THE MODULE STRUCTURE OF A GROUP ACTION ON A POLYNOMIAL RING: A FINITENESS THEOREM

DIKRAN B. KARAGUEUZIAN AND PETER SYMONDS

ABSTRACT. **Draft, 24 March 2006. A more recent version might be obtainable at http://www.ma.umist.ac.uk/pas/preprints.** Consider a group acting on a polynomial ring over a finite field. We study the polynomial ring as a module for the group and prove a structure theorem with several striking corollaries. For example, any indecomposable module that appears as a summand must also appear in low degree and so the number of isomorphism types of such summands is finite. There are also applications to invariant theory, giving a priori bounds on the degrees of the generators.

1. INTRODUCTION

We consider a polynomial ring S in n variables over a finite field k of characteristic p and an action of a finite group G on S by homogeneous linear substitutions. This is equivalent to taking the symmetric powers of an n-dimensional kG-module.

We want to understand S as a kG-module in a manner as explicit as possible. The ideal solution would be to give a decomposition into indecomposable summands. We are primarily interested in the modular case, when p divides the order of G, so the problem is much harder than that of determining the composition factors.

The case of two variables was studied by Glover [13] and Alperin and Kovacs [2] and the case of three variables by the authors in [11]. This paper generalizes the results of [11] to any number of variables and we prove a strong finiteness property as a consequence.

Theorem (17.1). *The kG-module S has only finitely many isomorphism types of indecomposable summands, provided that k is finite.*

Particularly notable are the applications to invariant theory.

Theorem (17.4). *The invariants S^G are generated as a ring by elements in degrees less than or equal to $\frac{q^n-1}{q-1}(nq-n-1)$, ($2q^2 - q - 2$ if $n = 2$), where q is the order of k.*

It is well known that the invariants are finitely generated and, since k is finite, there are only finitely many possible actions for a given n, so some bound on the degrees of the generators must exist for given n and k. The point of the corollary is that it gives an explicit bound ($|G|$ is such a bound in characteristic 0). For a long time no such bound was known (except in particular cases), but recently one was given by Derksen and Kemper, although it is very large (see Section 17 for more details).

There are more precise results if we replace the general finite group G by a p-group P.

Theorem (17.2). *Any indecomposable kP-module which is a summand of S is isomorphic to one occuring in degree less than or equal to $\frac{q^n-1}{q-1} - n$.*

Theorem (17.3). *If we can compute the decomposition into indecomposables of S as a kP-module in degrees less than or equal to $q^{n-1} - n$ then we can compute it in all degrees.*

Thus what is a priori an infinite problem becomes a finite one. Unfortunately the computation in the range required is beyond the capabilities of most computers in interesting cases with more than three variables.

All of the above results are obtained as corollaries of a Structure Theorem for the action of the group of upper triangular matrices with 1's on the diagonal, U_n. The ring of invariants under this group, for which we write S^{U_n}, is known to be polynomial in generators $\{d_i \mid i = 1, \ldots, n\}$, where the degree of d_i is q^{i-1}. Note that any p-group P acting on S may be considered to be a subgroup of U_n after a change of variables. Our Structure Theorem describes the kP-module structure of S for any such P:

Theorem 1.1 (§10). *There is an isomorphism of graded kP-modules*

$$S \cong \bigoplus_{J \subseteq I} k[d_i \mid i \in I \cup \{n\} - J] \otimes_k \bar{X}_J(I),$$

where $\bar{X}_J(I)$ is a finite dimensional graded kP-module, P acts trivially on $k[d_i]$, and I is $\{1, 2, \ldots, n-1\}$.

This should be read as saying that S contains one copy of $\bar{X}_J(I)$ for each monomial in the d_i with $i \in I \cup \{n\} - J$.

In fact we have a lot more information about the modules $\bar{X}_J(I)$. For example, they are induced from certain subgroups and we have explicit bounds on the degrees of the elements.

The idea behind the proof of the Main Theorem is that first we formulate a version for certain subgroups U_I of U_n that correspond to a subset $I \subseteq \{1, \ldots, n-1\}$ and in which only the rows indexed by elements of I can have non-zero off-diagonal entries. Next we construct the pieces $\bar{X}_J(I)$ by induction on $|I|$, controlling them via the leading monomials (in an appropriate sense) of the elements of their socles, and by their Poincaré series. To show that the pieces fit together exactly is a complicated exercise in accounting.

At one point in the construction we need to know that a certain monomial is the leading monomial of a trace (or orbit sum) over a subgroup. That this is the case is guaranteed by the Trace Lemma 16.1. The proof of this lemma fills a seemingly disproportionate part of the paper, comprising sections 11 to 16. Although the Trace Lemma appears as a difficult technical point in this context, it might be of independent interest in invariant theory.

It is a pleasure to thank all our colleagues who have listened patiently to our ideas on the subject, especially Stephen Siegel, who introduced us to the problem and suggested Theorem 17.1 in 1995. The first author would also like to thank Matt Brin for listening to a very detailed series of lectures on trace lemmas. The Trace Lemma and its proof are based on extensive calculations with MAGMA [4], in particular code for working with rings of invariants which was developed by Gregor Kemper (and has since been incorporated into MAGMA with help from Allan Steel).

Finally we thank the referee for his meticulous reading of the manuscript.

2. Background

The fundamental result about group actions on rings from our point of view is the Normal Basis Theorem in Galois Theory. Let S be a field and G a finite group of automorphisms of S and let R denote the invariant subfield. The Normal Basis Theorem states that S is a free RG-module of rank one.

One generalization of this in algebraic number theory is a theorem of Noether. Let S be the ring of integers in a number field and G a group of automorphisms with R as ring of invariants. If the extension S/R is tamely ramified then S is locally free of rank one as an RG-module. The study of this sort of problem is known as Galois Module Theory and contains a large number of deep results from number theory, particularly class field theory, and algebraic geometry.

