Journal of Algebra 323 (2010) 2818–2833

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Adams operations on the Green ring of a cyclic group of prime-power order ☆

R.M. Bryant, Marianne Johnson *

School of Mathematics, University of Manchester, Manchester M13 9PL, UK

ARTICLE INFO

Article history:
Received 27 July 2009
Available online 25 March 2010
Communicated by Michel Broué

Keywords:
Adams operation
Cyclic p-group
Exterior power
Symmetric power

ABSTRACT

We consider the Green ring R_{KC} for a cyclic p-group C over a field K of prime characteristic p and determine the Adams operations ψ^n in the case where n is not divisible by p. This gives information on the decomposition into indecomposables of exterior powers and symmetric powers of KC-modules.

1. Introduction

Let C be a cyclic group of order p^ν, where p is a prime and $\nu \geqslant 1$, and let K be a field of characteristic p. It is well known that there are, up to isomorphism, exactly p^ν indecomposable KC-modules, and these can be written as $V_1, V_2, \dots, V_{p^\nu}$, where V_r has dimension r, for $r = 1, \dots, p^\nu$. The exterior powers $\Lambda^n(V_r)$ and symmetric powers $S^n(V_r)$ have been studied intermittently for more than thirty years. Some of the main contributions have been by Almkvist and Fossum [2], Kouwenhoven [10], Hughes and Kemper [8], Gow and Laffey [6] and Symonds [19]. The main aim has been to describe $\Lambda^n(V_r)$ and $S^n(V_r)$, up to isomorphism, as direct sums of indecomposable modules. An explicit formula is probably not feasible, but one can look for a recursive description, so that, for example, $\Lambda^n(V_r)$ is described in terms of exterior powers $\Lambda^m(V_j)$ where $m < n$ or $j < r$. The case $\nu = 1$ was settled in [2], although further information was provided by a number of people in subsequent papers. However, for $\nu > 1$, the problem remains open in general.

It is helpful to work in the Green ring (or representation ring) R_{KC}. This consists of all formal $\mathbb{Z}$-linear combinations of $V_1, V_2, \dots, V_{p^\nu}$, with addition defined in the obvious way and multiplication

☆ Work supported by EPSRC Standard Research Grant EP/G024898/1.

* Corresponding author.
E-mail addresses: roger.bryant@manchester.ac.uk (R.M. Bryant), marianne.johnson@maths.manchester.ac.uk (M. Johnson).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2010.02.033

coming from the decomposition of tensor products into indecomposables. Finite-dimensional KC-modules may be regarded, up to isomorphism, as elements of R_{KC}. This ring was first studied in detail by Green [7] in 1962, and he gave recursive formulae that implicitly describe multiplication in R_{KC}. Improved formulae and algorithms were subsequently given by several other people: see, for example, [15–18].

In this paper we study the Adams operations ψ_Λ^n and ψ_S^n, for $n \geqslant 1$, following the treatment of these in [4]. Both ψ_Λ^n and ψ_S^n are $\mathbb{Z}$-linear maps from R_{KC} to R_{KC}. Furthermore, $\Lambda^n(V_r)$ is given in $\mathbb{Q} \otimes_{\mathbb{Z}} R_{KC}$ as a polynomial in $\psi_\Lambda^1(V_r), \ldots, \psi_\Lambda^n(V_r)$. For example,

$$\Lambda^2(V_r) = \frac{1}{2}\bigl(\psi_\Lambda^1(V_r)^2 - \psi_\Lambda^2(V_r)\bigr), \tag{1.1}$$

where $\psi_\Lambda^1(V_r) = V_r$. Similarly, $S^n(V_r)$ is given as a polynomial in $\psi_S^1(V_r), \ldots, \psi_S^n(V_r)$.

The main results of this paper determine $\psi_\Lambda^n(V_r)$ and $\psi_S^n(V_r)$ for n not divisible by p. Thus our results could be used to determine $\Lambda^n(V_r)$ and $S^n(V_r)$ for $n < p$. For n not divisible by p, it is known (see [4]) that $\psi_\Lambda^n = \psi_S^n$. Thus, in this case, we write ψ^n, where $\psi^n = \psi_\Lambda^n = \psi_S^n$. In Section 3 we establish the periodicity of these Adams operations (namely, $\psi^n = \psi^{n+2p}$) and a symmetry property (namely, $\psi^n = \psi^{2p-n}$ for $n = 1, \ldots, p-1$). We also prove a result (Proposition 3.6) that generalises the "reciprocity theorem" of Gow and Laffey [6, Theorem 1]. Most of the results of Section 3 extend work for $\nu = 1$ by Almkvist [1] and Kouwenhoven [10].

Our first main result (Theorem 4.7) describes $\psi^n(V_r)$ recursively in terms of the values $\psi^n(V_j)$ for $j < r$. This is a simple recursion that enables $\psi^n(V_r)$ to be calculated in a straightforward way by elementary arithmetic, and (strangely enough) the recursion does not require any ability to multiply within R_{KC}.

One can apply this result to find $\Lambda^2(V_r)$ in the case where p is odd, by means of (1.1). Given $\psi^2(V_r)$ it remains only to calculate V_r^2 by the methods available for multiplication in the Green ring. This settles a problem left open by Gow and Laffey [6] who showed how to compute $\Lambda^2(V_r)$ when $p = 2$.

Our second main result (Theorem 5.1) shows that $\psi^n(V_r)$ has a strikingly simple form (unlike the much more complicated form that one gets for $\Lambda^n(V_r)$ or $S^n(V_r)$). Indeed, it turns out that

$$\psi^n(V_r) = V_{j_1} - V_{j_2} + V_{j_3} - \cdots \pm V_{j_l},$$

where $p^\nu \geqslant j_1 > j_2 > \cdots > j_l \geqslant 1$. Thus the multiplicities of indecomposables in $\psi^n(V_r)$ are only $0, 1$ and -1, and the non-zero multiplicities alternate in sign.

The importance of using Adams operations in the study of KC-modules was recognised by Almkvist [1], who studied them in the case $\nu = 1$. An extremely useful contribution to the study of $\Lambda^n(V_r)$ in the general case ($\nu \geqslant 1$) was made by Kouwenhoven [10, Theorem 3.5], and his theorem is a key ingredient of our work. By this theorem it is possible to calculate the values of ψ_Λ^n (for all n) on a generating set of R_{KC}. However, for n not divisible by p, it is known (see [4]) that ψ^n is an endomorphism of R_{KC}. Thus, in this case, it becomes possible to calculate ψ^n on an arbitrary element of R_{KC}. Kouwenhoven studied Adams operations in his paper [10], and they also figure in his subsequent papers [11–14], but his published results seem to be confined to the case where $\nu = 1$.

Hughes and Kemper [8] exploited Kouwenhoven's theorem and, indeed, the results of [8, Section 4] provide, in principle, a method for calculating $\Lambda^n(V_r)$ and $S^n(V_r)$ for $n < p$. However, we believe that our results on Adams operations give a simpler and more attractive approach.

In a further paper we shall study ψ_Λ^n and ψ_S^n on R_{KC} for the general case where n may be divisible by p. We shall prove periodicity results and show that the work of Symonds [19] may be attractively formulated in terms of Adams operations.

2. Preliminaries

Let G be a group and K a field. We consider KG-modules, by which we always mean finite-dimensional right KG-modules, and we write R_{KG} for the associated Green ring (or representation ring). Thus R_{KG} is spanned, over $\mathbb{Z}$, by the isomorphism classes of KG-modules and has addition and multiplication coming from direct sums and tensor products, respectively. In fact, R_{KG} has a $\mathbb{Z}$-basis consisting of the isomorphism classes of indecomposable KG-modules.

