \to \mathcal{C}(F, A\mathbb{Q})\,, \qquad E^F(\alpha) := \exp_F(\alpha(t))\,,$$

where $\alpha(t) := \sum_{n\geq 1} \alpha_n t^n$. The map $H^F\colon W^F(A\mathbb{Q}) \to \mathcal{C}(F, A\mathbb{Q})$ defined by $H^F := E^F \circ w^F$ is known as an *Artin-Hasse type exponential map* associated with F. It is easy to check that

$$H^F(\alpha) = \sum_{n\geq 1}^F \alpha_n t^n\,.$$

For every positive integer r, the Verschiebung operator V_r is defined on $W^F(A\mathbb{Q})$ and on $Gh(A\mathbb{Q})$ as in (1.2), and on $\mathcal{C}(F, A\mathbb{Q})$ by

$$\mathrm{V}_r\,\alpha(t) = \alpha(t^r)\,. \tag{2.6}$$

The Frobenius operator f_r is defined on $Gh(A\mathbb{Q})$ and $\mathcal{C}(F, A\mathbb{Q})$ by

$$\mathrm{f}_{r,n}\,\alpha = r\alpha_{rn} \quad \text{and} \quad \mathrm{f}_r\,\alpha(t) = \alpha(\rho t^{1/r}) +_F \alpha(\rho^2 t^{1/r}) +_F \ldots +_F \alpha(\rho^r t^{1/r})\,, \tag{2.7}$$

respectively, where ρ is a primitive r-th root of unity (see [4]). The Frobenius operator is also defined on $W^F(A\mathbb{Q})$ such that it commutes with H^F. Clearly, V_r acts on $W^F(A)$, $Gh(A)$ and $\mathcal{C}(F, A)$, while f_r acts on $Gh(A)$ and $\mathcal{C}(F, A)$.

$$\begin{tikzcd} W^F(A\mathbb{Q}) \arrow[rr, "H^F"] \arrow[dr, "w^F"'] & & \mathcal{C}(F, A\mathbb{Q}) \\ & Gh(A\mathbb{Q}) \arrow[ur, "E^F"'] & \end{tikzcd} \tag{2.8}$$

Theorem 2.9. *(cf. [4], [7])*

1. *Addition in $W^F(A\mathbb{Q})$ is defined by polynomials with coefficients in A, whence A^∞ is a subgroup of $W^F(A\mathbb{Q})$ (this is the group of Witt vectors $W^F(A)$).*
2. *The maps w^F, E^F, and H^F are isomorphisms of abelian groups, and H^F restricts to an isomorphism between $W^F(A)$ and $\mathcal{C}(F, A)$.*
3. *The Frobenius operator f_r acts on $W^F(A)$. The maps w^F, E^F, and H^F commute with the actions of the operators V_r and f_r. Furthermore, V_r and f_r are endomorphisms of $W^F(A)$ and $\mathcal{C}(F, A)$.*

Remarks 2.10.

1. There is a standard descending filtration on $W^F(A)$ given by the subgroups $\mathrm{V}^n\,W^F(A)$ for $n \geq 0$.
2. If F is the multiplicative formal group law F_1 over A, then $W^F(A)$ coincides with the additive group of the ring $W(A)$ discussed in §1. As pointed out in [4], it is quite remarkable that in this case we are able to define a multiplicative structure on $W^F(A)$ such that $\nu \circ g^F$ is a ring homomorphism, for some map $\nu\colon Gh(A\mathbb{Q}) \to Gh(A\mathbb{Q})$ of the form $\nu_n(\alpha) = k_n\alpha_n$ with $k_n \in \mathbb{Q}$. In §5 we will prove that this actually happens for every formal group law F_q.

We now define generalized necklace polynomials associated with a formal group law F; they will enable us to relate the necklace algebra associated with F to the corresponding Witt vectors in a similar way to the classical case. Let us consider the *incidence algebra* over $A\mathbb{Q}$ of the lattice $D(n)$ of divisors of n (see e.g. [11]). Let ζ^F be the element of this algebra defined by

$$\zeta^F(d_1, d_2) := a_{d_2/d_1}\,,$$

for every $d_1, d_2 \in D(n)$ with $d_1|d_2$. Since $a_1 = 1$, the element ζ^F has a convolution inverse, which will be denoted by μ^F. It is easy to see that $\mu^1(d_1, d_2) = d_1/d_2\,\mu(d_1, d_2) =$

$d_1/d_2\,\mu(d_2/d_1)$. We now define the polynomials

$$M^F(x,n) := \sum_{d|n} \mu^F(d,n)\, a_d\, x^d \qquad \text{in } A\mathbb{Q}[x]\,.$$

Clearly, $M^1(x,n) = M(x,n)$, $M^F(x,1) = x$, and $M^F(1,n) = 0$ for $n > 1$. In order to give a combinatorial interpretation for the polynomials $M^F(x,n)$, we recall from [8] the polynomials $S(x,n) := nM(x,n)$. Let us also recall that a positive integer n is a *period* of the word w (on a given alphabet), if there is a word u such that $w = u^{|w|/n}$, where $|w|$ denotes the length of w; the smallest period is called the *primitive period.* A word with primitive period equal to its length is called *aperiodic.* It is not difficult to prove, via Möbius inversion, that $S(m,n)$ represents the number of aperiodic words of length n on an alphabet with m letters. Necklaces can be defined as equivalence classes of words under the conjugacy relation (that is $w \sim w'$ if and only if there are words u, v such that $w = uv$ and $w' = vu$); moreover, primitive necklaces can be defined as equivalence classes of aperiodic words.

Proposition 2.11. *The polynomials $M^F(x,n)$ can be expressed in the basis $\{S(x,i)\}$ of the $A\mathbb{Q}$-module $A\mathbb{Q}[x]$ by the following formula:*

$$M^F(x,n) = \sum_{d|n} \tau^F\left(\frac{n}{d}, n\right)\, S(x,d)\,,$$

where $\tau^F(i,n) := \sum_{j|i} \mu^F(1,j)\,\zeta^F(j,n)$.

It turns out that this proposition is a special case of Theorem 3.3, so we postpone the proof until then. Let us note that $\tau^F(n,n) = 0$ for $n > 1$, and that $\tau^1(i,n) = 0$ unless $i = 1$; indeed, we can pair the chains in $D(n)$ contributing to $\tau^1(i,n)$ such that each pair consists of a chain containing i, and the same chain with i removed. We now explain the combinatorial significance of the above formula in terms of a combinatorial object which we call *factorized word.* This is a word w (on a given alphabet), together with an expression of the following form:

$$w = (\ldots((w_0^{i_1})^{i_2})\ldots)^{i_k}\,.$$

Clearly, $|w_0| = |w|/(i_1 \ldots i_k)$. The word w_0 will be called the *root* of the factorized word. We define the *type* of the factorized word to be the element $(-1)^k a_{|w_0|} a_{i_1} \ldots a_{i_k}$ in $A\mathbb{Q}$. In this section, as well as in §3 and §4, we usually think of the formal group law F as being the universal one; then the type of a factorized word is a signed monomial in the polynomial generators m_i of $L\mathbb{Q}$. With these definitions, we can now state the following corollary of Proposition 2.11:

Corollary 2.12. *For all positive integers m, n, $M^F(m,n)$ in $A\mathbb{Q}$ enumerates by type the factorized words of length n on an alphabet with m letters.*

Proof. A factorized word $w = (\ldots((w_0^{i_1})^{i_2})\ldots)^{i_k}$ of length n on an alphabet with m letters is uniquely determined by the primitive period u of w (and w_0) and the chain $\{1 = d_0|d_1|\ldots|d_k|n\}$ in $D(n)$ with d_k dividing $n/|u|$. Indeed, we set $w_0 := u^{n/(|u|d_k)}$, and $i_j := d_{k-j+1}/d_{k-j}$ for $1 \le j \le k$. We can choose u of length d dividing n in $S(m,d)$ ways.

