NECKLACE ALGEBRAS AND WITT VECTORS ASSOCIATED WITH FORMAL GROUP LAWS

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). In this paper, we define and study a generalized necklace algebra, which is associated with an arbitrary formal group law $F(X,Y)$ over a torsion free ring A. The map from the ring of Witt vectors associated with $F(X,Y)$ 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 formal group-theoretic generalization of the *cyclotomic identity* is also presented. In general, the necklace algebra can only be defined over the rationalization $A \otimes \mathbb{Q}$. Nevertheless, we show that for an important family of formal group laws over $\mathbb{Z}$, namely $F_q(X,Y) = (X+Y-(1+q)XY)/(1-qXY)$, $q \in \mathbb{Z}$ (which contains the multiplicative formal group law), we can define the corresponding necklace algebra over $\mathbb{Z}$; furthermore, the generalized necklace polynomials turn out to be *numerical polynomials*, and they can be interpreted combinatorially when q is a prime power. These results enable us to define ring structures on the group of Witt vectors and the group of curves associated with the formal group laws $F_q(X,Y)$. We also discuss the universal p-typical formal group law.

1. THE CLASSICAL NECKLACE ALGEBRA AND RING OF WITT VECTORS

In [7], Metropolis and Rota studied the properties of the so-called *necklace polynomials*, which are defined for every n in $\mathbb{N}$ 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 m in $\mathbb{N}$, $M(m,n)$ 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

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

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 [7], 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 r in $\mathbb{N}$, namely the *Verschiebung operator* V_r, and the *Frobenius operator* f_r; the former is defined by

$$\mathrm{V}_{r,n}(\alpha) := \begin{cases} \alpha_i & \text{if } n = ri \\ 0 & \text{otherwise}. \end{cases} \tag{1.1}$$

The algebra $Nr(A)$ is closely related to the ring of *Witt vectors* $W(A)$ (see e.g. [5] pages 233–234), and the ring of unital formal power series $1 + tA[[t]]$ under *cyclic sum* and *cyclic product* (see [7]). To explain this relationship, we introduce the *ghost ring* $Gh(A)$, which is just A^∞ with addition and multiplication defined componentwise. We also define the following maps:

$$T\colon W(A\mathbb{Q}) \to Nr(A\mathbb{Q}), \qquad T(\alpha) := \sum_{n\geq 1} \mathrm{V}_n M(\alpha_n),$$

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

$$g\colon Nr(A\mathbb{Q}) \to Gh(A\mathbb{Q}), \qquad g_n(\alpha) := \sum_{d|n} d\alpha_d,$$

$$c\colon Nr(A\mathbb{Q}) \to 1 + tA\mathbb{Q}[[t]], \qquad c(\alpha) := \prod_{n\geq 1} \left(\frac{1}{1-t^n}\right)^{\alpha_n},$$

$$E\colon Gh(A\mathbb{Q}) \to 1 + tA\mathbb{Q}[[t]], \qquad E(\alpha) := \exp\left(\sum_{n\geq 1} \frac{\alpha_n}{n} t^n\right).$$

Theorem 1.2. *(cf. [7], [3], [12])*

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

$$\begin{array}{ccccc} W(A\mathbb{Q}) & \xrightarrow{\ T\ } & Nr(A\mathbb{Q}) & \xrightarrow{\ c\ } & 1 + tA\mathbb{Q}[[t]] \\ & {\scriptstyle w}\searrow & \downarrow{\scriptstyle g} & \nearrow{\scriptstyle E} & \\ & & Gh(A\mathbb{Q}) & & \end{array} \tag{1.3}$$

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* [11]*) holds:*

$$\prod_{n \geq 1} \left(\frac{1}{1 - kt^n} \right)^{M(m,n)} = \prod_{n \geq 1} \left(\frac{1}{1 - mt^n} \right)^{M(k,n)} \quad \text{in } 1 + t\mathbb{Z}[[t]], \tag{1.4}$$

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

We conclude this section by recalling that Dress and Siebeneicher interpreted the necklace algebra $Nr(\mathbb{Z})$ as the *Burnside-Grothendieck ring* of *almost finite cyclic sets* [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 give a surprising generalization of the ring of Witt vectors $W(A)$ in [2], namely the *Witt-Burnside ring* $W_G(A)$ associated with a profinite group G.

