Polynomials over Symmetric Polynomials

[semi-expository note based on the literature and emails of Darij Grinberg and Victor Reiner]

GPT-5.6 Sol, edited by Darij Grinberg

August 4, 2026

Abstract

Abstract. Let $\mathbf{k}$ be a commutative ring, and let the symmetric group $\mathfrak{S}_n$ act on $P = \mathbf{k}[x_1, x_2, \ldots, x_n]$ by permuting the variables. We prove four results that are known (at least in the case when $\mathbf{k}$ is a field) but not easily found in the literature. First, the coinvariant algebra (the quotient of P by the ideal generated by the symmetric polynomials with constant term 0) is a free $\mathbf{k}$-module of rank $n!$, with the residue classes of the Artin monomials as a basis. Second, P is a free module of rank $n!$ over the ring $P^{\mathfrak{S}_n}$ of symmetric polynomials, again with the Artin monomials as a basis. Third, if $n!$ is invertible in $\mathbf{k}$, the coinvariant algebra is the regular $\mathbf{k}[\mathfrak{S}_n]$-module. Fourth, under the same hypothesis, P is a free left $P^{\mathfrak{S}_n}[\mathfrak{S}_n]$-module of rank 1. The first result follows from an elementary normal-form lemma for monic polynomials with pairwise relatively prime leading monomials. The second is proved by lifting the Artin basis. For the third, we use orbit harmonics with a strongly discrete point orbit, and the fourth follows by equivariantly lifting a regular basis of the coinvariant algebra.

Manifest. The main ideas behind this paper are not new; I have learned some of them from Vic Reiner and Brendon Rhoades. The main novelty, to the extent it is one, is extending the proofs from fields to commutative rings. The text below was produced by GPT-5.6 based on a telegraphic outline. I have then edited it. – DG[1]

1 Statement and notation

Set $\mathbb{N} = \{0, 1, 2, \ldots\}$. For any $r \in \mathbb{N}$, let $[r]$ denote the set $\{1, 2, \ldots, r\}$.

Let n be a positive integer. Let $\mathfrak{S}_n$ denote the n-th *symmetric group*, that is, the group of all bijections $[n] \to [n]$. Throughout, $\mathbf{k}$ is a commutative ring with identity and $1_{\mathbf{k}} \neq 0$. (The requirement $1_{\mathbf{k}} \neq 0$ is unnecessary in essence; it just serves to make certain statements hold literally, e.g., ensuring that each free $\mathbf{k}$-module has a unique rank.[2]) For specific claims, we will impose further requirements on $\mathbf{k}$.

[1] This work is in the public domain.

[2] Of course, the case when $1_{\mathbf{k}} = 0$ is trivial, since $\mathbf{k}$ is a one-element set in this case.

Consider the polynomial ring

$$P = \mathbf{k}\left[x_1, x_2, \ldots, x_n\right].$$

We give P its usual grading by total degree:[3]

$$P = \bigoplus_{d \geq 0} P_d,$$

where P_d is the free $\mathbf{k}$-module of homogeneous polynomials of total degree d. The group $\mathfrak{S}_n$ acts on P (and on each P_d) by permuting the variables:

$$\sigma(x_i) = x_{\sigma(i)} \qquad \text{for all } \sigma \in \mathfrak{S}_n \text{ and } i \in [n].$$

This is an action by $\mathbf{k}$-algebra automorphisms.

Let

$$\Lambda = P^{\mathfrak{S}_n} = \{f \in P \mid \sigma(f) = f \text{ for all } \sigma \in \mathfrak{S}_n\}$$

be the subring of symmetric polynomials. For each $i \in [n]$, let

$$e_i = e_i(x_1, x_2, \ldots, x_n) = \sum_{1 \leq j_1 < j_2 < \cdots < j_i \leq n} x_{j_1} x_{j_2} \cdots x_{j_i}$$

denote the i-th elementary symmetric polynomial. The fundamental theorem of symmetric polynomials gives

$$\Lambda = \mathbf{k}\left[e_1, e_2, \ldots, e_n\right], \tag{1}$$

and says that $e_1, e_2, \ldots, e_n$ are algebraically independent over $\mathbf{k}$. Equivalently, the substitution map

$$\mathbf{k}\left[t_1, t_2, \ldots, t_n\right] \longrightarrow \Lambda, \qquad t_i \longmapsto e_i$$

(a $\mathbf{k}$-algebra homomorphism from the polynomial ring $\mathbf{k}\left[t_1, t_2, \ldots, t_n\right]$), is an isomorphism. The ring Λ is a graded subring of P; write

$$\Lambda_+ = \bigoplus_{d > 0} \Lambda_d$$

for its ideal of elements with constant term 0. This ideal Λ_+ is generated by the elementary symmetric polynomials $e_1, e_2, \ldots, e_n$:

Proposition 1. *We have*

$$\Lambda_+ = e_1\Lambda + e_2\Lambda + \cdots + e_n\Lambda. \tag{2}$$

Proof. The inclusion "$\supseteq$" is clear, since each e_i belongs to Λ_i and thus to Λ_+.

Conversely, let $a \in \Lambda_+$. By (1), we can write $a = F(e_1, e_2, \ldots, e_n)$ for some $F \in T := \mathbf{k}\left[t_1, t_2, \ldots, t_n\right]$. Evaluating at $x_1 = x_2 = \cdots = x_n = 0$ gives

$$\begin{aligned} F(0, 0, \ldots, 0) &= a(0, 0, \ldots, 0) \qquad (\text{since } e_i(0, 0, \ldots, 0) = 0 \text{ for all } i > 0) \\ &= 0 \qquad (\text{since } a \text{ has constant term } 0). \end{aligned}$$

Hence $F \in t_1 T + t_2 T + \cdots + t_n T$. Substituting $t_i = e_i$ yields $a \in e_1\Lambda + e_2\Lambda + \cdots + e_n\Lambda$ (since $F(e_1, e_2, \ldots, e_n) = a$). This proves the "$\subseteq$" inclusion. $\square$

[3]All gradings are $\mathbb{N}$-gradings in this note. If V is a graded abelian group, then V_d shall mean the d-th graded component of V.

Extending the ideal $\Lambda_+ = e_1\Lambda + e_2\Lambda + \cdots + e_n\Lambda$ from Λ to P gives the ideal

$$\begin{aligned} J := \Lambda_+ P &= \left(e_1\Lambda + e_2\Lambda + \cdots + e_n\Lambda\right) P \qquad \text{(by (2))} \\ &= e_1 P + e_2 P + \cdots + e_n P \end{aligned} \tag{3}$$

of P. The *coinvariant algebra* (of $\mathfrak{S}_n$ acting on P) is defined to be the quotient $\mathbf{k}$-algebra

$$C := P/J.$$

For any $f \in \Lambda$, $g \in P$, and $\sigma \in \mathfrak{S}_n$, we have

$$\begin{aligned} \sigma(fg) &= \sigma(f)\sigma(g) \qquad \text{(since } \mathfrak{S}_n \text{ acts by algebra automorphisms)} \\ &= f\sigma(g) \qquad \text{(since } f \in \Lambda \text{ entails } \sigma(f) = f\text{)}. \end{aligned} \tag{4}$$

Thus the action of $\mathfrak{S}_n$ on P is Λ-linear, and P is naturally a left module over the group algebra $\Lambda[\mathfrak{S}_n]$.

The action of $\mathfrak{S}_n$ on P also preserves the ideal J, since J is generated by symmetric polynomials. Hence the quotient algebra $C = P/J$ inherits an action of $\mathfrak{S}_n$ and is a left module over $\mathbf{k}[\mathfrak{S}_n]$.

We will prove the following folklore results mentioned, among other places, in [12, Section 1.5]:

Theorem 2.

(a) *The $\mathbf{k}$-module C is free of rank $n!$. More explicitly, call the $n!$ monomials*

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \qquad \text{with} \qquad 0 \leq a_i < i \quad \text{for every } i \in [n]$$

the Artin monomials. *Their residue classes in C form a $\mathbf{k}$-basis of C.*

(b) *The Λ-module P is free of rank $n!$; the Artin monomials form a Λ-basis of P.*

(c) *Assume that $n!$ is invertible in $\mathbf{k}$. Then* [4]

$$C \cong \mathbf{k}[\mathfrak{S}_n] \qquad \text{as a } \mathbf{k}[\mathfrak{S}_n]\text{-module.}$$

In other words, the coinvariant algebra $C = P/J$ is isomorphic to the regular $\mathbf{k}[\mathfrak{S}_n]$-module.

(d) *Assume that $n!$ is invertible in $\mathbf{k}$. Then*

$$P \cong \Lambda[\mathfrak{S}_n] \qquad \text{as a } \Lambda[\mathfrak{S}_n]\text{-module.}$$

In other words, P is isomorphic to the regular $\Lambda[\mathfrak{S}_n]$-module. Equivalently, there exists an element $f \in P$ such that the map

$$\Phi : \Lambda[\mathfrak{S}_n] \longrightarrow P, \qquad \sum_{\sigma \in \mathfrak{S}_n} a_\sigma \sigma \longmapsto \sum_{\sigma \in \mathfrak{S}_n} a_\sigma \sigma(f) \tag{5}$$

is an isomorphism of $\Lambda[\mathfrak{S}_n]$-modules.

[4] Here and in the following, "A-module" for a ring A shall always mean "left A-module". Thus, a $\mathbf{k}[\mathfrak{S}_n]$-module is the same thing as a representation of $\mathfrak{S}_n$ over $\mathbf{k}$.

We first prove an elementary normal-form lemma and use it to compute the coinvariant algebra, proving **(a)**. A lifting argument then proves **(b)**. Next, an orbit-harmonics argument proves **(c)**. Finally, combining the lifting argument with **(c)** proves **(d)**. The invertibility hypothesis in **(c)** and **(d)** cannot simply be omitted; we give a modular counterexample at the end.

2 A coprime-leading-monomial lemma

In this section, we shall prove a general property of certain ideals in polynomial rings. This property is part of the theory of Gröbner bases (see Remark 4), but we will give a self-contained proof avoiding the general theory, as the property is the only thing we will need.

Let R be a commutative ring with identity. Consider the polynomial ring

$$A := R\left[z_1, z_2, \ldots, z_N\right],$$

and fix a monomial order $\prec$ on A. That is, $\prec$ is a total well-order on the set of all monomials in A, and

$$u \prec v \quad \Longrightarrow \quad uw \prec vw$$

for all monomials u, v, w. For a nonzero polynomial $f \in A$, its *leading monomial* $\mathrm{LM}(f)$ is the largest monomial that occurs in f with a nonzero coefficient. We call f *monic* if the coefficient of $\mathrm{LM}(f)$ is 1. We say that two monomials u and v are *relatively prime* if the only monomial that divides them both is 1; equivalently, this means that they have no variable in common. (For instance, the monomials $z_1 z_3^2$ and $z_2 z_5$ are relatively prime, but the monomials $z_1 z_3^2$ and $z_3 z_5$ are not.)

Lemma 3 (Coprime-leading-monomial lemma)**.** *Let $g_1, g_2, \ldots, g_k \in A$ be monic polynomials whose leading monomials*

$$m_i = \mathrm{LM}(g_i) \qquad \text{(for } i \in [k]\text{)}$$

are pairwise relatively prime. A monomial q will be called reduced *if it is not divisible by any of $m_1, m_2, \ldots, m_k$ (that is, if $m_i \nmid q$ for each $i \in [k]$). Define an ideal I of A by*

$$I = g_1 A + g_2 A + \cdots + g_k A.$$

Then the residue classes of the reduced monomials form an R-module basis of A/I.

Proof. For each $i \in [k]$, write

$$g_i = m_i - r_i, \tag{6}$$

where every monomial occurring in r_i is strictly smaller than m_i. (We can write g_i in this form, since g_i is monic with leading monomial m_i.) Let A_{red} be the free R-submodule of A spanned by the reduced monomials.