According to the above remark, the sum of types of the factorized words of length n and primitive period u is

$$\sum (-1)^k \zeta^F(d_0, d_1) \ldots \zeta^F(d_k, n) = \sum_{d_k | n/d} \mu^F(1, d_k)\, \zeta^F(d_k, n) = \tau^F\left(\frac{n}{d}, n\right) ,$$

where the first summation ranges over all chains which can be associated with u as above; the first equality follows from the generalization of the formula for the Möbius function of a poset. $\square$

We are now able to define the necklace algebra associated with the formal group law F and relate it to the corresponding Witt vectors and curves. In general, this algebra is only defined over $A\mathbb{Q}$, so we denote it by $Nr^F(A\mathbb{Q})$. The module structure of $Nr^F(A\mathbb{Q})$ is the same as that of $Nr(A\mathbb{Q})$. Before discussing the multiplicative structure, let us introduce the following maps:

$$\begin{aligned}
&T^F \colon W^F(A\mathbb{Q}) \to Nr^F(A\mathbb{Q}) , && T^F(\alpha) := \sum_{n \geq 1} \mathrm{V}_n M^F(\alpha_n) , \\
&g^F \colon Nr^F(A\mathbb{Q}) \to Gh(A\mathbb{Q}) , && g_n^F(\alpha) := \sum_{d|n} a_{n/d}\, \alpha_d , \\
&c^F \colon Nr^F(A\mathbb{Q}) \to \mathcal{C}(F, A\mathbb{Q}) , && c^F(\alpha) := {\sum_{n \geq 1}}^F [\alpha_n]_F(t^n) ;
\end{aligned}$$

here $M_n^F(b) := M^F(b, n)$, and the Verschiebung operator V_r on $Nr^F(A\mathbb{Q})$ is defined as in (1.2). Note that $Nr^F(A\mathbb{Q})$ and $Gh(A\mathbb{Q})$ are filtered modules, the filtration being the same as that for $W^F(A\mathbb{Q})$. Furthermore, the maps T^F and g^F are compatible with the corresponding filtrations.

For every map $\nu \colon Gh(A\mathbb{Q}) \to Gh(A\mathbb{Q})$ of the form $\nu_n(\alpha) = k_n \alpha_n$ with $k_n \in \mathbb{Q}$, we define a multiplication in $Nr^F(A\mathbb{Q})$ by insisting that $\nu \circ g^F$ be a ring homomorphism. Considering the formal group law F_1 and $k_n = n$, we obtain the necklace algebra defined by Metropolis and Rota. Another important special case corresponds to the formal group law P defined in (2.4) and $k_n = 1$. It is not difficult to check that

$$g_n^P(\alpha) = \sum_{d|n} \alpha_d ,$$

and that multiplication is defined by

$$(\alpha \cdot \beta)_n = \sum_{[i,j]=n} \alpha_i\, \beta_j .$$

Hence, $\mathbb{Z}^\infty$ is a subring of $Nr^P(\mathbb{Q})$ which coincides with the *aperiodic ring* $Ap(\mathbb{Z})$ defined in [13].

The ring structure of $Nr^F(A\mathbb{Q})$ will only be important in §5; until then, we regard $Nr^F(A\mathbb{Q})$ only as an abelian group, unless otherwise specified.

Proposition 2.13.

1. *The maps T^F, g^F, and c^F are isomorphisms of abelian groups, commuting with the action of the Verschiebung operator; furthermore, the following diagram is commutative.*

$$\begin{tikzcd} W^F(A\mathbb{Q}) \arrow[r, "T^F"] \arrow[dr, "w^F"'] & Nr^F(A\mathbb{Q}) \arrow[r, "c^F"] \arrow[d, "g^F"] & \mathcal{C}(F, A\mathbb{Q}) \\ & Gh(A\mathbb{Q}) \arrow[ur, "E^F"'] & \end{tikzcd} \tag{2.14}$$

2. *If F is a formal A-module, then the maps T^F and $(c^F)^{-1}$ restrict to group isomorphisms from $W^F(A)$ and $\mathcal{C}(F,A)$ to A^∞ with pointwise addition. In particular, this happens for every formal group law over $\mathbb{Z}$ or $\mathbb{Z}_{(r)}$.*

Proof. (1) We note first that g^F is invertible, and that its inverse is defined by

$$(g^F)_n^{-1}(\alpha) = \sum_{d|n} \mu^F(d,n)\,\alpha_d\,. \tag{2.15}$$

We now have

$$\begin{aligned} ((g^F)^{-1} \circ w^F)_n(\alpha) &= \sum_{i|n} \mu^F(i,n) \left(\sum_{j|i} a_j\, \alpha_{i/j}^j \right)\,, \\ T_n^F(\alpha) &= \sum_{i|n} M^F\left(\alpha_i, \frac{n}{i}\right) = \sum_{i|n} \sum_{j|n/i} \mu^F\left(j, \frac{n}{i}\right)\, a_j\, \alpha_i^j \\ &= \sum_{i|n} \sum_{ij|n} \mu^F(ij,n)\, a_j\, \alpha_i^j = \sum_{k|n} \sum_{j|k} \mu^F(k,n)\, a_j\, \alpha_{k/j}^j\,; \end{aligned}$$

the last equality follows by setting $k := ij$. Hence $g^F \circ T^F = w^F$. To check the commutativity of the second triangle, we note that

$$(\log_F \circ E^F \circ g^F)(\alpha) = (g^F(\alpha))(t) \quad \text{and} \quad (\log_F \circ c^F)(\alpha) = \sum_{i\geq 1} \alpha_i\, \log_F(t^i)\,.$$

The coefficients of t^n in both power series above are equal to $\sum_{i|n} a_{n/i}\, \alpha_i$, whence $E^F \circ g^F = c^F$.

The map g^F is clearly an isomorphism of abelian groups, and commutes with the Verschiebung operator. By using the commutativity of diagram 2.14 and Theorem 2.9, we deduce that T^F and c^F have the same properties as g^F. Note that the inverse of T^F can be found by using an algorithm similar to the *clearing algorithm* in [8].

(2) If F is a formal A-module, then c^F restricts to a monomorphism from $Nr^F(A)$ to $\mathcal{C}(F,A)$. But every curve in $\mathcal{C}(F,A)$ can be written uniquely as $c^F(\alpha)$ for some α in A^∞, so c^F induces an isomorphism between $Nr^F(A)$ and $\mathcal{C}(F,A)$. Indeed, α may be found inductively using the fact that for every $k \geq 1$ we have

$$\sum_{n\geq k}{}^F [\alpha_n]_F(t^n) \equiv \alpha_k t^k \mod (t^{k+1})\,.$$

In order to complete the proof, it only remains to observe that $T^F = (c^F)^{-1} \circ H^F$. $\square$

Diagram 2.14 for $F = F_1$ is not exactly the same as diagram 1.7. In order to explain how to relate them, we define the following homomorphisms:

$$\lambda\colon Gh(A\mathbb{Q}) \to Gh(A\mathbb{Q})\,, \qquad \lambda_n(\alpha) := n\alpha_n\,,$$
$$\iota\colon \mathcal{C}(F_1, A\mathbb{Q}) \to 1 + tA\mathbb{Q}[[t]]\,, \qquad \iota(\alpha(t)) := \frac{1}{1-\alpha(t)}\,. \tag{2.16}$$

We can easily check that

$$w = \lambda \circ w^1\,, \;\; g = \lambda \circ g^1\,, \;\; c = \iota \circ c^1\,, \;\; E = \iota \circ E^1 \circ \lambda^{-1}\,.$$

It is well-known that $W^F(A)$ and $\mathcal{C}(F, A)$ are values of functors from formal group laws over A to groups, and that the Artin-Hasse exponential map is a natural equivalence of functors. In particular, a homomorphism $f(X)$ between formal group laws induces the homomorphism $\alpha(t) \mapsto f(\alpha(t))$ between their groups of curves. Similarly, we can view $Nr^F(A\mathbb{Q})$ as the value of a functor from formal group laws over $A\mathbb{Q}$ to $A\mathbb{Q}$-algebras in a natural way, i.e. such that the maps c^F represent a natural equivalence of functors; $\mathcal{C}(F, A\mathbb{Q})$ is now viewed as the ring defined by insisting that $w^F \circ (H^F)^{-1}$ be a ring isomorphism. The homomorphism $Nr(f)\colon Nr^F(A\mathbb{Q}) \to Nr^G(A\mathbb{Q})$ induced by the homomorphism $f(X) = \exp_G(b \log_F(X))$, $b \in A\mathbb{Q}$, between the formal group laws F and G is the unique homomorphism making the following diagram commutative:

$$\begin{tikzcd} Nr^F(A\mathbb{Q}) \arrow[r, "Nr(f)"] \arrow[d, "g^F"'] & Nr^G(A\mathbb{Q}) \arrow[d, "g^G"] \\ Gh(A\mathbb{Q}) \arrow[r, "\cdot b"] & Gh(A\mathbb{Q}) \end{tikzcd} \tag{2.17}$$

Hence it is specified by

$$\alpha \mapsto \beta\,, \quad \text{where } \beta_n = b \sum_{i|j|n} \zeta^F(i,j)\, \mu^G(j,n)\, \alpha_i\,. \tag{2.18}$$

Clearly, the map $Nr(f)$ is a map of filtered modules.