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

In this section, we generalize the constructions in §1 in the context of formal group laws. We shall see that the classical case corresponds to the multiplicative formal group law.

We start this section with a brief survey of 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. $F(X, F(Y, Z)) = F(F(X, Y), Z)$.

As in the previous section, we assume that A is a torsion free commutative ring with identity. Therefore, the formal group law $F(X, Y)$ 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 formal power series satisfying $\log_F(F(X, Y)) = \log_F(X) + \log_F(Y)$. The substitutional inverse of $\log_F(X)$ is denoted by $\exp_F(X)$.

In particular, for every integer q, we consider the formal group law over $\mathbb{Z}$

$$F_q(X, Y) := \frac{X + Y - (q+1)XY}{1 - qXY}, \tag{2.1}$$

with logarithm

$$\log_q(X) = \sum_{n \geq 1} \frac{[n]_q}{n} X^n \,, \qquad [n]_q := 1 + q + \ldots + q^{n-1} \,.$$

Note that we have written $\log_q(X)$ instead of $\log_{F_q}(X)$, for simplicity; the same notational convention will be applied throughout. Let us also note that $F_0(X,Y)$ is the multiplicative formal group law, while $F_{-1}(X,Y)$ gives the addition formula for the hyperbolic tangent. We will also refer to the universal formal group law $F_U(X,Y)$, which is defined over the 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 $F_U(X,Y)$; furthermore, according to Lazard's theorem, L is a $\mathbb{Z}$-polynomial algebra in infinitely many variables (see [4], [1], or [9]). It is worth mentioning that the formal group law $F_q(X,Y)$ is relevant to algebraic topology in the following sense: the ring homomorphism from the Lazard ring (which is isomorphic to the complex cobordism ring, see [1]) to $\mathbb{Z}$ mapping the coefficients of the universal formal group law to the coefficients of $F_q(X,Y)$ is precisely the *Euler characteristic* for $q = 1$, the *Todd genus* for $q = 0$, and the *L-genus* for $q = -1$ (see e.g. [8]).

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 $W^F(A\mathbb{Q})$ 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 $F(X,Y)$, that is the group $tA[[t]]$ with addition specified by

$$\alpha(t) +_F \beta(t) := F(\alpha(t), \beta(t)) \,.$$

The third condition in the definition of a formal group law allows us to iterate the notation $+_F$, whence it makes sense to write $\sum^F$. 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 $F(X,Y)$. 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 (1.1), and on $\mathcal{C}(F, A\mathbb{Q})$ by

$$\mathrm{V}_r\, \alpha(t) = \alpha(t^r) \,. \tag{2.2}$$

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

$$\mathrm{f}_{r,n}\,\alpha = r\alpha_{rn} \quad \text{and} \quad \mathrm{f}_r\,\alpha(t) = \alpha(\rho t^{1/r}) +_F \alpha(\rho^2 t^{1/r}) +_F \ldots +_F \alpha(\rho^r t^{1/r})\,, \tag{2.3}$$

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 $\mathcal{C}(F, A)$.

$$\begin{array}{ccc} W^F(A\mathbb{Q}) & \xrightarrow{\quad H^F \quad} & \mathcal{C}(F, A\mathbb{Q}) \\ & {\scriptstyle w^F} \searrow \quad \nearrow {\scriptstyle E^F} & \\ & Gh(A\mathbb{Q}) & \end{array} \tag{2.4}$$

Theorem 2.5. *(cf. [4], [6])*

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.*
3. *The image of $W^F(A)$ in $\mathcal{C}(F, A\mathbb{Q})$ is precisely $\mathcal{C}(F, A)$.*
4. *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.*

Note that if $F(X, Y)$ is the multiplicative formal group law $F_0(X, Y)$ over A, then $W^F(A)$ coincides with the additive group of $W(A)$. 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 $F_q(X, Y)$.

