Proc. Indian Acad. Sci. (Math. Sci.), Vol. 100, No. 1, April 1990, pp. 37–43.

Verschiebung and Frobenius operators*

K VARADARAJAN
University of Calgary, Calgary, Alberta Canada T2N 1N4

MS received 16 November 1988

Abstract. Metropolis and Rota introduced the concept of the necklace ring Nr(A) of a commutative ring A. When A contains $\mathbb{Q}$ as a subring there is a natural bijection γ: Nr(A) $\to 1 + tA[\![t]\!]$. Grothendieck has introduced a ring structure on $1 + tA[\![t]\!]$ while studying K-theoretic Chern classes. Nr(A) comes equipped with two families of operators F_r, V_r called the Frobenius and Verschiebung operators. Mathematicians studying formal group laws have introduced two families of operators F_r and V_r on $1 + tA[\![t]\!]$. Metropolis and Rota have not however tried to show that γ preserves these operators. They transport the operators from Nr(A) to $1 + tA[\![t]\!]$ using γ. In our present paper we show that γ does preserve all these operators.

Keywords. Necklace ring; unital power series ring; ring of Witt vectors.

Introduction

In [5] Metropolis and Rota introduce the concept of the necklace ring Nr(A) of a commutative ring A. It turns out that Nr(A) is a commutative ring provided with two families of operators V_r: Nr(A) $\to$ Nr(A) and F_r: Nr(A) $\to$ Nr(A) defined for every integer $r \geq 1$, referred to as the Verschiebung and the Frobenius operators respectively. Let $1 + tA[\![t]\!]$ denote the set of unital formal power series over A in the indeterminate t. When A contains $\mathbb{Q}$ (the field of rational numbers) as a subring, the map γ: Nr(A) $\to$ $1 + tA[\![t]\!]$ defined by $\gamma((c_1, c_2, c_3, c_4, \ldots\ldots\ldots)) = \prod_{k \geq 1} 1/(1 - t^k)^{c_k}$ can be easily seen to be a bijection. Using the bijection γ they transport the ring structure of Nr(A) and the operators V_r and F_r to $1 + tA[\![t]\!]$. It is clear that addition in Nr(A) gets transformed under γ to the usual multiplication of formal power series. They write $\oplus$ for the usual multiplication of power series and refer to it as the cyclic addition. The operation * in $1 + tA[\![t]\!]$ which corresponds to the multiplication in Nr(A) under γ is referred to as the cyclic multiplication. In general to be able to define the map γ we have to assume that A contains $\mathbb{Q}$ as a subring. However, when $A = \mathbb{Z}$, the ring of integers, γ as defined above turns out to be meaningful and yields a bijection Nr($\mathbb{Z}$) $\to 1 + t\,\mathbb{Z}[\![t]\!]$. Thus cyclic addition and cyclic multiplication can be defined in $1 + t\mathbb{Z}[\![t]\!]$ in exactly the same way.

While studying K-theoretic Chern classes, Grothendieck introduced a ring structure on $1 + tA[\![t]\!]$ for any commutative ring A. We will recall this definition in §1 of the

*Part of this work was done while the author was visiting the Institute of Mathematical Sciences, Madras.

present paper. When $A = \mathbb{Z}$, Dress and Siebeneicher [2], while studying the Burnside ring of the infinite cyclic group formed using almost finite cyclic sets, prove among many far reaching results that the ring structure on $1 + t\,\mathbb{Z}[[t]]$ under cyclic addition and cyclic multiplication agrees with the ring structure defined by Grothendieck. In our present paper we will prove that a similar result is also true for all commutative rings A containing $\mathbb{Q}$ as a subring. Our proof will not involve the theory of Burnside rings. Our proof is also valid when $A = \mathbb{Z}$.