We shall construct an R-linear map

$$\rho : A \longrightarrow A_{\mathrm{red}}$$

by recursively defining the values $\rho(u)$ for all monomials u; the recursion shall proceed along the well-founded order relation $\prec$. If a monomial u is reduced, set $\rho(u) = u$. If u is not reduced, choose an $i \in [k]$ such that $m_i \mid u$ and set

$$\rho(u) = \rho\left(\frac{u}{m_i} r_i\right). \tag{7}$$

On the right-hand side, ρ is applied termwise and R-linearly. This is legitimate because every monomial occurring in $(u/m_i)r_i$ is strictly smaller than u: indeed, every monomial of r_i is smaller than m_i, and a monomial order is compatible with multiplication.

We must check that (7) is independent of the choice of i. Suppose that both m_i and m_j divide u, where $i \neq j$. We must show that

$$\rho\left(\frac{u}{m_i} r_i\right) = \rho\left(\frac{u}{m_j} r_j\right). \tag{8}$$

Since the monomials m_i and m_j are relatively prime and both divide u, their product must divide u as well; thus

$$u = q m_i m_j$$

for some monomial q. By the recursive induction hypothesis, the definition of ρ is already independent of all choices on monomials strictly smaller than u. Every monomial t occurring in r_i satisfies $t \prec m_i$ and thus (since $\prec$ is a monomial order)

$$q t m_j \prec q m_i m_j = u.$$

When evaluating $\rho(q t m_j)$, we may therefore use the divisor m_j in (7), and obtain

$$\rho(q t m_j) = \rho\left(\frac{q t m_j}{m_j} r_j\right) = \rho(q t r_j).$$

Multiplying by the coefficient of t and summing over all monomials of r_i gives

$$\rho(q r_i m_j) = \rho(q r_i r_j).$$

The same argument (with the roles of i and j switched) yields

$$\rho(q r_j m_i) = \rho(q r_j r_i).$$

Since A is commutative, this is the same as

$$\rho(q m_i r_j) = \rho(q r_i r_j).$$

Hence, from $u = q m_i m_j$, we obtain

$$\rho\left(\frac{u}{m_i} r_i\right) = \rho(q r_i m_j) = \rho(q r_i r_j) = \rho(q m_i r_j) = \rho\left(\frac{u}{m_j} r_j\right),$$

which proves (8). Thus we have shown that the R-linear map $\rho : A \to A_{\mathrm{red}}$ is well-defined.

We next record two properties of ρ. First, for every monomial q and every $i \in [k]$, the definition allows us to reduce the monomial qm_i using m_i (that is, apply (7) to $u = qm_i$); hence

$$\rho(qm_i) = \rho(qr_i). \tag{9}$$

By linearity of ρ, this entails $\rho(q(m_i - r_i)) = 0$. In view of (6), this rewrites as

$$\rho(qg_i) = 0. \tag{10}$$

By R-linearity, (10) shows that

$$\rho(I) = 0.$$

Second, every $f \in A$ satisfies

$$f - \rho(f) \in I. \tag{11}$$

Indeed, by R-linearity, it is enough to prove this when f is a monomial; i.e., it is enough to show that $u - \rho(u) \in I$ for any monomial u. We do so by induction on u. If u is reduced, the claim is clear. Otherwise, choose i with $m_i \mid u$ and put $q = u/m_i$. Then $u = qm_i$ and therefore $\rho(u) = \rho(qm_i) = \rho(qr_i)$ by (9); hence,

$$\begin{aligned} u - \rho(u) &= qm_i - \rho(qr_i) \\ &= q(m_i - r_i) + \big(qr_i - \rho(qr_i)\big) \\ &= qg_i + \big(qr_i - \rho(qr_i)\big) \qquad \text{(by (6))}. \end{aligned}$$

The first addend belongs to I. Every monomial occurring in qr_i is strictly smaller than $qm_i = u$. Applying the induction hypothesis to these monomials and then using R-linearity gives $qr_i - \rho(qr_i) \in I$. Thus the second addend belongs to I as well. Thus, $u - \rho(u) \in I$. This proves (11).

Equation (11) shows that

$$A = I + A_{\mathrm{red}}.$$

This sum is direct. Indeed, if $h \in I \cap A_{\mathrm{red}}$, then $\rho(h) = 0$ because $\rho(I) = 0$, whereas $\rho(h) = h$ because ρ fixes every reduced monomial. Thus $h = 0$. Consequently,

$$A = I \oplus A_{\mathrm{red}}$$

as R-modules. Therefore, the canonical projection $A \to A/I$, restricted to A_{red}, becomes an R-module isomorphism. Since the reduced monomials form a basis of A_{red}, this shows that their residue classes form a basis of A/I. □

Remark 4. *In Gröbner-basis language, Lemma 3 says that $g_1, g_2, \ldots, g_k$ form a monic Gröbner basis and then applies the standard-monomial basis theorem. Over a field, this follows from Buchberger's first criterion; see, for example, [5, Chapter 1, especially the conclusion after Lemma 1.1.38]. The proof above avoids S-polynomials and Buchberger's criterion altogether. It is the particularly simple commutative case of a diamond-lemma argument in which the only competing reductions are*

$$qm_im_j \longrightarrow qr_im_j \longrightarrow qr_ir_j \quad \text{and} \quad qm_im_j \longrightarrow qm_ir_j \longrightarrow qr_ir_j.$$

For a more detailed treatment of monic reductions and Gröbner bases over arbitrary commutative rings, see [10, Section 3.2]. Compare also Bergman's diamond lemma [1, Theorem 1.2], which makes similar statements about noncommutative polynomial rings.

3 The Artin basis

We prove Theorem 2 **(a)** using Lemma 3. Our proof follows the ideas of [17, proof of Theorem 1.2.7]. Other proofs can be found in [13, (DIFF.1.3)], [3, Chapter IV, §6, no. 1, Theorem 1, part (c)], [7, Theorem, part (c)] and (over $\mathbb{Z}$ instead of $\mathbf{k}$) in [6, Proposition 3.4] and [14, (5.1)].

We shall use the shorthand notation x^a for the monomial $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, where $a = (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n$.

For $r \in \mathbb{N}$ and a finite list of variables $y_1, y_2, \ldots, y_m$, let $h_r(y_1, y_2, \ldots, y_m)$ denote the complete homogeneous symmetric polynomial of degree r in $y_1, y_2, \ldots, y_m$; this is defined as the sum of all monomials $y_1^{a_1} y_2^{a_2} \cdots y_m^{a_m}$ with $a_1 + a_2 + \cdots + a_m = r$. (In particular, $h_0 = 1$.) For $1 \leq i \leq n$, set

$$g_i = h_i(x_i, x_{i+1}, \ldots, x_n).$$

Lemma 5 (A generating-function identity)**.** *For each $i \in [n]$, we have the identity*

$$\left(\sum_{j=0}^{n} (-1)^j e_j t^j \right) \left(\sum_{r \geq 0} h_r(x_i, x_{i+1}, \ldots, x_n) t^r \right) = \prod_{j=1}^{i-1} (1 - x_j t) \tag{12}$$

in the formal power-series ring $P[[t]]$, where $e_0 = 1$.

Proof. The elementary symmetric polynomials satisfy Viète's identity

$$\sum_{j=0}^{n} (-1)^j e_j t^j = \prod_{j=1}^{n} (1 - x_j t). \tag{13}$$

Indeed, when the product on the right-hand side is expanded, choosing the term $-x_j t$ from exactly r of its factors produces $(-1)^r e_r t^r$. On the other hand, every power series $1 - x_j t$ in $P[[t]]$ has constant term 1 and is therefore a unit. We have

$$\sum_{r \geq 0} h_r(x_i, x_{i+1}, \ldots, x_n) t^r = \prod_{j=i}^{n} \frac{1}{1 - x_j t}. \tag{14}$$

To see this, expand each factor on the right-hand side as

$$\frac{1}{1 - x_j t} = (1 - x_j t)^{-1} = \sum_{a \geq 0} x_j^a t^a$$

by the geometric-series formula. Thus, the whole product rewrites as follows:

$$\prod_{j=i}^{n} \frac{1}{1 - x_j t} = \prod_{j=i}^{n} \sum_{a \geq 0} x_j^a t^a = \sum_{(a_i, a_{i+1}, \ldots, a_n) \in \mathbb{N}^{n-i+1}} x_i^{a_i} x_{i+1}^{a_{i+1}} \cdots x_n^{a_n} t^{a_i + a_{i+1} + \cdots + a_n}.$$

The coefficient of t^r in this is the sum of all monomials $x_i^{a_i} x_{i+1}^{a_{i+1}} \cdots x_n^{a_n}$ with $a_i + a_{i+1} + \cdots + a_n = r$. This is precisely $h_r(x_i, x_{i+1}, \ldots, x_n)$. Thus, (14) is proved.

Multiplying (13) and (14), we obtain

$$\left(\sum_{j=0}^{n}(-1)^j e_j t^j\right)\left(\sum_{r\geq 0} h_r(x_i, x_{i+1}, \ldots, x_n)t^r\right) = \prod_{j=1}^{n}(1-x_j t)\prod_{j=i}^{n}\frac{1}{1-x_j t} = \prod_{j=1}^{i-1}(1-x_j t),$$

since the factors $1-x_i t, 1-x_{i+1}t, \ldots, 1-x_n t$ cancel. Thus (12) is proved. □

Lemma 6 (Asymmetric generating set of J)**.** *We have the equality*

$$g_1 P + g_2 P + \cdots + g_n P = J \tag{15}$$

of ideals of P.

Proof. For each $i \in [n]$, the right-hand side of (12) has degree at most $i-1$ in t. Comparing coefficients of t^i in (12) therefore gives

$$\sum_{j=0}^{i}(-1)^j e_j h_{i-j}(x_i, x_{i+1}, \ldots, x_n) = 0. \tag{16}$$

The $j = 0$ addend on the left-hand side of this equality is $(-1)^0 e_0 h_i(x_i, x_{i+1}, \ldots, x_n) = h_i(x_i, x_{i+1}, \ldots, x_n) = g_i$; thus, we can rewrite (16) as

$$g_i + \sum_{j=1}^{i}(-1)^j e_j h_{i-j}(x_i, x_{i+1}, \ldots, x_n) = 0,$$

or, equivalently,

$$\begin{aligned} g_i &= -\sum_{j=1}^{i}(-1)^j e_j h_{i-j}(x_i, x_{i+1}, \ldots, x_n) \\ &= -\sum_{j=1}^{i-1}(-1)^j e_j h_{i-j}(x_i, x_{i+1}, \ldots, x_n) - (-1)^i e_i \end{aligned} \tag{17}$$

(since $h_{i-i}(x_i, x_{i+1}, \ldots, x_n) = 1$). Thus every g_i belongs to J (since $e_1, e_2, \ldots, e_i \in J$). This proves the "$\subseteq$" inclusion of (15).

Conversely, (17) gives

$$(-1)^i e_i = -g_i - \sum_{j=1}^{i-1}(-1)^j e_j h_{i-j}(x_i, x_{i+1}, \ldots, x_n). \tag{18}$$

We now prove by strong induction on i that

$$e_i \in g_1 P + g_2 P + \cdots + g_i P.$$

Indeed, assume that this claim is known for all smaller indices. Every e_j occurring on the right-hand side of (18) has $j < i$, so the induction hypothesis places it in $g_1 P + g_2 P + \cdots + g_j P$. Hence the left-hand side $(-1)^i e_i$, and therefore also e_i, belongs to $g_1 P + g_2 P + \cdots + g_i P$. Thus we conclude that $e_i \in g_1 P + g_2 P + \cdots + g_n P$ for each $i \in [n]$. In view of (3), this entails $J \subseteq g_1 P + g_2 P + \cdots + g_n P$. This proves the "$\supseteq$" inclusion in (15). Hence the equality of ideals (15) is proved. □

Proposition 7 (Artin basis)**.** *The residue classes of the Artin monomials*

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \qquad \text{with} \qquad 0 \leq a_i < i \quad \text{for every } i \in [n] \tag{19}$$

form a $\mathbf{k}$*-basis of* $P/J = C$*.*

Proof. From Lemma 6, we know that $J = g_1 P + g_2 P + \cdots + g_n P$. To obtain a $\mathbf{k}$-module basis of $C = P/J$, we shall apply Lemma 3 with $R = \mathbf{k}$, $N = n$, $A = P$, $k = n$, and $I = J$, using the generators $g_1, g_2, \ldots, g_n$. We therefore need a monomial order $\succ$ on P for which the g_i are monic and have pairwise relatively prime leading monomials. There are several valid choices here. The simplest one is to let $\succ$ be the lexicographic order $>_{\text{lex}}$ with

$$x_1 > x_2 > \cdots > x_n.$$

Thus, for exponent vectors $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$, we have $x^a \succ x^b$ if, at the first index r for which $a_r \neq b_r$, we have $a_r > b_r$. Alternatively, we can let $\succ$ be the degree-lexicographic order $>_{\text{grlex}}$, in which two monomials of equal degree are compared as in the lexicographic order, whereas two monomials of distinct degrees are compared by their degrees (that is, the monomial of larger degree is declared to be larger). Both of these orders are monomial orders (this is particularly easy to check for $>_{\text{grlex}}$, since there are only finitely many monomials of a given degree), and both have the property that each of the polynomials g_i is monic with leading monomial $\operatorname{LM}(g_i) = x_i^i$ (since $g_i = h_i(x_i, x_{i+1}, \ldots, x_n) = x_i^i +$ smaller monomials). These leading monomials are pairwise relatively prime.

