On the Structure of a Polynomial Quotient Ring Involving Symmetric Polynomials

Christopher C. Mihelich

under the direction of
Alexandre Soloviev
Department of Mathematics
Massachusetts Institute of Technology

Research Science Institute
August 6, 1997
Abstract

In this paper we examine the structure of the quotient ring $\mathbb{Z}[x_1, \ldots, x_n]/I_n^k$, where $I_n^k$ denotes the ideal generated by all fundamental symmetric polynomials in $x_1^k, \ldots, x_n^k$. We provide linear bases for this ring and a formula for obtaining the coefficients of some terms in the expansion of a polynomial function in this ring, as well as an algorithm for determining these coefficients when closed-form formulae are inapplicable. The study of the structure of this ring in the cases $k = 1, 2$ has applications to the theory of Lie algebras.
1 Introduction

In the mathematical theory of the cohomology and quantum cohomology rings of the Lie algebras $A_n$ and $B_n$, it is useful to investigate properties of the polynomial ring quotient $R^k_n := \mathbb{Z}[x_1, \ldots, x_n]/I^k_n$, where $I^k_n$ is the ideal generated by the elementary symmetric polynomials in $x_1^k, \ldots, x_n^k$. The importance of this ring is twofold. First, the special cases $R^1_n$ and $R^2_n$ are known to be canonically isomorphic to the cohomology rings of Lie algebras of types $A_n$ and $B_n$ respectively, so that any theorem on the structure of $R^k_n$ illuminates the structure of these cohomology rings. Second, the rings $R^k_n$ are important to quantum cohomology because the expansions of polynomials in $R^k_n$ as linear combinations of elements of an appropriate basis may be used to obtain readily the quantizations of those polynomials, as has been shown in [1] for the case $k = 1$.

In this paper we shall develop proofs of two theorems about the ring $R^k_n$. Theorem 1 gives a thorough description of the structure of $R^k_n$,\footnote{The case $k = 1$ of these formulae is given in [1].} while Theorem 2 gives a formula for certain coefficients in the expansion of an element of $R^k_n$ as a linear combination of basis elements, as well as a simple algorithm which yields every coefficient. Our proofs will depend heavily on properties of certain polynomials and linear operators that we introduce in Sections 2, 3.1, and 3.3.
2 Preliminary definitions

Our approach to the study of $R_n^k$ will depend heavily on the properties of the linear operators $d_k$, $1 \leq k \leq n - 1$, on $\mathbb{Z}[x_1, \ldots, x_n]$ defined by the equations

$$s_k f(x_k, x_{k+1}) = f(x_{k+1}, x_k);$$

$$d_k f(x_k, x_{k+1}) = \frac{f - s_k f}{x_k - x_{k+1}}.$$

The operators $d$ satisfy the nil-Hecke relations $d_k d_{k+1} = d_{k+1} d_k d_{k+1}$ and $d_k^2 = 0$.

We further denote by $e_j^k = e_j^k(x_1, \ldots, x_n)$ the $j^\text{th}$ elementary symmetric polynomial\footnote{A reader unfamiliar with symmetric polynomials may consult Appendix D for definitions and examples.} in $x_1, \ldots, x_k$ and by $h_j^k = h_j^k(x_1, \ldots, x_n)$ the $j^\text{th}$ complete symmetric polynomial in $x_1, \ldots, x_k$; by convention we let $e_j^k = 0$ unless $0 \leq j \leq k$, and $h_j^k = 0$ unless $j, k \geq 0$. We have then the following elementary propositions, which are proven in Appendix A.

(i) The quadratic relation. We have $e_i^k e_j^k = \sum_{l \geq 0} e_{i-l}^k e_{j+l}^k - \sum_{l \geq 1} e_{i-l}^k e_{j+l}^k$ for any $i, j, k$.

(ii) $d_l f g = fd_l g + (s_l g)(d_l f)$ for any $f, g \in \mathbb{Z}[x_1, \ldots, x_n]$.