Another generalization is described in [10, 5, 18]. If S is a polynomial ring over a field k and G is a finite group of automorphisms of S with R as ring of invariants then if we consider S as a kG-module we find that it is mostly projective in an asymptotic sense; it is even mostly free when viewed in the right way.

We emphasize that we are really only concerned with the modular case, when the characteristic p of k divides the order of G, otherwise all modules would be projective.

Of course, the study of group actions on polynomial rings leads to the vast classical subject of invariant theory, which we will not discuss here. We just mention that for the groups U_I that we consider the rings of invariants are easy to calculate and are polynomial. In general, neither property holds.

It is essential to distinguish between the two different problems of describing the composition factors of S and describing its indecomposable summands. The former is dealt with in principle by a generalization of Molien's formula (see e.g. [7] 3.2.5), although it can still be very difficult. It is the latter that concerns us here. For most groups it is not even possible to classify the indecomposable representations, so the problem could become very complicated.

The case of two variables was considered in detail by Glover [13], when $p = q$, and for general q by Alperin and Kovacs [2]. It turns out that S is periodic modulo projectives.

Rather than restricting the number of variables, one can restrict the group G. The case when G is of prime order p was dealt with by Almkvist and Fossum [1]. If the homogeneous component of S of degree 1 is indecomposable then again S is periodic of period p modulo projectives, although the periodic part is complicated to describe. There are also partial results for other cyclic groups [1, 14, 15, 19]. In this case, if S is indecomposable in degree 1 then the action is periodic modulo summands induced up from proper subgroups. This is a conjecture of Kemper that was proved in [19] as a corollary of the Main Theorem of the present paper. This periodicity does not extend to more complicated groups, however.

But cyclic groups have only finitely many isomorphism classes of indecomposable modules. Siegel and Totaro calculated many examples for the Klein four group, where there are infinitely many isomorphism types of indecomposables, but they can be classified. They observed that whenever they decomposed S as a sum of indecomposables only a finite number of isomorphism types of indecomposable summands actually occurred.

Motivated by this, we produced a theorem for polynomial rings in three variables [11], showing, in particular, that only a finite number of isomorphism types of indecomposable summands could arise. Instead of periodicity modulo projectives there is a more complicated system of multiple periodicities, which we called a *structure theorem*.

The main result of the present paper is a generalization of this structure theorem to an arbitrary number of variables, Theorem 10.1.

A commentary on the proof, together with some examples, generalizations and applications is given in [12].

When the field k is infinite and the group G is allowed to be infinite then the situation is quite different. Doty [8] calculates the submodule lattice for the natural action of $SL(n,k)$ when k is algebraically closed, and it follows that S is indecomposable in each degree. In particular, there are infinitely many non-isomorphic summands.

The theory has been generalized in two directions. One is in [20], where finitely generated graded modules over a ring RG are considered. These do not have to satisfy any finiteness property on the summands, but it is shown that the property of having only a finite number of isomorphism types of indecomposable summands is equivalent to the seemingly stronger property that there is a structure theorem of a similar form to that of Theorem 1.1.

The other direction is due to Bleher and Chinberg [3]. The polynomial ring S can be considered as the ring of regular functions on projective space $\mathbb{P}^{n-1}(k)$, and the group G acts on $\mathbb{P}^{n-1}(k)$. This generalizes to the ring of regular functions on any projective variety with an action of a finite group G. The authors of [3] prove that there are only finitely many isomorphism types of indecomposable kG-summands for curves, and for surfaces where the Sylow p-subgroup has a fixed point.

3. Organization of the Paper

Section 4 is devoted to various subgroups of U_n and their invariants. Section 5 introduces the parameter space $P(I)$ which indexes the monomials in the invariants, and we show how to partition it into pieces $S_J(I)$. Section 6 explains a convenient reduction from S to a truncated version T.

In Section 7 we order the monomials in the invariants and and show how to deal with the socle of a submodule in terms of the least monomials of its elements. This is one of the tools that we use to control the pieces; the other is their Poincaré series, and the lemmas that we will need to manipulate these are proved in Section 8.

Sections 9 and 10 use all this machinery to define the pieces $X_J(I)$ of T that correspond to the $S_J(I)$ and to prove the Main Theorem, assuming the validity of the Trace Lemma. Here $X_J(I)$ for $J \neq I$ is produced inductively from $X_J(J)$ using the Trace Lemma. We then show that $\oplus_{J \subsetneq I} X_J(I)$ is a summand of T using our control over the socles to show that the pieces are linearly independent and our computation of the Poincaré series to show that they span in high degrees. Then $X_I(I)$ is defined to be the complement.

Sections 11 through 16 contain the proof of the Trace Lemma, and Section 17 contains the proofs of the corollaries.

The reader might first wish to examine the proof of the Main Theorem in the case when $n = 3$ and $q = 3$, as is presented in [12]; this case should help shed light on many of the intricacies of the paper, even though the higher terms in the trace lemma are zero in this

case. (But note that in all references in [12] to specific results in this paper the section number should be increased by 1.)

There is an index of notation at the end.

4. Groups and Polynomials

In this section we define the groups whose representations we will be studying and describe their invariants.

Let k be the finite field of q elements, where $q = p^s$ for some prime p. Let $S = \oplus S_r = k[x_1, \ldots, x_n]$ denote the polynomial ring over k in n variables, graded by degree. This notation will remain fixed throughout the paper.

All the groups that we study are subgroups of the upper-triangular $n \times n$ matrices over k with 1's on the diagonal, denoted by U_n. This group is a Sylow p-subgroup of $GL_n(k)$. The group U_n is taken to act on the degree-1 part of the polynomial ring S_1 (not on its dual, as is often the case in invariant theory) in the natural way and this extends to the whole of S.

