J Algebr Comb (2008) 28: 169–187
DOI 10.1007/s10801-007-0117-9

Lie powers and Witt vectors

R.M. Bryant · Marianne Johnson

Received: 11 April 2007 / Accepted: 18 December 2007 / Published online: 10 January 2008

Abstract In the study of Lie powers of a module V in prime characteristic p, a basic role is played by certain modules B_n introduced by Bryant and Schocker. The isomorphism types of the B_n are not fully understood, but these modules fall into infinite families $\{B_k, B_{pk}, B_{p^2k}, \ldots\}$, one family $B(k)$ for each positive integer k not divisible by p, and there is a recursive formula for the modules within $B(k)$. Here we use combinatorial methods and Witt vectors to show that each module in $B(k)$ is isomorphic to a direct sum of tensor products of direct summands of the kth tensor power $V^{\otimes k}$.

Keywords Free Lie algebra · Lie power · Tensor power · Witt vector

1 Introduction

Let G be a group and F a field. For any finite-dimensional FG-module V, let $L(V)$ be the free Lie algebra on V (the free Lie algebra generated by any basis of V), and regard $L(V)$ as an FG-module on which each element of G acts as a Lie algebra automorphism. Each homogeneous component $L^n(V)$ is a finite-dimensional submodule of $L(V)$, called the nth Lie power of V.

The central problem on Lie powers is to describe the modules $L^n(V)$ up to isomorphism. We refer to [3] and the papers cited there for details of progress on this problem. As would be expected, the results are best when F has characteristic 0. The

To the memory of Manfred Schocker.

R.M. Bryant (✉) · M. Johnson
School of Mathematics, University of Manchester, Manchester M13 9PL, UK
e-mail: roger.bryant@manchester.ac.uk

M. Johnson
e-mail: marianne.johnson@maths.manchester.ac.uk

harder case, which we concentrate on in this paper, is when F has prime characteristic p.

One of the fundamental results in characteristic p is the 'Decomposition Theorem' of Bryant and Schocker [3], stated as Theorem 2.1 below. This reduces the study of arbitrary Lie powers of V to the study of certain Lie powers of p-power degree, namely, Lie powers $L^{p^i}(B_n)$, where, for each n, B_n is a certain direct summand of the nth tensor power $V^{\otimes n}$.

Let us write $n = p^m k$, where k is not divisible by p. In [4], a recursive formula was given for the modules B_k, B_{pk}, B_{p^2k}, ..., up to isomorphism. We state this as Theorem 2.2 below. However, the formula is rather intractable. It involves the Witt polynomials (as used to define operations on the ring of Witt vectors) and gives the $B_{p^m k}$ only as the components of a Witt vector with known 'ghost' components. The results of [3] and [4] give no explicit information about the modules $B_{p^m k}$ except that, as already mentioned, $B_{p^m k}$ is a direct summand of $V^{\otimes p^m k}$. In this paper we shall give much more precise information.

As a motivating example, consider the case where $k = 2$ and $p = 3$. Thus we take F of characteristic 3. It is well known and easily seen that $V^{\otimes 2} \cong S^2(V) \oplus \wedge^2(V)$, where $S^2(V)$ is the symmetric square of V and $\wedge^2(V)$ is the exterior square. The recursive formula from [4] gives $B_2 \cong L^2(V)$ and $3B_6 \oplus B_2^{\otimes 3} \cong L^2(V^{\otimes 3})$, where $3B_6$ denotes the direct sum of 3 isomorphic copies of B_6. Hence $B_2 \cong \wedge^2(V)$ and it can be shown that

$$B_6 \cong S^2(V) \otimes S^2(V) \otimes \wedge^2(V). \tag{1.1}$$

We shall verify this in Section 4 (see Example 4.4). Examples like this suggested that, in general, $B_{p^m k}$ is isomorphic to a direct sum of tensor products of direct summands of $V^{\otimes k}$, although we had no *a priori* reason to suspect this. The purpose of this paper is to prove this fact.

We shall see that $V^{\otimes k} \cong \bigoplus_{d|k} \phi(d) U_{k,d}$, for certain modules $U_{k,d}$ indexed by the divisors d of k, where ϕ denotes Euler's function and $\phi(d)U_{k,d}$ denotes the direct sum of $\phi(d)$ isomorphic copies of $U_{k,d}$. Thus

$$V^{\otimes p^m k} \cong (V^{\otimes k})^{\otimes p^m} \cong \bigoplus_{\lambda \in \Lambda} U_{k,\lambda(1)} \otimes \cdots \otimes U_{k,\lambda(p^m)},$$

where Λ is a finite set indexing a family of p^m-tuples $(\lambda(1), \ldots, \lambda(p^m))$ with $\lambda(1), \ldots, \lambda(p^m) \in \{d : d \mid k\}$. Our main result, Theorem 4.2, states that there is a subset Λ_0 of Λ such that

$$B_{p^m k} \cong \bigoplus_{\lambda \in \Lambda_0} U_{k,\lambda(1)} \otimes \cdots \otimes U_{k,\lambda(p^m)}.$$

This is, of course, much stronger than the statement that $B_{p^m k}$ is isomorphic to a direct summand of $V^{\otimes p^m k}$.

In Theorem 4.3 we shall obtain a version of Theorem 4.2 in which the modules $U_{k,d}$ are replaced by a set of modules indexed only by those divisors c of k such that c and k/c are coprime. This is a sharpening of Theorem 4.2 in the case where k is not square-free (that is, where k is divisible by the square of some prime).

The modules $U_{k,d}$ are of well-established interest. They are given by the eigenspaces of the action of a cycle of length k in the symmetric group $\mathrm{Sym}(k)$ of degree k acting by permutation of the factors of $V^{\otimes k}$. These modules have appeared repeatedly, in various guises, in the theory of free Lie algebras and the representation theory of groups. They correspond to the $F\mathrm{Sym}(k)$-modules induced from one-dimensional modules for the cyclic subgroup generated by a k-cycle, as considered in [12, Chapter 8].

Section 2 contains basic results about the $U_{k,d}$ and some related modules. The main results on the modules $B_{p^m k}$ are obtained in Section 4. However, the proofs of these results rest heavily on Section 3, which is largely combinatorial. We study certain polynomials defined in an arithmetic way and apply methods from elementary number theory, combinatorics and the theory of Witt vectors.

2 Summands of tensor powers

Let F be a field, G a group, and V a finite-dimensional (right) FG-module. The tensor algebra $T(V)$ is the free associative algebra on V, and the nth homogeneous component $T^n(V)$ may be identified with the nth tensor power of V, otherwise denoted by $V^{\otimes n}$. The free Lie algebra $L(V)$, as defined in Section 1, may be regarded as embedded in $T(V)$: see [3, Section 2] for further details.

The following result is the 'Decomposition Theorem', [3, Theorem 4.4].

Theorem 2.1 [3] *Let F be a field of prime characteristic p, G a group, and V a finite-dimensional FG-module. Let k be a positive integer not divisible by p. Then, for each non-negative integer m, there is a submodule $B_{p^m k}$ of $L^{p^m k}(V)$ such that $B_{p^m k}$ is a direct summand of $V^{\otimes p^m k}$ and*

$$L^{p^m k}(V) = L^{p^m}(B_k) \oplus L^{p^{m-1}}(B_{pk}) \oplus \cdots \oplus L^1(B_{p^m k}).$$

(The Lie powers $L^{p^m}(B_k), \ldots, L^1(B_{p^m k})$ may be regarded as subspaces of $L^{p^m k}(V)$ for the reasons explained in [3, Section 2].)

For an arbitrary field F, let R_{FG} denote the Green ring (representation ring) of G over F. This is the ring spanned by the isomorphism classes of finite-dimensional (right) FG-modules with sum and product coming from the direct sum and tensor product of modules. (It has a $\mathbb{Z}$-basis consisting of the isomorphism classes of the finite-dimensional indecomposable FG-modules.) If V is any finite-dimensional FG-module we often write V for the corresponding element of R_{FG}. Thus, for modules V_1 and V_2, we have $V_1 = V_2$ in R_{FG} if and only if $V_1 \cong V_2$. Note that the tensor power $V^{\otimes n}$ may be written as V^n in R_{FG}.