Hence Lemma 3 shows that the residue classes of the reduced monomials (i.e., of the monomials not divisible by any of $x_1^1, x_2^2, \ldots, x_n^n$) form a $\mathbf{k}$-basis of P/J. A monomial $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ is reduced if and only if $0 \leq a_i < i$ for every $i \in [n]$. These are exactly the Artin monomials in (19). Thus their residue classes form a basis of P/J.

This proves Proposition 7 and therefore Theorem 2 **(a)**. □

If $V = \bigoplus_{d \geq 0} V_d$ is a graded $\mathbf{k}$-module such that every V_d is finite free, its *Hilbert series* is the formal power series

$$\operatorname{Hilb}(V; q) := \sum_{d \geq 0} (\operatorname{rank}_{\mathbf{k}} V_d) q^d \in \mathbb{Z}\left[[q]\right]. \tag{20}$$

We will use Hilbert series only for graded $\mathbf{k}$-modules with finite free homogeneous components. Note that P, C and Λ are such graded $\mathbf{k}$-modules; indeed, the basis of C constructed in Proposition 7 is a *graded basis* (i.e., a basis consisting of homogeneous vectors).

Corollary 8. *We have*

$$\operatorname{Hilb}(C; q) = \prod_{i=1}^{n} (1 + q + \cdots + q^{i-1}) \qquad \text{and} \qquad \operatorname{rank}_{\mathbf{k}} C = n!.$$

Proof. By Proposition 7, the degree-d component of C has as a basis the residue classes of the Artin monomials $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ satisfying $0 \leq a_i < i$ and $a_1 + a_2 + \cdots + a_n = d$. Hence

its rank $\operatorname{rank}_{\mathbf{k}} C_d$ is the number of exponent tuples $(a_1, a_2, \ldots, a_n)$ satisfying $0 \leq a_i < i$ for all i as well as $a_1 + a_2 + \cdots + a_n = d$. Therefore

$$\begin{aligned}
\operatorname{Hilb}(C; q) &= \sum_{d \geq 0} \sum_{\substack{(a_1, a_2, \ldots, a_n); \\ 0 \leq a_i < i \text{ for each } i; \\ a_1 + a_2 + \cdots + a_n = d}} q^d \\
&= \sum_{\substack{(a_1, a_2, \ldots, a_n); \\ 0 \leq a_i < i \text{ for each } i}} q^{a_1 + a_2 + \cdots + a_n} \\
&= \sum_{0 \leq a_1 < 1} \sum_{0 \leq a_2 < 2} \cdots \sum_{0 \leq a_n < n} q^{a_1 + a_2 + \cdots + a_n} \\
&= \prod_{i=1}^{n} \left(\sum_{a=0}^{i-1} q^a \right) \\
&= \prod_{i=1}^{n} (1 + q + \cdots + q^{i-1}).
\end{aligned}$$

Evaluating this polynomial at $q = 1$ counts all Artin monomials and gives $\operatorname{rank}_{\mathbf{k}} C = 1 \cdot 2 \cdot \cdots \cdot n = n!$. □

4 Lifting the coinvariant algebra

We next prove Theorem 2 **(b)**. Over a field, one can start with an arbitrary graded vector-space complement to J in P. Over a general coefficient ring such complements need not exist, so we formulate the lifting argument for a chosen graded set of representatives. The Artin monomials provide such representatives.

We shall use the following elementary fact.

Lemma 9. *Let R be a commutative ring. Any surjective R-linear map between two finite free R-modules of the same rank is an isomorphism.*

Proof. Let f be a surjective R-linear map between two free R-modules of the same rank. We must prove that f is an isomorphism.

After choosing bases, the map f is represented by a square matrix A. Since its target is free, the surjection f has an R-linear right inverse g, represented by a matrix B. Thus $AB = I$. Taking determinants gives $\det(A) \det(B) = 1$, so $\det(A)$ is a unit. The adjugate formula $A \operatorname{adj}(A) = \operatorname{adj}(A) A = \det(A) \cdot I$ then shows that A is invertible. Hence, the corresponding linear map f is an isomorphism. □

Proposition 10. *Let*

$$H = \bigoplus_{d \geq 0} H_d$$

be a graded $\mathbf{k}$*-submodule of P such that each H_d is finite free and the quotient map $P \to C = P/J$ restricts to a graded* $\mathbf{k}$*-module isomorphism*

$$H \xrightarrow{\sim} C. \tag{21}$$

Then:

(a) *Multiplication induces an isomorphism of graded Λ-modules*

$$m : \Lambda \otimes_{\mathbf{k}} H \xrightarrow{\sim} P, \qquad a \otimes h \longmapsto ah.$$

Here the tensor product has its usual grading:

$$(\Lambda \otimes_{\mathbf{k}} H)_d = \bigoplus_{r+s=d} \Lambda_r \otimes_{\mathbf{k}} H_s.$$

(b) *If H is $\mathfrak{S}_n$-stable, then m is also $\mathfrak{S}_n$-equivariant, where $\mathfrak{S}_n$ acts on the second tensor factor.*

Proof. The map m is plainly graded and Λ-linear. We first prove that it is surjective, or equivalently that $P = \Lambda H$, by strong induction on degree. Let $p \in P_d$ be homogeneous. By (21), the quotient map $H \xrightarrow{\sim} C$ is an isomorphism; since it is graded, it thus restricts to an isomorphism $H_d \xrightarrow{\sim} C_d$. Thus, the residue class of p in C_d lies in the image of this restricted isomorphism; that is, there is an $h \in H_d$ such that $p - h \in J_d$. Since

$$J = e_1 P + e_2 P + \cdots + e_n P,$$

we can thus write

$$p - h = \sum_{i=1}^{n} e_i q_i,$$

where each $q_i \in P$. Moreover, by projecting both sides of this equality onto the d-th graded component of P, we obtain

$$p - h = \sum_{i=1}^{n} e_i \widetilde{q}_i, \tag{22}$$

where $\widetilde{q}_i$ is the $(d-i)$-th graded component of q_i (since each e_i is homogeneous of degree i). As usual, $\widetilde{q}_i = 0$ when $i > d$. By induction, each $\widetilde{q}_i$ lies in ΛH (since $\deg \widetilde{q}_i = d - i < d$). Since $e_i \in \Lambda$, the equality (22) thus yields $p - h \in \underbrace{\Lambda\Lambda}_{=\Lambda} H = \Lambda H$, and therefore $p \in \Lambda H$ as well (since $h \in H_d \subseteq H \subseteq \Lambda H$). So we have proved the surjectivity of m.

It remains to prove the injectivity of m. We do this degree by degree. By (1), the monomials

$$e_1^{a_1} e_2^{a_2} \cdots e_n^{a_n} \qquad (\text{with } a_1, a_2, \ldots, a_n \in \mathbb{N})$$

form a graded $\mathbf{k}$-basis of Λ, and they are homogeneous of degree $1a_1 + 2a_2 + \cdots + na_n$. Hence

$$\begin{aligned} \operatorname{Hilb}(\Lambda; q) &= \sum_{d \geq 0} \sum_{\substack{a_1, a_2, \ldots, a_n \in \mathbb{N}; \\ 1a_1 + 2a_2 + \cdots + na_n = d}} q^d = \sum_{a_1, a_2, \ldots, a_n \in \mathbb{N}} q^{1a_1 + 2a_2 + \cdots + na_n} \\ &= \prod_{i=1}^{n} \sum_{a \in \mathbb{N}} q^{ia} = \prod_{i=1}^{n} \frac{1}{1 - q^i} \end{aligned} \tag{23}$$

(since $\sum_{a\in\mathbb{N}} q^{ia} = \dfrac{1}{1-q^i}$ for each $i > 0$). Likewise, the ordinary monomial basis of P gives

$$\operatorname{Hilb}(P;q) = \frac{1}{(1-q)^n}. \tag{24}$$

Furthermore, (21) and Corollary 8 give

$$\begin{aligned}\operatorname{Hilb}(H;q) = \operatorname{Hilb}(C;q) &= \prod_{i=1}^{n} \underbrace{(1+q+\cdots+q^{i-1})}_{=\frac{1-q^i}{1-q}} \\ &= \frac{\prod_{i=1}^{n}(1-q^i)}{(1-q)^n}. \end{aligned} \tag{25}$$

If V and W are two graded $\mathbf{k}$-modules whose homogeneous components are finite free, then their Hilbert series multiply under tensor products, i.e., we have

$$\operatorname{Hilb}\left(V \otimes_{\mathbf{k}} W; q\right) = \operatorname{Hilb}\left(V; q\right) \cdot \operatorname{Hilb}\left(W; q\right),$$

since each $d \geq 0$ satisfies

$$\operatorname{rank}_{\mathbf{k}}(V \otimes_{\mathbf{k}} W)_d = \sum_{r+s=d} (\operatorname{rank}_{\mathbf{k}} V_r)(\operatorname{rank}_{\mathbf{k}} W_s).$$

Consequently,

$$\begin{aligned}\operatorname{Hilb}(\Lambda \otimes_{\mathbf{k}} H; q) &= \operatorname{Hilb}(\Lambda; q) \cdot \operatorname{Hilb}(H; q) \\ &= \left(\prod_{i=1}^{n} \frac{1}{1-q^i}\right) \cdot \frac{\prod_{i=1}^{n}(1-q^i)}{(1-q)^n} \qquad \text{(by (23) and (25))} \\ &= \frac{1}{(1-q)^n} = \operatorname{Hilb}(P;q) \qquad \text{(by (24))}. \end{aligned}$$

In other words, for each $d \geq 0$, we have $\operatorname{rank}_{\mathbf{k}}\left(\Lambda \otimes_{\mathbf{k}} H\right)_d = \operatorname{rank}_{\mathbf{k}} P_d$.

Thus, in every degree d, the map $m : \left(\Lambda \otimes_{\mathbf{k}} H\right)_d \to P_d$ is a surjection between finite free $\mathbf{k}$-modules of the same rank. Therefore, Lemma 9 shows that each homogeneous component of m is an isomorphism. Altogether, m is thus an isomorphism of graded $\mathbf{k}$-modules. This proves part **(a)**.

(b) If H is $\mathfrak{S}_n$-stable, then m is equivariant because of (4). □

Corollary 11. *The polynomial ring P is a free Λ-module of rank $n!$. More explicitly, the Artin monomials*

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \qquad \textit{(with } 0 \leq a_i < i \textit{ for every } i \in [n]\textit{)}$$

form a Λ-basis of P.

Proof. Let H be the free $\mathbf{k}$-submodule of P spanned by the Artin monomials. This is a graded $\mathbf{k}$-submodule of P, since each Artin monomial is homogeneous. The Artin monomials form a $\mathbf{k}$-basis of H. Meanwhile, their residue classes in $P/J = C$ form a $\mathbf{k}$-basis of C, by Proposition 7.