(iii) $d_l e_j^k = [k = l] e_{j-1}^{k-1}$ for any $j, k, l$.

(iv) $d_l h_j^k = [k = l] h_{j-1}^{k+1}$ for any $j, k, l$.

The function $[P]$ of a proposition $P$ denotes 1 if $P$ is true and 0 if $P$ is false.
3 The structure of the quotient $R^k_n$

We begin by describing the structure of the quotient ring $R^k_n$. Our investigations in this direction are summarized in

Theorem 1. (i) The quantities

$$x_1^{\epsilon_1} \ldots x_n^{\epsilon_{n-1}} x_i^k, \ldots, x_n^k, (0 \leq \epsilon_j \leq k - 1, 0 \leq i_j \leq j)$$

constitute a linear basis in $R^k_n$. In particular, the dimension of $R^k_n$ is $k^n n!$.

(ii) The monomials

$$x_1^{a_1} \ldots x_n^{a_n}, (0 \leq a_j \leq k(n-j+1) - 1)$$

constitute a linear basis in $R^k_n$.

(iii) A Groebner basis for $I^k_n$, with respect to the monomial order $x_1 < x_2 < \ldots < x_n$, is given by

$$h_j^{n+1-j}(x_1^k, \ldots, x_n^k), (1 \leq j \leq n).$$

3.1 The operators $\Delta_j(k)$ and $p_j(k, l)$

Let $f(x_1, \ldots, x_n) = \sum c(a_j)x_1^{a_1} \ldots x_n^{a_n}$ be a general element of $\mathbb{Z}[x_1, \ldots, x_n]$. It will be convenient in the proof of Theorem 1 below to define linear operators $\Delta_j(k)$ and $p_j(k, l)$ on $\mathbb{Z}[x_1, \ldots, x_n]$, where $1 \leq j \leq n - 1$ and $1 \leq l \leq k - 1$, by the equations

$$\Delta_j(k)f = \Delta_j(k) \sum c(a_j)x_1^{a_1} \ldots x_n^{a_n}$$
\[ s_j \left( \frac{x_j^{u_j} x_{j+1}^{u_{j+1}}}{x_j^{v_j} x_{j+1}^{v_{j+1}}} \right) \]

where \( u_j, u_{j+1}, v_j, v_{j+1} \) are the integers such that \( u_j k + v_j = a_j, u_{j+1} k + v_{j+1} = a_{j+1}, 0 \leq v_j, v_{j+1} < k; \) and

\[ p_j(k, l)f = p_j(k, l)f(x_j) = \sum_{0 \leq t < k} e^{-2\pi it/k} f(e^{2\pi it/k} x_j). \]

It is clear that \( \Delta \) is a well-defined operator mapping \( \mathbb{Z}[x_1, \ldots, x_n] \) into itself. This conclusion obtains less easily for \( p \) owing to the appearance of complex numbers in its definition; nevertheless

\[ p_j(k, l)x^m_j = x^{m-1}_j \sum_{0 \leq t < k} e^{2\pi it(m-l)/k} = x^{m-1}_j [m \equiv l \pmod{k}], \]

so that in particular \( p \) maps \( \mathbb{Z}[x_1, \ldots, x_n] \) to itself. We prove in Appendix B that these operators also map the ideal \( I^k_n \) to itself and hence operate well-definedly on \( R^k_n \).

### 3.2 Proof of Theorem 1

(i) The quantities

\[ x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} e_{i_1, \ldots, i_{n-1}} (x_1^k, \ldots, x_n^k), \quad (0 \leq \epsilon_j \leq k - 1, 0 \leq i_j \leq j) \]

constitute a linear basis in \( R^k_n \). In particular, the dimension of \( R^k_n \) is \( k^n n! \).