To be explicit, let $a_{ij}(\lambda)$ be the matrix with $\lambda \in k$ in row i, column j, 1's on the diagonal and 0's elsewhere: then $a_{ij}(\lambda) \cdot x_j = x_j + \lambda x_i$, while $a_{ij}(\lambda) \cdot x_l = x_l$ if $l \neq j$.

Notation 4.1. $[I, J, K]$ I, J, K will always be subsets of $\{1, \ldots, n-1\}$ such that $I = J \amalg K$. We enumerate their elements in ascending order: $I = \langle i_1, \ldots, i_{|I|} \rangle$, $J = \langle j_1, \ldots, j_{|J|} \rangle$, $K = \langle k_1, \ldots, k_{|K|} \rangle$. The notation $\langle \ldots \rangle$ is used to imply that the elements are listed in order and without repetition.

Thus, by convention, $K = I - J$ throughout this paper.

Notation 4.2. $[U_I]$ U_I is the subgroup of U_n with non-zero off-diagonal entries only in the rows corresponding to I.

Thus U_I contains the $a_{ij}(\lambda)$ with $i \in I$ and $j > i$.

Notation 4.3. $[J^{<i}]$ For any $i \in \mathbb{N}$, let $J^{<i} = \{j \in J \mid j < i\}$, and similarly for $>, \leq, \geq$.

Notation 4.4. $[\theta(z; I)]$ If $I = \langle i_1, \ldots, i_{|I|} \rangle \subseteq \{1, 2, \ldots n-1\}$, we define $\theta(z; I) \in k[z, x_{i_1}, \ldots, x_{i_{|I|}}]$ by

$$\theta(z; I) = \prod_{(\lambda_{i_1}, \ldots, \lambda_{i_{|I|}}) \in k^I} (z + \lambda_{i_1} x_{i_1} + \cdots + \lambda_{i_{|I|}} x_{i_{|I|}}).$$

When $I = \varnothing$ we interpret this to mean that $\theta(z; \varnothing) = z$.

Definition 4.5. $[d_i]$ For $i = 1, \ldots, n$ let $d_i = \theta(x_i; I^{<i})$.

Proposition 4.6. *The d_i are algebraically independent and generate the invariant ring of the group U_I, i.e. $S^{U_I} = k[d_1, \ldots, d_n]$.*

Proof. This result is well known in invariant theory: see, for example, [16] or [7] 3.7.5. For the convenience of the reader we sketch a proof.

In order to simplify the notation, let $U = U_I$ and let R be the purported ring of invariants and $\bar{R} = S^U$ the true ring of invariants. Clearly $R \subseteq \bar{R}$. We will use the letter Q to denote the field of fractions of a ring.

From Lemma 6.4 below we know that S is a free R-module with a basis consisting of $|U|$ elements. It follows that $Q(S)$ is a $Q(R)$-vector space of dimension $|U|$ so, by Galois Theory, $Q(R) = Q(S)^U = Q(\bar{R})$.

Suppose that $\bar{R} \neq R$, so there is an $r \in \bar{R}$ that is not in R. By expressing r in terms of the basis we see that it is not in $Q(R)$, hence not in $Q(\bar{R})$, a contradiction. $\square$

5. The Parameter Space

Here we develop the machinery needed to describe the pieces $\bar{X}_J(I)$ in the Main Theorem. We maintain control of these recursively constructed pieces in part by knowing the leading monomials of bases of their socles. The parameter space $P(I)$ (5.2) will index the monomials, and $\bar{X}_J(I)$ will correspond to a subset $\bar{S}_J(I) \subseteq P(I)$.

Definition 5.1. $[\mu]$ Let $J \subseteq \{1, \ldots, n-1\}$ and $l \in \mathbb{Z}$. Write $J^{>l} = \langle j_1, \ldots, j_m \rangle$ (4.3). Then $\mu(J, l) \in \mathbb{Z}$ is defined by

$$\mu(J, l) = [(n+1-j_m-1)q^m + (j_m - j_m - 1)q^{m-1} + \cdots + (j_2 - j_1 - 1)q + (j_1 - l - 1)](q-1).$$

(If $m = 0$, then $\mu(J, l) = (n - l)(q - 1)$.)

Equivalently, $\mu(J, l) = nq^m(q-1) - q^m + 1 - (j_m q^{m-1} + \cdots + j_1)(q-1)^2 - l(q-1)$.

Definition 5.2. $[P(I)]$ For any $I \subseteq \{1, \ldots, n-1\}$, the parameter space on I is $P(I) = \mathbb{N}_0^I$, i.e. the set of all $\mathbb{N}_0$-valued functions on I.

We shall often write $\vec{a} = (a_{i_1}, \ldots, a_{i_{|I|}})$ for an indeterminate element of $P(I)$. The restriction of $\vec{a}$ to $P(J)$ will be denoted by $\vec{a}_J$, or just by $\vec{a}$ when no no confusion is likely to arise (and similarly for any other subset).

Definition 5.3. $[\psi]$ If $J = \langle j_1, \ldots, j_{|J|} \rangle$ and $\vec{a} \in P(I)$ we define $\psi(J, \vec{a}) \in \mathbb{Z}[a_{j_1}, \ldots, a_{j_{|J|}}]$ to be $(a_{j_1} + qa_{j_2} + \cdots + q^{|J|-1}a_{j_{|J|}})(q-1)$. (So $\psi(\varnothing, \vec{a})) = 0$.)

Equivalently, $\psi(J, \vec{a}) = (q-1)\sum_{j \in J} q^{|J^{<j}|}a_j$.