For any KG-module V, we also write V for the corresponding element of R_{KG}. Thus, for KG-modules V and W we have $V = W$ in R_{KG} if and only if $V \cong W$. The elements $V + W$ and VW of R_{KG} correspond to $V \oplus W$ and $V \otimes_K W$, respectively, and the identity element 1 of R_{KG} is the 1-dimensional KG-module on which G acts trivially. If V is a KG-module and n is a non-negative integer, then we regard $\Lambda^n(V)$ and $S^n(V)$ as elements of R_{KG}.

The Adams operations on R_{KG} are certain $\mathbb{Z}$-linear maps from R_{KG} to R_{KG}. We follow the treatment in [4]. For this purpose we need to extend R_{KG} to a ring $\mathbb{Q}R_{KG}$ where we allow coefficients from $\mathbb{Q}$: thus $\mathbb{Q}R_{KG} \cong \mathbb{Q} \otimes_{\mathbb{Z}} R_{KG}$.

For any KG-module V, define elements of the power-series ring $R_{KG}[[t]]$ by

$$\Lambda(V,t) = 1 + \Lambda^1(V)t + \Lambda^2(V)t^2 + \cdots,$$
$$S(V,t) = 1 + S^1(V)t + S^2(V)t^2 + \cdots.$$

(Since V is assumed to be finite-dimensional, $\Lambda(V,t)$ actually belongs to the polynomial ring $R_{KG}[t]$.) Using the formal expansion of $\log(1+x)$, we have elements $\log \Lambda(V,t)$ and $\log S(V,t)$ of $\mathbb{Q}R_{KG}[[t]]$. Thus we define elements $\psi^n_\Lambda(V)$ and $\psi^n_S(V)$ of $\mathbb{Q}R_{KG}$, for $n = 1, 2, \ldots$, by the equations

$$\psi^1_\Lambda(V)t - \frac{1}{2}\psi^2_\Lambda(V)t^2 + \frac{1}{3}\psi^3_\Lambda(V)t^3 - \cdots = \log \Lambda(V,t),$$
$$\psi^1_S(V)t + \frac{1}{2}\psi^2_S(V)t^2 + \frac{1}{3}\psi^3_S(V)t^3 + \cdots = \log S(V,t). \tag{2.1}$$

It is not difficult to prove (for more details see [4]) that $\psi^n_\Lambda(V), \psi^n_S(V) \in R_{KG}$ and

$$\psi^n_\Lambda(V+W) = \psi^n_\Lambda(V) + \psi^n_\Lambda(W), \qquad \psi^n_S(V+W) = \psi^n_S(V) + \psi^n_S(W),$$

for all $n \geqslant 1$ and all KG-modules V and W. It follows that the definitions of ψ^n_Λ and ψ^n_S may be extended to give $\mathbb{Z}$-linear functions

$$\psi^n_\Lambda : R_{KG} \to R_{KG}, \qquad \psi^n_S : R_{KG} \to R_{KG},$$

called the nth Adams operations on R_{KG}. It is easily verified that ψ^1_Λ and ψ^1_S are equal to the identity map on R_{KG}.

For any element W of R_{KG} we may now define elements $\Lambda(W,t)$ and $S(W,t)$ of $\mathbb{Q}R_{KG}[[t]]$ by the equations

$$\Lambda(W,t) = \exp\left(\psi^1_\Lambda(W)t - \frac{1}{2}\psi^2_\Lambda(W)t^2 + \frac{1}{3}\psi^3_\Lambda(W)t^3 - \cdots\right),$$
$$S(W,t) = \exp\left(\psi^1_S(W)t + \frac{1}{2}\psi^2_S(W)t^2 + \frac{1}{3}\psi^3_S(W)t^3 + \cdots\right).$$

Hence Eqs. (2.1) hold if V is replaced by any element W of R_{KG}.

The following result is part of [4, Theorem 5.4].

Proposition 2.1. *For every positive integer n not divisible by the characteristic of K, we have $\psi^n_\Lambda = \psi^n_S$ and each of these maps is a ring endomorphism of R_{KG}. Furthermore, under composition of maps we have*

$$\psi_\Lambda^n \circ \psi_\Lambda^{n'} = \psi_\Lambda^{nn'}, \qquad \psi_S^n \circ \psi_S^{n'} = \psi_S^{nn'},$$

for all positive integers n and n′ such that n is not divisible by char K.

We shall be mainly concerned with Adams operations ψ_Λ^n and ψ_S^n for n not divisible by char K. For these operations we write ψ^n, where $\psi^n = \psi_\Lambda^n = \psi_S^n$. We also write δ for the 'dimension' map $\delta : R_{KG} \to \mathbb{Z}$. This is the $\mathbb{Z}$-linear map satisfying $\delta(V) = \dim V$ for every KG-module V.

If G_1 is a group of order 1 then any KG_1-module V may be written as $\delta(V)\cdot 1$ (where 1 is the identity element of R_{KG_1}) and it is easily verified that

$$\Lambda(V,t) = (1+t)^{\delta(V)}, \qquad S(V,t) = (1-t)^{-\delta(V)}.$$

It follows that $\psi_\Lambda^n(V) = \psi_S^n(V) = V$ for all n. Thus each ψ_Λ^n and each ψ_S^n is the identity map on R_{KG_1}.

For an arbitrary group G we have homomorphisms $G \to G_1$ and $G_1 \to G$ giving ring homomorphisms $\alpha : R_{KG_1} \to R_{KG}$ and $\beta : R_{KG} \to R_{KG_1}$, respectively. Here α is an embedding, β is given by restriction of modules to the identity subgroup, and $\alpha(\beta(W)) = \delta(W)\cdot 1$ for all $W \in R_{KG}$ (where 1 is the identity element of R_{KG}). The formation of exterior and symmetric powers commutes with restriction: hence $\beta \circ \psi_\Lambda^n = \psi_\Lambda^n \circ \beta$ and $\beta \circ \psi_S^n = \psi_S^n \circ \beta$, giving

$$\beta\bigl(\psi_\Lambda^n(W)\bigr) = \beta\bigl(\psi_S^n(W)\bigr) = \beta(W),$$

for all $W \in R_{KG}$. On applying α we obtain an equality of 'dimensions':

$$\delta\bigl(\psi_\Lambda^n(W)\bigr) = \delta\bigl(\psi_S^n(W)\bigr) = \delta(W), \tag{2.2}$$

for all $W \in R_{KG}$ and all $n \geqslant 1$.

Now let p be a prime and K a field of characteristic p. Let ν be a non-negative integer and let $C(p^\nu)$ denote a cyclic group of order p^ν. It is well known that there are, up to isomorphism, precisely p^ν indecomposable $KC(p^\nu)$-modules, $V_1, V_2, \dots, V_{p^\nu}$, where $\dim V_r = r$ for $r = 1, \dots, p^\nu$. (For a proof of this fact see [2, Proposition I.1.1] or [8, Proposition 2.1].) Here V_1 is the trivial 1-dimensional $KC(p^\nu)$-module and V_{p^ν} is the regular $KC(p^\nu)$-module.

If K' is an extension field of K there is an embedding $R_{KC(p^\nu)} \to R_{K'C(p^\nu)}$ given by extension of scalars, and the image of V_r is easily seen to be the indecomposable $K'C(p^\nu)$-module of dimension r. Thus $R_{KC(p^\nu)} \cong R_{K'C(p^\nu)}$. Hence we regard $R_{KC(p^\nu)}$ as the same for all fields of characteristic p, and write it as R_{p^ν}. The identity element of R_{p^ν} is sometimes written as 1 and sometimes V_1.

For each non-negative integer m, let $C(p^m)$ be a cyclic group of order p^m and choose a surjective homomorphism $C(p^{m+1}) \to C(p^m)$. Thus, for $j \geqslant m$, the group $C(p^m)$ may be regarded as a factor group of $C(p^j)$, and there is an injective homomorphism $R_{p^m} \to R_{p^j}$ mapping the r-dimensional indecomposable $KC(p^m)$-module to the r-dimensional indecomposable $KC(p^j)$-module, for $r = 1, \dots, p^m$.