People studying formal groups have introduced two families of operators V_r: $1 + tA[[t]] \to 1 + t\,A[[t]]$ and $F_r: 1 + tA[[t]] \to 1 + tA[[t]]$ for each integer $r \geqslant 1$, using elementary symmetric functions. We will recall the definition of these operators in §1 of the present paper. In our present paper we will show that when either $A = \mathbb{Z}$ or A contains $\mathbb{Q}$ as a subring, the operations V_r and F_r defined by Metropolis and Rota on $1 + tA[[t]]$ by transporting the same operations from $\mathrm{Nr}(A)$ by using the bijection γ, agree with the corresponding operations on $1 + tA[[t]]$, defined by people working on formal groups, using elementary symmetric functions.

In [7] the concept of the aperiodic ring $\mathrm{Ap}(A)$ for any commutative ring A was introduced and it was shown that it was a better behaved functor than $\mathrm{Nr}(A)$. In [8] we define operators V_r and F_r on $1 + tA[[t]]$ for each integer $r \geqslant 1$ by a method quite different from the method used by people studying formal groups. From the results in the present paper, it will follow that the operators V_r and F_r defined by us on $1 + tA[[t]]$ in [8] are the same as the operators V_r and F_r defined by people working on formal groups. In [8] we introduced a natural map $\chi: \mathrm{W}(A) \to \mathrm{Ap}(A)$ and using our definition of V_r and F_r on $1 + tA[[t]]$ we showed that χ is a ring homomorphism of $\mathrm{W}(A)$ into $\mathrm{Ap}(A)$ preserving the Verschiebung and Frobenius operators. We also characterised the image of χ. Further, we showed that $\mathrm{Ker}\,\chi = 0$ if and only if the additive group of A is torsion-free. Here $\mathrm{W}(A)$ denotes the ring of Witt vectors over A.

Throughout this paper A will denote a commutative ring with identity $1_A \neq 0$. All ring homomorphisms should preserve identity elements. For a subring B of A we want $1_B = 1_A$. We will adopt the notation in [4], [5], [6] and [7]. The Ghost ring will be defined as in [8].

1. The ring structure and the operators V_r and F_r on $1 + tA[[t]]$.

In this section we briefly recall the ring structure defined by Grothendieck on $1 + tA[[t]]$ and also the definition of the operators V_r and F_r. A good source where these are explicitly defined is [4]. Please refer to pages 119–123 of [4].

Let $\xi_1, \ldots, \xi_r; \eta_1, \ldots, \eta_s$ be indeterminates. We define X_i and Y_i by the equations

$$\prod_i (1 - \xi_i t) = 1 + X_1 t + X_2 t^2 + \cdots \tag{1}$$

$$\prod_i (1 - \eta_i t) = 1 + Y_1 t + Y_2 t^2 + \cdots \tag{2}$$

In other words the X_i and Y_i are the elementary symmetric functions in the ξ_j and η_j up to sign. Consider the products

$$\prod_{i,j} (1 - \xi_i \eta_j t) = 1 + P_1 t + P_2 t^2 + \cdots \tag{3}$$

$$\prod_i (1 - \xi_i^n t) = 1 + Q_{n,1} t + Q_{n,2} t^2 + \cdots \tag{4}$$

By the fundamental theorem on symmetric functions P_i can be written as a polynomial $P_i(X_1,\ldots,X_i;\, Y_1,\ldots,Y_i)$ in $X_1,\ldots,X_i$, $Y_1,\ldots,Y_i$ and $Q_{n,i}$ can be written as a polynomial in $X_1,\ldots,X_{ni}$, in every case with integer coefficients. Moreover these polynomiials $P_i(X;\, Y)$ and $Q_{n,i}(X)$ are independent of r and s (the number of ξ's and η's) provided $r \geqslant i$ and $s \geqslant i$ for $P_i(X;\, Y)$ and $r \geqslant ni$ for $Q_{n,i}$. This means formally we can write

$$\prod_{i=1}^{\infty}(1-\xi_i t) = 1 + X_1 t + X_2 t^2 + \cdots \tag{5}$$

and

$$\prod_{i=1}^{\infty}(1-\eta_i t) = 1 + Y_1 t + Y_2 t^2 + \cdots \tag{6}$$

imply

$$\prod_{i,j=1}^{\infty}(1-\xi_i\eta_j t) = 1 + P_1(X_1;\, Y_1)t + P_2(X_1, X_2;\, Y_1, Y_2)t^2 + \cdots \tag{7}$$

and

$$\prod_{i=1}^{\infty}(1-\xi_i^n t) = 1 + Q_{n,1}(X_1, X_2,\ldots,X_n)t + Q_{n,2}(X_1,\ldots,X_{2n})t^2 + \cdots. \tag{8}$$