A first result which validates our constructions is a formal group-theoretic generalization of the cyclotomic identity; in some cases, we are able to derive from it nice explicit identities, including a q-analogue of (1.8).

Proposition 2.19. *The following formal group-theoretic generalization of the cyclotomic identity (V. Strehl's form) holds:*

$$\sum_{n\geq 1}{}^F \, [M^F(u,n)]_F(vt^n) = \sum_{n\geq 1}{}^F \, [M^F(v,n)]_F(ut^n) \qquad \text{in } \mathcal{C}(F, A\mathbb{Q})\,, \tag{2.20}$$

where $u, v \in A\mathbb{Q}$. In particular, for F_q we obtain

$$\prod_{n\geq 1} \left(\frac{1}{1-qkt^n}\right)^{M^q(m,n)} = \prod_{n\geq 1} \left(\frac{1}{1-qmt^n}\right)^{M^q(k,n)}\,, \tag{2.21}$$

and for Q we obtain

$$\gamma(t;\, k,\, m) = \gamma(t;\, m,\, k)\,, \tag{2.22}$$

where $k, m \in \mathbb{Z}$*, and*

$$\gamma(t;\, i,\, j) := \frac{\prod_{n\geq 1}(1+it^{2n-1})^{M(j,2n-1)} - \prod_{n\geq 1}(1-it^{2n-1})^{M(j,2n-1)}}{\prod_{n\geq 1}(1+it^{2n-1})^{M(j,2n-1)} + \prod_{n\geq 1}(1-it^{2n-1})^{M(j,2n-1)}}\,.$$

Proof. For the first part, we use the following identity which holds in $Nr^F(A\mathbb{Q})$:

$$\sum_{n\geq 1} M^F(u,n)\,\mathrm{V}_n\,M^F(v) = \sum_{n\geq 1} M^F(v,n)\,\mathrm{V}_n\,M^F(u)\,;$$

indeed, the n-th term in both sequences is

$$\sum_{d|n} M^F(u,d)\,M^F\left(v,\frac{n}{d}\right)\,.$$

We apply c^F to this identity, using the facts

$$c^F(\mathrm{V}_n\,M^F(u)) = \mathrm{V}_n\,c^F(M^F(u)) = \mathrm{V}_n\,H^F(u,0,0,\dots) = ut^n \quad \text{and}$$

$$c^F(u\alpha) = \sum_{n\geq 1}{}^F [u\alpha_n]_F(t^n) = \sum_{n\geq 1}{}^F [u]_F([\alpha_n]_F(t^n)) = [u]_F(c^F(\alpha))\,;$$

here $u \in A\mathbb{Q}$ and $\alpha \in A\mathbb{Q}^\infty$.

Identity (2.21) follows easily from (2.20) by noting that

$$1 - q\left(\sum_{m\geq 1}{}^q X_m\right) = \prod_{m\geq 1}(1-qX_m)\,, \tag{2.23}$$

and

$$1 - q([-1]_q(X)) = (1-qX)^{-1}\,.$$

Combining these identities with the general fact

$$[k]_F(X) = \sum_{1\leq i\leq |k|}{}^F\,[\mathrm{sign}(k)]_F(X)$$

holding for any formal group law F and integer k, we can generalize (2.23) to

$$\sum_{m\geq 1}{}^q [k_m]_q(X_m) = \prod_{m\geq 1}(1-qX_m)^{k_m}\,.$$

This proves (2.21).

In order to derive (2.22) from (2.20), we proceed in a similar way, by noting that

$$\sum_{m\geq 1}{}^Q X_m = \frac{\prod_{m\geq 1}(1+X_m) - \prod_{m\geq 1}(1-X_m)}{\prod_{m\geq 1}(1+X_m) + \prod_{m\geq 1}(1-X_m)}\,, \tag{2.24}$$

and

$$[-1]_Q(X) = -X = \frac{(1+X)^{-1} - (1-X)^{-1}}{(1+X)^{-1} + (1-X)^{-1}}\,.$$

Hence (2.24) generalizes to

$$\sum_{m\geq 1}{}^Q [k_m]_Q(X_m) = \frac{\prod_{m\geq 1}(1+X_m)^{k_m} - \prod_{m\geq 1}(1-X_m)^{k_m}}{\prod_{m\geq 1}(1+X_m)^{k_m} + \prod_{m\geq 1}(1-X_m)^{k_m}}\,, \quad k_m \in \mathbb{Z}\,.$$

Finally, we note that

$$M^Q(i,m) = \begin{cases} M(i,m) & \text{if } m \text{ odd} \\ 0 & \text{otherwise}, \end{cases}$$

since $\log_Q(X) = X + X^3/3 + X^5/5 + \dots$. □

Let us note that (2.21) does not follow from the classical cyclotomic identity (1.8), because $M^q(x,n)$ does not generally coincide with $M(qx,n)/q$. Indeed, $M^q(x,1) = x$, but for any prime p we have

$$M^q(x,p) = \frac{q^{p-1}}{p}(x^p - x)\,, \quad M^q(x,p^2) = \frac{1}{p^2}\left(q^{p^2-1}x^{p^2} - q^{2p-2}x^p + (q^{2p-2} - q^{p^2-1})x\right)\,.$$

3. Verschiebung and Frobenius Operators

In the previous section, we have defined for all positive integers r the Verschiebung operator V_r and the Frobenius operator f_r on $Gh(R)$, $W^F(R)$, and $\mathcal{C}(F,R)$, where R is one of the rings $A\mathbb{Q}$ or A. We have also defined V_r on $Nr^F(A\mathbb{Q})$ and $Nr^F(A)$. We have seen that the isomorphisms in diagram 2.14 commute with the actions of these operators. It is natural to define f_r on $Nr^F(A\mathbb{Q})$ in a compatible way with the isomorphisms mentioned above. By the results in the previous section, f_r is an endomorphism of $Nr^F(A\mathbb{Q})$, and even of $Nr^F(A)$ if F is a formal A-module (although not in general). Let us recall the well-known identities concerning the interaction of the Verschiebung and Frobenius operators on any of the rings on which they act (see [4], [8], [3], [13]):

$$\begin{aligned} &\mathrm{V}_r\mathrm{V}_s = \mathrm{V}_{rs}\,, \qquad \mathrm{f}_r\mathrm{f}_s = \mathrm{f}_{rs}\,, \\ &\mathrm{f}_r\mathrm{V}_r = r\,\mathrm{Id}\,, \\ &\mathrm{f}_r\mathrm{V}_s = (r,s)\,\mathrm{f}_{r/(r,s)}\mathrm{V}_{s/(r,s)} = (r,s)\,\mathrm{V}_{s/(r,s)}\mathrm{f}_{r/(r,s)}\,; \end{aligned} \tag{3.1}$$

these identities are most easily checked in $Gh(A\mathbb{Q})$. In this section, we intend to express and interpret combinatorially the action of the Frobenius operator on $Nr^F(A\mathbb{Q})$.

Theorem 3.2. *The Frobenius operator* f_r *acts on* $Nr^F(A\mathbb{Q})$ *as follows:*

$$\mathrm{f}_{r,n}\,\alpha = r\sum_{d|rn} \tau^F\left(\frac{rn}{[r,d]}, \frac{rn}{d}\right)\,\alpha_d\,.$$

Proof. By (2.15), we have

$$\begin{aligned} \mathrm{f}_{r,n}\,\alpha &= (g^F)_n^{-1}(\mathrm{f}_r\,g^F(\alpha)) = r\sum_{i|n}\mu^F(i,n)\left(\sum_{d|ri} a_{ri/d}\,\alpha_d\right) \\ &= r\sum_{d|rn}\left(\sum_{d|ri,\,i|n}\mu^F\left(1,\frac{n}{i}\right)\,\zeta^F\left(\frac{n}{i},\frac{rn}{d}\right)\right)\,\alpha_d \\ &= r\sum_{d|rn}\left(\sum_{j|rn/[r,d]}\mu^F(1,j)\,\zeta^F\left(j,\frac{rn}{d}\right)\right)\,\alpha_d = r\sum_{d|rn}\tau^F\left(\frac{rn}{[r,d]},\frac{rn}{d}\right)\,\alpha_d\,. \end{aligned}$$

The fourth equality follows by setting $j := n/i$ and noting that the conditions $d|rn/j$ and $j|n$ are equivalent to $j|rn/[r,d]$. $\square$

Note that if $r|d$ and $d \neq rn$, then $\tau^F(rn/[r,d], rn/d) = 0$. On the other hand, according to the observations about μ^1 and τ^1 in §2, we have that $\tau^1(rn/[r,d], rn/d) = 0$ unless $[r,d] = rn$, in which case it is equal to d/rn; hence, we recover the classical formula (1.3) for the action of f_r on $Nr(A)$.