The following result is part of [4, Theorem 4.2].

Theorem 2.2 [4] *Further to Theorem 2.1, the equation*

$$p^m B_{p^m k} + p^{m-1}(B_{p^{m-1}k})^p + \cdots + p(B_{pk})^{p^{m-1}} + (B_k)^{p^m} = L^k(V^{p^m})$$

holds in the Green ring R_{FG} for every non-negative integer m.

It is possible to regard $B_{p^m k}$ as a 'strict polynomial functor' on the category of finite-dimensional vector spaces over F: see [7]. Thus the module $B_{p^m k}$ may be written as $B_{p^m k}(V)$, and this shows its dependence on V. Accordingly, Theorems 2.1 and 2.2 may be written functorially. However, we do not pursue the functorial approach as it does not seem to help to simplify our arguments.

Theorem 2.2 is the starting-point of our study of the modules $B_{p^m k}$. The equations of the theorem describe the $B_{p^m k}$ recursively in terms of the modules $L^k(V^{p^m})$, and the polynomials on the left-hand side of these equations may be recognised as the 'Witt polynomials' (see [14, Chapter II, Section 6]). Thus, to gain further information about the $B_{p^m k}$, we must expect to deal with Witt vectors.

Let p be a prime number. For any commutative ring R we write R^∞ for the set of all countably infinite 'vectors' $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ with $a_i \in R$ for $i \geq 0$. In the present context these vectors are called 'Witt vectors'. For $\mathbf{a} \in R^\infty$, where $\mathbf{a} = (a_0, a_1, a_2, \ldots)$, define $\gamma_p(\mathbf{a}) \in R^\infty$ by

$$\gamma_p(\mathbf{a}) = (b_0, b_1, b_2, \ldots), \tag{2.1}$$

where, for $i \geq 0$,

$$b_i = p^i a_i + p^{i-1} a_{i-1}^p + \cdots + p a_1^{p^{i-1}} + a_0^{p^i}. \tag{2.2}$$

In the language of Witt vectors, $b_0, b_1, \ldots$ are the 'ghost' components of $\mathbf{a}$.

The equations of Theorem 2.2 can now be written as

$$\gamma_p(B_k, B_{pk}, B_{p^2 k}, \ldots) = (L^k(V), L^k(V^p), L^k(V^{p^2}), \ldots). \tag{2.3}$$

Our problem is to try to unravel B_k, B_{pk}, $\ldots$ from this equation. Much of our effort will be devoted to writing the modules $L^k(V^{p^m})$ in the Green ring in a form that facilitates calculations with Witt vectors.

From now on in this section, we take F to be a field of arbitrary characteristic, G a group, and V a finite-dimensional FG-module. Furthermore, we take k to be a positive integer not divisible by $\mathrm{char}(F)$. Let E be the extension field of F obtained by adjoining (if necessary) a primitive kth root of unity ϵ, and let $\langle \epsilon \rangle$ denote the cyclic group generated by ϵ, consisting of all kth roots of unity in E.

We shall often need to use the following elementary fact about a cyclic group of order k: if x and y are elements of the group of the same order then there exists l prime to k such that $x^l = y$. We omit the straightforward proof and use this fact without further reference.

Let V_E denote the EG-module $E \otimes V$ (with tensor product taken over F), and let $V_E^{\otimes k}$ denote the kth tensor power of V_E, identified with $E \otimes V^{\otimes k}$. The symmetric group $\mathrm{Sym}(k)$ acts on the left on $V_E^{\otimes k}$ by permuting the tensor factors, and this action commutes with the right action of G. Let σ be the k-cycle $(1, 2, \ldots, k)$ in $\mathrm{Sym}(k)$. Then we can write $V_E^{\otimes k}$ as a direct sum of σ-eigenspaces, namely

$$V_E^{\otimes k} = \bigoplus_{\xi \in \langle \epsilon \rangle} (V_E^{\otimes k})_\xi, \tag{2.4}$$

where

$$(V_E^{\otimes k})_\xi = \{v \in V_E^{\otimes k} : \sigma v = \xi v\}.$$

(This can be proved from Maschke's theorem or by diagonalising the matrix representing the action of σ.) Clearly each $(V_E^{\otimes k})_\xi$ is an EG-submodule of $V_E^{\otimes k}$. Also, for l prime to k, σ and σ^l are conjugate in $\mathrm{Sym}(k)$, from which it follows that

$$(V_E^{\otimes k})_\xi \cong (V_E^{\otimes k})_{\xi'} \text{ when } |\xi| = |\xi'|. \tag{2.5}$$

Here $|\xi|$ denotes the (multiplicative) order of an element ξ of $\langle\epsilon\rangle$.

In [2, Section 4] it was shown, with different notation, that, for each $\xi \in \langle\epsilon\rangle$, there is an FG-submodule $(V^{\otimes k})_\xi$ of $V^{\otimes k}$ such that

$$E \otimes (V^{\otimes k})_\xi \cong (V_E^{\otimes k})_\xi. \tag{2.6}$$

(In the notation of [2], $(V^{\otimes k})_\xi$ corresponds to U_ξ^*.) By the Noether–Deuring theorem [5, (29.11)], two modules are isomorphic if they are isomorphic after field extension. Thus (2.4), (2.5) and (2.6) yield

$$V^{\otimes k} \cong \bigoplus_{\xi \in \langle\epsilon\rangle} (V^{\otimes k})_\xi \tag{2.7}$$

and

$$(V^{\otimes k})_\xi \cong (V^{\otimes k})_{\xi'} \text{ when } |\xi| = |\xi'|. \tag{2.8}$$

For each divisor d of k, let $U_{k,d}$ denote an FG-module satisfying

$$U_{k,d} \cong (V^{\otimes k})_\xi, \text{ where } |\xi| = d. \tag{2.9}$$

Thus we may write (2.7) in the Green ring as

$$V^k = \sum_{d|k} \phi(d) U_{k,d}. \tag{2.10}$$

Lemma 2.3 *We have* $U_{k,k} \cong L^k(V)$.

Proof By the Noether–Deuring theorem it suffices to obtain $E \otimes U_{k,k} \cong L^k(V_E)$. Since $|\epsilon| = k$, we have $U_{k,k} \cong (V^{\otimes k})_\epsilon$. Thus, by (2.6), $E \otimes U_{k,k} \cong (V_E^{\otimes k})_\epsilon$. Hence it suffices to show that

$$(V_E^{\otimes k})_\epsilon \cong L^k(V_E). \tag{2.11}$$

This holds by a result of Klyachko [10, Theorem].

A character-theoretic proof of (2.11) can be given in the following way. By the Noether–Deuring theorem, we may assume that E is infinite. Also, it is enough to prove (2.11) in the case where G is the general linear group $\mathrm{GL}(V_E)$. We can consider (formal) characters of modules as defined in [8], and, by [10, proof of Proposition 1], $(V_E^{\otimes k})_\epsilon$ and $L^k(V_E)$ have the same character, just as in characteristic 0. Furthermore,

$(V_E^{\otimes k})_\epsilon$ is a direct summand of $V_E^{\otimes k}$, by (2.4), and, as is well known, $L^k(V_E)$ is also a direct summand of $V_E^{\otimes k}$, because $\mathrm{char}(E) \nmid k$ (see [6, Section 3.1], for example). However, direct summands of $V_E^{\otimes k}$ with the same character are isomorphic (because they are tilting modules—see [6]). Thus (2.11) holds. □

Since the modules $(V^{\otimes k})_\xi$ or $U_{k,d}$ have a wider significance than for the purposes of this paper, we summarise a few facts about these modules. We shall not need to use these facts here, and, in any case, they are well known or, at least, closely related to well-known facts. Thus we do not give detailed proofs.

