UNIQUE FACTORIZATION IN INVARIANT POWER SERIES RINGS

DAVID BENSON AND PETER WEBB

Abstract. Let G be a finite group, k a perfect field, and V a finite dimensional kG-module. We let G act on the power series $k[[V]]$ by linear substitutions and address the question of when the invariant power series $k[[V]]^G$ form a unique factorization domain. We prove that for a permutation module for a p-group in characteristic p, the answer is always positive. On the other hand, if G is a cyclic group of order p, k has characteristic p, and V is an indecomposable kG-module of dimension r with $1 \leq r \leq p$, we show that the invariant power series form a unique factorization domain if and only if r is equal to 1, 2, $p-1$ or p. This contradicts a conjecture of Peskin.

1. Introduction

Let G be a finite group, and let k be a perfect field, which unless otherwise stated in this paper will have positive characteristic p. Let V be a finite dimensional kG-module. Then G also acts on the ring of polynomials $k[V]$ and the ring of formal power series $k[[V]]$. The question of when the invariants $k[V]^G$ form a unique factorization domain was settled by Nakajima [10, Theorem 2.11], who proved that this holds if and only if there are no nontrivial homomorphisms $G \to k^\times$ taking the value one on every pseudoreflection (a *pseudoreflection* is an element of G whose fixed points have codimension one in V). We are interested in the corresponding question for $k[[V]]^G$, which is the completion of $k[V]^G$ with respect to the ideal generated by the elements of positive degree. In this paper, we make two related contributions to this subject, one positive and one negative.

The following generalizes a theorem of Fossum and Griffith [6, Theorem 2.1], which deals with the case of the regular representation of a cyclic group of order p^n. The proof is given at the end of Section 2.

Theorem 1.1. *Let G be a finite p-group, let k be a perfect field of characteristic p and let V be a permutation module for kG. Then $k[[V]]^G$ is a unique factorization domain.*

2000 *Mathematics Subject Classification.* Primary 13A50; Secondary 20C20.

Key words and phrases. invariant theory, symmetric powers, unique factorization, modular representation.

The research of the first author was partly supported by NSF grant DMS-0242909.

The following generalization of Theorem 1.1 to arbitrary finite groups is analogous to the theorem of Nakajima [10] for $k[V]^G$, with the exception that it is restricted to direct summands of permutation modules. One way to state our result is to combine it with Nakajima's theorem and say that for such modules $k[[V]]^G$ and $k[V]^G$ have isomorphic divisor class groups, and so one of them is a unique factorization domain if and only if the other is. Our theorem is valid over fields of arbitrary characteristic, and we note that when the characteristic of k is zero or does not divide $|G|$, every module is a direct summand of a permutation module, because by Maschke's theorem it is a direct summand of a free module. When the characteristic of k divides $|G|$, direct summands of permutation modules are also known as p-permutation modules, or trivial source modules (at least, if they are indecomposable), and the condition is equivalent to the requirement that the restriction of the module to a Sylow p-subgroup is a permutation module.

Theorem 1.2. *Let G be a finite group and V be a direct summand of a permutation kG-module, where k is a perfect field of arbitrary characteristic. Then the divisor class group* $\mathrm{Cl}(k[[V]]^G)$ *is isomorphic to the subgroup of* $\mathrm{Hom}(G, k^\times)$ *consisting of those homomorphisms which take value one on every pseudoreflection. In particular, $k[[V]]^G$ is a unique factorization domain if and only if there are no nontrivial homomorphisms $G \to k^\times$ taking the value one on every pseudoreflection.*

The proof of Theorem 1.2 is given at the end of Section 2. The particular case of the theorem for the natural representation of the alternating groups is dealt with in Samuel [13, Appendix] for $p \geq 5$ and Singh [14, Theorems 1 and 2] for $p = 2$ or 3. The case where the characteristic of k is either zero or coprime to the order of G is due to Griffith [7, Theorem 2.5].

The situation for modules which are not direct summands of permutation modules is quite different. In [11, Conjecture 3.10], Peskin conjectures that for an indecomposable representation of a cyclic group of order p in characteristic p, the invariants are always a unique factorization domain. The following theorem gives a negative answer to this conjecture. The proof is given in Section 4.

Theorem 1.3. *Let $G = \mathbb{Z}/p$ and let k be a perfect field of characteristic p. If V_r is an r dimensional indecomposable kG-module (so that V_r is a single Jordan block of length r with $1 \leq r \leq p$) then $k[[V_r]]^G$ is a unique factorization domain if and only if r is equal to* 1, 2, $p-1$ *or* p.

We remark that by contrast, if k is a field of characteristic p and G is a finite p-group, $k[V]^G$ is always a unique factorization domain by the theorem of Nakajima. Examples of unique factorization domains whose completions are not unique factorization domains were known previously (see Fossum [5, Example

19.9], and Halanay [8]), but our examples seem particularly natural. In fact, Heitmann [9, Theorem 8] has shown that every complete local domain of depth at least two is the completion of a subring which is a unique factorization domain; this gives a wealth of complicated examples.

In order to prove these theorems, we develop a general method for reducing questions about unique factorization in power series invariants to questions in modular representation theory. The following theorem summarizes our method.