Addition $\oplus$ in $1 + tA[\![t]\!]$ is defined to be the same as the usual multiplication of formal power series. The product operation $\circ$ is defined as follows: Let

$$f(t) = 1 + a_1 t + a_2 t^2 + \cdots\cdots$$

and

$$g(t) = 1 + b_1 t + b_2 t^2 + \cdots\cdots.$$

Then

$$f(t)\circ g(t) = 1 + P_1(a_1;\, b_1)t + P_2(a_1, a_2;\, b_1, b_2)t^2 + \cdots\cdots \tag{9}$$

$1 + tA[\![t]\!]$ is a commutative ring under $\oplus$ as addition and $\circ$ as multiplication. 1 is the neutral element under $\oplus$ and $1 - t$ is the identity element for the product operation $\circ$. This ring structure was introduced by Grothendieck in [3] while studying K-theoretic Chern classes.

For each integer $r \geqslant 1$, the operators $V_r\colon 1 + tA[\![t]\!] \to 1 + tA[\![t]\!]$ and $F_r\colon 1 + tA[\![t]\!] \to 1 + tA[\![t]\!]$ are defined by

$$V_r(f(t)) = 1 + a_1 t^r + a_2 t^{2r} + a_3 t^{3r} + \cdots \tag{10}$$

$$F_r(f(t)) = 1 + Q_{r,1}(a_1,\ldots,a_r)t + Q_{r,2}(a_1,\ldots,a_{2r})t^2 + \cdots \tag{11}$$

V_r are "additive" homomorphisms and F_r are ring homomorphisms.

2. The isomorphism $E\colon W(A) \to 1 + tA[\![t]\!]$

Let W(A) denote the ring of Witt vectors over A (see pages 115–117 of [4] for the definition of W(A)). For any $\mathbf{a} = (a_1, a_2, a_3, \ldots)$ let $E(\mathbf{a}) = \prod_{k \geqslant 1}(1/(1 - a_k t^k))$. It is well known that E is a bijection. A result of Cartier [1] asserts that $E\colon \mathrm{W}(A) \to 1 + tA[\![t]\!]$ is a ring isomorphism. A proof of this result can also be found on page 121 of [4]. Using the isomorphism E^{-1} we transport the operators V_r and F_r to W(A).

Before proceeding further, we will give an alternative characterization of F_r on $1 + tA[\![t]\!]$, which takes into account the bijective nature of E.

Theorem 2.1. *For any two integers $r \geqslant 1$ and $k \geqslant 1$ and any $a \in A$ we have* $F_r(1/(1-at^k)) = (1/(1-a^{(r/(r,k))}t^{(k/(r,k))}))^{(r,k)}$

Proof: For the proof we need the following identities connecting the various F_r and V_s.

$$V_1 = F_1 = Id \tag{12}$$

$$V_r V_s = V_{rs} \tag{13}$$

$$F_r F_s = F_{rs} \tag{14}$$

$$F_r V_s = V_s F_r \text{ whenever } (r, s) = 1 \tag{15}$$

$$F_r V_r = [r] \tag{16}$$

Here $[r]$ is the map $f(t) \to (f(t))^r$ of $1 + tA[\![t]\!]$, noting that the addition $\oplus$ in $1 + tA[\![t]\!]$ is given by the usual multiplication of formal power series. For a proof of these identities the reader can refer to 17.3.9 and 17.3.10 on page 124 of [4] and 16.2.2, 16.2.3, 16.2.4, 16.2.6 and 16.2.9 on page 104 of [4].