Taking F to contain a primitive kth root of unity, we have $(V^{\otimes k})_\xi = e_\xi V^{\otimes k}$, where e_ξ is the idempotent of $F\mathrm{Sym}(k)$ defined, using a k-cycle σ, by

$$e_\xi = \frac{1}{k}\sum_{i=0}^{k-1} \xi^{-i}\sigma^i.$$

Thus, under the Schur correspondence, $(V^{\otimes k})_\xi$ corresponds to $e_\xi F\mathrm{Sym}(k)$, namely the $F\mathrm{Sym}(k)$-module induced from the one-dimensional $F\langle\sigma\rangle$-module on which σ acts as multiplication by ξ. A formula for the character of this induced module is given in [13, 4.17 Lemma], and this module is important in the work of Kraśkiewicz and Weyman [11]: see also [12, Chapter 8].

We note also that the modules $(V^{\otimes k})_\xi$ are involved in the definition of Adams operations ψ^n on R_{FG}, as explained in [2], further to the work of Benson [1]. For example, by [2, (4.4)], $\psi^k(V) = \sum_{d|k} \mu(d)U_{k,d}$, where μ is the Möbius function.

We return to the needs of the present paper. For each positive integer r and each divisor d of k, let $M_{k,d}^{(r)}$ denote an FG-module satisfying

$$M_{k,d}^{(r)} \cong \bigoplus_{\xi_1\cdots\xi_r=\xi} (V^{\otimes k})_{\xi_1} \otimes \cdots \otimes (V^{\otimes k})_{\xi_r}, \tag{2.12}$$

where $|\xi| = d$ and where the sum is over all r-tuples $(\xi_1, \ldots, \xi_r)$ of elements of $\langle\epsilon\rangle$ satisfying $\xi_1 \cdots \xi_r = \xi$. (It is easy to see that this sum is the same, up to isomorphism, for all $\xi \in \langle\epsilon\rangle$ of order d.)

Lemma 2.4 *For $d \mid k$ we have $M_{k,d}^{(r)} \cong ((V^{\otimes r})^{\otimes k})_\xi$, where $\xi \in \langle\epsilon\rangle$ has order d.*

Proof By (2.6) and (2.12), $E \otimes M_{k,d}^{(r)}$ is isomorphic to the module defined in the same way over E as $M_{k,d}^{(r)}$ is defined over F. If $E \otimes M_{k,d}^{(r)} \cong ((V_E^{\otimes r})^{\otimes k})_\xi$ then, by (2.6), we have $E \otimes M_{k,d}^{(r)} \cong E \otimes ((V^{\otimes r})^{\otimes k})_\xi$ and the required result follows by the Noether–Deuring theorem. Thus it is enough to prove the result over E and, to ease the notation, we may take $F = E$.

Let $M = \bigotimes_{(i,j)\in\Omega} V_{(i,j)}$, where $\Omega = \{(i, j) : 1 \le i \le k,\ 1 \le j \le r\}$ and $V_{(i,j)} \cong V$ for all (i, j). In the symmetric group on Ω, let τ be the cycle

$$((1, 1), (1, 2), \ldots, (1, r), (2, 1), (2, 2), \ldots, (2, r), \ldots, (k, 1), (k, 2), \ldots, (k, r)).$$

Thus τ^r has order k and is a product of k-cycles, namely $\tau^r = \sigma_1 \cdots \sigma_r$, where, for $j = 1, \ldots, r$, we have $\sigma_j = ((1, j), (2, j), \ldots, (k, j))$. Writing M as the direct sum of τ^r-eigenspaces, we have

$$M = \bigoplus_{\xi \in \langle \epsilon \rangle} M_\xi. \tag{2.13}$$

We may also write M in the form $M = N^{(1)} \otimes \cdots \otimes N^{(r)}$, where, for $j = 1, \ldots, r$,

$$N^{(j)} = V_{(1,j)} \otimes \cdots \otimes V_{(k,j)} \cong V^{\otimes k}.$$

Writing $N^{(j)}$ as the direct sum of σ_j-eigenspaces, we have $N^{(j)} = \bigoplus_{\xi \in \langle \epsilon \rangle} N^{(j)}_\xi$. Thus

$$M = \bigoplus_{\xi_1, \ldots, \xi_r \in \langle \epsilon \rangle} (N^{(1)}_{\xi_1} \otimes \cdots \otimes N^{(r)}_{\xi_r}). \tag{2.14}$$

Since $\tau^r = \sigma_1 \cdots \sigma_r$, we have

$$N^{(1)}_{\xi_1} \otimes \cdots \otimes N^{(r)}_{\xi_r} \subseteq M_{\xi_1 \cdots \xi_r}. \tag{2.15}$$

Therefore, by (2.13), (2.14) and (2.15),

$$M_\xi = \bigoplus_{\xi_1 \cdots \xi_r = \xi} (N^{(1)}_{\xi_1} \otimes \cdots \otimes N^{(r)}_{\xi_r}), \tag{2.16}$$

for all $\xi \in \langle \epsilon \rangle$. Since $N^{(j)} \cong V^{\otimes k}$, (2.12) and (2.16) give

$$M_\xi \cong M^{(r)}_{k,d}, \text{ where } |\xi| = d. \tag{2.17}$$

We now write M in the form

$$M = (V_{(1,1)} \otimes \cdots \otimes V_{(1,r)}) \otimes \cdots \otimes (V_{(k,1)} \otimes \cdots \otimes V_{(k,r)})$$

and note that τ^r permutes the k factors of M in a cycle of length k. Hence $M_\xi \cong ((V^{\otimes r})^{\otimes k})_\xi$, for all $\xi \in \langle \epsilon \rangle$. The lemma now follows from (2.17). □

Corollary 2.5 *For every positive integer r, $M^{(r)}_{k,k} \cong L^k(V^{\otimes r})$.*

Proof By Lemma 2.3 and (2.9), $L^k(V^{\otimes r}) \cong ((V^{\otimes r})^{\otimes k})_\epsilon$. Thus the result follows from Lemma 2.4. □

By Corollary 2.5 and (2.12), the modules $L^k(V^r)$ can be expressed, in the Green ring, as polynomials with positive integer coefficients in the modules $U_{k,d}$. In the case where F has prime characteristic p, it follows from (2.3) that the modules $B_{p^m k}$ can be written in $\mathbb{Z}[1/p] \otimes_{\mathbb{Z}} R_{FG}$ as polynomials in the $U_{k,d}$ with coefficients from $\mathbb{Z}[1/p]$. However, it is not obvious that the latter polynomials have integer coefficients or that these coefficients are positive. Our main theorem will establish these facts.

Let T be a cyclic group of order k generated by an element t, and recall that $\langle\epsilon\rangle$ is also a cyclic group of order k. Let $R_{FG}T$ be the group ring of T with coefficients in R_{FG} and let Φ be the element of $R_{FG}T$ defined by

$$\Phi = (V^{\otimes k})_1 t^0 + (V^{\otimes k})_\epsilon t^1 + \cdots + (V^{\otimes k})_{\epsilon^{k-1}} t^{k-1}. \tag{2.18}$$

By (2.8), the coefficient of t^i in Φ is equal to the coefficient of t^j whenever $|t^i| = |t^j|$. For each divisor d of k, let s_d be the sum of all elements of T of order d. Then

$$\Phi = \sum_{d|k} U_{k,d} s_d, \tag{2.19}$$

and Φ is fixed by every automorphism of $R_{FG}T$ that fixes coefficients in R_{FG} and maps t to t^l for some l prime to k. Clearly, for every positive integer r, Φ^r is fixed by these same automorphisms, and hence the coefficient of t^i in Φ^r is equal to the coefficient of t^j whenever $|t^i| = |t^j|$. We write $[\Phi^r]_k$ to denote the coefficient of t (or any element of order k) in Φ^r.