Consequently we may take $R_{p^0} \subset R_{p^1} \subset \cdots \subset R_{p^\nu}$, where R_{p^m} has $\mathbb{Z}$-basis $\{V_1, \dots, V_{p^m}\}$ for $m = 0, \dots, \nu$. Throughout the paper we also write $V_0 = 0$ and $V_{-r} = -V_r$ for $r = 1, \dots, p^\nu$.

Suppose that $\nu \geqslant 1$. For $m = 0, \dots, \nu - 1$ we define $X_m \in R_{p^{m+1}}$ by

$$X_m = V_{p^m+1} - V_{p^m-1},$$

modifying slightly the notation of [2]. In particular $X_0 = V_2$. These elements were earlier considered by Green [7] in a different notation.

Proposition 2.2. *Let* $m \in \{0, 1, \dots, \nu - 1\}$ *and* $r \in \{0, \dots, (p-1)p^m\}$. *Then*

$$X_m V_r = V_{r+p^m} + V_{r-p^m}.$$

Proof. For $0 < r < (p-1)p^m$ this is given directly by [7, (2.3a) and (2.3b)]. For $r = 0$ it is trivial, and for $r = (p-1)p^m$ it follows easily from [7, (2.3c)]. □

By the remark immediately after [7, Theorem 3] or by [2, Proposition I.1.6], the Green ring R_{p^ν} is generated by the elements $X_0, \dots, X_{\nu-1}$.

Let $m \in \{0, \dots, \nu\}$. Because V_{p^m} is the regular $KC(p^m)$-module, we have $V_{p^m} V_r = r V_{p^m}$ for $r = 1, \dots, p^m$ (by [9, VII.7.19 Theorem], for example). Hence

$$V_{p^m} W = \delta(W) V_{p^m}, \tag{2.3}$$

for all $W \in R_{p^m}$. It follows that $\mathbb{Z}V_{p^m}$ is an ideal of R_{p^m}. For $A, B \in R_{p^m}$ we write $A \equiv B \pmod{V_{p^m}}$ to denote that $A - B \in \mathbb{Z}V_{p^m}$. In fact, such a congruence gives an equation, by consideration of dimension, namely $A = B + p^{-m}\delta(A-B)V_{p^m}$.

Note that V_{p^m} is the only projective indecomposable $KC(p^m)$-module. Also, for $r \in \{1, \dots, p^m\}$, it is well known and easy to see that $V_{p^m - r}$ is the Heller translate of V_r as $KC(p^m)$-module: we write

$$\Omega_{p^m}(V_r) = V_{p^m - r}. \tag{2.4}$$

(For general properties of the Heller translate see [3], for example.) We extend Ω_{p^m} to a $\mathbb{Z}$-linear map $\Omega_{p^m} : R_{p^m} \to R_{p^m}$. Then, for all $W \in R_{p^m}$, we have

$$\Omega_{p^m}\big(\Omega_{p^m}(W)\big) \equiv W \pmod{V_{p^m}}. \tag{2.5}$$

For $KC(p^m)$-modules U and V, consideration of tensor products gives

$$\Omega_{p^m}(UV) \equiv \Omega_{p^m}(U)V \pmod{V_{p^m}}$$

(see [3, Corollary 3.1.6]). Hence, for all $A, B \in R_{p^m}$, we have

$$\Omega_{p^m}(AB) \equiv \Omega_{p^m}(A)B \pmod{V_{p^m}}. \tag{2.6}$$

3. Periodicity and symmetry

For the remainder of the paper, p is a prime and ν is a positive integer. We consider the Green ring R_{p^ν} for the cyclic group $C(p^\nu)$ and use the notation of Section 2. In particular, $X_m = V_{p^m+1} - V_{p^m-1}$ for $m = 0, \dots, \nu-1$.

As in [2, Section I.1] and [8, Section 4.1], let R_{p^ν} be extended to a ring $\widehat{R}_{p^\nu}$ generated by R_{p^ν} and elements $E_0, \dots, E_{\nu-1}$ satisfying $E_m^2 - X_m E_m + 1 = 0$ for $m = 0, \dots, \nu-1$. Thus each E_m is invertible in $\widehat{R}_{p^\nu}$ and $X_m = E_m + E_m^{-1}$. (Note that E_m is written as μ_m in [2] and [8].)

By [10, Theorem 3.5], we have $\Lambda(X_m, t) = 1 + X_m t + t^2$. Thus

$$\Lambda(X_m, t) = 1 + \big(E_m + E_m^{-1}\big)t + t^2 = (1 + E_m t)\big(1 + E_m^{-1} t\big),$$

and so, in $(\mathbb{Q} \otimes_{\mathbb{Z}} \widehat{R}_{p^\nu})[[t]]$, we have

$$\begin{aligned}\log \Lambda(X_m, t) &= \log(1 + E_m t) + \log\big(1 + E_m^{-1} t\big)\\ &= \big(E_m + E_m^{-1}\big)t - \frac{1}{2}\big(E_m^2 + E_m^{-2}\big)t^2 + \frac{1}{3}\big(E_m^3 + E_m^{-3}\big)t^3 - \cdots.\end{aligned}$$

Hence, by (2.1), we obtain

$$\psi_\Lambda^n(X_m) = E_m^n + E_m^{-n} \quad \text{for all } n \geqslant 1. \tag{3.1}$$

For the moment we fix m in the range $0 \leqslant m \leqslant \nu - 1$ and write $E = E_m$ and $E^{\langle n\rangle} = E^n + E^{-n}$ for all $n \geqslant 0$. Note that, for $n \geqslant 1$,

$$E^{\langle n\rangle} E^{\langle 1\rangle} = E^{\langle n+1\rangle} + E^{\langle n-1\rangle}. \tag{3.2}$$

Write $Z = V_{p^m} - V_{p^m - 1}$. Thus $Z^2 = 1$, by [8, (4.4)], and, by [8, Theorem 4.2],

$$(ZE - 1)\big((ZE)^{2p-1} - (ZE)^{2p-2} + \cdots + ZE - 1\big) = 0.$$

Since $Z^2 = 1$, we obtain

$$E^{2p} - 2ZE^{2p-1} + 2E^{2p-2} - \cdots - 2ZE + 1 = 0. \tag{3.3}$$

Lemma 3.1. *We have $E^{\langle p+1\rangle} = E^{\langle p-1\rangle}$.*

Proof. Assume first that p is odd. Multiplying (3.3) by E^{-p} we obtain

$$E^p - 2ZE^{p-1} + \cdots + 2E - 2Z + 2E^{-1} - \cdots - 2ZE^{-(p-1)} + E^{-p} = 0.$$

Hence

$$E^{\langle p\rangle} = 2ZE^{\langle p-1\rangle} - 2E^{\langle p-2\rangle} + \cdots - 2E^{\langle 1\rangle} + 2Z. \tag{3.4}$$

Therefore, by (3.2),

$$E^{\langle p+1\rangle} + E^{\langle p-1\rangle} = 2ZE^{\langle p\rangle} - 2E^{\langle p-1\rangle} + 4ZE^{\langle p-2\rangle} - \cdots + 4ZE^{\langle 1\rangle} - 4.$$

Hence, by (3.4), $E^{\langle p+1\rangle} + E^{\langle p-1\rangle} = 2E^{\langle p-1\rangle}$. This gives $E^{\langle p+1\rangle} = E^{\langle p-1\rangle}$, as required. The proof is similar for $p = 2$. $\square$

Proposition 3.2.