We now define and study the necklace algebra associated with the formal group law $F(X, Y)$. In general, we are only able to define it over $A\mathbb{Q}$, so we will denote it by $Nr^F(A\mathbb{Q})$. The module structure of $Nr^F(A\mathbb{Q})$ is the same as that of $Nr(A\mathbb{Q})$. In order to define the multiplicative structure, we need to associate with $F(X, Y)$ generalized necklace polynomials. Let us consider the *incidence algebra* over $A\mathbb{Q}$ of the lattice $D(n)$ of divisors of n (see e.g. [10]). 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 $\mu^0(d_1, d_2) = d_1/d_2\,\mu(d_1, d_2) = d_1/d_2\,\mu(d_2/d_1)$, and that $\mu^1(d_1, d_2) = \mu(d_2/d_1)$. 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, $M^0(x,n) = M(x,n)$, 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 [7] the polynomials $S(x,n) := nM(x,n)$. Let us also recall that n in $\mathbb{N}$ 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 2.6. *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 $\tau^0(i,n) = \tau^1(i,n) = 0$ unless $i = 1$; indeed, we can pair the chains in $D(n)$ contributing to $\tau^0(i,n)$ 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 $F(X,Y)$ as being the universal one; then the type of a factorized word is a signed monomial in the polynomial generators of $L\mathbb{Q}$. With these definitions, we can now state the following corollary of Proposition 2.6:

Corollary 2.7. *For all m, n in $\mathbb{N}$, $M^F(m,n)$ enumerates by type the factorized words of length n on an alphabet with m letters.*

We now relate $Nr^F(A\mathbb{Q})$ to the other groups in diagram 2.4, by defining the following maps:

$$T^F\colon W^F(A\mathbb{Q}) \to Nr^F(A\mathbb{Q}), \qquad T^F(\alpha) := \sum_{n\geq 1} \mathrm{V}_n M^F(\alpha_n),$$

$$g^F\colon Nr^F(A\mathbb{Q}) \to Gh(A\mathbb{Q}), \qquad g_n^F(\alpha) := \sum_{d|n} a_{n/d}\,\alpha_d,$$

$$c^F\colon Nr^F(A\mathbb{Q}) \to \mathcal{C}(F, A\mathbb{Q}), \qquad c^F(\alpha) := \sum_{n\geq 1}{}^F\, [\alpha_n]_F\, t^n;$$

here $M_n^F(b) := M^F(b,n)$, the Verschiebung operator V_r on $Nr^F(A\mathbb{Q})$ is defined as in (1.1), and

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

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. For $F(X,Y) = F_0(X,Y)$ and $k_n = n$, we obtain the necklace algebra defined by Metropolis and Rota. 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.

Proposition 2.8. *All the above maps are isomorphisms of abelian groups, commuting with the action of the Verschiebung operator, and the following diagram is commutative.*

$$\begin{array}{ccccc} W^F(A\mathbb{Q}) & \xrightarrow{\;T^F\;} & Nr^F(A\mathbb{Q}) & \xrightarrow{\;c^F\;} & \mathcal{C}(F, A\mathbb{Q}) \\ & {\scriptstyle w^F}\searrow & \downarrow{\scriptstyle g^F} & \swarrow{\scriptstyle E^F} & \\ & & Gh(A\mathbb{Q}) & & \end{array} \tag{2.9}$$

Diagram 2.9 for $F(X,Y) = F_0(X,Y)$ is not exactly the same as diagram 1.3. In order to explain how to relate them, we define the following homomorphisms:

$$\lambda\colon Gh(A\mathbb{Q}) \to Gh(A\mathbb{Q}), \qquad \lambda_n(\alpha) := n\alpha_n, \tag{2.10}$$

$$\iota\colon \mathcal{C}(F_0, A\mathbb{Q}) \to 1 + tA\mathbb{Q}[[t]], \qquad \iota(\alpha(t)) := \frac{1}{1-\alpha(t)}.$$

We can easily check that

$$w = \lambda \circ w^0, \quad g = \lambda \circ g^0, \quad c = \iota \circ c^0, \quad E = \iota \circ E^0 \circ \lambda^{-1}.$$

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.