By (2.18), the coefficient of t in Φ^r is

$$\sum_{\xi_1 \cdots \xi_r = \epsilon} (V^{\otimes k})_{\xi_1} \cdots (V^{\otimes k})_{\xi_r}.$$

Hence, by (2.12) and Corollary 2.5,

$$[\Phi^r]_k = L^k(V^r). \tag{2.20}$$

In order to obtain further information about the modules $L^k(V^r)$ we shall study the properties of the coefficients $[\Phi^r]_k$. We do this in the next section by working in a suitable polynomial ring.

3 Witt vectors and polynomials

We start this section by developing some methods for dealing with Witt vectors.

Let p be a prime number and let R be a commutative ring with identity in which p is not a zero-divisor. We write R^∞ for the set of all Witt vectors over R, as in Section 2, and we define $\gamma_p : R^\infty \to R^\infty$ by means of (2.1) and (2.2). For $\mathbf{b} \in R^\infty$, there can be at most one element $\mathbf{a}$ of R^∞ such that $\gamma_p(\mathbf{a}) = \mathbf{b}$. Furthermore, if p is a unit of R, there exists $\mathbf{a}$ such that $\gamma_p(\mathbf{a}) = \mathbf{b}$ and the components of $\mathbf{a}$ can be obtained recursively from (2.2).

In the following lemma we regard R^∞ as a ring under the operations of R taken componentwise.

Lemma 3.1 *Let $\mathbf{a}, \mathbf{a}', \mathbf{b}, \mathbf{b}' \in R^\infty$, where $\gamma_p(\mathbf{a}) = \mathbf{b}$ and $\gamma_p(\mathbf{a}') = \mathbf{b}'$. Let S be the subring of R generated by the components of $\mathbf{a}$ and $\mathbf{a}'$. Let $\mathbf{b}''$ be any element of the subring of R^∞ generated by $\mathbf{b}$ and $\mathbf{b}'$ under the componentwise operations. Then there exists $\mathbf{a}'' \in S^\infty$ such that $\gamma_p(\mathbf{a}'') = \mathbf{b}''$.*

Proof This is an immediate consequence of a theorem of Witt [15], for which we refer to [14, Theorem II.6]. □

Lemma 3.2 *Let k be a positive integer not divisible by p. Then there exists $\mathbf{c} \in \mathbb{Z}^\infty$ such that*

$$\gamma_p(\mathbf{c}) = (1, k^{p-1}, k^{p^2-1}, \ldots). \tag{3.1}$$

Proof Let $\mathbf{c}$ be the element of $(\mathbb{Z}[1/p])^\infty$ satisfying (3.1), where $\mathbf{c} = (c_0, c_1, \ldots)$. We prove by induction that $c_i \in \mathbb{Z}$ for all i. This shows that $\mathbf{c} \in \mathbb{Z}^\infty$.

By (3.1), we have

$$p^i c_i + p^{i-1} c_{i-1}^p + \cdots + p c_1^{p^{i-1}} + c_0^{p^i} = k^{p^i-1}$$

for all $i \geq 0$. Thus $c_0 = 1 \in \mathbb{Z}$ and, for $i \geq 1$, we have

$$p^i c_i = k^{p^i-1} - (p^{i-1} c_{i-1}^p + \cdots + p c_1^{p^{i-1}} + 1).$$

To prove that $c_i \in \mathbb{Z}$ it suffices to show that the right-hand side is congruent to 0 modulo p^i. By Euler's theorem, $a^{\phi(p^j)} \equiv 1 \pmod{p^j}$ for every positive integer j and every integer a not divisible by p. Since $\phi(p^j) = p^j - p^{j-1}$, it follows that $a^{p^j} \equiv a^{p^{j-1}} \pmod{p^j}$ for every integer a. Thus

$$\begin{aligned} k^{p^i-1} - (p^{i-1} c_{i-1}^p + \cdots + p c_1^{p^{i-1}} + 1) \\ \equiv k^{p^i-1} - (p^{i-1} c_{i-1} + \cdots + p c_1^{p^{i-2}} + 1) \pmod{p^i}. \end{aligned}$$

However, by (3.1), $p^{i-1} c_{i-1} + \cdots + p c_1^{p^{i-2}} + 1 = k^{p^{i-1}-1}$. Thus

$$k^{p^i-1} - (p^{i-1} c_{i-1}^p + \cdots + p c_1^{p^{i-1}} + 1) \equiv k^{p^i-1} - k^{p^{i-1}-1} \pmod{p^i}.$$

However,

$$k(k^{p^i-1} - k^{p^{i-1}-1}) = k^{p^i} - k^{p^{i-1}} \equiv 0 \pmod{p^i}.$$

Since k is not divisible by p, the result follows. □

Corollary 3.3 *Let k be a positive integer not divisible by p. Then there exists $\mathbf{d} \in (\mathbb{Z}[1/k])^\infty$ such that $\gamma_p(\mathbf{d}) = (k^{-1}, k^{-1}, k^{-1}, \ldots)$.*

Proof With componentwise multiplication, we have

$$(k^{-1}, k^{-1}, k^{-1}, \ldots) = (k^{-1}, k^{-p}, k^{-p^2}, \ldots)(1, k^{p-1}, k^{p^2-1}, \ldots).$$

However, $\gamma_p(k^{-1}, 0, 0, \ldots) = (k^{-1}, k^{-p}, k^{-p^2}, \ldots)$. Hence the result follows from Lemmas 3.1 and 3.2. □

From now on we consider polynomial rings $\mathbb{Z}[\mathcal{U}]$ and $\mathbb{Q}[\mathcal{U}]$, where $\mathcal{U}$ is a set of indeterminates. We state a consequence of the preceding results in a form suited for application later in this section.

Proposition 3.4 *Let* $\mathbf{b} \in (\mathbb{Z}[\mathcal{U}])^\infty$, *where* $\mathbf{b} = (b_0, b_1, \ldots)$. *Suppose that there exist* $r_1, \ldots, r_n \in \mathbb{Z}$, $g_1, \ldots, g_n \in \mathbb{Z}[\mathcal{U}]$, *and a positive integer* k *not divisible by* p, *such that* $b_i = k^{-1}(r_1 g_1^{p^i} + \cdots + r_n g_n^{p^i})$ *for all* $i \geq 0$. *Then there exists* $\mathbf{a} \in (\mathbb{Z}[\mathcal{U}])^\infty$ *such that* $\gamma_p(\mathbf{a}) = \mathbf{b}$.

Proof Since $\mathbf{b} \in (\mathbb{Z}[\mathcal{U}])^\infty$, there exists $\mathbf{a} \in (\mathbb{Z}[1/p][\mathcal{U}])^\infty$ such that $\gamma_p(\mathbf{a}) = \mathbf{b}$. However, by hypothesis, $\mathbf{b}$ belongs to the subring of $(\mathbb{Z}[1/k][\mathcal{U}])^\infty$ generated, componentwise, by $(k^{-1}, k^{-1}, k^{-1}, \ldots)$ and the elements $(g_j, g_j^p, g_j^{p^2}, \ldots)$ for $j = 1, \ldots, n$. Also, $\gamma_p(g_j, 0, 0, \ldots) = (g_j, g_j^p, g_j^{p^2}, \ldots)$. Thus, by Lemma 3.1 and Corollary 3.3, there exists $\mathbf{e} \in (\mathbb{Z}[1/k][\mathcal{U}])^\infty$ such that $\gamma_p(\mathbf{e}) = \mathbf{b}$. Hence $\mathbf{a} = \mathbf{e}$ and so

$$\mathbf{a} \in (\mathbb{Z}[1/p][\mathcal{U}])^\infty \cap (\mathbb{Z}[1/k][\mathcal{U}])^\infty = (\mathbb{Z}[\mathcal{U}])^\infty. \qquad \square$$

Any element of $\mathbb{Q}[\mathcal{U}]$ may be written as a sum, with rational coefficients, of monomials in the elements of $\mathcal{U}$. For $a, b \in \mathbb{Q}[\mathcal{U}]$, we write $a \preccurlyeq b$ if every coefficient in a is less than or equal to the corresponding coefficient in b, that is, if $b - a$ has only non-negative coefficients.