(i) *For $j = 0, \ldots, p$, we have $E^{\langle 2p-j\rangle} = E^{\langle j\rangle}$.*
(ii) *For all $c \geqslant 0$, we have $E^{\langle 2p+c\rangle} = E^{\langle c\rangle}$.*

Proof. By Lemma 3.1, $E^{\langle p+1\rangle} = E^{\langle p-1\rangle}$. Multiplying by $E^{\langle 1\rangle}$ we get

$$E^{\langle p+2\rangle} + E^{\langle p\rangle} = E^{\langle p\rangle} + E^{\langle p-2\rangle}$$

and so $E^{\langle p+2\rangle} = E^{\langle p-2\rangle}$. Continuing in this way we obtain $E^{\langle p+j\rangle} = E^{\langle p-j\rangle}$ for $j = 0, 1, \ldots, p$. This gives (i).

In particular we have $E^{\langle 2p\rangle} = E^{\langle 0\rangle} = 2$. This gives (ii) in the case $c = 0$. Multiplying the equation $E^{\langle 2p\rangle} = 2$ by $E^{\langle 1\rangle}$ we get $E^{\langle 2p+1\rangle} + E^{\langle 2p-1\rangle} = 2E^{\langle 1\rangle}$. Since $E^{\langle 2p-1\rangle} = E^{\langle 1\rangle}$, by (i), we have $E^{\langle 2p+1\rangle} = E^{\langle 1\rangle}$. This gives (ii) in the case $c = 1$. Continuing in this way we get the result for all c. $\square$

From now on we write $\psi^n = \psi_\Lambda^n$ for all n not divisible by p. (Thus, in fact, $\psi^n = \psi_\Lambda^n = \psi_S^n$.)

Theorem 3.3. *For $j = 1, \ldots, p-1$, we have $\psi^{2p-j} = \psi^j$. Also, if c is any positive integer not divisible by p, we have $\psi^{2p+c} = \psi^c$.*

Proof. As noted in Section 2, R_{p^ν} is generated by $\{X_m\colon\ 0 \leqslant m \leqslant \nu - 1\}$. Let j and c be as stated. Then Proposition 3.2 and (3.1) give $\psi^{2p-j}(X_m) = \psi^j(X_m)$ and $\psi^{2p+c}(X_m) = \psi^c(X_m)$ for all $m \in \{0, \ldots, \nu-1\}$. However, by Proposition 2.1, ψ^{2p-j}, ψ^j, ψ^{2p+c} and ψ^c are endomorphisms of R_{p^ν}. Thus the result follows. □

Let c be any positive integer not divisible by p. Then it is easy to see that there is a unique integer $\gamma(c)$ satisfying the conditions $1 \leqslant \gamma(c) \leqslant p-1$ and $c \equiv \pm\gamma(c) \pmod{2p}$. Theorem 3.3 has the following immediate consequences.

Corollary 3.4. *For c a positive integer not divisible by p, we have $\psi^c = \psi^{\gamma(c)}$.*

Corollary 3.5. *Suppose that $p = 2$. Then ψ^c is the identity map for every positive integer c not divisible by p.*

Let n be a positive integer not divisible by p, and let $m \in \{1, \ldots, \nu\}$. Then

$$V_{p^m-1}^2 = \left(p^m - 2\right)V_{p^m} + V_1,$$

by [7, (2.5b)]. Hence

$$V_{p^m-1}^n \equiv \begin{cases} V_{p^m-1} \pmod{V_{p^m}} & \text{if } n \text{ is odd,} \\ V_1 \pmod{V_{p^m}} & \text{if } n \text{ is even.} \end{cases} \tag{3.5}$$

By [4, p. 362], there are $KC(p^\nu)$-modules Y_d, for each divisor d of n, such that

$$V_{p^m-1}^n = \sum_{d|n} \phi(d) Y_d, \tag{3.6}$$

where ϕ is Euler's function. Also, by [4, (4.4) and Theorem 5.4],

$$\psi^n(V_{p^m-1}) = \sum_{d|n} \mu(d) Y_d, \tag{3.7}$$

where μ is the Möbius function.

Note that $\phi(d) = 1$ only if $d = 1$ or $d = 2$. Suppose first that n is odd. Then (3.5) and (3.6) give $Y_1 \equiv V_{p^m-1} \pmod{V_{p^m}}$ and $Y_d \equiv 0 \pmod{V_{p^m}}$ for all $d > 1$. Thus, by (3.7),

$$\psi^n(V_{p^m-1}) \equiv V_{p^m-1} \pmod{V_{p^m}}.$$

However, $\delta(\psi^n(V_{p^m-1})) = p^m - 1$ by (2.2). Hence $\psi^n(V_{p^m-1}) = V_{p^m-1}$.

Now suppose that n is even. By (3.5) and (3.6), there exists $e \in \{1, 2\}$ such that $Y_e \equiv V_1 \pmod{V_{p^m}}$ and $Y_d \equiv 0 \pmod{V_{p^m}}$ for all $d \neq e$. Hence, by (3.7),

$$\psi^n(V_{p^m-1}) \equiv \pm V_1 \pmod{V_{p^m}}.$$

Since n is even, $p \neq 2$. Thus, using (2.2), we get $\psi^n(V_{p^m-1}) = V_{p^m} - V_1$.

Therefore, for all n not divisible by p,

$$\psi^n(V_{p^m-1}) = \begin{cases} V_{p^m-1} & \text{if } n \text{ is odd,} \\ V_{p^m} - V_1 & \text{if } n \text{ is even.} \end{cases} \tag{3.8}$$

By similar, but much easier, arguments we obtain

$$\psi^n(V_{p^m}) = V_{p^m} \quad \text{for all } n \text{ not divisible by } p. \tag{3.9}$$

By [7, (2.5b)], we have

$$V_{p^m-1}V_r = (r-1)V_{p^m} + V_{p^m-r}, \tag{3.10}$$

for $r = 1, \ldots, p^m$. (Recall that $V_0 = 0$.) Hence, by Proposition 2.1 and (3.9),

$$\psi^n(V_{p^m-1})\psi^n(V_r) = (r-1)V_{p^m} + \psi^n(V_{p^m-r}), \tag{3.11}$$

for all n not divisible by p. Note that (3.8)–(3.11) hold, trivially, for $m = 0$. Thus they hold for all $m \in \{0, \ldots, \nu\}$.

Proposition 3.6. *Let n be an even positive integer not divisible by p (thus p is odd), and let $m \in \{0, \ldots, \nu\}$. Then, for $r = 1, \ldots, p^m$, we have*

$$\psi^n(V_r) + \psi^n(V_{p^m-r}) = V_{p^m}.$$

Proof. By (3.8) and (3.11),

$$(V_{p^m} - V_1)\psi^n(V_r) = (r-1)V_{p^m} + \psi^n(V_{p^m-r}).$$

However, $V_{p^m}\psi^n(V_r) = rV_{p^m}$ by (2.2) and (2.3). This gives the required result. □

By (3.10) and (2.4) we have, for all $W \in R_{p^m}$,

$$V_{p^m-1}W \equiv \Omega_{p^m}(W) \pmod{V_{p^m}}. \tag{3.12}$$

Proposition 3.7. *Let n be an odd positive integer not divisible by p, and let $m \in \{0, \ldots, \nu\}$. Then, for $r = 1, \ldots, p^m$, we have*

$$\psi^n(V_{p^m-r}) \equiv \Omega_{p^m}\big(\psi^n(V_r)\big) \pmod{V_{p^m}}.$$

Proof. By (3.8), $\psi^n(V_{p^m-1}) = V_{p^m-1}$. Hence, by (3.11),

$$V_{p^m-1}\psi^n(V_r) = (r-1)V_{p^m} + \psi^n(V_{p^m-r}).$$

Thus the result follows by (3.12). □

Propositions 3.6 and 3.7 are partial generalisations of [1, Propositions 5.4(d) and 5.4(e)]. Stronger results will be given below in Corollary 5.2.