Proposition 2.11. *The following formal group-theoretic generalization of the cyclotomic identity (V. Strehl's form) holds:*

$$\sum_{n\geq 1}^{F} [M^F(u,n)]_F \, vt^n = \sum_{n\geq 1}^{F} [M^F(v,n)]_F \, ut^n \qquad \text{in } \mathcal{C}(F, A\mathbb{Q}), \tag{2.12}$$

where $u, v \in A\mathbb{Q}$. In particular, for $F_0(X,Y)$ we obtain (1.4), and for $F_{-1}(X,Y)$ we obtain

$$\gamma(t;\, k,\, m) = \gamma(t;\, m,\, k), \tag{2.13}$$

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

$$\gamma(t;\, i,\, j) := \frac{\prod_{n\geq 1}(1+it^{2n-1})^{M(j,2n-1)} - \prod_{n\geq 1}(1-it^{2n-1})^{M(j,2n-1)}}{\prod_{n\geq 1}(1+it^{2n-1})^{M(j,2n-1)} + \prod_{n\geq 1}(1-it^{2n-1})^{M(j,2n-1)}} \qquad \text{in } \mathbb{Z}[[t]].$$

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 2.9 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. It turns out that, in general, f_r is not an operator on $Nr^F(A)$. 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], [7], [3], [12]):

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

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:*

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

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^0 and τ^0 in §2, we have that $\tau^0(rn/[r,d], rn/d) = 0$ unless $[r,d] = rn$, in which case it is equal to d/rn; hence, we recover the formula in [7] for the action of f_r on $Nr(A)$, namely

$$\mathrm{f}_{r,n}\,\alpha = \sum_{d} \frac{d}{n}\,\alpha_d ,$$

where the summation ranges over the set $\{d : [r,d] = rn\}$.

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 $m, n \in \mathbb{N}$.

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

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

Let us note that $\mathrm{f}_r \mathrm{V}_s\, M^F(x)$ can be easily computed now, by using (3.1). Proposition 2.6 follows from (3.5) by setting $r := 1$. Let us also note that $\tau^0(n/d, rn) = 0$ unless $d = n$, in which case it is equal to $1/(rn)$; hence, (3.5) implies Theorem 4 (p. 100) in [7], 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 $m, n \in \mathbb{N}$, $1/r\, \mathrm{f}_{r,n}\, M^F(m)$ 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.*

4. The p-Typification Idempotent

We denote, as usual, by $\mathbb{Z}_{(p)}$ the ring of integers localized at a prime p, that is $\{m/n \in \mathbb{Q} : (n,p) = 1\}$. Let $A_{(p)} := A \otimes \mathbb{Z}_{(p)}$. Recall from [4] that a curve $\alpha(t)$ in $C(F,A)$ 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 $C(F, A_{(p)})$, 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 $C(F_U, L_{(p)})$ is an isomorphism over $L_{(p)}$ between the universal formal group law and the universal p-typical formal grup law (see [4] or [9]). 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

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

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

Theorem 4.4. *We have that*

$$\varepsilon_{p,n}\,M^F(x) = \sum_{k=0}^{v_p(n)} \mu^F(p^k, n)\, a_{p^k}\, x^{p^k} \qquad \text{in } A\mathbb{Q}[x]\,. \tag{4.5}$$

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

$$\varepsilon_{p,n}\,M^F(x) = \sum_{k=0}^{v_p(n)} \left(\sum_{i=0}^{v_p(n)-k} \mu^F\left(1, \frac{n}{p^{i+k}}\right) a_{p^{i+k}} \right) S(x, p^k)\,. \tag{4.6}$$

We can interpret (4.6) combinatorially as follows.