Proposition 3.5 *Let* $\mathbf{b} = (b_0, b_1, \ldots) \in (\mathbb{Z}[\mathcal{U}])^\infty$. *Suppose that* $b_i \succcurlyeq 0$ *and*

$$b_i^{p^j} \preccurlyeq b_{i+j} \tag{3.2}$$

for all $i, j \geq 0$. *Let* $\mathbf{a}$ *be the element of* $(\mathbb{Z}[1/p][\mathcal{U}])^\infty$ *satisfying* $\gamma_p(\mathbf{a}) = \mathbf{b}$, *where* $\mathbf{a} = (a_0, a_1, \ldots)$. *Then* $a_0 = b_0 \succcurlyeq 0$ *and, for* $m \geq 1$,

$$0 \preccurlyeq p^m a_m \preccurlyeq b_m - b_0^{p^m}. \tag{3.3}$$

Proof For all $i \geq 0$, write $d_i = b_i - b_0^{p^i}$. Thus $d_i \succcurlyeq 0$, by (3.2). Hence, for all $i, j \geq 0$,

$$d_i^{p^j} + b_0^{p^{i+j}} \preccurlyeq (d_i + b_0^{p^i})^{p^j} = b_i^{p^j} \preccurlyeq b_{i+j}.$$

Therefore

$$d_i^{p^j} \preccurlyeq d_{i+j}. \tag{3.4}$$

Since $\gamma_p(\mathbf{a}) = \mathbf{b}$, we have $a_0 = b_0 \succcurlyeq 0$. It remains to prove (3.3) for $m \geq 1$, and this may be written as $0 \preccurlyeq p^m a_m \preccurlyeq d_m$. Since $\gamma_p(\mathbf{a}) = \mathbf{b}$ and $a_0 = b_0$, we have $pa_1 = b_1 - b_0^p = d_1$. Thus (3.3) is true for $m = 1$. We use induction on m. Since $\gamma_p(\mathbf{a}) = \mathbf{b}$ and $a_0 = b_0$,

$$\begin{aligned} p^{m+1} a_{m+1} &= b_{m+1} - p^m a_m^p - p^{m-1} a_{m-1}^{p^2} - \cdots - p a_1^{p^m} - b_0^{p^{m+1}} \\ &= d_{m+1} - p^m a_m^p - p^{m-1} a_{m-1}^{p^2} - \cdots - p a_1^{p^m}. \end{aligned} \tag{3.5}$$

Also, by the inductive hypothesis, $0 \preccurlyeq a_{m-i} \preccurlyeq p^{-(m-i)} d_{m-i}$ for $i = 0, \ldots, m-1$. Thus

$$0 \preccurlyeq p^{m-i} a_{m-i}^{p^{i+1}} \preccurlyeq p^{(m-i)(1-p^{i+1})} d_{m-i}^{p^{i+1}}$$

for $i = 0, \ldots, m-1$. Hence, by (3.5),

$$d_{m+1} \succcurlyeq p^{m+1} a_{m+1} \succcurlyeq d_{m+1} - p^{m(1-p)} d_m^p - p^{(m-1)(1-p^2)} d_{m-1}^{p^2} - \cdots - p^{(1-p^m)} d_1^{p^m}.$$

Therefore, by (3.4),

$$\begin{aligned} d_{m+1} \succcurlyeq p^{m+1} a_{m+1} &\succcurlyeq (1 - p^{m(1-p)} - p^{(m-1)(1-p^2)} - \cdots - p^{(1-p^m)}) d_{m+1} \\ &\succcurlyeq (1 - p^{-m} - p^{-(m-1)} - \cdots - p^{-1}) d_{m+1} \succcurlyeq 0. \end{aligned}$$

This completes the induction. □

From now on in this section, let k be a positive integer and let $\mathcal{U}$ be a set of indeterminates indexed by the divisors of k, namely, $\mathcal{U} = \{u_d : d \mid k\}$.

As in Section 2, let T be a cyclic group of order k generated by an element t. We consider the group ring $\Gamma = \mathbb{Z}[\mathcal{U}]T$. This consists of all elements of the form $g = g_0 t^0 + \cdots + g_{k-1} t^{k-1}$, with $g_i \in \mathbb{Z}[\mathcal{U}]$ for $i = 0, \ldots, k-1$.

For each positive integer l prime to k there is an automorphism of Γ that fixes all coefficients in $\mathbb{Z}[\mathcal{U}]$ and maps t to t^l. Let Γ^* be the subring of Γ consisting of those elements fixed by all such automorphisms. For $g = \sum g_i t^i \in \Gamma$, we have $g \in \Gamma^*$ if and only if $g_i = g_j$ whenever $|t^i| = |t^j|$. For $g \in \Gamma^*$ and each divisor d of k, we write $[g]_d$ to denote g_i where $|t^i| = d$. As in Section 2, let s_d be the sum of all elements of T of order d. Thus, for $g \in \Gamma^*$, we have

$$g = \sum_{d|k} [g]_d s_d, \tag{3.6}$$

where $[g]_d \in \mathbb{Z}[\mathcal{U}]$ for each divisor d of k.

Let ω be a primitive kth root of unity in $\mathbb{C}$. Thus $\langle \omega \rangle$ is a cyclic group of order k consisting of all complex kth roots of unity. For each non-negative integer j there is a homomorphism $\alpha_j : \Gamma \to \mathbb{C}[\mathcal{U}]$ that fixes all coefficients in $\mathbb{Z}[\mathcal{U}]$ and maps t to ω^j. For $g \in \Gamma$ we usually write $g(\omega^j)$ instead of $g\alpha_j$, because we think of α_j as the substitution $t \mapsto \omega^j$. It is easily verified that

$$s_d(\omega^j) = \rho_d(j), \tag{3.7}$$

where $\rho_d(j)$ denotes Ramanujan's sum, namely the sum of the jth powers of all complex primitive dth roots of unity. Note that $\rho_d(j) \in \mathbb{Z}$ (by [9, Theorem 271], for example). Thus α_j restricts to a homomorphism $\alpha_j : \Gamma^* \to \mathbb{Z}[\mathcal{U}]$. Indeed, for $g \in \Gamma^*$, (3.6) and (3.7) give

$$g(\omega^j) = \sum_{d|k} \rho_d(j) [g]_d. \tag{3.8}$$

We now show that (3.8) allows $[g]_k$ to be written in terms of the elements $g(\omega^j)$ by means of the Möbius function μ.

Lemma 3.6 *For all* $g \in \Gamma^*$,

$$k[g]_k = \sum_{e|k} \mu(e) g(\omega^{k/e}).$$

Proof By (3.8), we have

$$\sum_{e|k} \mu(e) g(\omega^{k/e}) = \sum_{e|k} \mu(e) \sum_{d|k} \rho_d(k/e)[g]_d.$$

However, by [9, Theorem 271],

$$\rho_d(k/e) = \sum_{m|(d,k/e)} \mu(d/m)m,$$

where the sum is over all m such that $m \mid d$ and $m \mid k/e$. Therefore

$$\sum_{e|k} \mu(e) g(\omega^{k/e}) = \sum_{e|k} \sum_{d|k} \sum_{m|(d,k/e)} \mu(e)\mu(d/m)m[g]_d.$$

Altering the order of summation gives

$$\sum_{e|k} \mu(e) g(\omega^{k/e}) = \sum_{d|k} \sum_{m|d} \sum_{e|(k/m)} \mu(e)\mu(d/m)m[g]_d.$$

However, $\sum_{e|(k/m)} \mu(e) = 0$ unless $m = k$. Also, if $m = k$ we must have $d = k$. Therefore

$$\sum_{e|k} \mu(e) g(\omega^{k/e}) = k[g]_k.$$

□

Imitating the description of Φ in (2.19), we let $f \in \Gamma$ be defined by

$$f = \sum_{d|k} u_d s_d. \tag{3.9}$$

Thus $f \in \Gamma^*$ and $f^r \in \Gamma^*$ for every positive integer r. Recall the definition of $\preccurlyeq$ given before Proposition 3.5. Then, for all $d \mid k$ and all r, we have

$$[f^r]_d \in \mathbb{Z}[\mathcal{U}] \text{ and } [f^r]_d \succcurlyeq 0. \tag{3.10}$$

Also, by Lemma 3.6,

$$[f^r]_k = \frac{1}{k} \sum_{e|k} \mu(e) (f(\omega^{k/e}))^r,$$

where $f(\omega^{k/e}) \in \mathbb{Z}[\mathcal{U}]$ for all e. Here, division by k is possible within $\mathbb{Z}[\mathcal{U}]$ because $[f^r]_k \in \mathbb{Z}[\mathcal{U}]$. Thus, by (3.8), we obtain

$$[f^r]_k = \frac{1}{k} \sum_{e|k} \mu(e) \left(\textstyle\sum_{d|k} \rho_d(k/e) u_d \right)^r. \tag{3.11}$$

We can now prove the key result of this section.