Theorem 1.4. *Let G be a finite p-group, let k be a perfect field of characteristic p, and let V be a finite dimensional kG-module. Let V^* be the dual representation, so that the mth symmetric power S^mV^* is the vector space of homogeneous polynomial functions on V of degree m. We regard S^mV^* as a submodule of $S^{mp}V^*$ via the pth power map on polynomials.*

Suppose that for all $m \geq 1$ the map

$$(S^{mp}V^*)^G \to (S^{mp}V^*/S^mV^*)^G \tag{1.5}$$

is surjective. Then $k[[V]]^G$ is a unique factorization domain.

Conversely, suppose that for some m not divisible by p, the map (1.5) *is not surjective. Suppose furthermore, that the cokernels of the pth power maps $S^{np}V^* \to S^{np^2}V^*$ are projective kG-modules for all $n \geq 1$. Then $k[[V]]^G$ is not a unique factorization domain.*

We will establish the first statement of this theorem in Section 2 by means of Propositions 2.5 and 2.6, and in Section 3 we establish the second statement using the Artin–Hasse exponential. We will use the theorem in Section 4 when we consider the group $\mathbb{Z}/p$ and prove Theorem 1.3. In this situation the cokernels of $S^{np}V^* \to S^{np^2}V^*$ are always projective (Lemma 4.2) and the rest of the proof of Theorem 1.3 is a question of determining when the map (1.5) is not surjective when p does not divide m.

2. Cohomology and unique factorization

The connection between degree one cohomology and unique factorization was developed by Krull and Samuel, and is described, for example, in Samuel [13] and in Chapter 3 of [4]. We summarize the theory here.

If A is a normal domain (i.e., a Noetherian integrally closed domain), we write $D(A)$ for the divisor group of A. This is a free abelian group with basis elements $d(\mathfrak{p})$ corresponding to the height one primes $\mathfrak{p}$ of A. A principal ideal in A determines an element of $D(A)$, and the subgroup generated by these elements is denoted $F(A)$. The divisor class group $\mathrm{Cl}(A)$ is the quotient $D(A)/F(A)$.

Theorem 2.1. *A normal domain A is a unique factorization domain if and only if* $\mathrm{Cl}(A) = 0$.

Proof. This is proved in Section 3.5 of [4]. □

Let $A \subseteq B$ be a finite extension of normal domains, with fields of fractions $L \subseteq L'$, a Galois extension with Galois group G. If $\mathfrak{P}$ is a height one prime ideal of B then $\mathfrak{p} = \mathfrak{P} \cap A$ is a height one prime ideal of A. The valuation $v_{\mathfrak{P}}$ on L' restricts to a positive integer multiple of $v_{\mathfrak{p}}$ on L,

$$v_{\mathfrak{P}} = e(\mathfrak{P}, \mathfrak{p}) v_{\mathfrak{p}}$$

where $e(\mathfrak{P}, \mathfrak{p})$ is the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$, characterized by the equation $\mathfrak{p}B_{\mathfrak{P}} = \mathfrak{P}^e B_{\mathfrak{P}}$. The map $j\colon D(A) \to D(B)$ defined by $j(d(\mathfrak{p})) = \sum e(\mathfrak{P}, \mathfrak{p}) d(\mathfrak{P})$, where the sum is indexed by the primes $\mathfrak{P}$ lying over $\mathfrak{p}$, passes down to a well defined map $\bar{\jmath}\colon \mathrm{Cl}(A) \to \mathrm{Cl}(B)^G$.

Theorem 2.2. *Suppose that L'/L is a finite Galois extension with Galois group G. Regarding the group of units $U(B)$ as a $\mathbb{Z}G$-module, there is an exact sequence*

$$0 \to \operatorname{Ker} \bar{\jmath} \to H^1(G, U(B)) \to \bigoplus_{\mathfrak{p}} \mathbb{Z}/e(\mathfrak{p}) \to \operatorname{Coker} \bar{\jmath} \to 0,$$

where $\mathfrak{p}$ runs over the height one primes in A which ramify in B. Here, the ramification index $e(\mathfrak{P}, \mathfrak{p})$ is independent of $\mathfrak{P}$, and is written $e(\mathfrak{p})$.

Proof. See Theorem 3.8.1 of [4]. □

In the case where $A = k[V]^G$ and $B = k[V]$, we have $\mathrm{Cl}(B) = 0$ and $U(B) = k^\times$. So the sequence reduces to a short exact sequence

$$0 \to \mathrm{Cl}(k[V]^G) \to H^1(G, k^\times) \to \bigoplus_{\mathfrak{p}} \mathbb{Z}/e(\mathfrak{p}) \to 0.$$

Furthermore, the action of G on $k^\times$ is trivial, so $H^1(G, k^\times)$ is just $\mathrm{Hom}(G, k^\times)$.

The height one primes which ramify correspond to reflecting hyperplanes for the pseudoreflections in G. If the prime $\mathfrak{p}$ in $k[V]^G$ corresponds to a reflecting hyperplane $W \subset V$, then the ramification index $e(\mathfrak{p})$ is equal to the order of the stabilizer of the corresponding hyperplane $|G_W|$ if k has characteristic zero, and equal to the p'-part $|G_W|_{p'}$ if k has characteristic p; see Lemma 3.9.1 of [4]. For the sake of notation, we shall write $|G_W|_{p'}$ in both cases, with the understanding that this means $|G_W|$ in the case of characteristic zero.