First we note that \( x^k_j = e^k_1(x_1^k, \ldots, x_n^k) - e^{k-1}_1(x_1^k, \ldots, x_n^k) \), so that any monomial in \( x_1^k, \ldots, x_n^k \) is expressible as a sum of products of the \( e^j_1 \); and the quadratic relation of Section 2 may be invoked repeatedly to obtain a proper representation in terms of \( e^1_{i_1 \cdots i_{n-1}} \). Since each
element of $R^k_n$ may be expressed as a sum of terms of the form $x_1^{e_1} \ldots x_n^{e_n} e_{i_1, \ldots, i_{n-1}}^1(x_1^k, \ldots, x_n^k)$, it follows at once that the basis elements postulated in the statement of Theorem 1(i) generate $R^k_n$, and it remains only to prove that these elements are independent.

In this direction let us assume, for the sake of contradiction, that there exists a nontrivial vanishing linear combination of the purported basis elements. Let $\Lambda$ denote such a linear combination of the minimal possible degree. If $\Lambda$ contains a term in which the $e_{i_1, \ldots, i_{n-1}}^1$ is of positive degree, let $l$ denote the number such that an $e_l$ appears in some term of $\Lambda$, but no $e_m$ with $m \leq l$ appears in $\Lambda$; then $\Delta_l(k)\Lambda$ is clearly a nontrivial vanishing linear combination of lower degree than $\Lambda$, a contradiction. Otherwise $\Lambda$ contains only terms of the form $x_1^{e_1} \ldots x_n^{e_n}$, and equating the constant terms on both sides of the equation $\Lambda = 0$ shows that the minimal degree of the terms in $\Lambda$ is positive. Let $l$ be any index for which the power $x_i^m$ for a number $m > 0$, appears in $\Lambda$. By Section 3.1 we have $p_l(k, m)x_i^m = x_i^{m-1}$, so that $p_l(k, m)\Lambda$ is a nontrivial vanishing linear combination of lesser degree than $\Lambda$, a contradiction. Thus the quantities in the statement of Theorem 1(i) are independent, and hence they form a linear basis in $R^k_n$. That $R^k_n$ has dimension $k^n n!$ is now obvious.

(ii) The monomials

$$x_1^{a_1} \ldots x_n^{a_n}, (0 \leq a_j \leq k(n - j + 1) - 1)$$

constitute a linear basis in $R^k_n$.

We shall show that every $x_1^{a_1} \ldots x_n^{a_n} e_{i_1, \ldots, i_n}$ is a linear combination of the above monomials; because the number of $x_1^{a_1} \ldots x_n^{a_n}$ is exactly $k^n n! = \dim R^k_n$, it will then follow that these monomials are a linear basis in $R^k_n$. The definition of $e_j^l$ shows easily that $\deg x_m e_j^l \leq k[j \geq m]$. 

5
and the number of $j$ with $m \leq j \leq n - 1$ is $n - m$. Therefore

$$\deg_{x_m} x_1^{e_1} \ldots x_n^{e_n} e_{i_1, \ldots, i_n} \leq k(n - m) + \deg_{x_m} x_1^{e_1} \ldots x_n^{e_n} \leq k(n - m + 1) - 1,$$

so that each term in the expanded form of $x_1^{e_1} \ldots x_n^{e_n} e_{i_1, \ldots, i_n}$ is a constant multiple of a monomial $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, completing the proof.

(iii) A Groebner basis$^3$ for $I_n^k$, with respect to the monomial order $x_1 < x_2 < \ldots < x_n$, is given by

$$h_{n+1-j}^j(x_1^k, \ldots, x_n^k), (1 \leq j \leq n).$$

We observe first that the relations$^4$ $h_n^1 = x_1^n \in I_n^k$ and $d_j h_{n+1-j}^j = h_{n-j}^{j+1}$ imply by induction that $h_{n+1-j}^j \in I_n^k$ for each $j$, as required.