Theorem 3.7 *Let k be a positive integer and let p be a prime number not dividing k. Let $\mathcal{U} = \{u_d : d \mid k\}$, T a cyclic group of order k, and $f \in \mathbb{Z}[\mathcal{U}]T$, as defined in (3.9). Then there exist elements $h_0, h_1, h_2, \ldots$ of $\mathbb{Z}[\mathcal{U}]$ satisfying*

$$\gamma_p(h_0, h_1, h_2, \ldots) = ([f]_k, [f^p]_k, [f^{p^2}]_k, \ldots) \tag{3.12}$$

and, for all $m \geq 0$,

$$0 \preccurlyeq p^m h_m \preccurlyeq \left(\textstyle\sum_{d|k} \phi(d) u_d\right)^{p^m},$$

where ϕ denotes Euler's function.

Proof The first statement follows from (3.10), (3.11) and Proposition 3.4. For the second statement we wish to apply Proposition 3.5 with $b_i = [f^{p^i}]_k$ for all i. Thus we need to verify the hypotheses of Proposition 3.5. For all $i \geq 0$, we have $[f^{p^i}]_k \in \mathbb{Z}[\mathcal{U}]$ and $[f^{p^i}]_k \succcurlyeq 0$ by (3.10). Also, we may write

$$f^{p^i} = [f^{p^i}]_k t + \sum_{x \in T} a_x x,$$

where $a_x \in \mathbb{Z}[\mathcal{U}]$ and $a_x \succcurlyeq 0$ for all $x \in T$. Therefore, for all $j \geq 0$,

$$f^{p^{i+j}} = (f^{p^i})^{p^j} = ([f^{p^i}]_k)^{p^j} t^{p^j} + \sum_{x \in T} b_x x,$$

where $b_x \in \mathbb{Z}[\mathcal{U}]$ and $b_x \succcurlyeq 0$ for all $x \in T$. However, t^{p^j} has order k. Thus we obtain $([f^{p^i}]_k)^{p^j} \preccurlyeq [f^{p^{i+j}}]_k$, and so the hypotheses of Proposition 3.5 are satisfied. By (3.3) and the fact that $h_0 = [f]_k$, we have $0 \preccurlyeq p^m h_m \preccurlyeq [f^{p^m}]_k$, for all $m \geq 0$.

Recall that $\alpha_0 : \Gamma^* \to \mathbb{Z}[\mathcal{U}]$ is the homomorphism that fixes coefficients in $\mathbb{Z}[\mathcal{U}]$ and maps t to 1. Clearly $f\alpha_0 = \sum_{d|k} \phi(d) u_d$. Thus

$$f^{p^m}\alpha_0 = \left(\textstyle\sum_{d|k} \phi(d) u_d\right)^{p^m}.$$

However, since $f^{p^m} = \sum_{d|k} [f^{p^m}]_d s_d$, we have $f^{p^m}\alpha_0 = \sum_{d|k} \phi(d) [f^{p^m}]_d$. Thus

$$[f^{p^m}]_k \preccurlyeq f^{p^m}\alpha_0 = \left(\textstyle\sum_{d|k} \phi(d) u_d\right)^{p^m}.$$

Hence we obtain the second statement of the theorem. □

We shall now move towards a result that is sharper than Theorem 3.7 in the case where k is not square-free. Let $\tilde{k}$ denote the product of the (distinct) prime divisors of k. We write $c \parallel k$ to denote that $c \mid k$ and that c and k/c are coprime. Thus $c \parallel k$ if and only if $c \mid k$ and c is a product of maximal prime-power factors of k. Each divisor d of k may be written uniquely in the form $d = d^* d'$ where $d^* \parallel k$ and $d' \mid k/\tilde{k}$.

Here d^* is the largest divisor of d such that $d^* \parallel k$ and $d' = d/d^*$. Note that the sets $\{u_d : d^* = c\}$ form a partition of $\mathcal{U}$, as c ranges over the divisors of k such that $c \parallel k$. For each such c, write

$$w_c = \sum_{d:d^*=c} \phi(d/c)u_d = u_c + \sum_{\substack{d:d^*=c \\ d\neq c}} \phi(d/c)u_d, \tag{3.13}$$

and set $\mathcal{W} = \{w_c : c \parallel k\}$. By (3.13), the subring of $\mathbb{Z}[\mathcal{U}]$ generated by $\mathcal{W}$ may be identified with the polynomial ring $\mathbb{Z}[\mathcal{W}]$. Thus we can take $\mathbb{Z}[\mathcal{W}] \subseteq \mathbb{Z}[\mathcal{U}]$ and $\mathbb{Q}[\mathcal{W}] \subseteq \mathbb{Q}[\mathcal{U}]$. Let $\preccurlyeq_{\mathcal{W}}$ be the relation on $\mathbb{Q}[\mathcal{W}]$ defined analogously to $\preccurlyeq$ on $\mathbb{Q}[\mathcal{U}]$, but using coefficients of monomials in elements of $\mathcal{W}$.

Lemma 3.8 (*i*) *Every element x of T may be written uniquely in the form $x = x^*x'$, such that, for $|x| = d$, we have $|x^*| = d^*$ and $|x'| = d'$.*
(*ii*) *Let $d \mid k$, and let y be an element of T of order d^*. Then the number of elements x of T satisfying $|x| = d$ and $x^* = y$ is $\phi(d/d^*)$.*

Proof Part (i) follows from the fact that $d = d^*d'$, where d^* and d' are coprime.

Let d and y be as in (ii) and, for $x \in T$, write $x = x^*x'$, as in (i). It is easy to verify that x satisfies $|x| = d$ and $x^* = y$ if and only if $y^{-1}x$ has order d/d^*. Thus the number of such elements x is $\phi(d/d^*)$. □

Lemma 3.9 *Let $d \mid k$ and $e \mid \tilde{k}$. Then $\rho_d(k/e) = \phi(d/d^*)\rho_{d^*}(k/e)$.*

Proof We apply Lemma 3.8 to $\langle\omega\rangle$ rather than T. For $x \in \langle\omega\rangle$, write $x = x^*x'$, as in Lemma 3.8 (i). Then

$$\rho_d(k/e) = \sum_{x:|x|=d} x^{k/e} = \sum_{x:|x|=d} (x^*)^{k/e}(x')^{k/e}.$$

However, $(x')^{k/e} = 1$, because k/e is divisible by $k/\tilde{k}$. Hence

$$\rho_d(k/e) = \sum_{x:|x|=d} (x^*)^{k/e}.$$

For each element y of $\langle\omega\rangle$ of order d^*, there are, by Lemma 3.8 (ii), exactly $\phi(d/d^*)$ elements x of order d such that $x^* = y$. Thus

$$\rho_d(k/e) = \sum_{x:|x|=d} (x^*)^{k/e} = \phi(d/d^*) \sum_{y:|y|=d^*} y^{k/e} = \phi(d/d^*)\rho_{d^*}(k/e).$$

This is the required result. □

Suppose that $e \mid \tilde{k}$. Then, by Lemma 3.9 and (3.13),

$$\sum_{d|k} \rho_d(k/e)u_d = \sum_{c\parallel k} \sum_{d:d^*=c} \phi(d/c)\rho_c(k/e)u_d$$

$$= \sum_{c \| k} \rho_c(k/e) w_c. \tag{3.14}$$

Note that $e \mid \tilde{k}$ holds if $e \mid k$ and $\mu(e) \neq 0$. Thus, by (3.11) and (3.14),

$$[f^r]_k = \frac{1}{k} \sum_{e \mid k} \mu(e) \left(\sum_{c \| k} \rho_c(k/e) w_c \right)^r, \tag{3.15}$$

for every positive integer r.