Restricting the quotient map $P \to P/J = C$ to H, we obtain a graded $\mathbf{k}$-linear map $\phi : H \to C$. This map ϕ sends the Artin monomials in H to their residue classes in C. Since the former form a $\mathbf{k}$-basis of H while the latter form a $\mathbf{k}$-basis of C, we thus conclude that ϕ is a $\mathbf{k}$-module isomorphism. Hence, Proposition 10 **(a)** shows that multiplication induces an isomorphism of graded Λ-modules

$$m : \Lambda \otimes_{\mathbf{k}} H \xrightarrow{\sim} P, \qquad a \otimes h \longmapsto ah.$$

But the Artin monomials $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ form a $\mathbf{k}$-basis of H. Hence, the tensors $1 \otimes_{\mathbf{k}} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ form a Λ-basis of $\Lambda \otimes_{\mathbf{k}} H$ (since base change respects bases). Therefore, the images of these tensors under m form a Λ-basis of P (since m is a Λ-module isomorphism). But these images are again the Artin monomials $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$. So we have shown that the Artin monomials form a Λ-basis of P. This proves Corollary 11 and, with it, Theorem 2 **(b)**. □

Remark 12 (Harmonic representatives)**.** *When* $\mathbf{k}$ *is a field of characteristic* 0*, one customary choice of* H *is the space of harmonic polynomials; compare Haiman's discussion of harmonics and the one-set case [12, Sections 1.3 and 1.5]. On* $\mathbb{Q}[x_1, x_2, \ldots, x_n]$*, consider the* apolar pairing*, i.e., the* $\mathbb{Q}$*-bilinear form given by*

$$\langle p, q \rangle = \big(p(\partial_{x_1}, \partial_{x_2}, \ldots, \partial_{x_n})q\big)(0).$$

The monomials are orthogonal with respect to this pairing, and satisfy

$$\langle x^a, x^a \rangle = a_1! a_2! \cdots a_n!.$$

Thus, after extension to $\mathbb{R}$*, this pairing is positive definite, and* $J^\perp$ *is a graded* $\mathfrak{S}_n$*-stable complement to* J*. After base change to any characteristic-*0 *field, one may therefore take* $H = J^\perp$ *in Proposition 10. This realization is not needed for the ring-valued theorem.*

Other proofs of Theorem 2 **(b)** can be found in [14, (5.1)] and in [9, Proposition 3.3]. (In both sources, the theorem is only stated for $\mathbf{k} = \mathbb{Z}$, but the general case can be easily derived from this via base change.)

5 Orbit harmonics and the regular representation

We now prove Theorem 2 **(c)**. The construction is the orbit-harmonics, or point-orbit, method used by Oh and Rhoades [15, Section 1]; their Section 3.1 applies it to the coinvariant algebra of a reflection group. We first record the associated-graded facts in the form needed over a commutative coefficient ring.

We begin with a simple and fundamental lemma about evaluation homomorphisms:

Lemma 13. *Let $y = (y_1, y_2, \ldots, y_n) \in \mathbf{k}^n$ be any point. Then, the map*

$$\begin{aligned} \epsilon_y : P &\to \mathbf{k}, \\ f &\mapsto f(y) = f(y_1, y_2, \ldots, y_n) \end{aligned}$$

is a $\mathbf{k}$*-algebra homomorphism, known as* evaluation at y*. Its kernel is the ideal*

$$\mathfrak{m}_y := (x_1 - y_1)P + (x_2 - y_2)P + \cdots + (x_n - y_n)P \tag{26}$$

of P*.*

Proof. The fact that ϵ_y is a homomorphism is completely elementary. To show that $\mathfrak{m}_y$ (as defined in (26)) is the kernel of ϵ_y, we can argue as follows: Any polynomial $f \in P$ can be transformed into $\epsilon_y(f) = f(y)$ by replacing $x_1, x_2, \ldots, x_n$ successively by $y_1, y_2, \ldots, y_n$. Each replacement changes the polynomial by a difference that is divisible by $x_i - y_i$; thus, the total difference $f - \epsilon_y(f)$ belongs to $(x_1 - y_1)P + (x_2 - y_2)P + \cdots + (x_n - y_n)P = \mathfrak{m}_y$. If $f \in \operatorname{Ker} \epsilon_y$, then $\epsilon_y(f) = 0$, so this means that f itself belongs to $\mathfrak{m}_y$. Thus, $\ker \epsilon_y \subseteq \mathfrak{m}_y$. The converse implication $\mathfrak{m}_y \subseteq \ker \epsilon_y$ is even more obvious, so $\ker \epsilon_y = \mathfrak{m}_y$ follows.

Alternatively, reduce the claim to the case $y = (0, 0, \ldots, 0)$ by substituting $x_i - y_i$ for each x_i. □

Recall that the polynomial ring P is graded. If

$$f = f_0 + f_1 + \cdots + f_d \qquad (\text{with } f_i \in P_i \text{ and } f_d \neq 0)$$

is a nonzero polynomial in P, then its *leading homogeneous part* is defined to be

$$\tau(f) := f_d.$$

For an arbitrary ideal $I \subseteq P$, define the graded ideal

$$\operatorname{in}_{\deg}(I) = \sum_{\substack{f \in I; \\ f \neq 0}} \tau(f) P. \tag{27}$$

Thus $\operatorname{in}_{\deg}(I)$ is generated by leading homogeneous parts (not by leading monomials!). Reiner and Rhoades call this ideal $\operatorname{gr} I$; compare [16, Proposition 2.1].

For any $d \in \mathbb{Z}$, define the $\mathbf{k}$-submodule

$$P_{\leq d} := \bigoplus_{i=0}^{d} P_i$$

(where an empty direct sum is understood to be $\{0\}$, so that $P_{\leq d} = 0$ for all negative d).

Thus, $P_{\leq d}$ consists of the polynomials of degree at most d, and we have

$$P_{\leq d} P_{\leq e} \subseteq P_{\leq d+e} \qquad \text{for all } d, e \in \mathbb{Z}.$$

Hence P is a filtered $\mathbf{k}$-algebra, with filtration $0 = P_{\leq -1} \subseteq P_{\leq 0} \subseteq P_{\leq 1} \subseteq \cdots$.

Lemma 14 (The associated graded quotient)**.** *Let I be any ideal of P. The* degree filtration *of P/I is the filtration $0 = F_{-1} \subseteq F_0 \subseteq F_1 \subseteq \cdots$ of P/I defined by setting*

$$F_d := F_d^{(P/I)} := \frac{P_{\leq d} + I}{I} \qquad \text{for each } d \in \mathbb{Z}.$$

Thus F_d is the image of $P_{\leq d}$ under the quotient map $P \to P/I$. This is a multiplicative filtration: $F_d F_e \subseteq F_{d+e}$.

The associated graded algebra *of P/I is the graded* $\mathbf{k}$*-algebra*

$$\operatorname{gr}_F(P/I) := \bigoplus_{d \geq 0} F_d/F_{d-1}.$$

Its multiplication is given explicitly by

$$(a + F_{d-1})(b + F_{e-1}) = ab + F_{d+e-1} \qquad \text{for all } a \in F_d \text{ and } b \in F_e. \tag{28}$$

There is a canonical isomorphism of graded $\mathbf{k}$*-algebras*

$$P/\operatorname{in}_{\deg}(I) \xrightarrow{\sim} \operatorname{gr}_F(P/I). \tag{29}$$

More explicitly, if $p \in P_d$ is homogeneous, then this isomorphism sends

$$p + \operatorname{in}_{\deg}(I) \quad \longmapsto \quad (p + I) + F_{d-1} \in F_d/F_{d-1}.$$

Equivalently, it identifies the degree-d component of the left-hand side with

$$\left(P/\operatorname{in}_{\deg}(I)\right)_d \cong \frac{P_{\leq d} + I}{P_{\leq d-1} + I}. \tag{30}$$

Proof. The inclusion $P_{\leq d} P_{\leq e} \subseteq P_{\leq d+e}$ implies $F_d F_e \subseteq F_{d+e}$. It also shows that the multiplication rule (28) is independent of the chosen representatives. For example, if $a' \in F_{d-1}$, then $a'b \in F_{d+e-1}$, so replacing a by $a + a'$ does not change the product $(a + F_{d-1})(b + F_{e-1})$ in F_{d+e}/F_{d+e-1}; the same argument applies to b. Thus $\operatorname{gr}_F(P/I)$ is indeed a graded algebra.

For each $d \geq 0$, define a $\mathbf{k}$-linear map

$$\varphi_d : P_d \longrightarrow F_d/F_{d-1}, \qquad p \longmapsto (p + I) + F_{d-1}.$$

Taking the direct sum of these φ_d over all d gives a graded $\mathbf{k}$-linear map

$$\varphi : P = \bigoplus_{d \geq 0} P_d \longrightarrow \operatorname{gr}_F(P/I).$$

This map is an algebra homomorphism. Indeed, if $p \in P_d$ and $q \in P_e$ are homogeneous, then

$$\begin{aligned} \varphi(p)\varphi(q) &= \big((p + I) + F_{d-1}\big)\big((q + I) + F_{e-1}\big) \\ &= (pq + I) + F_{d+e-1} \qquad \text{(by (28))} \\ &= \varphi(pq). \end{aligned}$$

It also sends 1 to 1, so it is a homomorphism of graded $\mathbf{k}$-algebras.

The map φ is surjective. Indeed, let an element of F_d/F_{d-1} be represented by $q+I \in F_d$, where $q \in P_{\leq d}$. Write the polynomial $q \in P_{\leq d}$ as

$$q = q_0 + q_1 + \cdots + q_d \qquad (\text{with } q_i \in P_i).$$

Thus, $q - q_d = q_0 + q_1 + \cdots + q_{d-1} \in P_{\leq d-1}$, so that the class of $q+I$ in F_d/F_{d-1} is $\varphi(q_d)$. This shows that the class of $q+I$ in F_d/F_{d-1} belongs to the image of φ. By linearity, we thus conclude that φ is surjective.

We next compute the kernel of φ. Let $f = f_0 + f_1 + \cdots + f_d \in I$ be a nonzero polynomial, with $f_i \in P_i$ and $f_d \neq 0$. Thus, $\tau(f) = f_d$. But $f_0 + f_1 + \cdots + f_d \in I$ entails

$$f_d + I = -(f_0 + f_1 + \cdots + f_{d-1}) + I \in F_{d-1} \qquad \text{in } P/I.$$

Therefore $\varphi(f_d) = 0$. That is, $\varphi(\tau(f)) = 0$ (since $\tau(f) = f_d$), so that $\tau(f) \in \ker\varphi$. Since $\ker\varphi$ is an ideal, it follows that

$$\operatorname{in}_{\deg}(I) \subseteq \ker\varphi. \tag{31}$$

We shall next prove the reverse inclusion. First note that φ is graded. Thus, if $p = \sum_{d\geq 0} p_d \in \ker\varphi$, where $p_d \in P_d$, then the direct sum decomposition of the target gives $\varphi(p_d) = 0$ for every d. Hence it is enough to consider a homogeneous element $p \in P_d$ satisfying $\varphi(p) = 0$. We must show that $p \in \operatorname{in}_{\deg}(I)$. If $p = 0$, then there is nothing to prove. Otherwise, $\varphi(p) = 0$ means that $p + I \in F_{d-1}$. By the definition of F_{d-1}, there exists $r \in P_{\leq d-1}$ such that

$$p - r \in I.$$

The polynomial $p - r$ is nonzero, because p is a nonzero homogeneous polynomial of degree d, whereas r has degree at most $d-1$. Its leading homogeneous part $\tau(p-r)$ is therefore p. Hence

$$p = \tau(p-r) \in \operatorname{in}_{\deg}(I) \qquad (\text{since } p - r \in I).$$

This proves $\ker\varphi \subseteq \operatorname{in}_{\deg}(I)$. Combining this with (31), we find

$$\ker\varphi = \operatorname{in}_{\deg}(I).$$

So $\varphi : P \to \operatorname{gr}_F(P/I)$ is a surjective graded $\mathbf{k}$-algebra homomorphism with kernel $\ker\varphi = \operatorname{in}_{\deg}(I)$. The first isomorphism theorem thus yields a canonical graded $\mathbf{k}$-algebra isomorphism (29). Thus, for each d, we have an isomorphism

$$\left(P/\operatorname{in}_{\deg}(I)\right)_d \longrightarrow F_d/F_{d-1} = \frac{(P_{\leq d}+I)/I}{(P_{\leq d-1}+I)/I} \cong \frac{P_{\leq d}+I}{P_{\leq d-1}+I}$$

(by the standard quotient-of-a-quotient isomorphism), which proves the componentwise description (30). No choices were made in the construction of φ, which is why the isomorphism is canonical. $\square$

We will use one of the staples of group representation theory (see, e.g., [11, proof of Theorem 4.4.14]), which we prove here for the sake of completeness:

Lemma 15 (Maschke splitting lemma)**.** *Let G be a finite group, and assume that $|G|$ is invertible in $\mathbf{k}$. Let*

$$0 \longrightarrow U \longrightarrow V \xrightarrow{\pi} W \longrightarrow 0 \tag{32}$$

be a short exact sequence of $\mathbf{k}[G]$-modules. If (32) splits as a sequence of $\mathbf{k}$-modules, then it also splits as a sequence of $\mathbf{k}[G]$-modules. In particular, this holds whenever W is projective as a $\mathbf{k}$-module.