Definition 5.4. $[\lambda]$ $\lambda(J, \vec{a}, l) = \mu(J, l) - \psi(J^{>l}, \vec{a})$. We can also regard this as a function in the last coordinate to obtain $\vec{\lambda}(J, \vec{a}) \in P(I)$.

Definition 5.5. $[S_J(I), \bar{S}_J(I), \mathrm{IE}_{J,i}, \mathrm{E}_{J,i}]$ We associate to $J \subseteq I$ a set $S_J(I) \subseteq P(I)$ defined by $|I|$ linear inequalities $\mathrm{IE}_{J,i}$ in the coordinates of $\vec{a} \in P(I)$, one for each $i \in I$.

$$\mathrm{IE}_{J,i} \text{ is } \begin{cases} a_i + \psi(J^{>i}, \vec{a}) < \mu(J, i) & \text{if } i \in J, \\ a_i + \psi(J^{>i}, \vec{a}) \geq \mu(J, i) & \text{if } i \notin J. \end{cases}$$

Similarly $\bar{S}_J(I)$ is defined by $|I|$ linear (in)equalities $\mathrm{E}_{J,i}$, where

$$\mathrm{E}_{J,i} \text{ is } \begin{cases} a_i + \psi(J^{>i}, \vec{a}) < \mu(J, i) & \text{if } i \in J, \\ a_i + \psi(J^{>i}, \vec{a}) = \mu(J, i) & \text{if } i \notin J. \end{cases}$$

In a context where I is fixed, we write S_J for $S_J(I)$.

It bears emphasizing that $\mu(J, i)$ is a constant. It depends on the elements of J, but not on the coordinates a_j.

Lemma 5.6. *If we consider $P(K)$ as the subset of $P(I)$ consisting of the vectors with coordinates 0 on elements of J, then there is a bijective map $\bar{S}_J(I) \times P(K) \to S_J(I)$ given by $(\vec{s}, \vec{n}) \mapsto \vec{s} + \vec{n}$.*

Proof. Notice that a_k for $k \in K$ appears only in the defining inequality $\mathrm{IE}_{J,k}$ of $S_J(I)$, and this is $a_k + \psi(J^{>i}, \vec{a}) \geq \mu(J, k)$, whereas a_k appears only in the defining (in)equality $\mathrm{E}_{J,k}$ of $\bar{S}_J(I)$ and this is $a_k + \psi(J^{>i}, \vec{a}) = \mu(J, k)$. $\qquad\square$

Lemma 5.7. $S_J(J) = \bar{S}_J(J)$ *and* $\bar{S}_J(I) = \{\vec{a} \in P(I) \mid \vec{a}_J \in S_J(J), \vec{a}_K = \vec{\lambda}(J, \vec{a}_J)\}$.

Proof. The first claim follows from the definitions (or from 5.6).

$\bar{S}_J(I)$ is defined by $|I|$ linear (in)equalities. The inequalities are the $E_{J,j}$ for $j \in J$ and these are exactly the $|J|$ (in)equalities that define $S_J(J)$. The equalities are the $E_{J,k}$ for $k \in K$ and these are of the form $a_k + \psi(J^{>k}, \vec{a}) = \mu(J, i)$, which can be written $a_k = \lambda(J, \vec{a}, k)$. $\qquad\square$

Lemma 5.8.   (1) $\mathrm{IE}_{J,i}$ *depends only on the set $J^{\geq i}$ and i; i.e. it is independent of $J^{<i}$.*
   (2) *If $i \notin J$ then $\mathrm{IE}_{J,i}$ and $\mathrm{IE}_{J \cup \{i\}, i}$ differ only in that the inequality sign $\geq$ is replaced by $<$.*

Proof. Examine the definitions. $\qquad\square$

Definition 5.9. $[X(L, v)]$ If $I = \langle i_1, \dots, i_t \rangle$ and $L \subset \langle i_v, \dots, i_t \rangle$ where $1 \leq v \leq t + 1$, we write $X(L, v)$ for the subset of $P(I)$ defined by $\mathrm{IE}_{L, i_v}, \dots, \mathrm{IE}_{L, i_t}$.

Proposition 5.10. *[Partitions] Let $I = \langle i_1, \dots, i_t \rangle$ be a sequence of positive integers, and $\{S_J \mid J \subseteq I\}$ the collection of 2^t subsets of $P(I)$ defined above. Then this collection of subsets is a partition of $P(I)$, i.e. if J and J' are distinct subsets of I, then $S_J \cap S_{J'} = \varnothing$, and $\bigcup_{J \subseteq I} S_J = P(I)$.*

We are not simply cutting up $P(I)$ along t hyperplanes, so this is not obvious.

Proof. This is a special case of the following lemma, since $P(I) = X(\varnothing, t + 1)$. $\qquad\square$

Notation 5.11. $[Q(L, v)]$ If $v \leq t + 1$ and $L \subset \{i_v, \dots, i_t\}$ we write $Q(L, v)$ for the following collection of subsets of $P(I)$: $\{S_J(I) \mid L \subseteq J \subseteq L \cup \{i_1, \dots, i_{v-1}\}\}$.

Lemma 5.12. *If $L \subset \langle i_v, \dots, i_t \rangle$ then $Q(L, v)$ is a partition of $X(L, v)$.*

Proof. We work by induction on v (but for all eligible L). The initial case ($v = 1$) is immediate since both $X(L, 1)$ and $Q(L, 1)$ are just $S_L(I)$.