We conclude this section by showing that, when $n = 2$, Proposition 3.6 implies Gow and Laffey's "reciprocity theorem" [6, Theorem 1]. This may be stated in the Green ring as follows (after correction of the obvious misprint in [6]).

Corollary 3.8. *Let p be odd and $m \in \{1, \dots, \nu\}$. Then, for $r = 1, \dots, p^m$,*

(i) $\Lambda^2(V_r) = (r - \frac{1}{2}(p^m + 1))V_{p^m} + S^2(V_{p^m-r})$,
(ii) $S^2(V_r) = (r - \frac{1}{2}(p^m - 1))V_{p^m} + \Lambda^2(V_{p^m-r})$.

Proof. Since (i) and (ii) are essentially the same we prove only (i). It is well known that $S^2(V_{p^m-r}) + \Lambda^2(V_{p^m-r}) = V_{p^m-r}^2$. Thus

$$\Lambda^2(V_r) - S^2(V_{p^m-r}) = \Lambda^2(V_r) + \Lambda^2(V_{p^m-r}) - V_{p^m-r}^2.$$

By (1.1) (which follows from (2.1)), we have $\Lambda^2(V_r) = \frac{1}{2}(V_r^2 - \psi^2(V_r))$; and a similar statement holds for $\Lambda^2(V_{p^m-r})$. Hence

$$\Lambda^2(V_r) - S^2(V_{p^m-r}) = \frac{1}{2}\left(V_r^2 - V_{p^m-r}^2\right) - \frac{1}{2}\left(\psi^2(V_r) + \psi^2(V_{p^m-r})\right).$$

However, by (2.5), (2.6) and (2.4), we have

$$V_r^2 \equiv \Omega_{p^m}\left(\Omega_{p^m}\left(V_r^2\right)\right) \equiv \left(\Omega_{p^m}(V_r)\right)^2 \equiv V_{p^m-r}^2 \pmod{V_{p^m}},$$

so that $V_r^2 - V_{p^m-r}^2 = (2r - p^m)V_{p^m}$. Also, we have $\psi^2(V_r) + \psi^2(V_{p^m-r}) = V_{p^m}$, by Proposition 3.6. Thus

$$\Lambda^2(V_r) - S^2(V_{p^m-r}) = \frac{1}{2}\left(2r - p^m\right)V_{p^m} - \frac{1}{2}V_{p^m},$$

which gives the required result. □

4. Recursion

Define elements $g_0(t), g_1(t), \dots$ of $\mathbb{Z}[t]$ by $g_0(t) = 2$, $g_1(t) = t$ and, for $n \geqslant 2$,

$$g_n(t) = tg_{n-1}(t) - g_{n-2}(t). \tag{4.1}$$

The $g_n(t)$ can be seen to be Dickson polynomials of the first kind, and can be given by an explicit formula, but we do not need this.

Proposition 4.1. *For $n \geqslant 1$ and $m \in \{0, \dots, \nu - 1\}$, we have*

$$\psi_\Lambda^n(X_m) = g_n(X_m).$$

Proof. Clearly $\psi_\Lambda^1(X_m) = X_m$ and, by (3.1), $\psi_\Lambda^2(X_m) = X_m^2 - 2$. Hence the result holds for $n \leqslant 2$. It is easy to check from (3.1) and (3.2) that, for $n \geqslant 3$,

$$\psi_\Lambda^n(X_m) = X_m\psi_\Lambda^{n-1}(X_m) - \psi_\Lambda^{n-2}(X_m).$$

Thus the result follows by induction and (4.1). □

For $n < p$, Proposition 4.1 can be deduced from (3.1) and [2, (I.1.4) and (I.1.5)]. Our next result is a reformulation of [5, Lemma 4.2], but we give a proof for the convenience of the reader.

Proposition 4.2. *Let $m \in \{0, \dots, \nu - 1\}$, $r \in \{1, \dots, p^m\}$, and $i \in \{0, \dots, p - 1\}$. Then*

$$g_i(X_m)V_r = V_{ip^m+r} - V_{ip^m-r}.$$

Proof. The result is clear for $i = 0$ because, by convention, V_{-r} denotes $-V_r$. Since $g_1(X_m) = X_m$, the result for $i = 1$ is given by Proposition 2.2. Now suppose that $2 \leqslant i \leqslant p - 1$ and the result holds for $i - 1$ and $i - 2$. Then, by (4.1) and the inductive hypothesis,

$$\begin{aligned} g_i(X_m)V_r &= X_m g_{i-1}(X_m)V_r - g_{i-2}(X_m)V_r \\ &= X_m(V_{(i-1)p^m+r} - V_{(i-1)p^m-r}) - (V_{(i-2)p^m+r} - V_{(i-2)p^m-r}). \end{aligned}$$

It is easy to verify that $(i - 1)p^m + r$ and $(i - 1)p^m - r$ belong to $\{0, \dots, (p - 1)p^m\}$. Hence, by Proposition 2.2,

$$\begin{aligned} g_i(X_m)V_r &= (V_{ip^m+r} + V_{(i-2)p^m+r}) - (V_{ip^m-r} + V_{(i-2)p^m-r}) - (V_{(i-2)p^m+r} - V_{(i-2)p^m-r}) \\ &= V_{ip^m+r} - V_{ip^m-r}, \end{aligned}$$

as required. □

For a positive integer c not divisible by p, let $\gamma(c)$ be as defined in Section 3. Note that $1 \leqslant \gamma(c) \leqslant p - 1$.

Corollary 4.3. *Let $m \in \{0, \dots, \nu - 1\}$. For $r \in \{1, \dots, p^m\}$ and c any positive integer not divisible by p, we have*

$$\psi^c(X_m)V_r = V_{\gamma(c)p^m+r} - V_{\gamma(c)p^m-r}.$$

Proof. By Corollary 3.4, $\psi^c(X_m) = \psi^{\gamma(c)}(X_m)$. Hence, by Proposition 4.1, $\psi^c(X_m) = g_{\gamma(c)}(X_m)$. Thus the result follows by Proposition 4.2. □

For $m \in \{0, \dots, \nu - 1\}$ and $i \in \{1, \dots, p - 1\}$ let $\theta_{ip^m} : R_{p^m} \to R_{p^{m+1}}$ be the $\mathbb{Z}$-linear map defined by

$$\theta_{ip^m}(V_r) = V_{ip^m+r} - V_{ip^m-r}, \tag{4.2}$$

for $r = 1, \dots, p^m$. Corollary 4.3 gives the following result.

Corollary 4.4. *Let $m \in \{0, \dots, \nu - 1\}$. Let c be any positive integer not divisible by p and let $W \in R_{p^m}$. Then*

$$\psi^c(X_m)W = \theta_{\gamma(c)p^m}(W).$$

Define elements $f_{-1}(t), f_0(t), f_1(t), \dots$ of $\mathbb{Z}[t]$ by $f_{-1}(t) = 0,\ f_0(t) = 1,\ f_1(t) = t$ and, for $n \geqslant 2$,

$$f_n(t) = tf_{n-1}(t) - f_{n-2}(t). \tag{4.3}$$

The $f_n(t)$ can be seen to be Dickson polynomials of the second kind, and can be given by an explicit formula, but we do not need this. The following result is straightforward to prove by induction.

Lemma 4.5. *For all $n \geqslant 0$,*

$$f_n = \begin{cases} g_n + g_{n-2} + \cdots + g_3 + g_1 & \text{if } n \text{ is odd,} \\ g_n + g_{n-2} + \cdots + g_2 + 1 & \text{if } n \text{ is even.} \end{cases}$$

Our next result is essentially the same as [15, Lemma 6], but we give a proof for the convenience of the reader.

Proposition 4.6. *Let $m \in \{0, \dots, \nu - 1\}$. Then, for $r \in \{1, \dots, p^m\}$ and $k \in \{0, \dots, p-1\}$, we have*

$$V_{kp^m+r} = f_k(X_m)V_r + f_{k-1}(X_m)V_{p^m-r}.$$

Proof. We use induction on k. The result is clear for $k = 0$. It is true for $k = 1$ because $V_{p^m+r} = X_m V_r + V_{p^m-r}$ by Proposition 2.2.