Proof. Assume that (32) splits as a sequence of $\mathbf{k}$-modules. Choose a $\mathbf{k}$-linear section $s : W \to V$ of π. Thus, $\pi s = \mathrm{id}$. Define a $\mathbf{k}$-linear map $\widetilde{s} : W \to V$ by

$$\widetilde{s}(w) = \frac{1}{|G|} \sum_{g \in G} g\, s(g^{-1} w) \qquad \text{for every } w \in W. \tag{33}$$

This map $\widetilde{s}$ is a section of π, since the G-equivariance of π gives

$$\pi\big(\widetilde{s}(w)\big) = \frac{1}{|G|} \sum_{g \in G} g\, \underbrace{\pi\big(s(g^{-1}w)\big)}_{\substack{= g^{-1}w \\ (\text{since } \pi s = \mathrm{id})}} = \frac{1}{|G|} \sum_{g \in G} \underbrace{g(g^{-1}w)}_{= w} = w$$

and thus $\pi\widetilde{s} = \mathrm{id}$. It is furthermore G-equivariant. Indeed, for $h \in G$ and $w \in W$, we have

$$\begin{aligned}
\widetilde{s}(hw) &= \frac{1}{|G|} \sum_{g \in G} g\, s(g^{-1} hw) \\
&= \frac{1}{|G|} \sum_{k \in G} hk\, s(\underbrace{(hk)^{-1} h}_{= k^{-1}} w) \qquad \text{(here, we have substituted } hk \text{ for } g) \\
&= \frac{1}{|G|} \sum_{k \in G} hk\, s(k^{-1} w) = h \cdot \underbrace{\frac{1}{|G|} \sum_{k \in G} k\, s(k^{-1} w)}_{= \widetilde{s}(w)} \\
&= h\widetilde{s}(w).
\end{aligned}$$

Thus $\widetilde{s}$ is a $\mathbf{k}[G]$-linear section of π, and therefore the sequence (32) splits as a sequence of $\mathbf{k}[G]$-modules.

The final assertion follows because a surjection onto a projective $\mathbf{k}$-module has a $\mathbf{k}$-linear section.

(This is the usual averaging argument behind Maschke's theorem; compare [11, Theorem 4.4.14].) □

Lemma 16 (Equivariance and splitting)**.** *Let a group G act on P by degree-preserving $\mathbf{k}$-algebra automorphisms, and let $I \subseteq P$ be a G-stable ideal.*

- ***(a)*** *The ideal $\mathrm{in}_{\deg}(I)$ and the degree filtration $0 = F_{-1} \subseteq F_0 \subseteq F_1 \subseteq \cdots$ from Lemma 14 are G-stable, and the canonical isomorphism (29) is G-equivariant.*

(b) *Assume, in addition, that G is finite, that $|G|$ is invertible in $\mathbf{k}$, that the filtration of P/I stabilizes (i.e., we have $F_D = P/I$ for some $D \in \mathbb{N}$), and that every $\mathbf{k}$-module F_d/F_{d-1} is projective. Then there is a (generally noncanonical) isomorphism of ungraded $\mathbf{k}[G]$-modules*

$$P/I \cong \operatorname{gr}_F(P/I). \tag{34}$$

(c) *The projectivity hypothesis from part* ***(b)*** *(i.e., the assumption that every $\mathbf{k}$-module F_d/F_{d-1} is projective) holds automatically if the associated graded algebra $\operatorname{gr}_F(P/I)$ has a graded $\mathbf{k}$-basis (i.e., a $\mathbf{k}$-basis consisting of homogeneous elements).*

Proof. **(a)** For $g \in G$ and $0 \neq f \in I$, degree preservation gives $\tau(gf) = g\tau(f)$. Hence $\operatorname{in}_{\deg}(I)$ is G-stable. That the filtration $0 = F_{-1} \subseteq F_0 \subseteq F_1 \subseteq \cdots$ is G-stable is even more obvious (since $P_{\leq d}$ and I are G-stable). The map φ in the proof of Lemma 14 is defined only from the grading, the quotient map, and the induced filtration, all of which are G-equivariant. Thus (29) is G-equivariant.

(b) Since the filtration stabilizes, there exists a large enough $D \in \mathbb{N}$ such that $F_D = P/I$. Consider this D. Of course, this entails that $F_d = P/I$ for all $d \geq D$; therefore, all successive quotients F_d/F_{d-1} with $d > D$ are zero.

For every d, the projectivity of F_d/F_{d-1} gives a $\mathbf{k}$-linear splitting of the short exact sequence

$$0 \longrightarrow F_{d-1} \longrightarrow F_d \longrightarrow F_d/F_{d-1} \longrightarrow 0.$$

Lemma 15 upgrades this to a $\mathbf{k}[G]$-linear splitting. Thus, we can choose a G-stable complement $L_d \subseteq F_d$ such that

$$F_d = F_{d-1} \oplus L_d \qquad \text{and therefore} \qquad L_d \cong F_d/F_{d-1}$$

as $\mathbf{k}[G]$-modules. Choose such L_d for each $d \geq 0$; note that all $d > D$ will satisfy $L_d = 0$ (since F_d/F_{d-1} is zero).

Now, successively applying the equalities $F_d = F_{d-1} \oplus L_d$, we see that each $k \geq 0$ satisfies

$$\begin{aligned} F_k &= \underbrace{F_{k-1}}_{=F_{k-2}\oplus L_{k-1}} \oplus L_k = \underbrace{F_{k-2}}_{=F_{k-3}\oplus L_{k-2}} \oplus L_{k-1} \oplus L_k \\ &= F_{k-3} \oplus L_{k-2} \oplus L_{k-1} \oplus L_k = \cdots = \underbrace{F_{-1}}_{=0} \oplus L_0 \oplus L_1 \oplus \cdots \oplus L_k \\ &= L_0 \oplus L_1 \oplus \cdots \oplus L_k = \bigoplus_{d=0}^{k} L_d. \end{aligned}$$

Applying this to $k = D$, we obtain an (ungraded) $\mathbf{k}[G]$-module isomorphism

$$F_D = \bigoplus_{d=0}^{D} \underbrace{L_d}_{\cong F_d/F_{d-1}} \cong \bigoplus_{d=0}^{D} F_d/F_{d-1} = \operatorname{gr}_F(P/I).$$

(since all successive quotients F_d/F_{d-1} with $d > D$ are zero). In view of $F_D = P/I$, this yields precisely (34).

(c) If $\operatorname{gr}_F(P/I)$ has a graded $\mathbf{k}$-basis, then each of its graded components F_d/F_{d-1} is a free $\mathbf{k}$-module (just take the appropriate subset of the basis of $\operatorname{gr}_F(P/I)$), and therefore is projective. $\square$

We shall now construct specific ideals I to apply the above results to. In the rest of this section, we shall really use the assumption that $1_{\mathbf{k}} \neq 0$. Of course, Theorem 2 **(c)** is trivial if $1_{\mathbf{k}} = 0$ (since any two modules over a trivial ring are isomorphic).

The symmetric group $\mathfrak{S}_n$ acts on $\mathbf{k}^n$ by

$$\sigma \cdot (b_1, b_2, \ldots, b_n) = (b_{\sigma^{-1}(1)}, b_{\sigma^{-1}(2)}, \ldots, b_{\sigma^{-1}(n)}).$$

This action is compatible with the action on P: that is,

$$(\sigma f)(\sigma \cdot v) = f(v) \qquad \text{for any } \sigma \in \mathfrak{S}_n,\ f \in P \text{ and } v \in \mathbf{k}^n$$

(where polynomials in P are evaluated at points in $\mathbf{k}^n$ in the obvious fashion).

Definition 17. *A finite subset $Y \subseteq \mathbf{k}^n$ will be called* strongly discrete *if, for any two distinct points*

$$y = (y_1, y_2, \ldots, y_n) \quad \text{and} \quad z = (z_1, z_2, \ldots, z_n)$$

of Y, at least one coordinate difference $y_i - z_i$ is a unit of $\mathbf{k}$.

Example 18. *Assume that $n!$ is invertible in $\mathbf{k}$. For any integer u, let $u_{\mathbf{k}}$ denote the image of u under the canonical ring homomorphism $\mathbb{Z} \to \mathbf{k}$ (that is, the element $u \cdot 1_{\mathbf{k}}$ of $\mathbf{k}$). Then, the pairwise differences of the n elements $1_{\mathbf{k}}, 2_{\mathbf{k}}, \ldots, n_{\mathbf{k}}$ are units of $\mathbf{k}$. Indeed, if $i < j$ are any two integers in $[n]$, then $j - i \in [n-1] \subseteq [n]$ and therefore $j - i \mid n!$, so that $j - i$ is invertible in $\mathbf{k}$ (since $n!$ is invertible in $\mathbf{k}$); in other words, $j_{\mathbf{k}} - i_{\mathbf{k}}$ is a unit of $\mathbf{k}$.*

Thus, the finite subset $\{1_{\mathbf{k}}, 2_{\mathbf{k}}, \ldots, n_{\mathbf{k}}\}^n \subseteq \mathbf{k}^n$ (which consists of all points in $\mathbf{k}^n$ whose all coordinates belong to $\{1_{\mathbf{k}}, 2_{\mathbf{k}}, \ldots, n_{\mathbf{k}}\}$) is strongly discrete: Any two distinct points in this set differ in at least one coordinate, and thus (by the preceding paragraph) the difference of these respective coordinates is a unit of $\mathbf{k}$.

If Y is a finite set, let $\mathbf{k}^Y$ denote the $\mathbf{k}$-algebra of all functions $Y \to \mathbf{k}$, with pointwise addition and multiplication.

Lemma 19. *Let Y be a finite strongly discrete subset of $\mathbf{k}^n$, and define the ideal*

$$I(Y) := \{p \in P \mid p(y) = 0 \text{ for every } y \in Y\}$$

of P (called the vanishing ideal *of Y). Then:*

(a) *Evaluation induces a canonical $\mathbf{k}$-algebra isomorphism*

$$\operatorname{ev}_Y : P/I(Y) \xrightarrow{\sim} \mathbf{k}^Y, \qquad p + I(Y) \longmapsto (y \longmapsto p(y)). \tag{35}$$

(b) *If Y is $\mathfrak{S}_n$-stable, then the isomorphism (35) is $\mathfrak{S}_n$-equivariant, where $\mathfrak{S}_n$ acts on $\mathbf{k}^Y$ by the rule*

$$(\sigma\varphi)(y) = \varphi(\sigma^{-1} \cdot y) \qquad \text{for all } \sigma \in \mathfrak{S}_n,\ \varphi \in \mathbf{k}^Y \text{ and } y \in Y.$$

Thus it is an isomorphism of $\mathbf{k}$-algebras and of $\mathbf{k}[\mathfrak{S}_n]$-modules.

Proof. For each point $y = (y_1, y_2, \ldots, y_n) \in Y$, define the ideal

$$\mathfrak{m}_y = (x_1 - y_1)P + (x_2 - y_2)P + \cdots + (x_n - y_n)P$$

of P. Evaluation at y is a surjective $\mathbf{k}$-algebra homomorphism $P \to \mathbf{k}$ with kernel $\mathfrak{m}_y$ (by Lemma 13). Hence, by the first isomorphism theorem, we have a $\mathbf{k}$-algebra isomorphism

$$P/\mathfrak{m}_y \xrightarrow{\cong} \mathbf{k}, \tag{36}$$

which sends each $p + \mathfrak{m}_y$ to $p(y)$.