It is easily seen that the highest term in $h_{n+1-j}^j$ is $x_j^{k(n+1-j)}$; thus we need to prove that if $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ is the highest term in the $e_{i_1, \ldots, i_{n-1}}$ occurring in an element $\Lambda \in I_n^k$, then $\alpha_{n-j} > j$ for some $j$. We note that if $\alpha_{n-j} \leq j$ then $\Delta_{n-j}(k) \ldots \Delta_{n-j+\alpha_{n-j}-1}(k)x_{n-j}^{\alpha_{n-j}}$ has leading term 1 and hence equals 1 exactly. Thus if we suppose, for the sake of contradiction, that $\alpha_{n-j} \leq j$ for all $j$, then

$$(\Delta_1(k) \ldots \Delta_{\alpha_1}(k))(\Delta_2(k) \ldots \Delta_{\alpha_2+1}(k)) \ldots (\Delta_{n-1}(k) \ldots \Delta_{n-2+\alpha_{n-1}}(k))f = 1.$$  

But since each $\Delta$ maps $I_n^k$ into itself, this implies that $1 \in I_n^k$, which is false. Hence $\alpha_{n-j} > j$ for some $j$, proving the assertion.

$^3$See Appendix C for the definition and fundamental properties of Groebner bases.
$^4$See Appendix D.
3.3 Compound difference operators

It is well known that the \( n^{\text{th}} \) coefficient in a power series \( f(x) \) may be obtained as \( \frac{f^{(n)}(0)}{n!} \).

In order to obtain a similar formula for the coefficient of \( e_{i_1, \ldots, i_{n-1}} \) in the expansion of a polynomial function \( f \in R_{n}^{1} \), we define compositions of difference operators inductively by the equations

\[
D_{a}^{0} = 1 \text{ for all } a;
\]

\[
D_{a}^{b} = d_{a+1-b}D_{a}^{b-1} \text{ for } b \geq 1;
\]

\[
D_{i_1, \ldots, i_{n-1}} = D_{i_{n-1}}^{i_{n-1}} \cdots D_{i_1}^{i_1}.
\]

The motivation for considering the operators \( D_{i_1, \ldots, i_{n-1}} \) is the straightforward observation that

\[
D_{i_1, \ldots, i_{n-1}} e_{i_1, \ldots, i_{n-1}} = 1.
\]

In the following section we prove a theorem giving the result when certain operators of this class are applied to a polynomial in \( R_{n}^{1} \) and the \( x \) are set to zero. Let \( f = \sum c_{i_1, \ldots, i_{n-1}} e_{i_1, \ldots, i_{n-1}} \) (where the \( c \) are constants) be a general element of \( R_{n}^{1} \); then we have

**Theorem 2.** (i) If \( i_{r+1} - i_{r} \leq 1 \) for each \( r \) then

\[
D_{i_1, \ldots, i_{n-1}} f \big|_{x_1 = \ldots = x_n = 0} = c_{i_1, \ldots, i_{n-1}}.
\]

\(^{5}\)As we are now concerned with \( R_{n}^{1} \) only, the variable \( k \) will hereafter be used to denote quantities other than the upper index of \( R_{n}^{k} \).
(ii) For each \( l \) we have

\[
D^{0,0,\ldots,0,l}f|_{x_1=\cdots=x_n=0} = \sum_{\substack{j_1=\ldots=j_{n-1}=0 \\ j_{n-1}+\ldots+j_{n-1} \geq r < l \\ j_{n-1}+\ldots+j_{n-1}=l}} c^{j_1,\ldots,j_{n-1}}.
\]

### 3.4 Proof of Theorem 2

(i) It is clear that \( D^l e_j^m = e_{j-l}^{m-l} \), and it follows readily that

\[
D^{i_1,\ldots,i_{n-1}} e_{j_1,\ldots,j_{n-1}} = e_{j_1-i_1,\ldots,j_{n-1}-i_{n-1}}^{1-i_1,\ldots,n-1-i_{n-1}}
\]

as desired, provided only that at no time do we apply an operator \( d_k \) to a term containing two \( e \)'s with upper index \( k \). In that case we should have \( l - i_l > l + 1 - i_{l+1} \) or \( i_{l+1} - i_l > 1 \) for some \( l \), contrary to hypothesis.