The homomorphism

$$\mathrm{Hom}(G, k^\times) \to \bigoplus_{W} \mathbb{Z}/|G_W|_{p'}$$

may be described as follows. Given a group homomorphism $\phi\colon G \to k^\times$ and a reflecting hyperplane W, then $O_p(G_W)$ is in the kernel of ϕ (where $O_p(G_W)$ denotes the largest normal p-subgroup of G_W if k has characteristic p, and the trivial subgroup if k has characteristic zero), and so there is an induced homomorphism from $G_W/O_p(G_W)$ to $k^\times$. The group $\mathbb{Z}/|G_W|_{p'}$ in the sum above may be regarded as $\mathrm{Hom}(G_W/O_p(G_W), k^\times)$. The map ϕ is then sent to the sum of the restrictions of ϕ to the hyperplane stabilizers. So we may rewrite the exact sequence as

$$0 \to \mathrm{Cl}(k[V]^G) \to \mathrm{Hom}(G, k^\times) \to \bigoplus_W \mathrm{Hom}(G_W/O_p(G_W), k^\times) \to 0.$$

All this is described in Section 3.9 of [4], where it is adapted from Nakajima [10]. One can easily deduce from this exact sequence the theorem of Nakajima described in the introduction.

Similarly, in the case where $A = k[[V]]^G$ and $B = k[[V]]$, we still have $\mathrm{Cl}(B) = 0$, but this time the units $U = U(k[[V]])$ are large. They decompose as $U = k^\times \times U_1$, where U_1 is the multiplicative group consisting of the power series with constant term equal to one. Again, the ramified primes correspond to reflecting hyperplanes, the ramification indices are the same as before, and the components of the map $\mathrm{Hom}(G, k^\times) \to \bigoplus_{\mathfrak{p}} \mathbb{Z}/e(\mathfrak{p})$ have the same description as before. So we obtain a short exact sequence

$$\begin{aligned} 0 \to \mathrm{Cl}(k[[V]]^G) \to \mathrm{Hom}(G, k^\times) &\oplus H^1(G, U_1) \\ &\to \bigoplus_W \mathrm{Hom}(G_W/O_p(G_W), k^\times) \to 0. \end{aligned} \tag{2.3}$$

The term $H^1(G, U_1)$ is less easy to describe, and that will be the main task of this paper in some special cases. We begin by remarking that if k has characteristic zero then U_1 is a divisible group, and so $H^1(G, U_1) = 0$. So we can assume that k has prime characteristic p.

Define U_n to be the subgroup of U_1 consisting of power series involving no monomials with degree positive and less than n. Then

$$U_1 = \varprojlim_n U_1/U_n,$$

and so U_1 is an abelian pro-p-group, and hence a $\mathbb{Z}_p$-module, where $\mathbb{Z}_p$ denotes the p-adic integers. Since the pth power of a power series f is the power series whose terms are the pth powers of the terms of f, we readily see that U_1 has no p-torsion, and no p-divisible elements, but it seems likely that it is not usually $\mathbb{Z}_p$-free; we make use of the lack of p-torsion via the following lemma.

Lemma 2.4. *Let G be a finite group, and let M be a p-torsion-free $\mathbb{Z}_pG$-module. Then $H^1(G, M) = 0$ if and only if $M^G \to (M/pM)^G$ is surjective.*

Proof. Since M is p-torsion-free, we have an exact sequence

$$0 \to M \xrightarrow{p} M \to M/pM \to 0.$$

Applying cohomology, we obtain an exact sequence

$$0 \to M^G \xrightarrow{p} M^G \to (M/pM)^G \to H^1(G,M) \xrightarrow{p} H^1(G,M).$$

Since $|G|_p$ annihilates $H^1(G,M)$, we have that $H^1(G,M) \neq 0$ if and only if multiplication by p has a nonzero kernel on it, which happens if and only if $M^G \to (M/pM)^G$ is not surjective. $\square$

Proposition 2.5. *Suppose that G is a finite p-group. Then the following are equivalent.*

(i) $k[[V]]^G$ *is a unique factorization domain.*

(ii) $H^1(G,U_1) = 0$.

(iii) *The map*

$$U_1^G \to (U_1/U_1^p)^G$$

is surjective; in other words, power series with constant term one which are invariant mod pth powers lift to invariant power series.

Proof. If G is a p-group then $O_p(G_W) = G_W$ always, and $\mathrm{Hom}(G,k^\times) = 0$, so using the short exact sequence (2.3), we have an isomorphism

$$\mathrm{Cl}(k[[V]]^G) \cong H^1(G,U_1)$$

and (i) and (ii) are equivalent. The equivalence of (ii) and (iii) follows from Lemma 2.4, noticing that we are writing the group U_1 multiplicatively. $\square$

Proposition 2.6. *Suppose that for all $m \geq 1$ the map*

$$(S^{mp}V^*)^G \to (S^{mp}V^*/S^mV^*)^G$$

is surjective. Then

$$U_1^G \to (U_1/U_1^p)^G$$

is surjective.

Here and elsewhere we use the fact that in characteristic p the map $S^mV^* \to S^{mp}V^*$ which sends each polynomial to its pth power is an injective kG-module homomorphism, and we identify S^mV^* with its image. Observe also that U_1^p consists of power series with constant term 1 in the pth powers of elements of V^*, and these power series are only non-zero in degrees divisible by p.

Proof. Let $u \in U_1$ be such that $uU_1^p \in (U_1/U_1^p)^G$. We construct inductively elements $u(n) \in U_1$ so that $u(n)U_1^p = uU_1^p$, in all degrees $d \leq n$ we have $g(u(n))_d = u(n)_d$ for all $g \in G$ and in all degrees $d \leq n-1$ we have $u(n)_d = u(n-1)_d$. We start with $u(0) = u$.