Moreover, by the definition of $I(Y)$, we have

$$I(Y) = \bigcap_{y \in Y} \mathfrak{m}_y. \tag{37}$$

The ideals $\mathfrak{m}_y$ for $y \in Y$ are pairwise comaximal. Indeed, if $y \neq z$, then strong discreteness of Y gives an i for which $u := y_i - z_i$ is a unit, and thus we have

$$1 = u^{-1}(y_i - z_i) = \underbrace{-u^{-1}(x_i - y_i)}_{\in \mathfrak{m}_y} + \underbrace{u^{-1}(x_i - z_i)}_{\in \mathfrak{m}_z} \in \mathfrak{m}_y + \mathfrak{m}_z,$$

which shows that $\mathfrak{m}_y$ and $\mathfrak{m}_z$ are comaximal. The Chinese remainder theorem thus gives $P/\bigcap_{y \in Y} \mathfrak{m}_y \cong \prod_{y \in Y} P/\mathfrak{m}_y$ as $\mathbf{k}$-algebras (and even as P-algebras). In view of (37), this rewrites as

$$P/I(Y) \cong \prod_{y \in Y} \underbrace{P/\mathfrak{m}_y}_{\substack{\cong \mathbf{k} \\ \text{(by (36))}}} \cong \prod_{y \in Y} \mathbf{k} = \mathbf{k}^Y \qquad \text{as } \mathbf{k}\text{-algebras.}$$

This is precisely the evaluation map in (35). Thus, **(a)** is proved.

(b) Assume that Y is $\mathfrak{S}_n$-stable. Let $\sigma \in \mathfrak{S}_n$ and $p \in P$. Then, each $y \in Y$ satisfies

$$\begin{aligned} \big(\sigma \operatorname{ev}_Y(p + I(Y))\big)(y) &= \big(\operatorname{ev}_Y(p + I(Y))\big)(\sigma^{-1} \cdot y) \\ &= p(\sigma^{-1} \cdot y) = (\sigma p)(y) = \big(\operatorname{ev}_Y(\sigma p + I(Y))\big)(y). \end{aligned}$$

In other words, $\sigma \operatorname{ev}_Y(p + I(Y)) = \operatorname{ev}_Y(\sigma p + I(Y))$. This shows that the map ev_Y is $\mathfrak{S}_n$-equivariant (since $\sigma p + I(Y) = \sigma(p + I(Y))$). Thus, **(b)** is proved. □

Proposition 20. *Assume that $n!$ is invertible in $\mathbf{k}$. Then the coinvariant algebra $C = P/J$ is isomorphic, as an ungraded $\mathbf{k}[\mathfrak{S}_n]$-module, to the regular module $\mathbf{k}[\mathfrak{S}_n]$.*

Proof. Let $1_\mathbf{k}, 2_\mathbf{k}, \ldots, n_\mathbf{k}$ be as in Example 18. Define a point

$$v := (1_\mathbf{k}, 2_\mathbf{k}, \ldots, n_\mathbf{k}) \in \mathbf{k}^n \qquad \text{and its } \mathfrak{S}_n\text{-orbit} \qquad X := \mathfrak{S}_n \cdot v.$$

The elements of X are the $n!$ points in $\mathbf{k}^n$ obtained from v by permuting its coordinates. Recall from Example 18 that the pairwise differences of the n elements $1_\mathbf{k}, 2_\mathbf{k}, \ldots, n_\mathbf{k}$ are units of $\mathbf{k}$; in particular, these n elements $1_\mathbf{k}, 2_\mathbf{k}, \ldots, n_\mathbf{k}$ are distinct (since $1_\mathbf{k} \neq 0$ entails that all units of $\mathbf{k}$ are nonzero). Hence, permuting the coordinates of the vector v leads to $n!$

distinct vectors. In other words, X is an $n!$-element set, and is an $\mathfrak{S}_n$-torsor (i.e., isomorphic to the regular $\mathfrak{S}_n$-set $\mathfrak{S}_n$ as an $\mathfrak{S}_n$-set). Moreover, X is strongly discrete (since the pairwise differences of the n elements $1_{\mathbf{k}}, 2_{\mathbf{k}}, \ldots, n_{\mathbf{k}}$ are units of $\mathbf{k}$). Lemma 19 **(a)** (applied to $Y = X$) therefore gives a $\mathbf{k}$-algebra isomorphism

$$P/I(X) \cong \mathbf{k}^X. \tag{38}$$

Moreover, Lemma 19 **(b)** (applied to $Y = X$) shows that this isomorphism is $\mathfrak{S}_n$-equivariant (since X is $\mathfrak{S}_n$-stable). Thus, it is an isomorphism of $\mathbf{k}[\mathfrak{S}_n]$-modules.

For $x \in X$, let $\delta_x \in \mathbf{k}^X$ be its indicator function (sending x to 1 and sending all other elements of X to 0). The functions $(\delta_x)_{x \in X}$ form a $\mathbf{k}$-basis of $\mathbf{k}^X$, and satisfy $\sigma \delta_x = \delta_{\sigma \cdot x}$ for all $x \in X$ and $\sigma \in \mathfrak{S}_n$. Since X is an $\mathfrak{S}_n$-torsor, the map

$$\mathbf{k}[\mathfrak{S}_n] \longrightarrow \mathbf{k}^X, \qquad \sigma \longmapsto \delta_{\sigma \cdot v} \tag{39}$$

is an isomorphism of $\mathbf{k}[\mathfrak{S}_n]$-modules.

Set

$$\begin{aligned} c_i &:= e_i(v) \in \mathbf{k} \qquad \text{for all } i \in [n], \qquad \text{and} \\ K &:= (e_1 - c_1)P + (e_2 - c_2)P + \cdots + (e_n - c_n)P. \end{aligned}$$

The ideal K satisfies

$$K \subseteq I(X).$$

(Indeed, for each $i \in [n]$, we have $e_i(x) = e_i(v)$ for each $x \in X$, because the polynomial e_i is symmetric (and x is obtained from v by permuting the coordinates). That is, $e_i(x) = e_i(v) = c_i$ for each $x \in X$; in other words, the polynomial $e_i - c_i$ vanishes on x. Since this holds for each $x \in X$, we thus obtain $e_i - c_i \in I(X)$. Since this holds for each $i \in [n]$, this shows that all the n generators of the ideal K belong to $I(X)$, and thus $K \subseteq I(X)$ follows.)

We next identify P/K explicitly. Evaluation at v restricts to a surjective $\mathbf{k}$-algebra homomorphism

$$\epsilon_v : \Lambda \longrightarrow \mathbf{k}, \qquad f \longmapsto f(v),$$

whose kernel is

$$\ker \epsilon_v = (e_1 - c_1)\Lambda + (e_2 - c_2)\Lambda + \cdots + (e_n - c_n)\Lambda.$$

(Indeed, if we identify Λ with the polynomial ring $\mathbf{k}[t_1, t_2, \ldots, t_n]$ using the isomorphism

$$\mathbf{k}[t_1, t_2, \ldots, t_n] \xrightarrow{\sim} \Lambda, \qquad t_i \longmapsto e_i,$$

then this map is simply evaluation at $(c_1, c_2, \ldots, c_n)$, and its kernel is therefore the ideal $(t_1 - c_1)\mathbf{k}[t_1, t_2, \ldots, t_n] + (t_2 - c_2)\mathbf{k}[t_1, t_2, \ldots, t_n] + \cdots + (t_n - c_n)\mathbf{k}[t_1, t_2, \ldots, t_n]$, by Lemma 13.) Thus,

$$\begin{aligned} (\ker \epsilon_v) P &= ((e_1 - c_1)\Lambda + (e_2 - c_2)\Lambda + \cdots + (e_n - c_n)\Lambda) P \\ &= (e_1 - c_1)P + (e_2 - c_2)P + \cdots + (e_n - c_n)P \\ &= K. \end{aligned}$$

Let $\mathcal{A}$ be the set of all $n!$ Artin monomials. Corollary 11 shows that $\mathcal{A}$ is a Λ-basis of P. This gives the graded direct-sum decomposition

$$P = \bigoplus_{m \in \mathcal{A}} \Lambda m. \tag{40}$$

Since $K = (\ker \epsilon_v) P$, this decomposition also gives

$$K = \bigoplus_{m \in \mathcal{A}} (\ker \epsilon_v) m. \tag{41}$$

Indeed, multiplying the decomposition (40) by the ideal $\ker \epsilon_v$ yields

$$(\ker \epsilon_v) P = (\ker \epsilon_v) \left(\bigoplus_{m \in \mathcal{A}} \Lambda m \right) = \sum_{m \in \mathcal{A}} \underbrace{(\ker \epsilon_v) \Lambda}_{= \ker \epsilon_v} m = \sum_{m \in \mathcal{A}} (\ker \epsilon_v) m,$$

and this sum is direct because it is contained in the direct sum $\bigoplus_{m \in \mathcal{A}} \Lambda m$.

Now, let H be the $\mathbf{k}$-submodule of P spanned by the Artin monomials. Thus, $\mathcal{A}$ is a basis of H. Moreover, $\Lambda = \mathbf{k} \oplus \ker \epsilon_v$ (where $\mathbf{k}$ denotes the span of $1 \in \Lambda$), since $\epsilon_v : \Lambda \to \mathbf{k}$ is a $\mathbf{k}$-algebra homomorphism that sends $1 \in \Lambda$ to $1 \in \mathbf{k}$ (so that each $f \in \Lambda$ satisfies $f - \epsilon_v(f) \cdot 1 \in \ker \epsilon_v$). Hence, each $m \in \mathcal{A}$ satisfies

$$\Lambda m = (\mathbf{k} \oplus \ker \epsilon_v)\, m = \mathbf{k} m \oplus (\ker \epsilon_v)\, m.$$

Indeed, multiplication by the monomial m is injective on P (it merely shifts the exponent vector of every monomial), so it preserves the directness of the decomposition $\Lambda = \mathbf{k} \oplus \ker \epsilon_v$. Therefore, (40) becomes

$$P = \bigoplus_{m \in \mathcal{A}} \underbrace{\Lambda m}_{= \mathbf{k} m \oplus (\ker \epsilon_v) m} = \bigoplus_{m \in \mathcal{A}} (\mathbf{k} m \oplus (\ker \epsilon_v)\, m) = \underbrace{\bigoplus_{m \in \mathcal{A}} \mathbf{k} m}_{= \operatorname{span} \mathcal{A} = H} \oplus \underbrace{\bigoplus_{m \in \mathcal{A}} (\ker \epsilon_v)\, m}_{\substack{= K \\ \text{(by (41))}}} = H \oplus K.$$

Consequently, the canonical projection $P \to P/K$ becomes an isomorphism when restricted to H. Thus the residue classes of the Artin monomials form a $\mathbf{k}$-basis of P/K (since the Artin monomials themselves form a $\mathbf{k}$-basis of H). In other words, the family $(\overline{m})_{m \in \mathcal{A}}$ is a basis of P/K, where $\overline{m}$ denotes the residue class $m + K$ of a given $m \in \mathcal{A}$ in P/K.

The inclusion $K \subseteq I(X)$ gives a $\mathbf{k}$-linear surjection

$$P/K \twoheadrightarrow P/I(X) \cong \mathbf{k}^X.$$

The source of this surjection has the $n!$ residue classes of Artin monomials as a basis (as we have shown in the above paragraph), while the target has the $n!$ indicator functions δ_x as a basis. Hence Lemma 9 shows that this surjection is an isomorphism. Thus

$$K = I(X). \tag{42}$$

We now consider the degree filtration of $P/I(X) = P/K$, that is, the filtration $0 = F_{-1}^{(P/K)} \subseteq F_0^{(P/K)} \subseteq F_1^{(P/K)} \subseteq \cdots$ defined by

$$F_d^{(P/K)} := \frac{P_{\leq d} + K}{K} \qquad \text{for every } d \geq -1.$$

This is the filtration $0 = F_{-1} \subseteq F_0 \subseteq F_1 \subseteq \cdots$ from Lemma 14, but constructed for P/K instead of P/I. Thus, $\operatorname{gr}_F(P/K) = \bigoplus_{d\geq 0} F_d^{(P/K)}/F_{d-1}^{(P/K)}$. Note that $P_{\leq -1} = 0$.