(ii) We require the observation that

\[
D^{0,0,\ldots,0,l,1,\ldots,1-l,l} e_{i_1,\ldots,i_{n-1},j_1,j_2} |_{x_1=\cdots=x_n=0} = [j_1,j_2 \geq 0] D^{0,0,\ldots,0,l-1,1,\ldots,1-l-1} e_{i_1,\ldots,i_{n-1},j_1,j_2-1} |_{x_1=\cdots=x_n=0}.
\]

To prove this, we invoke the quadratic relation of Section 2 to find that

\[
d_l e_{j_1}^k e_{j_2}^k = \sum_{l \geq 0} e_{j_1-l}^{k+1} e_{j_2-1+l}^{k-1} - \sum_{l \geq 1} e_{j_1-1}^{k-1} e_{j_2+l}^{k+1}.
\]

We note that in applying \( D \) we shall never apply an operator which could alter the terms with upper index \( k + 1 \). Hence those terms will remain at the end of the calculation, and setting \( x_1 = \cdots = x_n = 0 \) will cause the terms to vanish unless their lower indices are zero.
The lower index is zero only in the $j_1^{th}$ term of the first summation, so that we may replace $e^{k}_{j_1} e^{k}_{j_2}$ with $e^{k}_{j_1+j_2}$, establishing the claim.

Then we have

$$D_{0,\ldots,l-1} e^{1,\ldots,n-1}_{i_1,\ldots,i_{n-1}}$$

$$= D_{0,\ldots,l-1} e^{1,\ldots,n-2,2}_{i_1,\ldots,i_{n-2},i_{n-1}-1}$$

$$= [i_{n-1} > 0] D_{0,\ldots,l-2} e^{1,\ldots,n-3,2}_{i_1,\ldots,i_{n-3},i_{n-2}+i_{n-1}-1}$$

$$= [i_{n-1} > 0][i_{n-2} + i_{n-1} > 1] D_{0,\ldots,l-3} e^{1,\ldots,n-4,2}_{i_1,\ldots,i_{n-4},i_{n-3}+i_{n-2}+i_{n-1}-2}$$

$$\vdots$$

$$= [i_{n-1} > 1][i_{n-2} + i_{n-1} \geq 2] [i_{n-l+1} + \ldots + i_{n-1} \geq l - 1] e^{1,\ldots,l-1}_{i_1,\ldots,i_{n-l-1},i_{n-l}+\ldots+i_{n-1}-l},$$

which clearly vanishes at $x_1 = \cdots = x_n = 0$ except under the conditions of the summation in Theorem 2(ii).

### 3.5 An algorithm for obtaining coefficients

Though we cannot give a general formula for the coefficient of every $e_{i_1,\ldots,i_{n-1}}$ in the expansion of an $f \in R^1_n$, we can give a recursive method for obtaining all such coefficients. This is based on the observation that if $(j_1,\ldots,j_{n-1}) < (i_1,\ldots,i_{n-1})$ lexicographically,\(^6\) then

$$D^{i_1,\ldots,i_{n-1}} e^{j_1,\ldots,j_{n-1}} = 0.$$ 

\(^6\)That is, there is an index $m$ such that $j_l = i_l$ for all $l < m$ while $j_m < i_m$. 

9
To prove this, let \( m \) be the smallest integer such that \( j_m < i_m \); then

\[
D^{i_1, \ldots, i_{n-1}} e_{j_1, \ldots, j_{n-1}} = D^{0, \ldots, i_m, \ldots, i_{n-1}} e_{0, \ldots, j_m - i_m, \ldots, j_{n-1}} = 0
\]

because \( j_m - i_m < 0 \).