Note that since elements of U_1^p are only non-zero in degrees divisible by p, the inductive condition for $n-1$ implies that for every degree d strictly less than the least multiple of p above $n-1$ we have $g(u(n))_d = u(n)_d = u_d$, so that if $u(n-1)$

has already been defined we may define $u(n) = u(n-1)$ unless n is divisible by p. We thus assume $n = mp$ for some m and deal with this case.

For each $g \in G$ we have $gu(n-1) = u(n-1)\cdot(1+v^p+w^p)$ for some $v \in S^m$ and where all terms of w lie in degrees higher than m. Thus $gu(n-1)_n = u(n-1)_n + v^p$. By hypothesis we can find $v' \in S^m$ so that $u(n-1)_n + v'^p \in (S^n)^G$. Now taking $u(n) = u(n-1)(1+v')^p$ produces an element $u(n)$ with the desired properties.

Finally, the sequence of power series $u(n)$ defines a power series which is fixed by G and whose image in U_1/U_1^p is u. □

Theorem 1.1 follows immediately from Propositions 2.5 and 2.6, because in this case the basis of monomials shows that the image of S^mV^* under the pth power map is a direct summand of $S^{mp}V^*$, so that invariants in the quotient lift. By Proposition 2.6, $U_1^G \to (U_1/U_1^p)^G$ is surjective. So $H^1(G, U_1) = 0$ and $k[[V]]^G$ is a unique factorization domain by Proposition 2.5.

To prove Theorem 1.2, we argue as follows. If k has characteristic zero then U_1 is a divisible group and so $H^1(G, U_1) = 0$. If k has prime characteristic p, we observe that if S is a Sylow p-subgroup of G then the restriction map $H^1(G, U_1) \to H^1(S, U_1)$ is injective. Since $H^1(S, U_1) = 0$, we have $H^1(G, U_1) = 0$. In both cases, the exact sequence (2.3) reduces to

$$0 \to \mathrm{Cl}(k[[V]]^G) \to \mathrm{Hom}(G, k^\times) \to \bigoplus_W \mathrm{Hom}(G_W/O_pG_W, k^\times) \to 0.$$

In particular, $\mathrm{Cl}(k[[V]]^G) = 0$ if and only if every nontrivial homomorphism $G \to k^\times$ has nontrivial restriction to some G_W.

3. The Artin–Hasse exponential

Throughout this section, we assume that k is a perfect field of characteristic p. The Artin–Hasse exponential [3] is the power series defined by

$$E(X) = \exp\Big(\sum_{r=0}^{\infty} \frac{X^{p^r}}{p^r}\Big) = 1 + X + \cdots. \tag{3.1}$$

We shall develop the properties we need here, but for general background material on the Artin–Hasse exponential, see Chapter 7 of Robert [12].

Initially, (3.1) is to be thought of as a power series with rational coefficients. We write $\mathbb{Z}_{(p)}$ for the ring of rational numbers with denominators prime to p.

Lemma 3.2. *The coefficients of the power series $E(X)$ are in $\mathbb{Z}_{(p)}$.*

Proof. Let $\mu(n)$ be the Möbius function. Then we have

$$\begin{aligned}\sum_{(i,p)=1} -\frac{\mu(i)}{i}\log(1-X^i) &= \sum_{(i,p)=1}\Big(-\frac{\mu(i)}{i}\sum_{m\geq 1}\frac{-X^{im}}{m}\Big)\\ &= \sum_{n\geq 1}\Big(\sum_{\substack{(i,p)=1\\ i\mid n}}\mu(i)\Big)\frac{X^n}{n} \qquad\qquad \text{(where } n=im)\\ &= \sum_{r\geq 0}\frac{X^{p^r}}{p^r}.\end{aligned}$$

The last equality holds since the inner sum is a sum over the divisors of the p'-part of n, and is zero unless n is a power of p.

Set $\lambda(X) = \sum_{r=0}^{\infty}\frac{X^{p^r}}{p^r}$. Then the calculation above shows that

$$E(X) = \exp(\lambda(X)) = \exp\Big(\sum_{(i,p)=1} -\frac{\mu(i)}{i}\log(1-X^i)\Big) = \prod_{(i,p)=1}(1-X^i)^{-\frac{\mu(i)}{i}}.$$

We interpret $-\mu(i)/i$ as a p-adic integer, so that $(1-X^i)^{-\mu(i)/i}$ can be expanded as a power series with p-adic integer coefficients. Specifically, if we write $-\mu(i)/i = \sum_{j\geq 0} a_j p^j$ as a power series, where $0 \leq a_j \leq p-1$ for all j, then

$$(1-X^i)^{-\frac{\mu(i)}{i}} = \prod_{j\geq 0}(1-X^i)^{a_j p^j}$$

is a product of polynomials which allows us to compute the coefficients in the expansion of the left side as p-adic integers. The fact that $\mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}_{(p)}$ shows that the coefficients are in $\mathbb{Z}_{(p)}$. □

It follows from the lemma that the Artin–Hasse exponential function $E(X)$ can be reduced modulo p to give a power series with coefficients in $\mathbb{F}_p$, which we continue to denote $E(X)$. The main property of $E(X)$ which we shall be using is given in the following lemma.

Lemma 3.3. *We have*

$$E(X+Y) = E(X)E(Y)\phi(X,Y)$$

where every term in the power series $\phi(X,Y)$ has total degree in X and Y divisible by p.