Corollary 4.7. *For all $m, n \in \mathbb{N}$, $\varepsilon_{p,n}\,M^F(m)$ 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.*

5. Special Cases

The main special case which we consider is the family of formal group laws $F_q(X,Y)$, $q \in \mathbb{Z}$, over $\mathbb{Z}$ defined in (2.1). Recall that the classical ring of Witt vectors and the necklace algebra of Metropolis and Rota correspond to $q = 0$ (in other words, to the multiplicative formal group law). According to the general constructions, we have the group of Witt vectors $W^q(\mathbb{Z})$ and the necklace algebra $Nr^q(\mathbb{Q})$, where the multiplicative structure of the latter 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.

Let us consider first the case $q = 1$ and $\nu = \mathrm{Id}$. We have that

$$g_n^1(\alpha) = \sum_{d|n} \alpha_d \,.$$

Hence, according to [12], $\mathbb{Z}^\infty$ is a subring of $Nr^1(\mathbb{Q})$, and this is precisely the *aperiodic ring* $Ap(\mathbb{Z})$. Multiplication in $Ap(\mathbb{Z})$ is defined by

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

¿From now on, we set $\nu := \lambda$, where λ was defined in (2.10). 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 5.3 represents the main result of this section, generalizing the classical necklace algebra construction (which can be recovered for $q = 0$); its proof is based on the following two lemmas.

Lemma 5.1.

1. *If $q \equiv 1$ mod p for a given prime p, then $[p^l m]_q$ is divisible by p^l for any positive integers l, m.*
2. *The polynomials $n/d\,\tau^q(d,n)$ in $\mathbb{Q}[q]$ are numerical polynomials for all positive integers d, n with $d|n$.*

Lemma 5.2. *For every $q \neq 1$, we have that*

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

where $e_{r,s} = \delta_{r,s}$.

Theorem 5.3.

1. *The polynomials $M^q(x,n)$ are numerical polynomials in x and q.*
2. *Multiplication in $Nr^q(\mathbb{Q})$ is defined by numerical polynomials $P_{n,i,j}(q)$ in $\mathbb{Q}[q]$, with $[i,j]$ dividing n, in the sense that*

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

   Hence, there is a $\mathbb{Z}$-algebra structure on $Nr^q(\mathbb{Z})$.
3. *The Frobenius operator f_r acts on $Nr^q(\mathbb{Z})$.*
4. *The map T^q induces a group isomorphism between $W^q(\mathbb{Z})$ and $Nr^q(\mathbb{Z})$.*

The main thrust of Theorem 5.3 is the existence of necklace algebras $Nr^q(\mathbb{Z})$ for all $q \in \mathbb{Z}$. We now use the maps T^q and H^q to define multiplicative structures on $W^q(\mathbb{Z})$ and $C(F^q, \mathbb{Z})$.

Corollary 5.4. *There are ring structures on $W^q(\mathbb{Z})$ and $C(F^q, \mathbb{Z})$ such that the restrictions of the maps T^q, H^q and c^q are ring isomorphisms, and the restriction of $\lambda \circ w^q$ is a ring homomorphism.*

Thus, we have identified a family of formal group laws not mentioned in [4], for which the corresponding groups of Witt vectors and curves have ring structures compatible with the maps in diagram 2.9.

Recall the formula $\mathrm{f}_{r,n}\, M(x) = M(x^r, n)$ in [7], which holds in $Nr(A)$, and which was generalized to $Nr^F(A\mathbb{Q})$ in (3.5). We present here a conjecture, which attempts to provide a different generalization of the original formula of Metropolis and Rota.

Conjecture 5.5. *We have that*

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

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

If q is a prime power p^k, we are able to give a combinatorial interpretation for the polynomials $M^q(x,n)$. Our ingredients are: the field $\mathrm{GF}(q)$, an alphabet Γ with m letters, and the free monoid $(\Gamma \times \mathrm{GF}(q))^*$ generated by $\Gamma \times \mathrm{GF}(q)$. We let $\mathrm{GF}(q) \setminus \{0\}$ act on this monoid by

$$(\theta, (c_1,\omega_1)\dots(c_s,\omega_s)) \mapsto (c_1, \theta\omega_1)\dots(c_s,\theta\omega_s)\,.$$