Let us now evaluate $F_r(1/(1-at^k))$. We have $F_r(1/(1-at^k)) = F_r V_k(1/(1-at))$

$$= \frac{F_r}{(r,k)} F_{(r,k)} V_{(r,k)} \frac{V_k}{(r,k)} \left(\frac{1}{1-at}\right) \text{ by (13) and (14)}$$

$$= \frac{F_r}{(r,k)} \circ [(r,k)] \circ \frac{V_k}{(r,k)} \left(\frac{1}{1-at}\right) \text{ by (16)}$$

$$= [(r,k)] \frac{F_r}{(r,k)} \frac{V_k}{(r,k)} \left(\frac{1}{1-at}\right)$$

$$= [(r,k)] \frac{V_k}{(r,k)} \frac{F_r}{(r,k)} \left(\frac{1}{1-at}\right) \text{ by (15).}$$

Observe that $F_s\left(\frac{1}{1-at}\right) = \left(\frac{1}{1-a^s t}\right)$ from the very definition. Hence

$$F_r\left(\frac{1}{1-at^k}\right) = \left\{\frac{1}{(1-a^{(r/(r,k))}t^{(k/(r,k))})}\right\}^{(r,k)}$$

$$= \left(\frac{1}{1-a^{(1/(r,k))}t^{(k/(r,k))}}\right)^{(r,k)}. \tag{17}$$

COROLLARY 2.2.

Let $f(t) = \prod_{k \geqslant 1} \left(\frac{1}{1-a_k t^k}\right)$. Then for any integer $r \geqslant 1$ we have

$$F_r f(t) = \prod_{k \geqslant 1} \left(\frac{1}{1-a_k^{(r/(r,k))}t^{(k/(r,k))}}\right)^{(r,k)}. \tag{18}$$

Remark 2.3. In our paper [8] we defined the Frobenius operators F_r on $1 + tA[\![t]\!]$ by formula (18). In this section we have just checked that our definition of F_r in

[8] agrees with the definition given by people working on formal groups as described in [4].

3. The map γ: $\mathrm{Nr}(A) \to 1 + tA[[t]]$ for rings A containing $\mathbb{Q}$ as a subring

Let $\mathscr{C}$ denote the class of rings A satisfying the condition that $\mathbb{Q}$ is a subring of A. Throughout this section A will denote a ring belonging to $\mathscr{C}$. The following was stated in [7].

PROPOSITION 3.1.

Let $A \in \mathscr{C}$. Then every element $\mathbf{c} \in \mathrm{Nr}(A)$ can be written as $\mathbf{c} = \sum_{k \geq 1} V_k\, \mathbf{M}(\mathbf{a}_k)$ where $\mathbf{M}(\mathbf{a}) = (M(a,1), M(a,2), M(a,3), \ldots) \in \mathrm{Nr}(A)$ for any $a \in A$. Moreover the expression is unique.

As commented in [7] the proof is similar to that of theorem 2, §4 of [5].

Let $\gamma: \mathrm{Nr}(A) \to 1 + tA[[t]]$ be the map defined by $\gamma(\mathbf{c}) = \prod_{k \geq 1} (1/(1 - t^k))^{c_k}$ where $\mathbf{c} = (c_1, c_2, c_3, \ldots) \in \mathrm{Nr}(A)$. From the very definition of V_r we have $V_r\mathbf{c} = \mathbf{x} = (x_1, x_2, x_3, \ldots)$ where $x_j = 0$ if $r \nmid j$ and $x_{kr} = c_k$. Hence

$$\gamma(V_r\mathbf{c}) = \prod_{k \geq 1} \left(\frac{1}{1 - t^{kr}}\right)^{c_k} = V_r\gamma(\mathbf{c}).$$