Proof. Working in characteristic zero, we have

$$\frac{E(X+Y)}{E(X)E(Y)} = \exp\Big(\sum_{r=1}^{\infty}\frac{(X+Y)^{p^r}}{p^r} - \frac{X^{p^r}}{p^r} - \frac{Y^{p^r}}{p^r}\Big),$$

because the terms with $r = 0$ cancel. The coefficients on the left, and therefore on the right, are in $\mathbb{Z}_{(p)}$. So this formula can be reduced modulo p to prove that the same property holds for $E(X)$ over $\mathbb{F}_p$. □

Theorem 3.4. *Let V be a kG-module where k is a perfect field of characteristic p. Suppose that m is coprime to p, and that*

$$(S^{mp}V^*)^G \to (S^{mp}V^*/S^mV^*)^G$$

is not surjective. Suppose, furthermore, that the cokernels of the pth power maps $S^{np}V^* \to S^{np^2}V^*$ are projective kG-modules for all $n \geq 1$. Then the map

$$U_1^G \to (U_1/U_1^p)^G$$

is not surjective.

Proof. Let U' be the subgroup of U_1 consisting of power series whose terms have degree divisible by p, and let U'' be the subgroup of U_1 consisting of power series whose terms have degree divisible by p^2. We recall also that U_1^p consists of power series in the pth powers of elements of V^*. Consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & S^mV^* \arrow[r] \arrow[d, tail] & S^{mp}V^* \arrow[r] \arrow[d, tail, "E"] & S^{mp}V^*/S^mV^* \arrow[r] \arrow[d, tail, "E"] & 0 \\
0 \arrow[r] & U''U_1^p/U'' \arrow[r] & U'/U'' \arrow[r] & U'/U''U_1^p \arrow[r] & 0 \\
0 \arrow[r] & U_1^p \arrow[r] \arrow[u, two heads] & U' \arrow[r] \arrow[u, two heads] & U'/U_1^p \arrow[r] \arrow[u, two heads] & 0
\end{tikzcd}$$

in which each row is a short exact sequence. The lower vertical arrows are obtained from the factor homomorphism $U' \to U'/U''$. The middle upper vertical arrow is obtained from the Artin-Hasse exponential $E : S^{mp}V^* \to U'$ by composing with the factor map $U' \to U'/U''$. Since the image of S^m under the pth power map followed by E is contained in U_1^p, we obtain the top right vertical map, and hence also the top left vertical map, and we call the two top right maps E by abuse of notation.

Observe that all maps in this diagram are homomorphisms of kG-modules, since it is immediate from the definition of E that $E(gf) = gE(f)$ for each $g \in G$.

Starting from an element of $(S^{mp}V^*/S^mV^*)^G$ which does not lift to $(S^{mp}V^*)^G$ we will produce an element of $(U'/U_1^p)^G$ which does not lift to $(U')^G$, and to establish this we first present some lemmas.

Lemma 3.5. *With the hypotheses of Theorem 3.4, the map*

$$(U'/U_1^p)^G \to (U'/U''U_1^p)^G$$

is surjective.

Proof. We claim that for each $n \geq 1$ there is an exact sequence of kG-modules

$$0 \to S^{np^2}V^*/S^{np}V^* \to U'/(U'' \cap U_{(n+1)p^2})U_1^p \to U'/(U'' \cap U_{np^2})U_1^p \to 0.$$

(recall that U_n is defined just before Lemma 2.4) where in the left term we use additive notation and in the middle and right terms we use multiplicative notation. We obtain such a sequence because the kernel of the right hand map may be identified as

$$(U'' \cap U_{np^2})U_1^p/(U'' \cap U_{(n+1)p^2})U_1^p \cong (U'' \cap U_{np^2})/(U'' \cap U_{(n+1)p^2})(U'' \cap U_{np^2} \cap U_1^p)$$

(using the diamond isomorphism theorem and the modular law) and elements of this quotient are represented by polynomials $1 + f$ where $f \in S^{np^2}V^*$ is taken up to pth powers. By hypothesis $S^{np^2}V^*/S^{np}V^*$ is a projective (or equivalently, injective) kG-module, and so this sequence splits. Thus for each n, the invariants in $U'/(U'' \cap U_{np^2})U_1^p$ lift to invariants in $U'/(U'' \cap U_{(n+1)p^2})U_1^p$. Observe that when $n = 1$ we have $U'/(U'' \cap U_{p^2})U_1^p = U'/U''U_1^p$, and also that

$$U'/U_1^p = \varprojlim_n U'/(U'' \cap U_{np^2})U_1^p.$$

Starting with any element of $(U'/U''U_1^p)^G$ we may lift it to a compatible family of elements in the $(U'/(U'' \cap U_{np^2})U_1^p)^G$, which define an element in the inverse limit which is again G-invariant. $\square$

Lemma 3.6. *If m is not divisible by p then the homomorphism*

$$E \colon S^{mp}V^*/S^mV^* \to U'/U''U_1^p$$

is injective.