In particular, if \( e_{i_1, \ldots, i_{n-1}} \) is the lexicographically highest term as defined above, then

\[
D^{i_1, \ldots, i_{n-1}} f = e^{i_1, \ldots, i_{n-1}},
\]

where \( f \) is a general element of \( R_n^1 \) as in the last section. Thus we can obtain all coefficients by repeatedly extracting the lexicographically highest coefficient that has not yet been extracted, thereafter subtracting the corresponding term from \( f \). This provides a method for extracting coefficients when Theorem 2 is inapplicable.

4 Conclusion

We have presented a precise description of the structure of the quotient ring \( R_n^k \) and a partial solution to the problem of determining the coefficients of basis elements in the expansion of a general element of \( R_n^k \). However, the latter problem, in its full generality, remains an open question.

5 Acknowledgments

The author wishes to thank the RSI staff and Dr. Hartley Rogers for providing this research opportunity and Mr. Alexandre Soloviev for sage guidance throughout the internship.
A Elementary properties of $e, d, h$

We prove here the elementary propositions postulated in Section 2.

First we note that the equality $e^j_i = e^j_i + x_{j+1}e^j_{i-1}$ is a trivial consequence of the definition of $e$. We now can prove

(i) $e_i^k e_j^k = \sum_{l \geq 0} e_{i-l}^{k+1} e_{j+l}^k - \sum_{l \geq 1} e_{i-l}^k e_{j+l}^{k+1}$ for any $i, j, k$.

For $(e_i^{k+1} - e_i^k) e_{j-1}^k = x_{k+1} e_{i-1}^k e_{j-1}^k = (e_j^{k+1} - e_j^k) e_{i-1}^k$, whence also

$$e_j^k (e_{i+1}^k - e_{i+1}^{k+1}) = -e_i^k (e_{j+1}^{k+1} - e_{j+1}^k)$$

$$= e_i^{k+1} e_{j+1}^k - e_{j+1}^{k+1} e_i^k + e_{j+1} (e_i^k - e_i^{k+1})$$

$$= e_i^k e_{j+1}^k - e_{j+1} e_i^k + \sum_{l \geq 1} (e_{i-l}^{k+1} e_{j+1+l}^k - e_{j+1+l}^{k+1} e_{i-l}^k)$$

$$= \sum_{l \geq 1} (e_{i+1}^{k+1} e_{j+l}^k - e_{j+l}^{k+1} e_{i+1-l}^k)$$

by induction on $i$.

(ii) $d_l f g = f d_l g + (s_l g)(d_l f)$ for any $f, g \in \mathbb{Z}[x_1, \ldots, x_n]$.

For $d_l f g = \frac{f(g-s_l g)}{x_l-x_{l+1}} = \frac{f(g-s_l g)+s_l g(f-s_l f)}{x_l-x_{l+1}} = f d_l g + s_l g d_l f$.

(iii) $d_l e_j^k = [k = l] e_{j-1}^{k-1}$ for any $j, k, l$.

This is trivial if $l \neq k$, for in that case $e_j^k$ is symmetric in $x_l, x_{l+1}$ and both sides are manifestly zero. If $l = k$ we argue with $d_l e_j^k = d_l (e_{j-1}^{k-1} + x_k e_{j-1}^{k-1}) = e_{j-1}^{k-1}$.
(iv) \( d_i h^k_j = [k = l] h^{k+1}_{j-1} \) for any \( j, k, l \).