Let $\iota : \mathbb{Q}[\mathcal{W}] \to \mathbb{Q}[\mathcal{U}]$ be the inclusion homomorphism given, for $c \parallel k$, by

$$w_c \iota = w_c = u_c + \sum_{\substack{d : d^* = c, \\ d \neq c}} \phi(d/c) u_d,$$

and let $\kappa : \mathbb{Q}[\mathcal{U}] \to \mathbb{Q}[\mathcal{W}]$ be the homomorphism given by $u_d \kappa = w_d$, if $d \parallel k$, and $u_d \kappa = 0$, otherwise. Thus $\iota\kappa$ is the identity on $\mathbb{Q}[\mathcal{W}]$.

By (3.15), $[f^r]_k \in \mathbb{Q}[\mathcal{W}]$. This is enough for the following theorem. However, $[f^r]_k \iota \in \mathbb{Z}[\mathcal{U}]$, by (3.10), and so, by applying κ, we have $[f^r]_k \in \mathbb{Z}[\mathcal{W}]$.

Theorem 3.10 *Further to Theorem 3.7, let $\mathcal{W} = \{w_c : c \parallel k\}$, where w_c is defined by (3.13). Then we have $h_m \in \mathbb{Z}[\mathcal{W}]$, for all m, and*

$$0 \preccurlyeq_{\mathcal{W}} p^m h_m \preccurlyeq_{\mathcal{W}} \left(\sum_{c \| k} \phi(c) w_c \right)^{p^m}.$$

Proof By (3.15), we have $[f]_k, [f^p]_k, [f^{p^2}]_k, \ldots \in \mathbb{Q}[\mathcal{W}]$. It follows, by (3.12), that $h_m \in \mathbb{Q}[\mathcal{W}]$ for all m. Let ι and κ be defined as above, where $\iota\kappa$ is the identity on $\mathbb{Q}[\mathcal{W}]$. By Theorem 3.7, $h_m \iota \in \mathbb{Z}[\mathcal{U}]$ and

$$0 \preccurlyeq p^m (h_m \iota) \preccurlyeq \left(\sum_{d \mid k} \phi(d) u_d \right)^{p^m}.$$

Applying κ, we find that $h_m \in \mathbb{Z}[\mathcal{W}]$ and

$$0 \preccurlyeq_{\mathcal{W}} p^m h_m \preccurlyeq_{\mathcal{W}} \left(\sum_{c \| k} \phi(c) w_c \right)^{p^m}. \qquad \square$$

4 Main results

Let F be a field, G a group, V a finite-dimensional FG-module, and k a positive integer not divisible by $\mathrm{char}(F)$. We use the notation of Sections 2 and 3. In particular, for each divisor d of k, s_d is the sum of the elements of T of order d, $\Phi = \sum_{d \mid k} U_{k,d} s_d$, $f = \sum_{d \mid k} u_d s_d$, and $\mathcal{U} = \{u_d : d \mid k\}$.

Let $\chi : \mathbb{Z}[\mathcal{U}] \to R_{FG}$ be the homomorphism given by the substitution $u_d \mapsto U_{k,d}$ for all d. This extends to a homomorphism $\chi : \mathbb{Z}[\mathcal{U}]T \to R_{FG}T$, fixing the elements of T, and we have $f\chi = \Phi$. Hence, by (2.20), for every positive integer r,

$$[f^r]_k \chi = [\Phi^r]_k = L^k(V^r). \tag{4.1}$$

Applying χ to (3.11) and using (4.1), we obtain the following result in R_{FG}.

Proposition 4.1 *For every positive integer r,*

$$L^k(V^r) = \frac{1}{k}\sum_{e|k}\mu(e)\left(\textstyle\sum_{d|k}\rho_d(k/e)U_{k,d}\right)^r.$$

This can be compared with a result concerning Adams operations in the Green ring that follows from [2, Theorem 6.1]:

$$L^k(V^r) = \frac{1}{k}\sum_{e|k}\mu(e)(\psi^e(V^{k/e}))^r.$$

Indeed, for every divisor e of k, it can be shown that

$$\psi^e(V^{k/e}) = \sum_{d|k}\rho_d(k/e)U_{k,d}. \tag{4.2}$$

We omit the proof of (4.2) since it is not needed for our purposes here.

Suppose now that F has prime characteristic p, and let $h_0, h_1, \ldots$ be the elements of $\mathbb{Z}[\mathcal{U}]$ given by Theorem 3.7. Thus, by (3.12) and (4.1),

$$\gamma_p(h_0\chi, h_1\chi, h_2\chi, \ldots) = (L^k(V), L^k(V^p), L^k(V^{p^2}), \ldots).$$

By comparison with (2.3) we obtain

$$h_m\chi = B_{p^m k}, \text{ for all } m \geq 0. \tag{4.3}$$

Also, by (2.10),

$$\left(\textstyle\sum_{d|k}\phi(d)u_d\right)^{p^m}\chi = V^{p^m k}. \tag{4.4}$$

However, we may write

$$\left(\textstyle\sum_{d|k}\phi(d)u_d\right)^{p^m} = \sum_{\lambda\in\Lambda} u_{\lambda(1)}\cdots u_{\lambda(p^m)},$$

where Λ is a set of cardinality k^{p^m} indexing a family of (not necessarily distinct) p^m-tuples $(\lambda(1), \ldots, \lambda(p^m))$ with $\lambda(1), \ldots, \lambda(p^m) \in \{d : d \mid k\}$. Thus, by (4.4),

$$V^{\otimes p^m k} \cong \bigoplus_{\lambda\in\Lambda} U_{k,\lambda(1)} \otimes \cdots \otimes U_{k,\lambda(p^m)}. \tag{4.5}$$

The inequality for $p^m h_m$ in Theorem 3.7 implies

$$0 \preccurlyeq h_m \preccurlyeq \left(\textstyle\sum_{d|k}\phi(d)u_d\right)^{p^m}.$$

Hence there is a subset Λ_0 of Λ such that

$$h_m = \sum_{\lambda\in\Lambda_0} u_{\lambda(1)}\cdots u_{\lambda(p^m)}. \tag{4.6}$$

Our first main result now follows from (4.3) by applying χ to (4.6).

Theorem 4.2 *Let F be a field of prime characteristic p, G a group, and V a finite-dimensional FG-module. Let k be a positive integer not divisible by p and let m be a non-negative integer. Write*

$$V^{\otimes p^m k} \cong \bigoplus_{\lambda\in\Lambda} U_{k,\lambda(1)}\otimes\cdots\otimes U_{k,\lambda(p^m)},$$

as in (4.5). *Let $B_{p^m k}$ be the module given by Theorem* 2.1. *Then there exists a subset Λ_0 of Λ such that*

$$B_{p^m k} \cong \bigoplus_{\lambda\in\Lambda_0} U_{k,\lambda(1)}\otimes\cdots\otimes U_{k,\lambda(p^m)}.$$

By Theorem 4.2, $B_{p^m k}$ is isomorphic to a direct summand of $V^{\otimes p^m k}$ of a very specific form. Also, we see that $B_{p^m k}$ may be written in the Green ring as a polynomial in the modules $U_{k,d}$. The polynomial has positive integer coefficients and is homogeneous of degree p^m. This polynomial is, of course, the polynomial h_m of Theorem 3.7. Thus it depends only on k, p and m.