Proof. The degree mp terms of elements of $U''U_1^p$ are pth powers. This means that if $f \in S^{mp}V^*$ is such that $E(f) = 0 \in U'/U''U_1^p$ then since $E(f) = 1 + f +$ (higher degree) it follows that f is a pth power. $\square$

We now continue with the proof of Theorem 3.4. Let f be an element of $(S^{mp}V^*/S^mV^*)^G$ which does not lift to $(S^{mp}V^*)^G$. Its image $E(f) \in (U'/U''U_1^p)^G$ is the image of an element $x \in U'/U_1^p$, by Lemma 3.5. If there were a G-invariant lift of x to U_1, say y, it would have to lie in U', and now the image yU'' of y in U'/U'' would be a G-invariant lift of $E(f)$. Now the degree mp term of yU'' in $S^{mp}V^*$ would be a G-invariant element which lifts f, by Lemma 3.6, since its image in $U'/U''U_1^p$ has the same degree mp part as $E(f)$. This is not possible. $\square$

Combining Propositions 2.5, 2.6 and Theorem 3.4 completes the proof of Theorem 1.4.

4. Cyclic groups of order p

In this section, we apply Theorem 3.4 in the case where G is cyclic of order p, k has characteristic p, and V is an indecomposable kG-module. The relevant information about the symmetric powers of V comes from papers of Almkvist [1], Almkvist and Fossum [2].

We begin by fixing notation. Let $G = \langle t \mid t^p = 1\rangle$ be a cyclic group of order p and let k be a field of characteristic p. We write V_r for the r dimensional indecomposable kG-module with $1 \le r \le p$, and we note that $V_r^* \cong V_r$. Let $x_1, \dots, x_r$ be a basis of V_r^*, so that $k[V_r] = k[x_1, \dots, x_r]$ in such a way that $t(x_i) = x_i + x_{i+1}$ for $1 \le i \le r-1$ and $t(x_r) = x_r$. Set

$$N(x_1) = x_1 \cdot t(x_1) \cdot t^2(x_1) \cdots t^{p-1}(x_1),$$

so that $N(x_1) \in (S^p V_r^*)^G$.

Lemma 4.1. *For each integer $n \ge 1$, the vector space $S^{np}V_r^*$ decomposes as a direct sum of a one dimensional kG-module spanned by $N(x_1)^n$ and a projective kG-module spanned by $x_2 \cdot S^{np-1}V_r^*, \dots, x_r \cdot S^{np-1}V_r^*$.*

Proof. It is clear that $S^{np}V_r^*$ decomposes as a direct sum of the given submodules because the second submodule is the span of all the monomials of degree np except x_1^{np}, and the coefficient of x_1^{np} in $N(x_1)^n$ is non-zero. What is not clear is that the second module is projective. But it is proved in Section III of [2] that $S^{np}V_r^*$ decomposes as a direct sum of a trivial module of dimension one and a projective module. Since $N(x_1)^n$ spans a trivial direct summand, by the Krull-Schmidt theorem the remaining direct summand is projective. □

Lemma 4.2. *For all $n \ge 1$, the cokernel of the pth power map $S^{np}V_r^* \to S^{np^2}V_r^*$ is a projective kG-module.*

Proof. The pth power map takes $N(x_1)^n$ to $N(x_1)^{np}$. It also takes the submodule of $S^{np}V_r^*$ spanned by $x_2 \cdot S^{np-1}V_r^*, \dots, x_r \cdot S^{np-1}V_r^*$ into the submodule of $S^{np^2}V_r^*$ spanned by $x_2 \cdot S^{np^2-1}V_r^*, \dots, x_r \cdot S^{np^2-1}V_r^*$ and so the quotient of the last two modules is isomorphic to the cokernel of the pth power map. Since projective kG-modules are injective, the cokernel of an injective map of projective kG-modules is projective. □

Lemma 4.3. *Let $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 \to 0$ be a short exact sequence of kG-modules, with $G = \mathbb{Z}/p$. If $M_2 \cong k \oplus P$ with P projective and $\beta\colon M_2^G \to M_3^G$ is surjective then M_1 has at most one nonprojective summand.*

Proof. Let $N_G = 1 + t + \cdots + t^{p-1}$. Then the hypothesis on M_2 implies that $M_2^G/N_G M_2$ is one dimensional, being the image of the trivial summand of M_2. Since $\beta\colon M_2^G \to M_3^G$ is surjective, so is the induced map

$$\bar\beta\colon M_2^G/N_G M_2 \to M_3^G/N_G M_3.$$

So M_3^G/N_GM_3 is at most one dimensional, which implies that M_3 has at most one nonprojective summand. The remaining projective summands of M_3 lift to summands of M_2. If M_3 is projective then the sequence splits and we are done. So we may assume that $\bar{\beta}$ is an isomorphism, which implies that the trivial summand of M_2 is not in the kernel of β. By removing the projective summands from M_3, without loss of generality M_3 is a nonprojective indecomposable module. We obtain a short exact sequence

$$0 \to M_1 \to P \to M_3/\beta(k) \to 0.$$

It follows that

$$M_1 \cong \Omega(M_3/\beta(k)) \oplus (\text{projective}).$$

Since $M_3/\beta(k)$ is indecomposable, this proves the lemma. $\square$

Example 4.4. Let $G = \mathbb{Z}/7$ and $V = V_3 \cong V_3^*$. Then $S^2V_3 \cong V_5 \oplus V_1$ has two nonprojective summands. It follows from Section III of [2] that

$$S^{14}V_3 \cong k \oplus (\text{projective}).$$

So by Lemma 4.3, $(S^{14}V_3)^G \to (S^{14}V_3/S^2V_3)^G$ is not surjective. Using Lemma 4.2, we can now apply Theorem 3.4 to see that $U_1^G \to (U_1/U_1^p)^G$ is not surjective. Finally, applying Proposition 2.5, we see that $k[[V_3]]^{\mathbb{Z}/7}$ is not a unique factorization domain.