For every $d \geq 0$, we claim that

$$\text{the } \mathbf{k}\text{-module } F_d^{(P/K)} \text{ has basis } \left(\overline{m}\right)_{m\in\mathcal{A};\ \deg m\leq d}, \tag{43}$$

where $\overline{m}$ denotes the residue class $m + K$ of $m \in P$ modulo K.

(*Proof:* The residue classes $\overline{m}$ for $m \in \mathcal{A}$ satisfying $\deg m \leq d$ clearly belong to $F_d^{(P/K)}$, since the corresponding m's belong to $P_{\leq d}$. Moreover, the family $\left(\overline{m}\right)_{m\in\mathcal{A};\ \deg m\leq d}$ is a subfamily of the basis $\left(\overline{m}\right)_{m\in\mathcal{A}}$ of P/K, and thus is $\mathbf{k}$-linearly independent. It remains to show that this family spans $F_d^{(P/K)}$. To prove this, we let $\overline{p} = p + K$ be an arbitrary element of $F_d^{(P/K)}$, with $p \in P_{\leq d}$. We must show that $\overline{p}$ is a $\mathbf{k}$-linear combination of the family $\left(\overline{m}\right)_{m\in\mathcal{A};\ \deg m\leq d}$.

By decomposing $p \in P_{\leq d}$ into its homogeneous components, it is enough to treat the case in which p is homogeneous of some degree at most d; replacing d by this degree, we may assume that p is homogeneous of degree d. We can write p uniquely as

$$p = \sum_{m\in\mathcal{A}} \lambda_m m \qquad \text{with } \lambda_m \in \Lambda \tag{44}$$

(since $\mathcal{A}$ is a basis of the Λ-module P). By projecting this equality onto the d-th graded component of P, we obtain

$$p = \sum_{\substack{m\in\mathcal{A};\\ \deg m\leq d}} \widetilde{\lambda}_m m, \tag{45}$$

where $\widetilde{\lambda}_m$ is the $(d - \deg m)$-th homogeneous component of λ_m (since each $m \in \mathcal{A}$ is homogeneous, and since p is homogeneous of degree d). Projecting this equality onto P/K yields

$$\overline{p} = \sum_{\substack{m\in\mathcal{A};\\ \deg m\leq d}} \underbrace{\overline{\widetilde{\lambda}_m}}_{\substack{=\epsilon_v\left(\widetilde{\lambda}_m\right)\\ \left(\text{since } \widetilde{\lambda}_m - \epsilon_v\left(\widetilde{\lambda}_m\right) \in \ker\epsilon_v \subseteq (\ker\epsilon_v)P = K \right.\\ \left. \text{and thus } \widetilde{\lambda}_m \equiv \epsilon_v\left(\widetilde{\lambda}_m\right) \bmod K\right)}} \qquad \overline{m} = \sum_{\substack{m\in\mathcal{A};\\ \deg m\leq d}} \epsilon_v\left(\widetilde{\lambda}_m\right)\overline{m},$$

which is clearly a $\mathbf{k}$-linear combination of the family $\left(\overline{m}\right)_{m\in\mathcal{A};\ \deg m\leq d}$, just as we desired to show. Thus, (43) is proved.)

Consequently, for every $d \geq 0$,

$$\text{the } \mathbf{k}\text{-module } F_d^{(P/K)}/F_{d-1}^{(P/K)} \text{ has basis } \left(m^*\right)_{m\in\mathcal{A};\ \deg m=d}, \tag{46}$$

where m^* is the residue class of $\overline{m} \in F_d^{(P/K)}$ in $F_d^{(P/K)}/F_{d-1}^{(P/K)}$.

(*Proof:* The $\mathbf{k}$-module $F_d^{(P/K)}$ has basis $\left(\overline{m}\right)_{m\in\mathcal{A};\ \deg m\leq d}$ (by (43)), whereas the $\mathbf{k}$-module $F_{d-1}^{(P/K)}$ has basis $\left(\overline{m}\right)_{m\in\mathcal{A};\ \deg m\leq d-1}$ (again by (43)). The latter basis is clearly a subfamily of the former basis. Thus, a basis of the quotient $\mathbf{k}$-module $F_d^{(P/K)}/F_{d-1}^{(P/K)}$ can be obtained by listing the (residue classes of the) elements of the former basis that don't belong to the latter basis. This means listing the m^* for all $m\in\mathcal{A}$ that satisfy $\deg m\leq d$ but don't satisfy $\deg m\leq d-1$ – that is, that satisfy $\deg m=d$. Thus, (46) is proved.)

Note that if d is larger than the degrees of all Artin monomials $m\in\mathcal{A}$, then the basis $\left(m^*\right)_{m\in\mathcal{A};\ \deg m=d}$ in (46) is empty, so that (46) shows that $F_d^{(P/K)}/F_{d-1}^{(P/K)}=0$, that is, $F_d^{(P/K)}=F_{d-1}^{(P/K)}$. This shows that the filtration $0=F_{-1}^{(P/K)}\subseteq F_0^{(P/K)}\subseteq F_1^{(P/K)}\subseteq\cdots$ of P/K stabilizes.

Taking the direct sum of (46) over all $d\geq 0$, we conclude that the associated graded algebra

$$\operatorname{gr}_F(P/K)=\bigoplus_{d\geq 0}F_d^{(P/K)}/F_{d-1}^{(P/K)}$$

has the graded $\mathbf{k}$-basis

$$\left(m^*\right)_{m\in\mathcal{A}}. \tag{47}$$

For each $i\in[n]$, we have $\tau\left(e_i-c_i\right)=e_i$ (since $e_i\in P_i$ while $c_i\in\mathbf{k}=P_0$), so that $e_i=\tau\left(e_i-c_i\right)\in\operatorname{in}_{\deg}\left(I\left(X\right)\right)$ (since $e_i-c_i\in K=I\left(X\right)$). Therefore, by (3), we obtain

$$J\subseteq\operatorname{in}_{\deg}(I(X)).$$

Thus we obtain a canonical surjective graded homomorphism

$$C=P/J\twoheadrightarrow P/\operatorname{in}_{\deg}(I(X))\xrightarrow{\sim}\operatorname{gr}_F(P/I(X)) \tag{48}$$

by Lemma 14 (applied to $I=I\left(X\right)$); moreover, this homomorphism is $\mathfrak{S}_n$-equivariant by Lemma 16 **(a)** (since the ideal $I\left(X\right)$ is $\mathfrak{S}_n$-stable). This homomorphism sends the residue class $m+J$ of each Artin monomial m to $m^*\in\operatorname{gr}_F(P/I(X))$. Proposition 7 says that the former classes are a $\mathbf{k}$-basis of C, whereas our observation (47) says that the latter classes are a $\mathbf{k}$-basis of $\operatorname{gr}_F(P/K)=\operatorname{gr}_F(P/I(X))$ (since $K=I\left(X\right)$). Hence, (48) is an isomorphism (since a $\mathbf{k}$-linear map sending a basis to a basis must be an isomorphism). In particular, the first arrow $P/J\twoheadrightarrow P/\operatorname{in}_{\deg}(I(X))$ in (48) must be injective, so that

$$J=\operatorname{in}_{\deg}(I(X)). \tag{49}$$

Also, (48) is an $\mathfrak{S}_n$-equivariant $\mathbf{k}$-module isomorphism, hence a $\mathbf{k}\left[\mathfrak{S}_n\right]$-module isomorphism.

The filtration $0=F_{-1}^{(P/K)}\subseteq F_0^{(P/K)}\subseteq F_1^{(P/K)}\subseteq\cdots$ stabilizes (as we saw above). Moreover, the basis (47) is graded, so Lemma 16 **(c)** (applied to $I=I(X)=K$) shows that every successive quotient $F_d^{(P/K)}/F_{d-1}^{(P/K)}$ is projective. Hence Lemma 16 **(b)** (applied to $I=I(X)=K$) gives an isomorphism of ungraded $\mathbf{k}\left[\mathfrak{S}_n\right]$-modules

$$P/I(X)\cong\operatorname{gr}_F(P/I(X)) \tag{50}$$

(since $|\mathfrak{S}_n| = n!$ is invertible in $\mathbf{k}$). Now, we have the following chain of isomorphisms of ungraded $\mathbf{k}[\mathfrak{S}_n]$-modules:

$$\begin{aligned} C &\cong \mathrm{gr}_F(P/I(X)) && \text{(by (48))} \\ &\cong P/I(X) && \text{(by (50))} \\ &\cong \mathbf{k}^X && \text{(by (38))} \\ &\cong \mathbf{k}[\mathfrak{S}_n] && \text{(by (39))}. \end{aligned}$$

This proves Proposition 20, i.e., Theorem 2 **(c)**. □

Thus, we have recovered the classical statement recorded by Haiman that the coinvariant algebra affords the regular representation [12, Section 1.5]. Over a field of characteristic 0, this result is due to Chevalley [4, last sentence of Theorem (B)] (in the more general setting of a Coxeter group).

Remark 21. *The preceding proof follows the orbit-harmonics strategy of Oh and Rhoades [15, Section 1] at two distinct points: it passes from the coordinate ring of the finite orbit X to its associated graded algebra, and it uses the fact that the function module of a free orbit is the regular module. The proof concerns the coinvariant algebra only as an* ungraded *$\mathfrak{S}_n$-module. In graded refinements of orbit harmonics, special point sets involving roots of unity carry an additional cyclic symmetry whose eigenvalues record the grading; no such refinement is needed here.*

Remark 22. *The part of the construction preceding the equivariant splitting requires less than the invertibility of $n!$. Namely, suppose that $a_1, a_2, \ldots, a_n \in \mathbf{k}$ have pairwise invertible differences, and let*

$$v = (a_1, a_2, \ldots, a_n) \in \mathbf{k}^n, \qquad X = \mathfrak{S}_n \cdot v.$$

Then X is a strongly discrete $\mathfrak{S}_n$-torsor, and the same argument gives the canonical graded isomorphism

$$C \cong \mathrm{gr}_F(P/I(X)).$$

The invertibility of $n!$ is used only to average the splittings that identify the filtered module $P/I(X)$ with its associated graded module equivariantly (as we did in the proof of Lemma 15).

6 Proof of the equivariant normal-basis statement

We are now ready to prove the last part of Theorem 2: part **(d)**, about the $\Lambda[\mathfrak{S}_n]$-module structure of P.

*Proof of Theorem 2 **(d)**.* Assume that $n!$ is invertible in $\mathbf{k}$. For each $d \geq 0$, the $\mathbf{k}$-module C_d is free (since Proposition 7 shows that C has a graded basis), and thus the quotient map

$$P_d \twoheadrightarrow C_d$$

has a $\mathbf{k}$-linear section. That is, the short exact sequence

$$0 \longrightarrow J_d \longrightarrow P_d \longrightarrow C_d \longrightarrow 0$$

of $\mathbf{k}[\mathfrak{S}_n]$-modules (where $J_d \to P_d$ is the inclusion and $P_d \to C_d$ the projection) splits as a sequence of $\mathbf{k}$-modules. Since $|\mathfrak{S}_n| = n!$ is invertible in $\mathbf{k}$, this sequence thus also splits as a sequence of $\mathbf{k}[\mathfrak{S}_n]$-modules by Lemma 15. That is, the quotient map $P_d \twoheadrightarrow C_d$ has a $\mathbf{k}[\mathfrak{S}_n]$-linear section. Let $H_d \subseteq P_d$ be the image of this section, and set

$$H = \bigoplus_{d \geq 0} H_d.$$

Then H is a graded $\mathbf{k}[\mathfrak{S}_n]$-submodule of P, and the quotient map $P \to C$ restricts to an isomorphism

$$H \xrightarrow{\sim} C$$

of graded $\mathbf{k}[\mathfrak{S}_n]$-modules.