Now suppose that $k \in \{2, \dots, p-1\}$ and that the result is true for $k-1$ and $k-2$. By (4.3), the inductive hypothesis, and Proposition 2.2, we obtain

$$\begin{aligned} f_k(X_m)V_r + f_{k-1}(X_m)V_{p^m-r} &= X_m\big(f_{k-1}(X_m)V_r + f_{k-2}(X_m)V_{p^m-r}\big) \\ &\quad - \big(f_{k-2}(X_m)V_r + f_{k-3}(X_m)V_{p^m-r}\big) \\ &= X_m V_{(k-1)p^m+r} - V_{(k-2)p^m+r} \\ &= V_{kp^m+r}, \end{aligned}$$

as required. □

In the statement of the main result of this section it is convenient to extend the definition of γ by setting $\gamma(0) = 0$. Recalling that θ_{ip^m} is defined by (4.2) for $i \in \{1, \dots, p-1\}$, we also define θ_0 to be the identity map on R_{p^m}.

Theorem 4.7. *Let $m \in \{0, \dots, \nu - 1\}$ and let n be a positive integer not divisible by p. Let s be a positive integer satisfying $p^m < s \leqslant p^{m+1}$ and write $s = kp^m + r$, where $1 \leqslant r \leqslant p^m$ and $1 \leqslant k \leqslant p-1$. Then*

$$\psi^n(V_s) = \sum_{\substack{j \in \{0,\dots,k\} \\ j \equiv k \ (\mathrm{mod}\ 2)}} \theta_{\gamma(jn)p^m}\big(\psi^n(V_r)\big) + \sum_{\substack{j \in \{0,\dots,k\} \\ j \not\equiv k \ (\mathrm{mod}\ 2)}} \theta_{\gamma(jn)p^m}\big(\psi^n(V_{p^m-r})\big).$$

Proof. By Proposition 4.6, we have $V_s = f_k(X_m)V_r + f_{k-1}(X_m)V_{p^m-r}$. Suppose first that k is odd. Then, by Lemma 4.5 and Proposition 4.1, we obtain

$$\begin{aligned} V_s &= \big(\psi^k + \psi^{k-2} + \cdots + \psi^1\big)(X_m)V_r \\ &\quad + \big(\psi^{k-1} + \psi^{k-3} + \cdots + \psi^2\big)(X_m)V_{p^m-r} + V_{p^m-r}. \end{aligned}$$

By Proposition 2.1 it follows that

$$\begin{aligned} \psi^n(V_s) &= \big(\psi^{kn} + \psi^{(k-2)n} + \cdots + \psi^n\big)(X_m)\psi^n(V_r) \\ &\quad + \big(\psi^{(k-1)n} + \psi^{(k-3)n} + \cdots + \psi^{2n}\big)(X_m)\psi^n(V_{p^m-r}) + \psi^n(V_{p^m-r}). \end{aligned}$$

Therefore, by Corollary 4.4,

$$\begin{aligned}\psi^n(V_s) &= (\theta_{\gamma(kn)p^m} + \theta_{\gamma((k-2)n)p^m} + \cdots + \theta_{\gamma(n)p^m})\big(\psi^n(V_r)\big)\\ &\quad + (\theta_{\gamma((k-1)n)p^m} + \theta_{\gamma((k-3)n)p^m} + \cdots + \theta_{\gamma(2n)p^m} + \theta_0)\big(\psi^n(V_{p^m-r})\big),\end{aligned}$$

as required. The proof for even k is similar. $\square$

Theorem 4.7 allows us to calculate $\psi^n(V_s)$ for all s, and for all n not divisible by p, by elementary arithmetic and without the need for multiplication in R_{p^ν}.

For example, take $p = 7$ and $\nu = 2$. Let us calculate $\psi^4(V_{23})$. Thus $n = 4$ and $s = 23$. In order to apply Theorem 4.7 we take $m = 1$ and write $23 = 3 \cdot 7 + 2$. (Thus $k = 3$ and $r = 2$.) It is easy to check that $\gamma(4) = 4$, $\gamma(2 \cdot 4) = 6$ and $\gamma(3 \cdot 4) = 2$. Thus, by Theorem 4.7,

$$\psi^4(V_{23}) = (\theta_{28} + \theta_{14})\big(\psi^4(V_2)\big) + (\theta_0 + \theta_{42})\big(\psi^4(V_5)\big). \tag{4.4}$$

We next calculate $\psi^4(V_2)$, writing $2 = 1 \cdot 1 + 1$ in order to use Theorem 4.7. Thus

$$\psi^4(V_2) = \theta_4\big(\psi^4(V_1)\big) + \theta_0\big(\psi^4(V_0)\big) = \theta_4(V_1) = V_5 - V_3.$$

We can calculate $\psi^4(V_5)$ in a similar way, or by means of Proposition 3.6, to obtain $\psi^4(V_5) = V_7 - V_5 + V_3$. Thus, by (4.4),

$$\begin{aligned}\psi^4(V_{23}) &= (\theta_{28} + \theta_{14})(V_5 - V_3) + (\theta_0 + \theta_{42})(V_7 - V_5 + V_3)\\ &= (V_{33} - V_{23}) + (V_{19} - V_9) - (V_{31} - V_{25}) - (V_{17} - V_{11})\\ &\quad + V_7 + (V_{49} - V_{35}) - V_5 - (V_{47} - V_{37}) + V_3 + (V_{45} - V_{39})\\ &= V_{49} - V_{47} + V_{45} - V_{39} + V_{37} - V_{35} + V_{33} - V_{31} + V_{25}\\ &\quad - V_{23} + V_{19} - V_{17} + V_{11} - V_9 + V_7 - V_5 + V_3.\end{aligned}$$

We see that the indecomposables occurring have all subscripts of the same parity and have multiplicities that alternate between $+1$ and -1, in decreasing order of subscript. It turns out that these statements hold in general. We shall prove them in Theorem 5.1 in the next section.

5. The form of $\psi^n(V_s)$

Theorem 5.1. *Let n be a positive integer not divisible by p, and let $s \in \{1, \dots, p^\nu\}$. Write $\lambda(s)$ for the smallest non-negative integer such that $s \leqslant p^{\lambda(s)}$.*

(i) *There are integers $j_1, \dots, j_l$ such that $p^{\lambda(s)} \geqslant j_1 > j_2 > \cdots > j_l \geqslant 1$ and*

$$\psi^n(V_s) = V_{j_1} - V_{j_2} + V_{j_3} - \cdots \pm V_{j_l}.$$

(ii) *If n is even (so that p is odd) then $j_1, \dots, j_l$ are odd. If n is odd then $j_1, \dots, j_l$ have the same parity as s.*

Before giving the proof we derive an improvement of Propositions 3.6 and 3.7.

Corollary 5.2. *Let n be a positive integer not divisible by p, and let $s \in \{1, \ldots, p^m\}$, where $m \in \{0, \ldots, \nu\}$.*

(i) *If n is even then one of $\psi^n(V_s)$ and $\psi^n(V_{p^m-s})$ has the form*

$$V_{j_1} - V_{j_2} + \cdots \pm V_{j_l}$$

and the other has the form

$$V_{p^m} - V_{j_1} + V_{j_2} - \cdots \mp V_{j_l},$$

where $j_1, \ldots, j_l$ are odd and $p^m > j_1 > j_2 > \cdots > j_l \geqslant 1$.