We shall apply the method of the above example in general for $3 \leq r \leq p-2$ to show that $k[[V_r]]^{\mathbb{Z}/p}$ is not a unique factorization domain. The cases $r = p-2$ and $r = p-3$ require special treatment, as the symmetric powers have at most one nonprojective summand in these cases.

Lemma 4.5. *Suppose that $3 \leq r \leq p-4$. Then S^2V_r has at least two nonprojective indecomposable summands.*

Proof. This follows from the description of the symmetric powers of V_r given in Almkvist [1]. $\square$

Lemma 4.6. *Let $p \geq 5$ and suppose that $r = p-2$. Then the map*

$$(S^{2p}V_r)^G \to (S^{2p}V_r/S^2V_r)^G$$

is not surjective.

Proof. It follows from Almkvist [1] that S^2V_r is isomorphic to $k \oplus (\text{projective})$. Let $w \in S^2V_r$ be a generator for the trivial summand. Since $p \geq 5$ we have $r \geq 2$, and so by direct calculation of the effect of $t-1$ on all the monomials x_i^2 and x_ix_j we have

$$(t-1)(x_1^2 + \cdots) = 2x_1x_2 + \cdots \neq 0.$$

Thus the element w cannot involve the monomial x_1^2. It follows using Lemma 4.1 that w^p is in the projective summand of $S^{2p}V_r = k \oplus \text{(projective)}$. So

$$S^{2p}V_r/S^2V_r \cong k \oplus V_{p-1} \oplus \text{(projective)}$$

where the V_{p-1} summand arises as the quotient of an indecomposable projective module by the image of w^p. A G-invariant element in V_{p-1} is not in the image of $N_G = 1 + t + \cdots + t^{p-1}$, so it does not lift to a G-invariant element of $S^{2p}V_r$. □

Lemma 4.7. *Let $p \geq 7$ and suppose that $r = p - 3$. Then the map*

$$(S^{2p}V_r)^G \to (S^{2p}V_r/S^2V_r)^G$$

is not surjective.

Proof. It follows from Almkvist [1] that S^2V_r is isomorphic to $V_3 \oplus \text{(projective)}$. Let $w \in S^2V_r$ be a generator for the V_3 summand. Since $p \geq 7$ we have $r \geq 3$, and so

$$\begin{aligned}(t-1)^3(x_1^2 + \cdots) &= (t-1)^2(2x_1x_2 + \cdots)\\ &= (t-1)(2x_1x_3 + 2x_2^2 + \cdots)\\ &= 6x_2x_3 + \cdots\\ &\neq 0.\end{aligned}$$

So no element of V_3 can involve the monomial x_1^2, and in particular w does not involve x_1^2. It follows using Lemma 4.1 that w^p is in the projective summand of $S^{2p}V_r = k \oplus \text{(projective)}$, so

$$S^{2p}V_r/S^2V_r \cong k \oplus V_{p-3} \oplus \text{(projective)}.$$

A G-invariant element in V_{p-3} is not in the image of $N_G = 1 + t + \cdots + t^{p-1}$, so it does not lift to a G-invariant element of $S^{2p}V_r$. □

Proposition 4.8. *Let $G = \mathbb{Z}/p$, and suppose that $3 \leq r \leq p - 2$. Then $k[[V_r]]^G$ is not a unique factorization domain.*

Proof. We first claim that the map $(S^{2p}V_r)^G \to (S^{2p}V_r/S^2V_r)^G$ is not surjective. If $3 \leq r \leq p-4$, this follows from Lemmas 4.1, 4.3 and 4.5. The remaining cases where $r = p-2$ or $r = p-3$ are dealt with in Lemmas 4.6 and 4.7. Using Lemma 4.2, we can now apply Theorem 3.4 to see that $U_1^G \to (U_1/U_1^p)^G$ is not surjective. Finally, using Proposition 2.5, we see that $k[[V_r]]^G$ is not a unique factorization domain. □

Proposition 4.9. *Let $G = \mathbb{Z}/p$. Then $k[[V_r]]^G$ is a unique factorization domain in the cases $r = 1$, $r = 2$, $r = p - 1$ and $r = p$.*

Proof. The case $r = 1$ is obvious, and the case $r = p$ is dealt with in Theorem 1.1, which is proved at the end of Section 2. So it remains to deal with the cases $r = 2$ and $r = p - 1$.

In the case $r = 2$, it is shown in Almkvist and Fossum [2] that if $0 \le s \le p-1$ then

$$S^{s+np}V_2 \cong V_{s+1} \oplus (\text{projective}).$$

Now if $1 \le s \le p-1$ then $x_1^s N(x_1)^n$ is an element of degree $s+np$ which is killed by $(t-1)^{s+1}$ but is not in the image of $(t-1)$. This is because $N(x_1)$ is invariant, $x_1^s \in S^s(V_2) \cong V_{s+1}$, and the image of $t-1$ contains no vector with x_1^s in its support. So we can take V_{s+1} to be the submodule generated by $x_1^s N(x_1)^n$. It follows using Lemma 4.1 that the image of the summand V_{s+1} of $S^{s+np}V_2$ under the pth power map is not contained in the projective summand of $S^{p(s+np)}V_2$ described in that lemma. Therefore the quotient takes the form

$$S^{p(s+np)}V_2/S^{s+np}V_2 \cong V_{p-s} \oplus (\text{projective}).$$

We may see this by observing that the pth power map

$$V_{s+1} \oplus (\text{projective}) \to V_1 \oplus (\text{projective})$$

may be written as the direct sum of an inclusion of projectives and a map $V_{s+1} \to V_1 \oplus V_p$, using the injectivity of projectives and the fact that we may factor any map $V_{s+1} \to$ (projective) as $V_{s+1} \to V_p \to$ (projective) where the latter map is a split injection. The component map $V_{s+1} \to V_1$ is non-zero, so the factor module $(V_1 \oplus V_p)/V_{s+1}$ is generated by the image of V_p, so is cyclic and hence indecomposable. By counting dimensions, this factor is V_{p-s}.