We now interpret combinatorially the action of f_r on $Nr^F(A\mathbb{Q})$ by computing $\mathrm{f}_{r,n}\, M^F(m)$ for positive integers m, n.

Theorem 3.3. *We have that*

$$\mathrm{f}_{r,n}\, M^F(x) = r \sum_{d|n} \mu^F(d,n)\, a_{rd}\, x^{rd}\,. \tag{3.4}$$

The above polynomial can be expressed in the basis $\{S(x,i)\}$ of the $A\mathbb{Q}$-module $A\mathbb{Q}[x]$ by the following formula

$$\mathrm{f}_{r,n}\, M^F(x) = r \sum_{d|n} \tau^F\left(\frac{n}{d}, rn\right)\, S(x^r, d)\,. \tag{3.5}$$

Proof. Formula (3.4) follows easily:

$$\begin{aligned} \mathrm{f}_{r,n}\, M^F(x) &= (g^F)_n^{-1}(\mathrm{f}_r\, w^F(x,0,0,\ldots)) = r\,(g^F)_n^{-1}(a_r x^r, a_{2r}x^{2r}, \ldots) \\ &= r \sum_{d|n} \mu^F(d,n)\, a_{rd}\, x^{rd}\,. \end{aligned}$$

Formula (3.5) follows by rewriting its right-hand side:

$$\begin{aligned} \sum_{d|n} \tau^F\left(\frac{n}{d}, rn\right) S(x^r, d) &= \sum_{d|n} \left(\sum_{i|n/d} \mu^F(1,i)\, \zeta^F(i, rn)\right) \left(\sum_{j|d} \mu(j,d)\, x^{rj}\right) \\ &= \sum_{j|n} \sum_{i|n/j} \mu^F(1,i)\, \zeta^F(i,rn)\, x^{rj} \left(\sum_{j|d|n/i} \mu(j,d)\right) \\ &= \sum_{j|n} \mu^F\left(1, \frac{n}{j}\right) \zeta^F\left(\frac{n}{j}, rn\right) x^{rj} \\ &= \sum_{j|n} \mu^F(j,n)\, a_{rj}\, x^{rj} = \mathrm{f}_{r,n}\, M^F(x)\,. \end{aligned}$$

$\square$

Let us note that $\mathrm{f}_r \mathrm{V}_s\, M^F(x)$ can be easily computed now, by using (3.1). Proposition 2.11 follows from (3.5) by setting $r := 1$. Let us also note that $\tau^1(n/d, rn) = 0$ unless $d = n$, in which case it is equal to $1/(rn)$; hence, (3.5) implies Theorem 4 (pp. 100) in [8], namely the fact that $\mathrm{f}_{r,n}\, M(x) = M(x^r, n)$.

We now define the *repetition factor* of a word w to be the quotient of $|w|$ by the primitive period of w. With this definition, we can interpret (3.5) as follows.

Corollary 3.6. *For all positive integers m, n, $1/r\, \mathrm{f}_{r,n}\, M^F(m)$ in $A\mathbb{Q}$ enumerates by type those factorized words of length rn on an alphabet with m^r letters, for which r divides the repetition factor of the root.*

Proof. Let us recall from the proof of Corollary 2.12 the correspondence between factorized words $w = (\ldots((w_0^{i_1})^{i_2})\ldots)^{i_k}$ and pairs consisting of an aperiodic word u and a chain $\{1 = d_0|d_1|\ldots|d_k\}$ with d_k dividing $|w|/|u|$. In this case, the alphabet has size m^r, the words w have length rn, the length of their primitive period u divides n, and $d_k = rn/|w_0|$ divides $n/|u|$. The last condition is equivalent to "r divides $|w_0|/|u|$", and this implies the fact that $|u|$ divides n. ☐

4. The p-Typification Idempotent

Let p be a prime and recall from [4] that a curve $\alpha(t)$ in $\mathcal{C}(F, A)$ is called *p-typical* if $\log_F(\alpha(t))$ is of the form $\sum_{n\geq 0} \beta_n t^{p^n}$. There is a remarkable idempotent ε_p on $\mathcal{C}(F, A_{(p)})$, which is a projection onto the subgroup of p-typical curves; we will call it the *p-typification idempotent*. It is expressed in terms of V_r and f_r as follows:

$$\varepsilon_p = \sum_{(r,p)=1} \frac{1}{r}\mu(r)\, \mathrm{V}_r\, \mathrm{f}_r\,.$$

The p-typification idempotent has an important role in formal group theory, since the curve $\varepsilon_p\, t$ in $\mathcal{C}(F_U, L_{(p)})$ is an isomorphism over $L_{(p)}$ between the universal formal group law and the universal p-typical formal grup law (see [4] or [10]). We can define ε_p on $Gh(A)$ (not just $Gh(A_{(p)})$), $W^F(A_{(p)})$, and $Nr^F(A\mathbb{Q})$. The action on $Gh(A)$ is very easy to describe, namely:

$$\varepsilon_{p,n}\, \alpha = \begin{cases} \alpha_n & \text{if } n = p^k \\ 0 & \text{otherwise}\,. \end{cases}$$

In order to describe the action of ε_p on $Nr^F(A\mathbb{Q})$, we need some additional notation. First, we denote by $v_p(n)$ the p-valuation of n (that is the largest integer k such that $p^k|n$). Now assume that $m \neq p^k$, $k > 0$, and consider the poset $D_p(m)$ obtained from the lattice of divisors of m by removing all non-zero powers of p. Let μ_p^F denote the convolution inverse of ζ^F in the incidence algebra (over $A\mathbb{Q}$) of this poset. We will write $\mu_p^F(m)$ for $\mu_p^F(1, m)$ if $m \neq p^k$, $k > 0$; otherwise, we set $\mu_p^F(m) = 0$.

Theorem 4.1. *The idempotent ε_p acts on $Nr^F(A\mathbb{Q})$ as follows*

$$\varepsilon_{p,n}\, \alpha = \sum_{k=0}^{v_p(n)} \mu_p^F\left(\frac{n}{p^k}\right) \alpha_{p^k}\,. \tag{4.2}$$

In particular, the idempotent ε_p acts on $Nr(A_{(p)})$ by

$$\varepsilon_{p,n}\, \alpha = \frac{p^{v_p(n)}}{n}\, \mu\left(\frac{n}{p^{v_p(n)}}\right) \alpha_{p^{v_p(n)}}\,. \tag{4.3}$$

Proof. From $g^F(\varepsilon_p\,\alpha)=\varepsilon_p\,g^F(\alpha)$, it follows that

$$\sum_{d|n} a_{n/d}\,\varepsilon_{p,d}\,\alpha=\begin{cases}\sum_{i=0}^{k} a_{p^{k-i}}\,\alpha_{p^i} & \text{if } n=p^k\\ 0 & \text{otherwise}.\end{cases} \tag{4.4}$$

An easy induction provides $\varepsilon_{p,p^k}\,\alpha=\alpha_{p^k}$; hence (4.2) holds in this case, according to the convention $\mu_p^F(p^k)=0$ for $k>0$. We now use induction once more and (4.4) to prove (4.2) for $n\neq p^k$, $k>0$:

$$\begin{aligned}\varepsilon_{p,n}\,\alpha&=-\sum_{d|n,\,d\neq n} a_{n/d}\,\varepsilon_{p,d}\,\alpha=-\sum_{d|n,\,d\neq n} a_{n/d}\left(\sum_{l=0}^{v_p(d)}\mu_p^F\left(\frac{d}{p^l}\right)\alpha_{p^l}\right)\\
&=\sum_{l=0}^{v_p(n)}\left(-\sum_{p^l|d|n,\,d\neq n} a_{n/d}\,\mu_p^F\left(\frac{d}{p^l}\right)\right)\alpha_{p^l}\\
&=\sum_{l=0}^{v_p(n)}\left(-\sum_{i|n/p^l,\,i\neq n/p^l}\mu_p^F(1,i)\,\zeta^F\left(i,\frac{n}{p^l}\right)\right)\alpha_{p^l}\\
&=\sum_{l=0}^{v_p(n)}\mu_p^F\left(\frac{n}{p^l}\right)\alpha_{p^l}\,.\end{aligned}$$