(ii) *If n is odd then $\psi^n(V_s)$ and $\psi^n(V_{p^m-s})$ have the forms*

$$\psi^n(V_s) = V_{j_1} - V_{j_2} + V_{j_3} - \cdots + V_{j_l},$$
$$\psi^n(V_{p^m-s}) = V_{p^m-j_l} - \cdots + V_{p^m-j_3} - V_{p^m-j_2} + V_{p^m-j_1},$$

where l is odd, $j_1, \ldots, j_l$ have the parity of s, and $p^m \geqslant j_1 > j_2 > \cdots > j_l \geqslant 0$.

Proof. (i) This is immediate from Theorem 5.1 and Proposition 3.6.

(ii) If $p = 2$ then ψ^n is the identity map, by Corollary 3.5, and the result is clear. Thus we may assume that p is odd. We argue according to the parity of s.

Suppose first that s is odd. By Theorem 5.1 we may write

$$\psi^n(V_s) = V_{j_1} - V_{j_2} + V_{j_3} - \cdots \pm V_{j_l},$$

where $j_1, \ldots, j_l$ are odd and $p^m \geqslant j_1 > j_2 > \cdots > j_l \geqslant 1$. By (2.2),

$$\delta(V_{j_1} - V_{j_2} + \cdots \pm V_{j_l}) = s.$$

Since s is odd it follows that l must be odd, and so $\psi^n(V_s)$ has the required form. By Theorem 5.1, $\psi^n(V_{p^m-s})$ is a linear combination of terms V_i where i has the parity of $p^m - s$; so $\psi^n(V_{p^m-s})$ does not involve V_{p^m}. Thus, by Proposition 3.7,

$$\psi^n(V_{p^m-s}) = V_{p^m-j_l} - \cdots + V_{p^m-j_3} - V_{p^m-j_2} + V_{p^m-j_1}.$$

(Note here that we may have $p^m - j_1 = 0$.) Thus the result holds for s odd. If s is even then $p^m - s$ is odd and we may interchange the roles of V_s and V_{p^m-s} in the above argument. $\square$

Proof of Theorem 5.1. For each integer a let $[a]$ denote the congruence class of a modulo 2 and let $R[a]$ denote the additive subgroup of R_{p^ν} spanned by all V_i with $[i] = [a]$. Thus $R[a] = R[0]$ or $R[a] = R[1]$. Observe that (i) and (ii) of Theorem 5.1 are equivalent to (i) and the statement that $\psi^n(V_s) \in R[ns + n + 1]$.

To prove the theorem we use induction on m, where $m = \lambda(s)$. Since $\psi^n(V_1) = V_1$, statements (i) and (ii) are trivial for $m = 0$. Let $m < \nu$ and assume that (i) and (ii) hold for all s with $\lambda(s) \leqslant m$. Now take s such that $\lambda(s) = m + 1$. We shall prove that (i) and (ii) hold for V_s. Write $q = p^m$, so that $pq = p^{m+1}$. Also, write $s = kq + r$, where $1 \leqslant r \leqslant q$ and $1 \leqslant k \leqslant p - 1$, as in Theorem 4.7. Thus $\psi^n(V_r)$ and $\psi^n(V_{q-r})$ are covered by the inductive hypothesis.

For each non-negative integer a define U_a by

$$U_a = \begin{cases} \psi^n(V_r) & \text{if } [a] = [k], \\ \psi^n(V_{q-r}) & \text{if } [a] \neq [k]. \end{cases}$$

Then, by Theorem 4.7,

$$\psi^n(V_s) = \sum_{j=0}^{k} \theta_{\gamma(jn)q}(U_j). \tag{5.1}$$

We have $\psi^n(V_r) \in R[nr+n+1]$ and $\psi^n(V_{q-r}) \in R[n(q-r)+n+1]$, by the inductive hypothesis. It follows easily that $U_j \in R[nr+n+1+(j+k)nq]$ for $j = 0, \dots, k$. By the definition of $\theta_{\gamma(jn)q}$ (see (4.2)), we obtain

$$\theta_{\gamma(jn)q}(U_j) \in R\big[nr+n+1+(j+k)nq+\gamma(jn)q\big].$$

However, $[\gamma(jn)] = [jn]$. Thus

$$\theta_{\gamma(jn)q}(U_j) \in R\big[n(kq+r)+n+1\big] = R[ns+n+1].$$

Hence, by (5.1), we have $\psi^n(V_s) \in R[ns+n+1]$. Thus it remains only to prove that (i) holds. We deal separately with the cases where n is even and n is odd.

Suppose first that n is even, so that p is odd. Clearly $\lambda(pq-s) \leqslant m+1$. Also, by Proposition 3.6, $\psi^n(V_s) + \psi^n(V_{pq-s}) = V_{pq}$. It follows that if (i) holds for V_{pq-s} then it holds for V_s. Thus, by the inductive hypothesis, we may assume that $\lambda(pq-s) = m+1$. Either $s < \frac{1}{2}pq$ or $pq-s < \frac{1}{2}pq$. Therefore, without loss of generality, we may assume that $s < \frac{1}{2}pq$.

Since $s = kq + r < \frac{1}{2}pq$, we have $k \leqslant \frac{1}{2}(p-1)$. Suppose that $\gamma(s_1 n) = \gamma(s_2 n)$, where $s_1, s_2 \in \{1, \dots, k\}$. Then $s_1 n \equiv \pm s_2 n \pmod{2p}$. Since $p \nmid n$ we obtain $s_1 \equiv \pm s_2 \pmod{p}$. Hence $s_1 \mp s_2 \equiv 0 \pmod{p}$. However, $s_1, s_2 \in \{1, \dots, \frac{1}{2}(p-1)\}$ because $k \leqslant \frac{1}{2}(p-1)$. Therefore $s_1 = s_2$. Thus the numbers $\gamma(n), \gamma(2n), \dots, \gamma(kn)$ are distinct. They are even, since n is even. Hence we may write

$$\big\{\gamma(n), \gamma(2n), \dots, \gamma(kn)\big\} = \{a_1, a_2, \dots, a_k\},$$

where the a_j are even and $p-1 \geqslant a_1 > a_2 > \cdots > a_k \geqslant 2$. Also, set $a_{k+1} = 0$.

By (5.1) we have

$$\psi^n(V_s) = \theta_{a_1 q}(W_1) + \cdots + \theta_{a_k q}(W_k) + \theta_{a_{k+1} q}(W_{k+1}), \tag{5.2}$$

where $W_j \in \{\psi^n(V_r), \psi^n(V_{q-r})\}$ for each j.

For integers a and b with $pq \geqslant a \geqslant b \geqslant 0$, let $M[a,b]$ denote the set of all elements Y of R_{pq} that can be written in the form

$$Y = V_{i_1} - V_{i_2} + V_{i_3} - \cdots + V_{i_{h-1}} - V_{i_h},$$

where h is even and $a \geqslant i_1 \geqslant i_2 \geqslant \cdots \geqslant i_h \geqslant b$. To prove (i) it suffices to show that $\psi^n(V_s) \in M[pq, 0]$, for then we obtain the required expression for $\psi^n(V_s)$ by cancellation and by removal of terms V_0.

Suppose that $pq \geqslant c_1 \geqslant c_2 \geqslant \cdots \geqslant c_{d+1} \geqslant 0$ and $Y_j \in M[c_j, c_{j+1}]$ for $j = 1, \dots, d$. Then, clearly, $Y_1 + Y_2 + \cdots + Y_d \in M[c_1, c_{d+1}]$.

By the inductive hypothesis, each W_j belongs to $M[q, 0]$, since we may introduce a term V_0 if necessary to give even length to the expression for W_j. It follows easily that $\theta_{a_j q}(W_j)$ belongs to $M[(a_j+1)q, (a_j-1)q]$, for $j = 1, \dots, k$. Hence

$$\theta_{a_j q}(W_j) \in M\big[(a_j+1)q, (a_{j+1}+1)q\big],$$

for $j = 1, \dots, k$, because $a_j \geqslant a_{j+1} + 2$. Also,

$$\theta_{a_{k+1}q}(W_{k+1}) = W_{k+1} \in M[q,0] = M\big[(a_{k+1}+1)q,0\big].$$

Therefore, by (5.2), we have $\psi^n(V_s) \in M[(a_1+1)q,0] \subseteq M[pq,0]$, as required.