Again this result is a trivial consequence of symmetry if \( k \neq l \). To examine the case \( k = l \) we observe that

\[
h^k_j = \sum_{0 \leq a_1, \ldots, a_k \atop a_1 + \cdots + a_k = j} a_1^{a_1} \cdots a_k^{a_k},
\]

thus we find that

\[
d_k h^k_j = \sum_{0 \leq a_1, \ldots, a_k \atop a_1 + \cdots + a_k = j} a_1^{a_1} \cdots x_{k-1}^{a_{k-1}} d_k x_k^{a_k}
\]

\[
= \sum_{0 \leq a_1, \ldots, a_k \atop a_1 + \cdots + a_k = j} a_1^{a_1} \cdots x_{k-1}^{a_{k-1}} \sum_{0 \leq l_1, l_2 \atop l_1 + l_2 = a_k - 1} a_{k+1}^{l_1} x_k^{l_2}
\]

\[
= \sum_{0 \leq a_1, \ldots, a_{k-1}, l_1, l_2 \atop a_1 + \cdots + a_{k-1} + l_1 + l_2 = j-1} a_1^{a_1} \cdots x_{k-1}^{a_{k-1}} a_k^{l_1} x_k^{l_2} = h^{k+1}_{j-1}.
\]

\[\text{B Action of } \Delta, p \text{ on } R^k_n\]

We prove here that \( \Delta \) and \( p \) map the ideal \( I^k_n \) to itself and hence constitute well-defined operators on the quotient \( R^k_n \).

First we note that if \( f = \sum c x_j^{a_j+k} x_{j+1}^{a_{j+1}+k+b_{j+1}} \) and \( g = \sum c' x_j^{a'_j+k} x_{j+1}^{a'_{j+1}+k} \), where the \( c \) and \( c' \) are independent of \( x_j \) and \( x_{j+1} \), are functions in \( \mathbb{Z}[x_1, \ldots, x_n] \), then \( \Delta_j(k)fg = g\Delta_j(k)f + q\Delta_j(k)g \) for a suitable \( q \in \mathbb{Z}[x_1, \ldots, x_n] \). For

\[
\Delta_j(k)fg = \Delta \sum c c' x_j^{(a_j+a'_j)k+b_j} x_{j+1}^{(a_{j+1}+a'_{j+1})k+b_{j+1}}
\]

\[
= \sum c c' x_j^{b_j} x_{j+1}^{b_{j+1}} \Delta((x_j^{a_j+k} x_{j+1}^{a_{j+1}+k})(x_j^{a'_j+k} x_{j+1}^{a'_{j+1}+k}))
\]
\[
\sum \sum c' c x_j^{a_j} x_{j+1}^{a_j+1} (x_j^{a_j} x_{j+1}^{a_j+1}) \Delta (x_j^{a_j} x_{j+1}^{a_j+1}) + \Delta (x_j^{a_j} x_{j+1}^{a_j+1}) s_j (x_j^{a_j} x_{j+1}^{a_j+1})
\]

\[= g \Delta f + q \Delta g\]

where \(q \in \mathbb{Z}[x_1, \ldots, x_n]\), as claimed. If we now observe that each element of the ideal \(I_n^k\) is a sum of terms \(fg\), where \(f, g \in \mathbb{Z}[x_1, \ldots, x_n]\) and \(g\) is a symmetric polynomial in \(x_1^k, \ldots, x_n^k\), then clearly

\[\Delta \sum fg = \sum (g \Delta f + q \Delta g) = \sum g \Delta f\]

is also an element of \(I_n^k\), as claimed. We note also that \(g(e^{2\pi it/k} x_j) = g(x_j)\) for each \(t\), whence

\[p_j(k, l) \sum fg = \sum gp_j f\]

is also in \(I_n^k\), as desired.

\section*{C Groebner bases}

Here we give a brief review of the definition and elementary properties of Groebner bases.

Preliminary to the definition of a Groebner basis, we make the following definitions.

\(i\) A total order \(<\) on monomials is called a \textit{monomial order} if and only if \(1 \leq m_1\) and 
\(m_1 < m_2 \Rightarrow m_1 m_3 < m_2 m_3\) for all monomials \(m_1, m_2, m_3\).