Let us now compute $\mu_p(n):=n\mu_p^1(n)$. We use a formula in [11] which expresses the Möbius function of a subposet in terms of the Möbius function of the whole poset. Assuming that $n\neq p^k$, $k>0$, we have

$$\begin{aligned}\mu_p(n)=\mu_{D_p(n)}(1,n)&=\sum_{l=0}^{v_p(n)}\sum_{0=l_0<l_1<\ldots<l_r=l}(-1)^r\,\mu(1,p^{l_1})\ldots\mu(p^{l_{r-1}},p^l)\,\mu(p^l,n)\\
&=\sum_{l=0}^{v_p(n)}\mu\left(\frac{n}{p^l}\right)\,.\end{aligned}$$

Here we have used

$$\mu(p^k)=\begin{cases}0 & \text{if } k>1\\ -1 & \text{if } k=1\,.\end{cases}$$

Recalling the additional fact that $\mu(rs)=\mu(r)\,\mu(s)$ if $(r,s)=1$, we finally have

$$\mu_p(n)=\begin{cases}0 & \text{if } p|n\\ \mu(n) & \text{otherwise}.\end{cases}$$

This is clearly true for $n=p^k$ as well, whence (4.3) holds. □

Finally, we interpret combinatorially the action of ε_p on $Nr^F(A\mathbb{Q})$ by computing $\varepsilon_{p,n}\,M^F(m)$ for positive integers m,n.

Theorem 4.5. *We have that*

$$\varepsilon_{p,n}\,M^F(x)=\sum_{k=0}^{v_p(n)}\mu^F(p^k,n)\,a_{p^k}\,x^{p^k}\qquad in\ \ A\mathbb{Q}[x]\,. \tag{4.6}$$

The above polynomial can be expressed in the basis $\{S(x,i)\}$ of the $A\mathbb{Q}$-module $A\mathbb{Q}[x]$ by the following formula

$$\varepsilon_{p,n}\, M^F(x) = \sum_{k=0}^{v_p(n)} \left(\sum_{i=0}^{v_p(n)-k} \mu^F\left(1, \frac{n}{p^{i+k}}\right) a_{p^{i+k}} \right) S(x,p^k)\,. \tag{4.7}$$

Proof. Formula (4.6) follows easily:

$$\begin{aligned}\varepsilon_{p,n}\, M^F(x) &= (g_n^F)^{-1}(\varepsilon_p\, w^F(x,0,0,\ldots))\\ &= (g_n^F)^{-1}(x,0,\ldots,0,a_p x^p,0,\ldots,0,a_{p^2}x^{p^2},0,\ldots)\\ &= \sum_{k=0}^{v_p(n)} \mu^F(p^k,n)\, a_{p^k}\, x^{p^k}\,.\end{aligned}$$

Formula (4.7) follows by noting that its right-hand side can be written as

$$\sum_{i=0}^{v_p(n)} \mu^F\left(1,\frac{n}{p^i}\right) a_{p^i}\, x + \sum_{k=1}^{v_p(n)} \left(\sum_{i=0}^{v_p(n)-k} \mu^F\left(1,\frac{n}{p^{i+k}}\right) a_{p^{i+k}} \right) (x^{p^k} - x^{p^{k-1}})\,.$$

Hence the coefficient of x^{p^k} (with $0 \le k \le v_p(n)$) in the right-hand side is equal to

$$\sum_{i=0}^{v_p(n)-k} \mu^F\left(1,\frac{n}{p^{i+k}}\right) a_{p^{i+k}} - \sum_{i=0}^{v_p(n)-k-1} \mu^F\left(1,\frac{n}{p^{i+k+1}}\right) a_{p^{i+k+1}} = \mu^F(p^k,n)\, a_{p^k}\,;$$

here the second sum does not appear if $k = v_p(n)$. □

We can interpret (4.7) combinatorially as follows.

Corollary 4.8. *For all positive integers m,n, $\varepsilon_{p,n}\, M^F(m)$ in $A\mathbb{Q}$ enumerates by type those factorized words of length n on an alphabet with m letters for which the root length is a power of p.*

Proof. We recall once again from the proof of Corollary 2.12 the correspondence between factorized words $w = (\ldots((w_0^{i_1})^{i_2})\ldots)^{i_l}$ and pairs consisting of an aperiodic word u and a chain $\{1 = d_0|d_1|\ldots|d_l\}$ with d_l dividing $|w|/|u|$. In this case the alphabet has size m, the words w have length n, their primitive period u has length p^k for some $0 \le k \le v_p(n)$, and $n/|w_0| = d_l = n/p^{i+k}$ for some $0 \le i \le v_p(n) - k$. The last two conditions are equivalent to $|w_0|$ being a power of p. □

5. A q-Deformation of the Classical Necklace Algebra

In this section we study the necklace algebras $Nr^q(\mathbb{Q})$ corresponding to the family of formal group laws F_q, $q \in \mathbb{Z}$, over $\mathbb{Z}$ defined in (2.2). Recall that the multiplicative structure of $Nr^q(\mathbb{Q})$ depends on the choice of a map $\nu\colon Gh(\mathbb{Q}) \to Gh(\mathbb{Q})$ of the form $\nu_n(\alpha) = k_n\alpha_n$ with $k_n \in \mathbb{Q}$; more precisely, this structure is defined by insisting that $\nu \circ g^q$ be an algebra map. We choose ν to be the map λ defined in (2.16). We have already seen that the classical ring of Witt vectors and the necklace algebra of Metropolis and Rota correspond to $q = 1$ (in other words, to the multiplicative formal group law).

In order to simplify notation, we set $\widetilde{g}^q := \nu \circ g^q$ and $\widetilde{\tau}^q(d,n) := n\tau^q(d,n)$. Theorem 5.8 represents the main result of this section; it states that $Nr^q(\mathbb{Z})$ is a subalgebra of $Nr^q(\mathbb{Q})$, and it determines its structure, thus generalizing the classical necklace algebra construction (which can be recovered for $q = 1$). The proof of this theorem is based on the following two lemmas.

Lemma 5.1. *The polynomials $n/d\,\tau^q(d,n)$ in $\mathbb{Q}[q]$ are numerical polynomials for all positive integers d, n with $d|n$.*

Proof. We fix q in $\mathbb{Z}$, and divide the proof into two steps.

Step 1. We first show that p^k divides $\widetilde{\tau}^q(p^k, np^k)$ if p is a prime and n a positive integer. If $q \equiv 0 \pmod p$, then this is clearly true; indeed, every term of $\widetilde{\tau}^q(p^k, np^k)$ is of the form $\pm q^{p^{l_1}-1} \ldots q^{p^{l_s}-1} q^{np^{l_{s+1}}-1}$ with $l_1 + \ldots + l_{s+1} = k$, and q^{mp^l-1} is divisible by p^l (since $p^l - l - 1 \geq 0$).

If $q \not\equiv 0 \pmod p$, we use induction on k, which obviously starts at 0. Partitioning the terms in $\widetilde{\tau}^q(p^k, np^k)$ according to the smallest element different from 1 in the chains from 1 to np^k in $D(np^k)$ corresponding to them, we obtain

$$\widetilde{\tau}^q(p^k, np^k) = q^{np^k-1} - q^{p^k-1}\, q^{n-1} - \sum_{i=1}^{k-1} q^{p^i-1}\, \widetilde{\tau}^q(p^{k-i}, p^{k-i}n)\,. \tag{5.2}$$

We know that p^l divides $q^{mp^l} - q^{mp^{l-1}}$ for all positive integers l, m, since $M(x, p^l)$ is a numerical polynomial; hence p^l divides $q^{mp^l-1} - q^{mp^{l-1}-1}$, by the assumption on q. Applying this fact and induction to (5.2), we deduce that $\widetilde{\tau}^q(p^k, np^k)$ is congruent modulo p^k to

$$q^{np^{k-1}-1} - q^{p^{k-1}-1}\, q^{n-1} - \widetilde{\tau}^q(p^{k-1}, np^{k-1}) - \sum_{i=2}^{k-1} q^{p^{i-1}-1}\, \widetilde{\tau}^q(p^{k-i}, np^{k-i})\,.$$

But this is equal to 0, by using (5.2) once again.