We now turn to the remaining case, and assume that n is odd.

Since Theorem 5.1 holds for V_r and V_{q-r}, by the inductive hypothesis, Corollary 5.2(ii) holds for V_r and V_{q-r}. Thus we may write

$$\psi^n(V_r) = V_{j_1} - V_{j_2} + V_{j_3} - \cdots + V_{j_l}, \tag{5.3}$$

$$\psi^n(V_{q-r}) = V_{q-j_l} - \cdots + V_{q-j_3} - V_{q-j_2} + V_{q-j_1}, \tag{5.4}$$

where l is odd and $q \geqslant j_1 > j_2 > \cdots > j_l \geqslant 0$.

Suppose that $\gamma(s_1 n) = \gamma(s_2 n)$, where $s_1, s_2 \in \{1,\dots,k\}$. Then we have $s_1 n \equiv \pm s_2 n \pmod{2p}$. Since n is coprime to $2p$ we obtain $s_1 \equiv \pm s_2 \pmod{2p}$. Hence $s_1 \mp s_2 \equiv 0 \pmod{2p}$. Since $s_1, s_2 \in \{1,\dots,p-1\}$, it follows that $s_1 = s_2$. Consequently, the numbers $\gamma(n), \gamma(2n), \dots, \gamma(kn)$ are distinct and we may write

$$\big\{\gamma(n), \gamma(2n), \dots, \gamma(kn)\big\} = \{a_1, a_2, \dots, a_k\},$$

where $p-1 \geqslant a_1 > a_2 > \cdots > a_k \geqslant 1$. Also, set $a_{k+1} = 0$.

Since n is odd, we have $[\gamma(jn)] = [j]$, and (5.1) may be written

$$\psi^n(V_s) = \theta_{a_1 q}(U_{a_1}) + \theta_{a_2 q}(U_{a_2}) + \cdots + \theta_{a_k q}(U_{a_k}) + \theta_{a_{k+1}q}(U_{a_{k+1}}). \tag{5.5}$$

With $j_1, \dots, j_l$ as in (5.3) and (5.4), define T_{aq}, for each $a \in \{0,\dots,p-1\}$, by

$$T_{aq} = \begin{cases} V_{aq+j_1} - V_{aq+j_2} + \cdots + V_{aq+j_l} & \text{if } [a] = [k], \\ V_{aq+q-j_l} - \cdots - V_{aq+q-j_2} + V_{aq+q-j_1} & \text{if } [a] \neq [k]. \end{cases}$$

Then it can be checked that $\theta_{aq}(U_a) = T_{aq} - T_{(a-1)q}$ for all $a \in \{1,\dots,p-1\}$. Also, $\theta_{0q}(U_0) = T_{0q}$. Thus, by (5.5),

$$\psi^n(V_s) = T_{a_1 q} - T_{(a_1-1)q} + T_{a_2 q} - T_{(a_2-1)q} + \cdots + T_{a_k q} - T_{(a_k-1)q} + T_{a_{k+1}q}.$$

If $a_j - 1 = a_{j+1}$ for some $j \in \{1,\dots,k\}$ then we may cancel two adjacent terms in this expression. After all such cancellations we obtain

$$\psi^n(V_s) = T_{b_1 q} - T_{b_2 q} + \cdots - T_{b_{d-1}q} + T_{b_d q}, \tag{5.6}$$

where d is odd and $p-1 \geqslant b_1 > b_2 > \cdots > b_d \geqslant 0$.

For integers a and b where $pq \geqslant a \geqslant b \geqslant 0$, let $N[a,b]$ denote the set of all elements Y of R_{pq} that can be written in the form

$$Y = V_{i_1} - V_{i_2} + \cdots - V_{i_{h-1}} + V_{i_h},$$

where h is odd and $a \geqslant i_1 \geqslant i_2 \geqslant \cdots \geqslant i_h \geqslant b$. To prove (i) it suffices to show that $\psi^n(V_s) \in N[pq,0]$.

By the definition of T_{aq} we see that $T_{b_j q} \in N[(b_j+1)q, b_j q]$ for $j = 1,\dots,d$. However, $b_j q \geqslant (b_{j+1}+1)q$, for $j \leqslant d-1$. Therefore, by (5.6),

$$\psi^n(V_s) \in N\big[(b_1+1)q, b_d q\big] \subseteq N[pq,0],$$

as required. $\square$

References

[1] G. Almkvist, Representations of Z/pZ in characteristic p and reciprocity theorems, J. Algebra 68 (1981) 1–27.
[2] G. Almkvist, R. Fossum, Decomposition of exterior and symmetric powers of indecomposable Z/pZ-modules in characteristic p and relations to invariants, in: Séminaire d'Algèbre Paul Dubreil, 30ème année, Paris, 1976–1977, in: Lecture Notes in Math., vol. 641, Springer, Berlin, 1978, pp. 1–111.
[3] D.J. Benson, Representations and Cohomology I, Cambridge University Press, Cambridge, 1995.
[4] R.M. Bryant, Free Lie algebras and Adams operations, J. Lond. Math. Soc. (2) 68 (2003) 355–370.
[5] R.M. Fossum, Decompositions revisited, in: Séminaire d'Algèbre Paul Dubreil et Marie-Paule Malliavin, 34ème année, Paris, 1981, in: Lecture Notes in Math., vol. 924, Springer, Berlin, 1982, pp. 260–295.
[6] R. Gow, T.J. Laffey, On the decomposition of the exterior square of an indecomposable module of a cyclic p-group, J. Group Theory 9 (2006) 659–672.
[7] J.A. Green, The modular representation algebra of a finite group, Illinois J. Math. 6 (1962) 607–619.
[8] I. Hughes, G. Kemper, Symmetric powers of modular representations, Hilbert series and degree bounds, Comm. Algebra 28 (2000) 2059–2088.
[9] B. Huppert, N. Blackburn, Finite Groups II, Springer, Berlin, 1982.
[10] F.M. Kouwenhoven, The λ-structure of the Green rings of cyclic p-groups, Proc. Sympos. Pure Math. 47 (1987) 451–466.
[11] F.M. Kouwenhoven, The λ-structure of the Green ring of $GL(2, \mathbb{F}_p)$ in characteristic p, Comm. Algebra 18 (1990) 1645–1671.
[12] F.M. Kouwenhoven, The λ-structure of the Green ring of $GL(2, \mathbb{F}_p)$ in characteristic p, II, Comm. Algebra 18 (1990) 1673–1700.
[13] F.M. Kouwenhoven, The λ-structure of the Green ring of $GL(2, \mathbb{F}_p)$ in characteristic p, III, Comm. Algebra 18 (1990) 1701–1728.
[14] F.M. Kouwenhoven, The λ-structure of the Green ring of $GL(2, \mathbb{F}_p)$ in characteristic p, IV, Comm. Algebra 18 (1990) 1729–1747.
[15] J.D. McFall, How to compute the elementary divisors of the tensor product of two matrices, Linear Multilinear Algebra 7 (1979) 193–201.
[16] T. Ralley, Decomposition of products of modular representations, J. London Math. Soc. 44 (1969) 480–484.
[17] J.-C. Renaud, The decomposition of products in the modular representation ring of a cyclic group of prime power order, J. Algebra 58 (1979) 1–11.
[18] B. Srinivasan, The modular representation ring of a cyclic p-group, Proc. London Math. Soc. (3) 14 (1964) 677–688.
[19] P. Symonds, Cyclic group actions on polynomial rings, Bull. Lond. Math. Soc. 39 (2007) 181–188.