We shall now see how Theorem 4.2 can be sharpened when k is not square-free. As in Section 3, let $\tilde{k}$ denote the product of the prime divisors of k and, for $d \mid k$, write $d = d^* d'$ where $d^* \parallel k$ and $d' \mid k/\tilde{k}$.

Recall from Section 2 that ϵ is a primitive kth root of unity in an extension field of F. Let Θ be the set of all elements θ of $\langle\epsilon\rangle$ such that $|\theta|$ and $k/|\theta|$ are coprime. Every element ξ of $\langle\epsilon\rangle$ may be written uniquely in the form $\xi = \xi^*\xi'$, as in Lemma 3.8 (i), where $\xi^* \in \Theta$. For each $\theta \in \Theta$, define

$$W_\theta = \bigoplus_{\xi:\xi^*=\theta} (V^{\otimes k})_\xi. \tag{4.7}$$

Thus, by (2.7), we have

$$V^{\otimes k} \cong \bigoplus_{\theta\in\Theta} W_\theta. \tag{4.8}$$

For each c such that $c \parallel k$, let $W_{k,c}$ denote a module isomorphic to W_θ, where $|\theta| = c$. (It is easy to see that $W_\theta \cong W_{\theta'}$ when $|\theta| = |\theta'|$.) Thus, in the Green ring,

$$V^k = \sum_{c\parallel k} \phi(c) W_{k,c}. \tag{4.9}$$

Suppose that $c \parallel k$ and $|\theta| = c$. If $\xi^* = \theta$ then the order of ξ is some number d satisfying $d^* = c$. Also, by Lemma 3.8 (ii), for each d such that $d^* = c$, the number

of elements ξ of order d satisfying $\xi^* = \theta$ is $\phi(d/c)$. Thus we may write (4.7) in the Green ring as

$$W_{k,c} = \sum_{d:d^*=c} \phi(d/c) U_{k,d}. \tag{4.10}$$

Let $\mathcal{W} = \{w_c : c \parallel k\}$, as in Section 3. Then, by (3.13) and (4.10), $w_c\chi = W_{k,c}$ for all c. Thus, by (4.9),

$$\left(\sum_{c\parallel k} \phi(c) w_c\right)^{p^m} \chi = V^{p^m k}. \tag{4.11}$$

However, we may write

$$\left(\sum_{c\parallel k} \phi(c) w_c\right)^{p^m} = \sum_{\delta\in\Delta} w_{\delta(1)} \cdots w_{\delta(p^m)},$$

where Δ is a finite set indexing a family of p^m-tuples $(\delta(1), \ldots, \delta(p^m))$ with $\delta(1), \ldots, \delta(p^m) \in \{c : c \parallel k\}$. Thus, by (4.11),

$$V^{\otimes p^m k} \cong \bigoplus_{\delta\in\Delta} W_{k,\delta(1)} \otimes \cdots \otimes W_{k,\delta(p^m)}. \tag{4.12}$$

Our second main result now follows from Theorem 3.10 in the same way as Theorem 4.2 follows from Theorem 3.7.

Theorem 4.3 *Further to Theorem 4.2, write*

$$V^{\otimes p^m k} \cong \bigoplus_{\delta\in\Delta} W_{k,\delta(1)} \otimes \cdots \otimes W_{k,\delta(p^m)},$$

as in (4.12). *Then there exists a subset* Δ_0 *of* Δ *such that*

$$B_{p^m k} \cong \bigoplus_{\delta\in\Delta_0} W_{k,\delta(1)} \otimes \cdots \otimes W_{k,\delta(p^m)}.$$

Theorem 4.3 expresses $B_{p^m k}$, up to isomorphism, in terms of modules $W_{k,c}$ indexed by the divisors c of k satisfying $c \parallel k$. Such a divisor c is determined uniquely by the set of prime divisors of k that divide c. Thus, in effect, the modules $W_{k,c}$ are indexed by the subsets of the set of all prime divisors of k.

We conclude with a simple example to illustrate how the modules $B_{p^m k}$ may be calculated up to isomorphism.

Example 4.4 Suppose that k is a prime, and let $\mathrm{char}(F) = p$, where $p \neq k$. We shall find B_{pk} as an element of R_{FG}.

Since k is a prime, the only modules $U_{k,d}$ are $U_{k,1}$ and $U_{k,k}$, and, by (2.10),

$$V^k = U_{k,1} + (k-1)U_{k,k}.$$

Also, by Lemma 2.3, $U_{k,k} = L^k(V)$ in R_{FG}. By Proposition 4.1,

$$L^k(V^p) = \frac{1}{k}((U_{k,1} + (k-1)U_{k,k})^p - (U_{k,1} - U_{k,k})^p)$$
$$= \frac{1}{k}\sum_{i=0}^{p}\binom{p}{i}((k-1)^i - (-1)^i)U_{k,1}^{p-i}U_{k,k}^i.$$

Thus, by (2.3), $B_k = L^k(V) = U_{k,k}$ and

$$B_{pk} = \frac{1}{p}(L^k(V^p) - U_{k,k}^p) = \sum_{i=0}^{p} m_i U_{k,1}^{p-i}U_{k,k}^i,$$

where

$$m_i = \begin{cases} 0 & \text{for } i = 0, \\ \frac{1}{pk}\binom{p}{i}((k-1)^i - (-1)^i) & \text{for } 0 < i < p, \\ \frac{1}{pk}((k-1)^p - (-1)^p) - \frac{1}{p} & \text{for } i = p. \end{cases}$$

In the case where $k = 2$ and $p = 3$, we obtain $B_6 = U_{k,1}^2 U_{k,k}$. In this case it is easily verified that $U_{k,1} = S^2(V)$ and $U_{k,k} = \wedge^2(V)$. Thus we obtain (1.1).

References

1. Benson, D.J.: Lambda and psi operations on Green rings. J. Algebra **87**, 360–367 (1984)
2. Bryant, R.M.: Free Lie algebras and Adams operations. J. Lond. Math. Soc. (2) **68**, 355–370 (2003)
3. Bryant, R.M., Schocker, M.: The decomposition of Lie powers. Proc. Lond. Math. Soc. (3) **93**, 175–196 (2006)
4. Bryant, R.M., Schocker, M.: Factorisation of Lie resolvents. J. Pure Appl. Algebra **208**, 993–1002 (2007)
5. Curtis, C.W., Reiner, I.: Representation Theory of Finite Groups and Associative Algebras. Wiley-Interscience, New York (1962)
6. Donkin, S., Erdmann, K.: Tilting modules, symmetric functions, and the module structure of the free Lie algebra. J. Algebra **203**, 69–90 (1998)
7. Friedlander, E.M., Suslin, A.: Cohomology of finite group schemes over a field. Invent. Math. **127**, 209–270 (1997)
8. Green, J.A.: Polynomial Representations of GL_n. Lecture Notes in Mathematics, vol. 830. Springer, Berlin (1980)
9. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers. Clarendon, Oxford (1938)
10. Klyachko, A.A.: Lie elements in the tensor algebra. Sib. Mat. Zh. **15**, 1296–1304 (1974) (Russian), Sib. Math. J. **15**, 914–921 (1975) (English)
11. Kraśkiewicz, W., Weyman, J.: Algebra of coinvariants and the action of a Coxeter element. Bayreuth. Math. Schr. **63**, 265–284 (2001)
12. Reutenauer, C.: Free Lie Algebras. Clarendon, Oxford (1993)
13. Schocker, M.: Über die höheren Lie-Darstellungen der symmetrischen Gruppen. Bayreuth. Math. Schr. **63**, 103–263 (2001)
14. Serre, J.-P.: Local Fields. Springer, New York (1979)
15. Witt, E.: Zyklische Körper und Algebren der Charakteristik p vom Grade p^n. J. Reine Angew. Math. **176**, 126–140 (1936)