Step 2. We prove that d divides $\widetilde{\tau}^q(d,n)$ for every $d|n$. Given a prime p dividing d, we have $d = mp^k$ and $n = mrp^k$ for some positive integers k, m, r with $(p,m) = 1$. We now use the following identity:

$$\widetilde{\tau}^q(mp^k, mrp^k) = \sum (-1)^{s-1}\, \widetilde{\tau}^q(p^{i_1}, j_1 p^{i_1}) \ldots \widetilde{\tau}^q(p^{i_s}, j_s p^{i_s})\,, \tag{5.3}$$

where the summation ranges over all $i_t \geq 0$, $j_t > 1$ with $i_1 + i_2 + \ldots + i_s = k$, $j_1 j_2 \ldots j_s = mr$, and $r|j_s$. According to the previous step, we have $p^k | \widetilde{\tau}^q(d,n)$. To prove (5.3), we consider the sets $\mathcal{C}(i_1, \ldots, i_s; j_1, \ldots, j_s)$, with i_t, j_t as above, consisting of all chains from 1 to n in $D(n)$ of the form

$$1|p^{i_{11}}| \ldots |p^{i_{1l_1}}|j_1 p^{i_1}|j_1 p^{i_1+i_{21}}| \ldots |j_1 p^{i_1+i_{2l_2}}|j_1 j_2 p^{i_1+i_2}| \ldots |j_1 \ldots j_{s-1} p^{i_1+\ldots+i_{s-1}+i_{sl_s}}|n\,.$$

These sets determine a partition of the chains from 1 to n in $D(n)$ contributing to $\widetilde{\tau}^q(d,n)$. Furthermore, the sum of terms corresponding to the chains in $\mathcal{C}(i_1, \ldots, i_s; j_1, \ldots, j_s)$ is precisely $(-1)^{s-1}\, \widetilde{\tau}^q(p^{i_1}, j_1 p^{i_1}) \ldots \widetilde{\tau}^q(p^{i_s}, j_s p^{i_s})$, whence (5.3) is proved. ∎

Lemma 5.4. *For every $q \neq 0$, we have that*

$$e_i \cdot e_j = \frac{j}{q}\,\mathrm{V}_{[i,j]}\left(\sum_{d|n} \tau^q\left(\frac{n}{d}, \frac{[i,j]}{i}n\right)\, S(q^{[i,j]/j}, d)\right)_{n\geq 1},$$

where $e_{r,s} = \delta_{r,s}$. Furthermore, $e_i \cdot e_j$ is a sequence of integers divisible by (i,j).

Proof. We base our computation of $e_i \cdot e_j$ on the following formula:

$$e_i \cdot e_j = (\widetilde{g}^q)^{-1}(\widetilde{g}^q(e_i) \cdot \widetilde{g}^q(e_j))\,. \tag{5.5}$$

In order to make the map $\widetilde{g}^q\colon Nr^q(\mathbb{Q}) \to Gh(\mathbb{Q})$ commute with the Verschiebung operator, we have to consider the operator $\mathrm{V}'_r := r\mathrm{V}_r$. We have

$$\widetilde{g}^q(e_i) \cdot \widetilde{g}^q(e_j) = (\mathrm{V}'_i\,\widetilde{g}^q(e_1)) \cdot (\mathrm{V}'_j\,\widetilde{g}^q(e_1))\,,$$

and $\widetilde{g}^q_n(e_1) = q^{n-1}$, whence

$$\widetilde{g}^q(e_i) \cdot \widetilde{g}^q(e_j) = ij\,\mathrm{V}_{[i,j]}\,\pi = (i,j)\,\mathrm{V}'_{[i,j]}\,\pi\,,$$

where $\pi_n := q^{kn-1}q^{ln-1}$, and $k := [i,j]/i$, $l := [i,j]/j$. By (5.5), we have

$$e_i \cdot e_j = (i,j)\,\mathrm{V}_{[i,j]}\,(\widetilde{g}^q)^{-1}(\pi)\,. \tag{5.6}$$

On the other hand, by (2.15) and (3.4) we have

$$\begin{aligned}(\widetilde{g}^q)^{-1}_n(\pi) &= \sum_{d|n} \mu^q(d,n)\,\frac{\pi_d}{d} = k\sum_{d|n}\mu^q(d,n)\,\frac{q^{kd-1}}{kd}\,q^{ld-1}\\ &= \mathrm{f}_{k,n}\,M^q(x)\,, \quad x^{kr} \equiv q^{lr-1}\,;\end{aligned}$$

the "umbral notation" $x^{kr} \equiv q^{lr-1}$ means that x^{kr} is replaced by q^{lr-1} after collecting powers of x in $\mathrm{f}_{k,n}\,M^q(x)$. Furthermore, combining this result with (3.5), we have

$$\begin{aligned}(\widetilde{g}^q)^{-1}_n(\pi) &= k\sum_{d|n}\tau^q\left(\frac{n}{d}, kn\right)\, S(x^k, d)\\ &= \frac{k}{q}\sum_{d|n}\tau^q\left(\frac{n}{d}, kn\right)\, S(q^l, d)\,, \quad x^{kr} \equiv q^{lr-1}\,.\end{aligned} \tag{5.7}$$

The formula for $e_i \cdot e_j$ now follows by combining this result with (5.6).

To complete the proof, it is enough to show that

$$N(d) := \frac{nj}{(i,j)\,q}\tau^q\left(\frac{n}{d}, \frac{[i,j]}{i}n\right)\, S(q^{[i,j]/j}, d) = \frac{1}{q}\widetilde{\tau}^q\left(\frac{n}{d}, \frac{[i,j]}{i}n\right)\, S(q^{[i,j]/j}, d)$$

is divisible by n for every divisor d of n. We know that n divides $qN(d)$ by Lemma 5.1, and the fact that $M(x,d) = S(x,d)/d$ is a numerical polynomial. Assuming that p^r is an arbitrary power of a prime p dividing n, we will now show that p^r divides $N(d)$. If q is prime to p, then this is true by the previous remark. Otherwise, we use the fact that q divides $S(q^{[i,j]/j}, d)$, and that p^r divides every term of $\widetilde{\tau}^q(n/d, [i,j]n/i)$ (essentially because p^s divides q^{mp^s-1} for every $m, s > 0$). $\square$

Theorem 5.8.

1. *The map T^q induces a group isomorphism between $W^q(\mathbb{Z})$ and $Nr^q(\mathbb{Z})$, while the map c^q induces a group isomorphism bewteen $Nr^q(\mathbb{Z})$ and $\mathcal{C}(F_q, \mathbb{Z})$. In particular, $M^q(x,n)$ is a numerical polynomial in q and x. Furthermore, we have the following expression for the polynomials $M^q(x,n)$ as a sum of products of numerical polynomials in q and x:*
$$M^q(x,n) = \sum_{d|n} \left(d\,\tau^q\left(\frac{n}{d}, n\right)\right) \frac{S(x,d)}{d}\,.$$
2. *We have*
$$(\alpha \cdot \beta)_n = \sum_{[i,j]|n} (i,j)\, P_{n,i,j}(q)\, \alpha_i\, \beta_j\,,$$
where $P_{n,i,j}(q)$, $[i,j]|n$, are numerical polynomials in $\mathbb{Q}[q]$ given by
$$P_{n,i,j}(q) = \frac{j}{(i,j)\,q} \sum_{d|n/[i,j]} \tau^q\left(\frac{n}{[i,j]\,d}, \frac{n}{i}\right) S(q^{[i,j]/j}, d)\,.$$
Hence, there is a $\mathbb{Z}$-algebra structure on $Nr^q(\mathbb{Z})$.
3. *The Verschiebung and Frobenius operators are endomorphisms of the algebra $Nr^q(\mathbb{Z})$; the latter acts on $Nr^q(\mathbb{Z})$ by*
$$\mathrm{f}_{r,n}\,\alpha = r \sum_{d|rn} \tau^q\left(\frac{rn}{[r,d]}, \frac{rn}{d}\right) \alpha_d\,.$$

Proof. (1) The fact that T^q and c^q restrict to group isomorphisms is a special case of Proposition 2.13 (2). The formula for the polynomials $M^q(x,n)$ follows from Proposition 2.11. The fact that $d\,\tau^q(n/d, n)$ is a numerical polynomial follows from Lemma 5.1.