To prove the general case we note that, for $L \subset \langle i_v, \dots, i_t \rangle$, $X(L, v) = X(L \cup \{i_{v-1}\}, v - 1) \amalg X(L, v - 1)$, because $\mathrm{IE}_{L,i}$ and $\mathrm{IE}_{L \cup \{i_{v-1}\}, i}$ are the same for $i \geq i_v$, while $\mathrm{IE}_{L, i_{v-1}}$ and $\mathrm{IE}_{L \cup \{i_{v-1}\}, i_{v-1}}$ are opposites, by 5.8.

Also it is easy to verify that $Q(L, v) = Q(L \cup \{i_{v-1}\}, v - 1) \amalg Q(L, v - 1)$. By the induction hypothesis, $Q(L \cup \{i_{v-1}\}, v - 1)$ is a partition of $X(L \cup \{i_{v-1}\}, v - 1)$ and $Q(L, v - 1)$ is a partition of $X(L, v - 1)$. $\qquad\square$

Lemma 5.13. $\bar{S}_J(I)$ *is a finite set.*

Proof. All the defining inequalities are of the form $<$ and all the a_i and their coefficients are non-negative, so certainly $0 \leq a_i \leq \mu(J, i)$ for each $i \in I$. $\qquad\square$

Lemma 5.14. $\bar{S}_\varnothing(I)$ *consists of just one point* $\vec{p} = \vec{p}_I$*, with coordinates* $(\vec{p}_I)_i = (n - i)(q-1)$*. (We will mostly omit the subscript I.)*

Proof. The defining equalities reduce to this. $\qquad\square$

It will be convenient to make a change of coordinates on our parameter space $P(I)$. We think of $(a_{i_1}, \ldots, a_{i_{|I|}})$ as the standard coordinates, and for each $J \subseteq I$, we define new coordinates $(b^J_{i_1}, \ldots, b^J_{i_{|I|}})$ in terms of these.

Definition 5.15. $[b^J_i]$ For any $J \subseteq I$ and $i \in I$ we set $b^J_i = a_i - \lambda(J, \vec{a}, i) = a_i + \psi(J^{>i}, \vec{a}) - \mu(J, i)$.

We can evaluate the b's at the point $\vec{p}$ from 5.14.

Lemma 5.16. $b^J_i(\vec{p}) = q^{|J^{>i}|} - 1$.

Proof. Let $J^{>i} = \langle j_1, \ldots, j_s \rangle$ and substitute the values given in 5.14 into the definitions of the constituent parts of b^J_i (5.15, 5.3, 5.1):

$$p_i + \psi(J^{>i}, \vec{p}) = (n - i)(q - 1) + [(n - j_1) + \cdots + (n - j_s)q^{s-1}](q - 1)^2$$
$$= -i(q - 1) - [j_1 + \cdots j_s q^{s-1}](q - 1)^2 + nq^s(q - 1),$$

$$\mu(J, i) = nq^s(q - 1) - [j_s q^{s-1} + \cdots + j_1](q - 1) - i(q - 1) - q^s + 1.$$

The difference is $b^J_i(\vec{p}) = q^s - 1$, as required. $\qquad\square$

Lemma 5.17. *For any* $J \subseteq I$ *and* $i \in I$ *we have* $a_i - p_i = (b^J_i - b^J_i(\vec{p})) - (q - 1)\sum_{j \in J^{>i}}(b^J_j - b^J_j(\vec{p}))$.

Proof. Both sides are linear combinations of a_i, the a_j for $j \in J^{>i}$ and a constant.

Clearly the coefficients of a_i match, and the constant will look after itself by construction, so we calculate the coefficient of a_l on the right hand side for $l \in J^{>i}$. If we set $\bar{J} = (J^{>i})^{<l}$, for convenience, then the coefficient of a_l in b^J_j for $j \in \bar{J}$ or $j = i$ is $(q-1)q^{|\bar{J}^{>j}|}$ and the coefficient of a_l in b^J_l is 1.

Thus the total coefficient of a_l on the right hand side is $(q - 1)q^{|\bar{J}|} - (q - 1)((\sum_{j \in \bar{J}}(q - 1)q^{|\bar{J}^{>j}|}) + 1)$. But this is equal to $(q - 1)(q^{|\bar{J}|} - ((q - 1)(\sum_{u=1}^{|\bar{J}|} q^{u-1}) + 1))$, which collapses to 0. $\qquad\square$

Lemma 5.18. *If* $\vec{a} \in S_J(I)$ *then* $a_k \geq p_k$ *for* $k \in K$.

Proof. By definition of $S_J(I)$, we know that $b^J_k \geq 0$ for $k \in K$ and $b^J_j \leq -1$ for $j \in J$. Now substitute this information into the statement of 5.17 with k in place of i to obtain $a_k - p_k \geq -b^J_k(\vec{p}) - (q - 1)\sum_{j \in J^{>k}}(-1 - b^J_j(\vec{p}))$.

By 5.16, the right hand side is $1 - q^{|J^{>k}|} + (q - 1)\sum_{j \in J^{>k}} q^{|J^{>j}|}$, which collapses to 0. $\quad\square$

Definition 5.19. $[\deg_I(\vec{a})]$ For $\vec{a} \in P(I)$ we define $\deg_I(\vec{a}) = \frac{1}{q-1}\psi(I, \vec{a})$.

$\deg_I(\vec{a})$ will be the degree of the monomial associated to $\vec{a}$ when this is defined in 7.1.

The next few lemmas are elementary, but tricky, and will only be used to obtain explicit bounds in the corollaries to the Main Theorem. The reader who is not interested in this, or who is willing to take Lemmas 5.21 and 5.22 on trust, can skip to 5.23.