\(ii\) The \textit{initial monomial} of a polynomial \(f\) with respect to the monomial order \(<\),
denoted by \text{init} \(f\), is the highest monomial in \(f\) with respect to \(<\).
(iii) The \textit{initial ideal} of an ideal $I \subset \mathbb{C}[x_1, \ldots, x_n]$, denoted by $\text{init} I$, is the ideal generated by the initial monomials of all polynomials in $I$.

(iv) The monomials which do not belong to $\text{init} I$ are called \textit{standard}; all other monomials are \textit{non-standard}.

Given a monomial order $<$ and an ideal $I$, we call a finite subset $G := g_1, \ldots, g_s \subset I$ a \textit{Groebner basis} for $I$ if and only if $\text{init} I$ is generated by $\text{init} g_1, \ldots, \text{init} g_s$. A Groebner basis $G$ of an ideal $I$ of a polynomial ring $R$ has the following properties.

\textit{Proposition.} (i) $G$ generates $I$. (ii) The standard monomials with respect to $G$ constitute a linear basis for the quotient $R/I$.

For the proof of the Proposition and for further information on Groebner basis theory, see [2].

We note that part (ii) of the Proposition enables us easily to deduce Theorem 1(ii) from Theorem 1(iii); for Theorem 1(iii) implies that the standard monomials with respect to $G$ are precisely the basis elements claimed in Theorem 1(ii). The proof in the main text is included because it is more elementary, requiring no appeal to properties of Groebner bases except their definition.

\textbf{D Symmetric polynomials}

We provide a more detailed definition of $e^k_j$ and $h^k_j$ than that given in Section 2.

The $j^{\text{th}}$ \textit{elementary symmetric polynomial} in the $k$ variables $x_1, \ldots, x_k$, denoted by $e^k_j$, is defined as the sum of all square-free $j^{\text{th}}$-degree monomials in $x_1, \ldots, x_k$. For illustration we
observe that

\[ e_0^4 = 1; \]

\[ e_1^4 = x_1 + x_2 + x_3 + x_4; \]

\[ e_2^4 = x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4; \]

\[ e_3^4 = x_1 x_2 x_3 + x_2 x_3 x_4 + x_3 x_4 x_1 + x_4 x_1 x_2; \]

\[ e_4^4 = x_1 x_2 x_3 x_4. \]

Since there are no monomials of negative degree, we see that \( e_j^k = 0 \) for any \( k \) and any negative \( j \). Furthermore, since each variable \( x_j \) may appear in a monomial no more than once, the degree of each monomial is no more than \( k \), whence \( e_j^k = 0 \) for any \( k \) and any \( j > k \).

The elementary symmetric polynomials can be obtained from the generating function identity

\[ (z - x_1) \cdots (z - x_k) = \sum_{0 \leq j \leq k} (-1)^j e_j^k z^{k-j}, \]

which is easily verified by expansion of the left-hand side. An interesting consequence of this identity is that \( x_j^n = 0 \) in \( R_n^1 \) for each \( j \). For in \( R_n^1 \) we have \( e_l^n = 0 \) for each \( l \geq 1 \), whence

\[ (z - x_1) \cdots (z - x_n) = z^n \]

and hence

\[ 0 = \prod_{1 \leq l \leq n} (x_j - x_l) = x_j^n, \]
as desired.

The $j^{th}$ full symmetric polynomial in $x_1, \ldots, x_k$, denoted by $h_j^k$, is the sum of all monomials, whether squarefree or not, in $x_1, \ldots, x_k$. Thus

\[ h_0^k = 1; \]

\[ h_1^k = x_1 + x_2 + x_3; \]

\[ h_2^3 = x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_2x_3 + x_3x_1; \]

\[ h_3^3 = x_1^3 + x_2^3 + x_3^3 + x_1^2x_2 + x_2^2x_3 + x_3^2x_1 + x_1^2x_3 + x_2^2x_1 + x_3^2x_2 + x_1x_2x_3, \]

and so forth. As before we have $h_j^k = 0$ for any $j < 0$. 

16
References