The G-invariants in the projective part of the quotient lift automatically, and the G-invariants in V_{p-s} lift to the trivial summand of $S^{p(s+np)}V_2$. Combining this with Lemma 4.2, we see that the conditions of Proposition 2.6 are satisfied, so that $U_1^G \to (U_1/U_1^p)^G$ is surjective. We now apply Proposition 2.5 to deduce that $k[[V_2]]^G$ is a unique factorization domain.

The proof in the case $r = p-1$ is similar. In this case, again using the results of Almkvist and Fossum [2], $S^{s+np}V_{p-1}$ is projective for $2 \le s \le p-1$, so the only case we need to worry about is $s = 1$. In this case, we have

$$S^{1+np}V_{p-1} \cong V_{p-1} \oplus (\text{projective}).$$

The element $x_1 N(x_1)^n$ is killed by $(t-1)^{p-1}$ but not in the image of $(t-1)$, and so we can take V_{p-1} to be the submodule generated by this element. It follows using Lemma 4.1 that the image of the summand V_{p-1} of $S^{1+np}V_{p-1}$ under the pth power map is not contained in the projective summand of $S^{p(1+np)}V_{p-1}$ described in that lemma. Therefore the quotient takes the form

$$S^{p(1+np)}V_{p-1}/S^{1+np}V_{p-1} \cong V_2 \oplus (\text{projective}).$$

The G-invariants in the projective part of the quotient lift automatically, and the G-invariants in V_2 lift to the trivial summand of $S^{p(1+np)}V_{p-1}$. Combining this with Lemma 4.2, we see that the conditions of Proposition 2.6 are satisfied, so that $U_1^G \to (U_1/U_1^p)^G$ is surjective. We now apply Proposition 2.5 to deduce that $k[[V_{p-1}]]^G$ is a unique factorization domain. $\square$

Combining Propositions 4.8 and 4.9, we have completed the proof of Theorem 1.3.

Acknowledgment We thank Dino Lorenzini for stimulating our interest in this problem, and for providing some references to the literature. We acknowledge also the hospitality and support of the Centre Bernoulli, EPFL, Lausanne, where this work was undertaken.

References

1. G. Almkvist, *The number of nonfree components in the decomposition of symmetric powers in characteristic p*, Pacific Journal of Math. **77** (1978), 293–301.
2. G. Almkvist and R. Fossum, *Decomposition of exterior and symmetric powers of indecomposable $\mathbb{Z}/p\mathbb{Z}$-modules in characteristic p and relations to invariants*, Séminaire d'Algèbre Paul Dubreil, 30ème année (Paris, 1976–1977), Lecture Notes in Mathematics, vol. 641, Springer-Verlag, Berlin/New York, 1978, pp. 1–111.
3. E. Artin and H. Hasse, *Die beiden Ergänzungssatze zum Reziprozitätsgesetz der ℓ^n-ten Potenzreste im Körper der ℓ^n-ten Einheitswurzeln*, Abh. Math. Sem. Univ. Hamburg **6** (1928), 146–162, Coll. Papers Artin (1965), 142–158; Math. Abh. Hasse I, 326–342.
4. D. J. Benson, *Polynomial invariants of finite groups*, London Math. Soc. Lecture Note Series, vol. 190, Cambridge University Press, 1993.
5. R. M. Fossum, *The divisor class group of a Krull domain*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 74, Springer-Verlag, Berlin/New York, 1973.
6. R. M. Fossum and P. A. Griffith, *Complete local factorial rings which are not Cohen–Macaulay in characteristic p*, Ann. Scient. Éc. Norm. Sup. **8** (1975), 189–199.
7. P. Griffith, *Completions of rings of invariants and their divisor class groups*, Nagoya Math. J. **72** (1978), 71–82.
8. E. Halanay, *An example of a unique factorization domain whose completion is not a unique factorization domain*, Stud. Cerc. Mat. **30** (1978), 495–497, Romanian, English summary.
9. R. C. Heitmann, *Characterization of completions of unique factorization domains*, Trans. Amer. Math. Soc. **337** (1993), 379–387.
10. H. Nakajima, *Relative invariants of finite groups*, J. Algebra **79** (1982), 218–234.
11. B. Peskin, *Quotient-singularities and wild p-cyclic actions*, J. Algebra **81** (1983), 72–99.
12. A. M. Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics, vol. 198, Springer-Verlag, Berlin/New York, 2000.
13. P. Samuel, *Lectures on unique factorization domains*, Tata Institute Lecture Note Series, Bombay, 1964.
14. B. Singh, *Unique factorization in power series rings*, Invent. Math. **3** (1967), 348–355.

Department of Mathematics, University of Georgia
E-mail address: `\/b\e/n\s/o\n/d\j/ (without the slashes) at maths dot abdn dot ac dot uk`

School of Mathematics, University of Minnesota, Minneapolis MN 55455
E-mail address: `/w\e/b\b/ (without the slashes) at math dot umn dot edu`