Thus γ preserves the Verschiebung operators. The cyclotomic identity $(1/(1 - at)) = \prod_{k \geq 1} (1/(1 - t^k))^{M(a,k)}$ which is valid for any $a \in A$ shows that $\gamma(\sum_{k \geq 1} V_k \mathbf{M}(\mathbf{a}_k)) = \prod_{k \geq 1} (1/(1 - a_k t^k))$. We have already seen that any element of $1 + tA[[t]]$ can be uniquely written as $\prod_{k \geq 1} (1/(1 - a_k t^k))$. Thus γ is a bijection. Moreover $E^{-1} \circ \gamma: \mathrm{Nr}(A) \to \mathrm{W}(A)$ is given by $E^{-1} \circ \gamma(\sum_{k \geq 1} V_k \mathbf{M}(\mathbf{a}_k)) = \mathbf{a} = (a_1, a_2, a_3, \ldots)$ in $\mathrm{W}(A)$.

Let $\theta: \mathrm{Nr}(A) \to \mathrm{Gh}(A)$ be the natural map defined in [5] and [7]. Namely $\theta(c_1, c_2, c_3, \ldots) = \mathbf{g} = (g_1, g_2, g_3, \ldots)$ where $g_n = \sum_{d/n} dc_d$. As already seen in [7], when $A \in \mathscr{C}$, $\theta: \mathrm{Nr}(A) \to \mathrm{Gh}(A)$ is a ring isomorphism preserving V_r and F_r.

Theorem 3.2. *Let $A \in \mathscr{C}$. Then $\gamma: \mathrm{Nr}(A) \to 1 + tA[[t]]$ is a ring isomorphism preserving the operators V_r and F_r.*

Proof. Let $\Delta: \mathrm{W}(A) \to \mathrm{Gh}(A)$ be the natural map defined by $\Delta(a_1, a_2, a_3, \ldots) = \mathbf{g} = (g_1, g_2, \ldots)$ where $g_n = \sum_{d/n} da_d^{n/d}$. We know that Δ is a ring homomorphism. We claim that

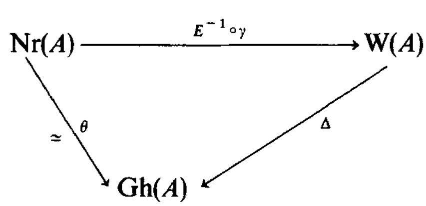

Diagram 1

is a commutative diagram.

In fact $\Delta\circ E^{-1}\circ\gamma(\sum_{k\geq 1} V_k M(a_k))$

$$= \Delta(a_1, a_2, a_3, \ldots)$$

$$= \mathbf{g} = (g_1, g_2, g_3, \ldots)$$

with $g_n = \sum_{d/n} da_d^{n/d}$.

Also $\theta(\sum_{k\geq 1} V_k \mathbf{M}(\mathbf{a}_k)) = \mathbf{h} = (h_1, h_2, h_3, \ldots)$ where $h_n = \sum_{d/n} da_d^{n/d}$ by Proposition 6.2 in [7]. Hence $\theta = \Delta\circ E^{-1}\circ\gamma$.

Since $E^{-1}\circ\gamma$ and θ are bijections, it follows that Δ is a bijection. In particular $\Delta: \mathrm{W}(A)\to \mathrm{Gh}(A)$ is a ring isomorphism. Since θ is a ring isomorphism [Proposition 4.2 of [7]], it follows that $E^{-1}\circ\gamma$: $\mathrm{Nr}(A)\to \mathrm{W}(A)$ is a ring isomorphism. From Cartier's result [1] we know that $E: \mathrm{W}(A)\to 1 + tA[\![t]\!]$ is a ring isomorphism. It follows that $\gamma: \mathrm{Nr}(A)\to 1 + tA[\![t]\!]$ is a ring isomorphism.

We have already seen that γ preserves the operators V_r. Thus to complete the proof of theorem 3.2, we have only to prove that γ preserves the Frobenius operators.