(2) This is immediate from Lemma 5.4.

(3) The Frobenius operator acts on $Nr^q(\mathbb{Z})$ since it acts on $\mathcal{C}(F_q, \mathbb{Z})$ and it commutes with the isomorphism c^q between these groups. On the other hand, V_r and f_r are endomorphisms of $Gh(\mathbb{Z})$ with pointwise addition and multiplication, and they commute with the map $\widetilde{g}^q$; hence they are endomorphisms of $Nr^q(\mathbb{Z})$. The formula for the action follows from and Theorem 3.2.

□

Theorem 5.8 shows the existence of necklace algebras $Nr^q(\mathbb{Z})$ for all $q \in \mathbb{Z}$, and completely determines their structure. We have already seen that $M^q(x,n)$ specialize to the classical necklace polynomials, and that the action of the Frobenius operator specializes to (1.3) for $q = 1$. On the other hand, it is easy to check that the product formula specializes to (1.1).

We can now use the maps T^q and c^q to define multiplicative structures on $W^q(\mathbb{Z})$ and $\mathcal{C}(F_q, \mathbb{Z})$. Furthermore, we can substitute $\mathbb{Z}$ with any torsion free commutative ring with identity. We have already seen in §2 that any formal group law over a torsion free ring is a formal $\mathbb{Z}_{(r)}$-module; hence, by Theorem 2.13 (2), $W^q(\mathbb{Z}_{(r)})$, $Nr^q(\mathbb{Z}_{(r)})$, and $\mathcal{C}(F_q, \mathbb{Z}_{(r)})$ are isomorphic rings via the restrictions of the maps T^q and c_q. On the other hand, we can view q as an indeterminate, and define the corresponding structures appropriately. Hence we have the following immediate corollary of Theorem 5.8, which is essentially a generalization of the classical Theorem 1.6.

Corollary 5.9.

1. *There is a ring structure on $W^q(\mathbb{Z})$ such that the restriction of $\lambda \circ w^q$ is a ring homomorphism. The map H^q provides an isomorphic ring structure on $\mathcal{C}(F_q, \mathbb{Z})$.*
2. *Let A be a torsion free commutative ring with identity. There are ring structures on $Nr^q(A)$, $W^q(A)$, and $\mathcal{C}(F_q, A)$ such that the restrictions of $\lambda \circ g^q$ and $\lambda \circ w^q$ are ring homomorphisms, and the restriction of H^q is a ring isomorphism. The corresponding Frobenius and Verschiebung operators are endomorphisms of these rings.*
3. *If A is a $\mathbb{Q}$-algebra or $A = \mathbb{Z}$ or $A = \mathbb{Z}_{(r)}$, there are restrictions of the maps T^q and c^q to the rings $Nr^q(A)$, $W^q(A)$, and $\mathcal{C}(F_q, A)$, and they are isomorphisms. Furthermore, the Verschiebung and Frobenius operators commute with the maps T^q and c^q.*
4. *The statements in (2) also hold if q is viewed as an indeterminate, and A is an algebra over the ring of numerical polynomials in q (in particular, if it coincides with this ring).*

Alternative proof for (1) (due to M. Hopkins [5]). We can assume that $q \neq 0$. Consider the polynomial ring $A = \mathbb{Z}[\alpha_1, \alpha_2, \dots; \beta_1, \beta_2, \dots]$ and the elements α, β in $W^q(A\mathbb{Q})$. The n-th component γ_n of the product $\gamma := \alpha \cdot \beta$ is a polynomial in $A\mathbb{Q}$. We wish to investigate when it has integer coefficients, which depends only on the strict isomorphism class of F_q. Recall formula (2.3) for the logarithm of F_q. On the other hand, we shall see below that the unique strict isomorphism from the multiplicative formal group law to F_q is given by

$$\frac{1-(1-x)^q}{q}\,. \tag{5.10}$$

Over $\mathbb{Z}[1/q]$, formula (5.10) tells us that F_q is strictly isomorphic to the multiplicative formal group law. Hence γ_n has its coefficients in $\mathbb{Z}[1/q]$. Over the localization $\mathbb{Z}_{(q)}$ of $\mathbb{Z}$ at q (see the definition at the beginning of §2), formula (2.3) tells us that F_q is isomorphic to the additive formal group law; indeed, if a prime p divides q, and p^k is the highest power of p dividing n, then p^k also divides q^{n-1} since $k \leq n-1$. This implies that γ_n has its coefficients in $\mathbb{Z}_{(q)}$. Combining the information above, we can see that γ_n has integer coefficients. □

Remark 5.11. If we are interested just in the existence of ring structures on $W^q(\mathbb{Z})$ and $\mathcal{C}(F_q, \mathbb{Z})$, then the argument of M. Hopkins suffices. As in many other situations, combinatorics is useful when one wants some explicit formulas. The necklace algebra $Nr^q(\mathbb{Z})$ is an isomorphic structure to $W^q(\mathbb{Z})$ and $\mathcal{C}(F_q, \mathbb{Z})$ where such formulas can be found. Furthermore, we shall see below that $Nr^q(\mathbb{Z})$ is not just a purely algebraic construction, but it has a nice combinatorial interpretation as well.

Our next task is to classify the algebras $Nr^q(\mathbb{Z})$ up to isomorphism of filtered algebras. Closely related to this is the classification of the formal group laws F_q, $q \in \mathbb{Z}$, up to strict isomorphism over the integers.

Theorem 5.12. *The formal group laws F_q are classified up to strict isomorphism over the integers by the set of prime divisors of q (we adopt the convention that 0 has an empty set of divisors). Furthermore, $Nr^q(\mathbb{Z})$ are classified up to isomorphism of filtered algebras in the same way.*

Proof. Clearly, the additive formal group law F_0 is the only one in its strict isomorphism class, so we may assume $q \neq 0$. We have

$$\log_q(X) = -\frac{\log(1-qX)}{q}, \quad \exp_q(X) = \frac{1-\exp(-qX)}{q}.$$

Hence the unique strict isomorphism over $\mathbb{Q}$ from F_q to F_r is given by

$$f(X) := \frac{1-(1-qX)^{r/q}}{r} = X + \sum_{n\geq 2}(-1)^{n-1}\frac{(r-q)\ldots(r-(n-1)q)}{n!}X^n.$$

Let us assume first that there is a prime p dividing either r or q (but not both). Then the coefficient of X^p in $f(X)$ is not an integer, because its numerator is not divisible by p. Now assume that the sets of prime divisors of q and r are the same, choose an arbitrary prime p, and consider the coefficient c_n of X^n in $f(X)$. If p divides both q and r, then the highest power of p dividing the numerator of c_n is at least $n-1$. On the other hand, the highest power of p dividing $n!$ is $N(n,p) := \sum_{k=1}^{\infty}\lfloor n/p^k\rfloor$, where $\lfloor x\rfloor$ is the greatest integer less or equal to x. But $N(n,p) < n/(p-1) \leq n$. Finally, consider a prime p dividing neither q nor r. We note that $f(X) = q/r\,[r/q]_q(X)$ and $r/q, q/r \in \mathbb{Z}_{(p)}$, whence $f(X)$ has its coefficients in $\mathbb{Z}_{(p)}$ (recall that F_q is a formal $\mathbb{Z}_{(p)}$-module).