Lemma 5.20. *For any $J \subseteq I$ we have $\deg_I(\vec{a}) - \deg_I(\vec{p}) = \sum_{i \in I} \omega_i^J(b_i^J - b_i^J(\vec{p}))$, where $\omega_i^J = 1$ if $i \in J$ and $\omega_i^J = q^{|I^{<i}|}$ if $i \notin J$.*

Proof. The right hand side is a linear combination of the b_i^J and the constant term is correct by construction. Using the definitions and 5.17 we obtain

$$\deg_I(\vec{a}) - \deg_I(\vec{p}) = \sum_{i \in I}(a_i - p_i)q^{|I^{<i}|}$$

$$\equiv \sum_{i \in I}\left[b_i^J - (q-1)\sum_{j \in J^{>i}}b_j^J\right]q^{|I^{<i}|} \quad \text{modulo a constant.}$$

If $l \notin J$ then b_l^J appears only once, with coefficient $q^{|I^{<l}|}$. If $l \in J$ then the total coefficient of b_l^J is $q^{|I^{<l}|} - (q-1)\sum_{i \in I^{<l}}q^{|I^{<i}|}$, which collapses to 1. $\qquad\square$

Lemma 5.21. *For $\vec{a} \in \bar{S}_J(I)$ we have $\deg_I(\vec{a}) \le \deg_I(\vec{p}) \le \frac{q^n-1}{q-1} - n$.*

Proof. By definition of $\bar{S}_J(I)$ we know that each $b_i^J \le 0$. Using 5.16, we see that $b_i^J(\vec{p}) \ge 0$, hence the right hand side of the expression in 5.20 is less than or equal to 0, and the first inequality follows.

From 5.14 we obtain the formula $\deg_I(\vec{p}_I) = \sum_{i \in I}(n-i)(q-1)q^{|I^{<i}|}$ and we see that if we add an element to I then each term corresponding to $i \in I$ can not decrease and the new term is positive. Repeating this we see that $\deg_I(\vec{p}_I) \le \deg_{\langle 1,\ldots,n-1\rangle}(\vec{p}_{\langle 1,\ldots,n-1\rangle})$. Finally, $\deg_{\langle 1,\ldots,n-1\rangle}(\vec{p}_{\langle 1,\ldots,n-1\rangle}) = \sum_{i=1}^{n-1}(n-i)(q-1)q^{i-1} = (\sum_{i=0}^{n-1}q^i) - n = \frac{q^n-1}{q-1} - n.$ $\qquad\square$

Lemma 5.22. *For $\vec{a} \in \bar{S}_J(I)$ we have $\deg_I(\vec{a}) \le \deg_I(\vec{p}) - \sum_{j \in J}q^{|I^{<j}|}$ and for $\vec{a} \in \bar{S}_I(I)$ we have $\deg_I(\vec{a}) \le (n - |I|)q^{|I|} - n \le q^{n-1} - n.$*

Proof. From 5.16 and 5.20, we know that

$$\deg_I(\vec{a}) - \deg_I(\vec{p}) = \sum_{i \in J}(b_i^J - q^{|J^{>i}|} + 1) + \sum_{i \in K}q^{|I^{<k}|}(b_i^J - q^{|J^{>i}|} + 1).$$

Since $\vec{a} \in \bar{S}_J(I)$, we know from 5.5 and 5.15 that if $i \in J$ then $b_i^J < 0$, hence $b_i^J \le -1$, and if $i \in K$ then $b_i^J = 0$.

Thus $\deg_I(\vec{a}) - \deg_I(\vec{p}) \le -\sum_{i \in J}q^{|J^{>i}|} - \sum_{i \in K}q^{|I^{<i}|}(q^{|J^{>i}|} - 1)$, so

$$\deg_I(\vec{a}) - \deg_I(\vec{p}) + \sum_{j \in J}q^{|I^{<j}|} \le -\sum_{i \in J}(q^{|J^{>i}|} - q^{|I^{<i}|}) - \sum_{i \in K}q^{|I^{<i}|}(q^{|J^{>i}|} - 1).$$

Let A denote the negative of the right hand side. We need to show that $A \ge 0$, but in fact we claim that $A = 0$.

Since $I^{<i} = J^{<i} \amalg K^{<i}$ and for $i \in K$ we have $J = J^{<i} \amalg J^{>i}$ we find that

$$A = \sum_{i \in J}(q^{|J^{>i}|} - q^{|I^{<i}|}) + \sum_{i \in K}(q^{|K^{<i}|}q^{|J|} - q^{|I^{<i}|})$$

$$= \sum_{i \in J}q^{|J^{>i}|} + q^{|J|}\sum_{i \in K}q^{|K^{<i}|} - \sum_{i \in I}q^{|I^{<i}|}$$

$$= \tfrac{1}{q-1}\left[(q^{|J|} - 1) + q^{|J|}(q^{|K|} - 1) - (q^{|I|} - 1)\right]$$

$$= 0.$$

For the second claim of the lemma we have $J = I$, so the first claim yields $\deg_I(\vec{a}) - \deg_I(\vec{p}) \leq -\sum_{i \in I} q^{|I^{<i}|}$.

From 5.14 and 5.19, we obtain $\deg_I(\vec{p}) = \sum_{i \in I} p_i q^{|I^{<i}|} = \sum_{i \in I} (n-i)(q-1)q^{|I^{<I}|}$.

So $\deg_I(\vec{a}) \leq \sum_{i \in I}((n-i)(q-1)-1)q^{|I^{<i}|}$. Observe that, as I varies but $t = |I|$ remains constant, the sum on the right hand side is largest when $I = \langle 1, \ldots, t \rangle$ and then its value is $B = \sum_{i=1}^{t}((n-i)(q-1)-1)q^{i-1}$. Notice, for later use, that this increases with t.

$$B = \left[n(q-1)-1\right]\sum_{i=1}^{t} q^{i-1} - \sum_{i=1}^{t} i(q-1)q^{i-1}$$

$$= \left[n(q-1)-1\right]\sum_{i=1}^{t} q^{i-1} - \left[tq^t - \sum_{i=1}^{t} q^{i-1}\right]$$

$$= (n-t)q^t - n.$$

We have remarked that this increases with t: the largest value of t allowed is $n-1$, which gives $q^{n-1} - n$. $\qquad \square$

The remaining results in this section are technical observations, which will only be used in the proof of the Trace Lemma.