Note that the equivalence relation determined by the orbits of this action is not a congruence. We define a *q-word* as an orbit in $(\Gamma \times \mathrm{GF}(q))^* \setminus (\Gamma \times \{0\})^*$. We call $s \in \mathbb{N}$ a period of the q-word $[w]$ if there is w_0 in $(\Gamma \times \mathrm{GF}(q))^*$ of length s and $\omega_1, \dots, \omega_t$ in $\mathrm{GF}(q)$ such that $[w] = [(\omega_1 w_0)\dots(\omega_t w_0)]$ (here $0w_0$ is defined in the obvious way). The primitive period of w, aperiodic q-words, q-necklaces, and primitive q-necklaces can now be defined in the usual way. Let us denote $n\, M^q(x,n)$ by $S^q(x,n)$. We claim that these polynomials are uniquely defined by the relations

$$\sum_{d|n} [n/d]_q\, S^q(x,d) = [n]_q\, x^n\,; \tag{5.6}$$

indeed, we have that

$$(\lambda \circ g^q \circ M^q)_n(x) = (\lambda \circ w^q)_n(x,0,0,\dots) = [n]_q\, x^n\,.$$

Examining (5.6), we obtain the combinatorial interpretation mentioned above.

Proposition 5.7. *For every $m,n \in \mathbb{N}$, $S^q(m,n)$ represents the number of aperiodic q-words of length n, and $M^q(m,n)$ represents the number of aperiodic q-necklaces of length n on the given alphabet Γ with m letters.*

We suggest that the constructions of Dress and Siebeneicher [3], [2] could be extended to the above setting.

We conclude this section with a brief reference to the universal *p-typical formal group law* $F_V(X,Y)$ corresponding to the prime p, which is defined over the summand V of $L_{(p)}$ determined by the restriction of the idempotent of $L\mathbb{Q}$ mapping m_k to itself if k is a power of p, and to 0 otherwise (see e.g. [4] or

[9]). The group $W^V(V\mathbb{Q})$ is defined as the subgroup of $W^U(L\mathbb{Q})$ consisting of those infinite sequences α of elements of $V\mathbb{Q}$ for which $\alpha_k = 0$ whenever k is not a power of p; we define $Nr^V(V\mathbb{Q})$ similarly, and abbreviate the sequence $(\alpha_1, 0, \dots, 0, \alpha_p, 0, \dots, 0, \alpha_{p^2}, 0, \dots)$ in $W^V(V\mathbb{Q})$, $Nr^V(V\mathbb{Q})$, or $Gh^V(V\mathbb{Q})$ to $(\alpha_1, \alpha_p, \alpha_{p^2}, \dots)$.

It is known that V is a polynomial $\mathbb{Z}_{(p)}$-algebra. Various polynomial generators for V exist, such as *Hazewinkel's generators* v_k, $k \geq 1$, and *Araki's generators* w_k, $k \geq 0$ (see [9]); these are defined recursively in terms of $m_{(i)} := m_{p^i}$ by

$$pm_{(k)} = \sum_{i=0}^{k-1} m_{(i)}\, v_{k-i}^{p^i} \quad \text{and} \quad pm_{(k)} = \sum_{i=0}^{k} m_{(i)}\, w_{k-i}^{p^i}, \tag{5.8}$$

where $w_0 = p$. It turns out that we can express these generators very easily using the necklace algebra $Nr^V(V\mathbb{Q})$ associated with $F_V(X, Y)$.

Proposition 5.9. *We have that*

$$T^V(v_1, v_2, \dots) = \mathrm{f}_p(1, 0, 0, \dots) \quad \textit{and} \quad T^V(w_0, w_1, w_2, \dots) = (p, 0, 0, \dots).$$

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

[6] C. Lenart. Formal group laws and symmetric functions. Preprint, University of Manchester, 1995.

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

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

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

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

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

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

Mathematics Department, University of Manchester, Manchester M13 9PL, England

E-mail address: lenart@ma.man.ac.uk