For any $a\in A$, we have

$$F_r\gamma(V_k\mathbf{M}(\mathbf{a})) = F_r\left(\frac{1}{1-at^k}\right)$$

$$= \left(\frac{1}{1-a^{(r/(r,k))}t^{(k/(r,k))}}\right)^{(r,k)} \text{ by (17).} \tag{19}$$

Also $\gamma(F_r V_k \mathbf{M}(\mathbf{A})) = \gamma\left((r,k)\frac{V_k}{(r,k)}\frac{F_r}{(r,k)}\mathbf{M}(\mathbf{a})\right)$ by 5.5 in [7]

$$= [(r,k)]\frac{V_k}{(r,k)}\gamma\left(\frac{F_r}{(r,k)}\mathbf{M}(\mathbf{a})\right)$$

$$= [(r,k)]\frac{V_k}{(r,k)}\gamma(\mathbf{M}(\mathbf{a}^{(r/(r,k))})) \text{ from §4 of [5]}$$

$$= [(r,k)]\frac{V_k}{(r,k)}\left(\frac{1}{1-a^{(r/(r,k))}t}\right)$$

$$= \left(\frac{1}{1-a^{(r/(r,k))}t^{(r/(r,k))}}\right)^{(r,k)} \tag{20}$$

(19) and (20) yield

$$F_r\gamma(V_k\mathbf{M}(\mathbf{a})) = \gamma(F_r V_k \mathbf{M}(\mathbf{a})). \tag{21}$$

Since every element of $\mathrm{Nr}(A)$ can be expressed as $\sum_{k>1} V_k\mathbf{M}(\mathbf{a}_k)$ from (21) we immediately get $F_r\gamma(\mathbf{c}) = \gamma(F_r\mathbf{c})$ for any $\mathbf{c}\in \mathrm{Nr}(A)$. This completes the proof of theorem 3.2. □

Remark 3.3. In case $A = \mathbb{Z}$ (thus $A\notin\mathscr{C}$), in diagram 1, θ is an injective ring homomorphism and so is Δ. It follows that $E^{-1}\circ\gamma: \mathrm{Nr}(\mathbb{Z})\to \mathrm{W}(\mathbb{Z})$ is a ring isomorphism and hence $\gamma: \mathrm{Nr}(\mathbb{Z})\to 1 + t\,\mathbb{Z}[\![t]\!]$ is a ring isomorphism. The proof that γ preserves F_r and V_r is exactly similar to the later part of theorem 3.2.

4. Conclusion

When A is an arbitrary commutative ring, in [7] the concept of the aperiodic ring Ap(A) of A was introduced. In [8] we defined a subring D(A) of Ap(A) and showed that there is a natural onto ring homomorphism $\chi: W(A) \to D(A)$ preserving the operators V_r and F_r. In that paper we defined F_r by formula (18) and transported to W(A) using the bijection E. Thus the present paper fills a lacuna by showing that F_r defined by formula (18) agrees with F_r defined by people working on formal groups, by using elementary symmetric functions.

Acknowledgement

This research work was done while the author was partially supported by NSERC grant A8225.

References

[1] Cartier P, Groupes formel associées aux anneaux de Witt géneralisées, *C.R. Acad. Sci. Paris* **265** (1967) 49–52
[2] Dress A W M and Siebeneicher C, The Burnside ring of the infinite cyclic group and its relations to the necklace algebra, λ-rings and the universal ring of Witt. vectors. *Adv. Math.* (to appear)
[3] Grothendieck A, La theorie des classes de Chern, *Bull. Soc. Math. France* **86** (1958) 137–154
[4] Hazewinkel M, *Formal Groups and Applications* (Academic Press) (1978)
[5] Metropolis N and Gian Carlo Rota, Witt vectors and the algebra of necklaces, *Adv. Math.* **50** (1983) 95–125
[6] Metropolis N and Gian Carlo Rota, The cyclotomic identity, *Contemp. Math.* **34** (1984) 19–27
[7] Varadarajan K and Wehrhahn K, Aperiodic rings, necklace rings and Witt vectors, *Adv. Math.* (to appear)
[8] Varadarajan K, Aperiodic rings, necklace rings and Witt vectors-II, *Proc. Indian Acad. Sci.* **99** (1989) 7–15