Forgetting the gradings in this isomorphism gives an isomorphism $H \xrightarrow{\sim} C$ of ungraded $\mathbf{k}[\mathfrak{S}_n]$-modules. Proposition 20 gives an isomorphism $\mathbf{k}[\mathfrak{S}_n] \xrightarrow{\sim} C$ of such modules. Composing the latter isomorphism with the inverse of $H \xrightarrow{\sim} C$, we obtain an isomorphism $\mathbf{k}[\mathfrak{S}_n] \xrightarrow{\sim} H$. So choose a $\mathbf{k}[\mathfrak{S}_n]$-module isomorphism

$$\theta : \mathbf{k}[\mathfrak{S}_n] \xrightarrow{\sim} H,$$

and put $f := \theta(1)$. For every $\sigma \in \mathfrak{S}_n$, we have $\sigma = \sigma \cdot 1$ and thus

$$\begin{aligned} \theta(\sigma) &= \theta(\sigma \cdot 1) = \sigma \cdot \theta(1) \qquad (\text{since } \theta \text{ is } \mathfrak{S}_n\text{-equivariant}) \\ &= \sigma(f) \qquad (\text{since } \theta(1) = f). \end{aligned} \tag{51}$$

Thus the family $(\sigma(f))_{\sigma \in \mathfrak{S}_n}$ is the image of the basis $(\sigma)_{\sigma \in \mathfrak{S}_n}$ of $\mathbf{k}[\mathfrak{S}_n]$ under the isomorphism θ. Hence, the former family $(\sigma(f))_{\sigma \in \mathfrak{S}_n}$ is a $\mathbf{k}$-basis of H (since a $\mathbf{k}$-module isomorphism sends bases to bases). Consequently, the family $(1 \otimes \sigma(f))_{\sigma \in \mathfrak{S}_n}$ is a Λ-basis of $\Lambda \otimes_{\mathbf{k}} H$.

But Proposition 10 **(a)** says that the multiplication map

$$m : \Lambda \otimes_{\mathbf{k}} H \xrightarrow{\sim} P, \qquad a \otimes h \longmapsto ah$$

is an isomorphism of graded Λ-modules. This isomorphism sends each $1 \otimes \sigma(f)$ to $\sigma(f)$. Hence the family $(\sigma(f))_{\sigma \in \mathfrak{S}_n}$ is a Λ-basis of P (since it is the image of the Λ-basis $(1 \otimes \sigma(f))_{\sigma \in \mathfrak{S}_n}$ of $\Lambda \otimes_{\mathbf{k}} H$ under this Λ-module isomorphism m).

Note that the Λ-module isomorphism m is also $\mathfrak{S}_n$-equivariant by Proposition 10 **(b)**, and thus is a $\Lambda[\mathfrak{S}_n]$-module isomorphism. Also, $\mathrm{id}_\Lambda \otimes \theta : \Lambda \otimes_{\mathbf{k}} \mathbf{k}[\mathfrak{S}_n] \to \Lambda \otimes_{\mathbf{k}} H$ is a $\Lambda[\mathfrak{S}_n]$-module isomorphism (since $\theta : \mathbf{k}[\mathfrak{S}_n] \to H$ is a $\mathbf{k}[\mathfrak{S}_n]$-module isomorphism), and there is a canonical $\Lambda[\mathfrak{S}_n]$-module isomorphism

$$\kappa : \Lambda \otimes_{\mathbf{k}} \mathbf{k}[\mathfrak{S}_n] \to \Lambda[\mathfrak{S}_n], \qquad a \otimes \sigma \mapsto a\sigma.$$

Composing the $\Lambda[\mathfrak{S}_n]$-module isomorphisms

$$\Lambda[\mathfrak{S}_n] \xrightarrow{\kappa^{-1}} \Lambda \otimes_{\mathbf{k}} \mathbf{k}[\mathfrak{S}_n] \xrightarrow{\mathrm{id}_\Lambda \otimes \theta} \Lambda \otimes_{\mathbf{k}} H \xrightarrow{m} P,$$

we thus obtain a $\Lambda[\mathfrak{S}_n]$-module isomorphism from $\Lambda[\mathfrak{S}_n]$ to P, which shows that $P \cong \Lambda[\mathfrak{S}_n]$ as $\Lambda[\mathfrak{S}_n]$-modules. Moreover, this composed isomorphism is easily seen to send each $a\sigma$ (with $a \in \Lambda$ and $\sigma \in \mathfrak{S}_n$) to $a\theta(\sigma) = a\sigma(f)$ (by (51)), and thus must send each $\sum_{\sigma \in \mathfrak{S}_n} a_\sigma \sigma$ (with $a_\sigma \in \Lambda$) to $\sum_{\sigma \in \mathfrak{S}_n} a_\sigma \sigma(f)$. So it is precisely the map Φ from (5). Thus the proof of Theorem 2 **(d)** is complete. $\square$

Remark 23 (The isomorphism is not graded)**.** *The element f in the above proof cannot be chosen homogeneous when $n \geq 2$. Indeed, if $\deg f = d$, then all $\sigma(f)$ have degree d, and the resulting isomorphism would imply*

$$\mathrm{Hilb}(P; q) = q^d n!\ \mathrm{Hilb}(\Lambda; q),$$

which is false. What is graded is the decomposition

$$P \cong \Lambda \otimes_{\mathbf{k}} H,$$

where H has the nontrivial coinvariant grading. Only after forgetting this grading is H the regular module.

Example 24. *Let $n = 2$ and assume that 2 is invertible in $\mathbf{k}$. Then*

$$\Lambda = \mathbf{k}\,[x_1 + x_2, x_1 x_2] \qquad \text{and} \qquad H = \mathrm{span}_{\mathbf{k}}\{1, x_1 - x_2\}.$$

For the transposition $s = (1\ 2)$, the element

$$f = 1 + (x_1 - x_2)$$

has orbit

$$f = 1 + (x_1 - x_2), \qquad s(f) = 1 - (x_1 - x_2),$$

which is a $\mathbf{k}$-basis of H and therefore a Λ-basis of P.

7 A modular counterexample

The invertibility hypothesis in Theorem 2 **(c)** and **(d)** cannot simply be omitted. For example, take $n = 2$ and $\mathbf{k} = \mathbb{F}_2$. Writing $s = (1\ 2)$, we have

$$C = \frac{\mathbf{k}\,[x_1, x_2]}{(x_1 + x_2)P + x_1 x_2 P} \cong \frac{\mathbf{k}\,[t]}{t^2 \mathbf{k}\,[t]}.$$

The relation $x_1 + x_2 = 0$ becomes $x_1 = x_2$, so s acts trivially on all of C. On the other hand, s does not act trivially on the regular module $\mathbf{k}\,[\mathfrak{S}_2]$: it interchanges the basis vectors 1 and s. Hence, C is not isomorphic to $\mathbf{k}\,[\mathfrak{S}_2]$ as $\mathbf{k}\,[\mathfrak{S}_2]$-modules, and Theorem 2 **(c)** fails.

Theorem 2 **(d)** fails as well in this generality. Indeed, tensoring a hypothetical $\Lambda\,[\mathfrak{S}_2]$-module isomorphism $P \cong \Lambda\,[\mathfrak{S}_2]$ over Λ with $\Lambda/\Lambda_+ \cong \mathbf{k}$ — or, equivalently, reducing modulo $\Lambda_+ P = e_1 P + e_2 P$ — would produce the impossible isomorphism $C \cong \mathbf{k}\,[\mathfrak{S}_2]$.

Notes on the origins of the proofs

The two field-valued ingredients underlying Theorem 2 are stated in Haiman's treatment of the ordinary coinvariant algebra [12, Section 1.5]: the coinvariant algebra affords the regular representation, and a homogeneous space of representatives freely generates the polynomial ring over the invariant subring. The proofs above formulate both statements over a commutative coefficient ring, under the hypotheses stated in Theorem 2.

The degeneration from a finite point locus to the quotient by leading homogeneous parts follows the orbit-harmonics framework of Oh and Rhoades [15, Section 1]; their Section 3.1 explains the reflection-group coinvariant case via a regular orbit. Our orbit

$$(1_{\mathbf{k}}, 2_{\mathbf{k}}, \ldots, n_{\mathbf{k}})$$

is chosen so that distinct orbit points are strongly discrete. The additional cyclic action used in graded refinements of orbit harmonics is not needed here. The associated-graded construction is also recorded by Reiner and Rhoades [16, Propositions 2.1 and 2.7]. Significant changes were necessary to make the proofs of **(c)** and **(d)** apply not only to fields of "good" characteristic, but to arbitrary commutative rings $\mathbf{k}$ in which $n!$ is invertible, as this level of generality rendered several linear-algebraic shortcuts inaccessible.

Our proof of Theorem 2 **(a)** imitates [17, proof of Theorem 1.2.7], but replaces the additional variables $y_1, y_2, \ldots, y_n$ by $0, 0, \ldots, 0$.

References

[1] George M. Bergman, *The diamond lemma for ring theory*, Advances in Mathematics **29** (1978), no. 2, 178–218.

[2] Emil Artin, *Galois theory*, lectures delivered at the University of Notre Dame, edited and supplemented by Arthur N. Milgram, Notre Dame Mathematical Lectures **2**, University of Notre Dame Press, 2nd edition, 6th printing 1971.

[3] Nicolas Bourbaki, *Algebra II: Chapters 4–7*, Springer 2003.

[4] Claude Chevalley, *Invariants of Finite Groups Generated by Reflections*, American Journal of Mathematics **77** (1955), No. 4, pp. 778–782.

[5] Willem de Graaf, *Computational Algebra*, lecture notes; see Chapter 1, especially Sections 1.1.6–1.1.7 and Theorem 1.1.33.
`https://degraaf.maths.unitn.it/algnotes/compalg.pdf`. See `https://www.cip.ifi.lmu.de/~grinberg/algebra/compalg-errata-v2.pdf` for unofficial errata.

[6] Sergey Fomin, Sergei Gelfand, Alexander Postnikov, *Quantum Schubert polynomials*, Journal of the American Mathematical Society **10**, number 3 (1997), pp. 565–596.

[7] Pierre-Yves Gaillard, Math StackExchange answer #4261642, "Basis for $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ over $\mathbb{Z}[e_1, e_2, \ldots, e_n]$."
`https://math.stackexchange.com/q/4261642`.

[8] Adriano M. Garsia, *Pebbles and Expansions in the Polynomial Ring*, 21 July 2002.
`http://www.math.ucsd.edu/~garsia/somepapers/fnewpebbles.pdf`

[9] GPT-5.5 and Darij Grinberg, *Splitting a Polynomial into Linear Factors after an Injective Ring Extension*, 19 July 2026.
`https://www.cip.ifi.lmu.de/~grinberg/algebra/factorpoly-gpt.pdf`

[10] Darij Grinberg, *t-unique reductions for Mészáros's subdivision algebra*, updated version of 16 June 2016.
https://www.cip.ifi.lmu.de/~grinberg/algebra/subdiv-v7.pdf

[11] Darij Grinberg, *An introduction to the symmetric group algebra*, arXiv:2507.20706v1.
https://arxiv.org/abs/2507.20706v1

[12] Mark D. Haiman, *Conjectures on the quotient ring by diagonal invariants*, J. Algebraic Combin. **3** (1994), no. 1, 17–76; see Section 1.5 for the classical one-set-of-variables case, https://math.berkeley.edu/~mhaiman/ftp/diagonal/diagonal.pdf.

[13] D. Laksov, A. Lascoux, P. Pragacz, and A. Thorup, *The LLPT Notes*, edited by A. Thorup, 1995–2018,
http://web.math.ku.dk/noter/filer/sympol.pdf.

[14] Ian G. Macdonald, *Notes on Schubert polynomials*, Laboratoire de combinatoire et d'informatique mathématique, Université du Québec à Montréal, 1991. https://lacim.uqam.ca/les-parutions/LACIM-Publications-Volume-06.pdf
See https://www.cip.ifi.lmu.de/~grinberg/algebra/mcd-schub-errata.pdf for errata.

[15] Jaeseong Oh and Brendon Rhoades, *Cyclic sieving and orbit harmonics*, Math. Z. **300** (2022), 639–660, doi:10.1007/s00209-021-02800-z.

[16] Victor Reiner and Brendon Rhoades, *Harmonics and graded Ehrhart theory*, preprint, arXiv:2407.06511v3 (2024); see Propositions 2.1 and 2.7, https://arxiv.org/abs/2407.06511v3.

[17] Bernd Sturmfels, *Algorithms in Invariant Theory*, 2nd edition, Springer 2008. See https://www.cip.ifi.lmu.de/~grinberg/algebra/sturmfels-ait-errata.pdf for unofficial errata.