We define a slight variation on $\lambda(\cdot, \cdot, \cdot)$ (5.4) to emphasize the dependency on the last variable. This function will frequently occur as an exponent in the proof of the Trace Lemma.

Definition 5.23. $[f(l)]$ For fixed J and $\vec{a} \in P(J)$ we define $f(l) = \lambda(J, \vec{a}, l-1)$. (See 5.4.)

Thus $f(l)$ depends implicitly on $J^{\geq l}$ and $\vec{a}_{J \geq l}$ as well as on l.

Lemma 5.24. $f(n+1) = 0$ and f satisfies:

$$f(l) = \begin{cases} qf(l+1) - a_l(q-1) & l \in J \\ f(l+1) + q - 1 & l \notin J. \end{cases}$$

Proof. The first part follows from the definitions and the second from Lemma 5.25, which is straightforward to prove. $\qquad \square$

Lemma 5.25. μ satisfies

$$\mu(J, l-1) = \begin{cases} q\mu(J, l) & l \in J \\ \mu(J, l) + q - 1 & l \notin J \end{cases}$$

and ψ satisfies

$$\psi(J^{>l-1}, \vec{a}) = \begin{cases} q\psi(J^{>l}, \vec{a}) + (q-1)a_l & l \in J, \\ \psi(J^{>l}, \vec{a}) & l \notin J. \end{cases}$$

We will also need another variation on this theme. Recall our convention that $I = J \amalg K$.

Definition 5.26. $[S_J(J)$-k-compatible] Let $\vec{a} \in P(J)$ and let $k \in I$. We say that $\vec{a}$ is $S_J(J)$-k-compatible if $\text{IE}_{J,j}$ is satisfied for each $j \in J^{>k}$.

Lemma 5.27. *If $\vec{a}$ is $S_J(J)$-$(l-1)$-compatible then $f(l+1) < f(l)$ and if also $l \in J$ then $a_l < f(l+1)$.*

Proof. By hypothesis and the definition of IE we know that if $l \in J$ then $a_l + \psi(J^{>l}, \vec{a}) < \mu(J, l)$. Now move the ψ term to the other side of the inequality and apply the definition of f (5.23) to see that $a_l < f(l+1)$.

For the first inequality use 5.24. If $l \notin J$ the result is clear and if $l \in J$ then $f(l) = qf(l+1) - a_l(q-1) > qf(l+1) - f(l+1)(q-1) = f(l+1)$. $\square$

Lemma 5.28. *If $\vec{a}$ is $S_J(J)$-k-compatible, then it is $S_J(J)$-l-compatible for any $l \geq k$ and $f(l) \geq 0$ for any $l > k$.*

Proof. The first claim follows from the definitions. The second is because $f(n+1) = 0$ (5.24) and $f(l) > f(l+1) > \cdots > f(n+1)$, by 5.27. $\square$

Lemma 5.29. *The $S_J(J)$-k-compatibility of $\vec{a} \in P(J)$ depends only on the values of a_j for $j \in J^{>k}$.*

Proof. Examine the definitions. $\square$

For the next two lemmas we write $K = \langle k_1, \ldots, k_{|K|} \rangle$ and suppose that $1 < m \leq |K|$. We are given $\vec{a} \in P(J)$ and define $\vec{\alpha} \in P(J \cup K^{\leq k_{m-1}})$ to have i-th coordinate a_i if $i \in J$ and $\lambda(J, \vec{a}, i)$ if $i \in K^{\leq k_{m-1}}$.

Lemma 5.30. $\lambda(J \cup K^{\leq k_{m-1}}, \vec{\alpha}, k_m) = \lambda(J, \vec{a}, k_m)$.

Proof. Note that $(J \cup K^{\leq k_{m-1}})^{>k_m} = J^{>k_m}$ and apply the definition of λ. $\square$

Lemma 5.31. *If $\vec{a}$ is $S_J(J)$-k_1-compatible, then α is $S_{J \cup K^{\leq k_{m-1}}}(J \cup K^{\leq k_{m-1}})$-$k_m$-compatible.*

Proof. Since none of $k_1, \ldots, k_m$ are strictly greater than k_m, the k_i-coordinates do not matter (5.29), and to see that $\vec{\alpha}$ is $S_{J \cup K^{\leq k_{m-1}}}(J \cup K^{\leq k_{m-1}})$-$k_m$-compatible it is enough to show that $\vec{a}$ is $S_J(J)$-k_m-compatible. But $\vec{a}$ is $S_J(J)$-k_1-compatible by hypothesis, and this is a stronger condition (5.28). $\square$

6. The Splitting of the Polynomial Ring

There is a certain easily defined kU_I-submodule of S, which we denote by $T(I)$, from which we can recover the whole of S as a kU_I-module. Recall that the invariants under U_I are denoted by d's.

Definition 6.1. [$T(I)$] Let $T(I) = \oplus T_r$ be the k-subspace of $k[x_1, \ldots, x_n]$ spanned by $\{x_1^{a_1} \cdots x_n^{a_n} \mid a_u < \deg d_u \text{ for } u \notin I\}$.