If F_q and F_r are isomorphic, then the corresponding necklace algebras will be isomorphic as filtered algebras, by the functoriality of the necklace algebra construction (cf. §2). It remains to show that if q and r have a different set of prime divisors, then $Nr^q(\mathbb{Z})$ and $Nr^r(\mathbb{Z})$ are not isomorphic as filtered algebras. Let us assume that there is such an isomorphism h. Recall the notation e_k for the vector defined by $e_{k,l} = \delta_{k,l}$. Consider the infinite matrix whose rows are the vectors $h(e_k)$, for $k = 1, 2, \ldots$. Since h is an isomorphism of filtered algebras, this matrix is upper triangular with ± 1 on the diagonal. Hence h extends to a filtered isomorphism between $Nr^q(\mathbb{Q})$ and $Nr^r(\mathbb{Q})$, and it induces a filtered automorphism $\widetilde{h}$ of $Gh(\mathbb{Q})$. Now consider the infinite upper triangular matrix with rows $\widetilde{h}(e_k)$. Since $\widetilde{h}(e_k)\cdot\widetilde{h}(e_k) = \widetilde{h}(e_k)$, this is a 0,1-matrix, with 1's on the diagonal. On the other hand, each column contains at most one entry equal to 1; indeed, if $\widetilde{h}(e_k)$ and $\widetilde{h}(e_l)$ contain a 1 in the same column ($k \neq l$), then $\widetilde{h}(e_k+e_l)\cdot\widetilde{h}(e_k+e_l) \neq \widetilde{h}(e_k+e_l)$, which is a contradiction to $\widetilde{h}$ being a ring homomorphism. So our matrix is the identity matrix, which means that $\widetilde{h}$ is the identity map, and h is the map in (2.18) with $b = 1$, $F = F_q$, $G = F_r$. Now consider a prime p dividing q and not dividing r (or vice versa). According to (2.18), we have

$$h_p(e_1) = \frac{q^{p-1}}{p} - \frac{r^{p-1}}{p},$$

which is clearly not an integer. This shows that there is no isomorphism of filtered algebras between $Nr^q(\mathbb{Z})$ and $Nr^r(\mathbb{Z})$ if q and r have a different set of prime divisors. □

We conclude with a combinatorial interpretation of the q-necklace polynomials in terms of so-called q-words. Consider an alphabet Γ, and the free monoid $(\mathbb{Z}/(q)\times\Gamma)^*$ generated by $\mathbb{Z}/(q)\times\Gamma$. We define an action of the group $\mathbb{Z}/(q)$ on $(\mathbb{Z}/(q)\times\Gamma)^*$ by letting the generator of $\mathbb{Z}/(q)$ act as follows:

$$((r_1,a_1),\ldots,(r_n,a_n))\mapsto((r_1+1,a_1),\ldots,(r_n+1,a_n))\,.$$

We call *q-words* the orbits of this action. Note that the corresponding equivalence relation is not a congruence, so we cannot define the concatenation of q-words in the usual way. We concentrate instead on defining the periods of a q-word. Let $[w]$ denote the q-word with representative w. We call a positive integer k a period if there is an element w_0 in $(\mathbb{Z}/(q)\times\Gamma)^*$ of length k and r_i in $\mathbb{Z}/(q)$ for $1\le i\le |w|/k$, such that

$$w=(r_1\,w_0)\cdot\ldots\cdot(r_{|w|/k}\,w_0)\,.$$

It is easy to see that a multiple of a period is not necessarily a period, but the greatest common divisor of two periods is also a period. Hence the periods of $[w]$ still form a sublattice of the lattice of divisors of the length of w, and we can define the primitive period as the zero element of this sublattice. Aperiodic words are then defined as usual. Clearly, for $q=1$ one obtains the classical objects.

We can visualize the above construction in the following way. Consider a cylinder placed horizontally and n circles lying on its surface (the distances between circles are considered irrelevant). Then consider q equidistant parallel lines on the surface of the cylinder which intersect each circle in q points. A q-word of length n with letters from Γ is obtained by attaching a letter to some point (exactly one) on every circle. Concatenation of q-words is defined in the obvious way, by placing two cylinders (assumed to be of the same radius) next to each other, such that the parallel lines coincide in pairs, and the right base of the first cylinder coincides with the left base of the second cylinder. Clearly, there are q ways to concatenate two q-words. The periods of a q-word can now be defined in the usual way, namely k is a period of $[w]$ if there is a way to concatenate $|w|/k$ copies of a q-word $[w_0]$ to get $[w]$.

Let us denote $n\,M^q(x,n)$ by $S^q(x,n)$. We claim that these polynomials are uniquely defined by the relations

$$\sum_{d|n} q^{n/d-1}\,S^q(x,d)=q^{n-1}\,x^n\,. \tag{5.13}$$

Indeed, we have that

$$(\lambda\circ g^q\circ M^q)_n(x)=(\lambda\circ w^q)_n(x,0,0,\ldots)=q^{n-1}x^n\,.$$

We obtain the following combinatorial interpretation for the q-necklace polynomials.

Proposition 5.14. *For all positive integers m,n, $S^q(m,n)$ represents the number of aperiodic q-words of length n with letters chosen from an alphabet of size m.*

Proof. We prove the statement concerning $S^q(m,n)$ by induction on n, which starts at $n=1$. Clearly, there are $q^{n-1}m^n$ q-words of length n with letters chosen from an alphabet of size m. Given an aperiodic q-word of length d dividing n, we can form $q^{n/d-1}$ q-words of length n by considering all possible ways to concatenate n/d copies of the primitive q-word. Since all q-words of length n arise in this way (d being their primitive period), the combinatorial interpretation of $S^q(m,n)$ follows by induction from (5.13). ☐

Unfortunately, for generic q, the obvious actions (by circular permutations) of $\mathbb{Z}/(n)$ on q-words of length n fail to partition the primitive q-words into orbits of size n. Thus, although we know that $S^q(m,n)$ is divisible by n, we are not able to give a combinatorial interpretation of this fact in terms of some objects we would call *q-necklaces*. It seems quite challenging to find such a combinatorial interpretation which would specialize to the classical one for $q=1$.

We now derive a q-analogue of the classical identity (1.4).

Proposition 5.15. *We have*

$$M^q(qxy) = qM^q(x)\cdot M^q(y) \qquad \text{in } Nr^q(\mathbb{Q}[x,y])\,.$$

Proof. We show that the identity holds after applying the map $\lambda\circ g^q$. We use the fact that $\lambda\circ g^q\circ T^q = \lambda\circ w^q$, and the fact that $\lambda\circ g^q$ is an algebra map from $Nr^q(\mathbb{Z})$ to $Gh(\mathbb{Q})$. Hence we have

$$(\lambda\circ g^q)(M^q(qxy)) = \left(q^{2n-1}x^ny^n\right)_{n\geq 1}\,,$$

and

$$(\lambda\circ g^q)(qM^q(x)\cdot M^q(y)) = q(\lambda\circ g^q)(M^q(x))\cdot(\lambda\circ g^q)(M^q(y)) = \left(q^{2n-1}x^ny^n\right)_{n\geq 1}\,.$$

□

As far as formula (1.5) is concerned, we have already presented a generalization of it in Theorem 3.3, which works for any formal group law. We present here a conjecture, which attempts to provide a different generalization of (1.5).

Conjecture 5.16. *We have that*

$$\mathrm{f}_{r,n}\, M^q(x) = \sum_{d\mid n} Q_{r,n,d}(q)\, M^q(x^r,d) \qquad \text{in } \mathbb{Q}[x,q]\,,$$

where $Q_{r,n,d}(q)$ in $\mathbb{Q}[q]$ are numerical polynomials.

References

[1] J. F. Adams. *Stable Homotopy and Generalised Homology.* Chicago Univ. Press, Chicago, 1972.

[2] A. W. M. Dress and C. Siebeneicher. The Burnside ring of profinite groups and the Witt vector construction. *Adv. Math.*, 70:87–132, 1988.

[3] A. W. M. Dress and C. Siebeneicher. The Burnside ring of the infinite cyclic group and its relation to the necklace algebra, λ-rings, and the universal ring of Witt vectors. *Adv. Math.*, 78:1–41, 1989.

[4] M. Hazewinkel. *Formal Groups and Applications.* Academic Press, New York, 1978.

[5] M. Hopkins. Personal communication. October 1996.

[6] S. Lang. *Algebra.* Addison-Wesley, Reading, MA, 1965.

[7] C. Lenart. Symmetric functions, formal group laws and Lazard's theorem. to appear in *Adv. Math.*.

[8] N. Metropolis and G.-C. Rota. Witt vectors and the algebra of necklaces. *Adv. Math*, 50:95–125, 1983.

[9] J. W. Milnor and J. D. Stasheff. *Characteristic Classes*, volume 76 of *Ann. of Math. Stud.* Princeton Univ. Press, Princeton, NJ, 1974.

[10] D. C. Ravenel. *Complex Cobordism and Stable Homotopy Groups of Spheres.* Academic Press, New York, 1986.

[11] R. P. Stanley. *Enumerative Combinatorics.* Wadsworth & Brooks/Cole, Monterey, CA, 1986.

[12] V. Strehl. Cycle counting for isomorphism types of endofunctions. *Bayreuth. Math. Schr.*, 40:153–167, 1992.

[13] K. Varadarajan and K. Wehrhahn. Aperiodic rings, necklace rings, and Witt vectors. *Adv. Math.*, 81:1–29, 1990.

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, U.S.A.

E-mail address: lenart@math.mit.edu