Lemma 6.2. *$T(I)$ is a kU_I-submodule of $k[x_1, \ldots, x_n]$. It is closed under multiplication by x_i for each $i \in I$.*

Proof. Note that if $g \in U_I$ and $v \notin I$, then $g \cdot x_v = x_v + \sum_{i \in I^{<v}} c_i x_i$ for some $c_i \in k$. $\square$

Lemma 6.3. *$T(I)$ is closed under multiplication by d_i for $i \in I$, and also under multiplication by h_j for $j \in J$.*

Proof. Apply Lemma 6.2 and the formula for the invariants (4.5). $\square$

If we order the x's by $x_1 < x_2 < \cdots < x_n$, and monomials lexicographically, then $d_u = x_u^{\deg d_u} + (\text{lower terms})$, and the lower terms are monomials in x_u and the x_i with $i \in I$.

Lemma 6.4. $k[x_1, \ldots, x_n] \cong k[d_u \mid u \notin I] \otimes T(I)$ *as a graded* $k[d_{i_1}, \ldots, d_{i_{|I|}}]U_I$*-module.*

Proof. The multiplication map from the right hand side to the left is $k[d_{i_1}, \ldots, d_{i_{|I|}}]U_I$-equivariant, so we need only show that it is a bijection.

Let $H \subseteq \{1, \ldots, n\}$ be disjoint from I. Let $T(I, H)$ be the subspace of S spanned by $\{x_1^{a_1} \cdots x_n^{a_n} \mid a_u < \deg d_u \text{ for } u \in H\}$.

We claim that $S \cong k[d_i \mid i \in H] \otimes T(I, H)$ by the multiplication map. The proof is by induction on $|H|$; the case $H = \varnothing$ is trivial and the case $I \amalg H = \{1, \ldots, n\}$ is the statement of the lemma.

Let $u \in H$ and let $H' = H - \{u\}$. For the induction step it suffices to show that $T(I, H) \cong k[d_u] \otimes T(I, H')$. But we mentioned above that $d_u = x_u^{\deg d_u} + (\text{lower terms})$, and the lower terms are in $T(I) \subseteq T(I, H')$. Also, it is clear from the definitions that $T(I, H) = k[x_u^{\deg d_u}] \otimes T(I, H')$. It is easy to check that $d_u T(I, H) \cap T(I, H') = 0$, hence $T(I, H) = d_u T(I, H) \oplus T(I, H')$, by considering the dimension in each degree. The induction step follows by repeated substitution for $T(I, H)$. $\square$

Lemma 6.5. $T(I)^{U_I} = k[d_{i_1}, \ldots, d_{i_{|I|}}]$.

Proof. $T(I)^{U_I} = k[x_1, \ldots, x_n]^{U_I} \cap T(I) = k[d_1, \ldots, d_n] \cap T(I) = k[d_{i_1}, \ldots, d_{i_{|I|}}]$. $\square$

Lemma 6.6. *If* $J \subseteq I$*, then* $T(J)$ *is a* U_J*-submodule of* $T(I)$*.*

Proof. By Lemma 6.2, $T(J)$ is a U_J-module and so is $T(I)$, by restriction. From the definition of $T(J)$ (6.1), it is clear that $T(J) \subseteq T(I)$. $\square$

7. Monomials

In this section we make the association of a collection of monomials to a submodule of one of our polynomial rings precise. We also prove that we can perform certain constructions (most notably that of direct complements, 7.19) in a way that preserves this leading-monomial information.

We will apply the results of this section to several different groups and their rings of invariants; for convenience here we will take the group to be U_I and so the polynomial generators of the invariant ring are d's.

Notation 7.1. $[d_I, \ d_I^{\vec{a}}]$ We write $d_I = \{d_i \mid i \in I\}$. For $\vec{a} \in P(I)$, we write $d_I^{\vec{a}}$ for the monomial $\prod_{i \in I} d_i^{a_i}$.

The map $\vec{a} \mapsto d_I^{\vec{a}}$ gives a one-to-one correspondence between the elements of $P(I)$ and monomials in the d_i for $i \in I$. Notice that this is compatible with 5.19 in the sense that $\deg(d_I^{\vec{a}}) = \deg_I(\vec{a})$.

Definition 7.2. [Ordering] We legislate that the d_i are ordered as $d_1 < d_2 < \cdots < d_n$ and then the monomials in $k[d_1, \ldots, d_n]$ are lexicographically ordered. We regard 0 as the least element of the set of monomials. This ordering is transferred to $P(I)$.

Lemma 7.3. *Suppose that $\vec{v} = (v_{l+1}, \ldots, v_n)$ and $\vec{a} = (a_{l+1}, \ldots, a_n)$ are in $P(\{l + 1, \ldots, n\})$ and that m, m' are any monomials involving only $d_1, \ldots, d_l$. If $d^{\vec{v}} > d^{\vec{a}}$, then we have $m \cdot d^{\vec{v}} > m' \cdot d^{\vec{a}}$.*

Definition 7.4. $[H(\vec{a})]$ Given $\vec{a} \in P(I)$, we write $H(\vec{a})$ for the vector space spanned by $\{d_I^{\vec{v}} \mid \vec{v} \in P(I) \text{ and } \vec{v} > \vec{a}\}$. Sometimes for clarity we write $H(\vec{a}, k[d_I])$, or $H(d^{\vec{a}}, k[d_I])$.

Lemma 7.5. $H(\vec{a})$ *is an ideal in $k[d_I]$.*

We refer to $H(\vec{a})$ as the ideal of "higher terms", or the "error ideal" corresponding to $\vec{a}$.

Notation 7.6. [LM] For $f \in k[d_I]$, we write $\text{LM}(f)$ for the least monomial of f in the ordering described above, i.e. the monomial *lowest* in the ordering which appears with non-zero coefficient in the expression for f as a sum of monomials. If $f = 0$ then $\text{LM}(f) = 0$.

Notice that LM ignores any coefficient that this monomial may have. We may choose to regard the value of LM as an element of $P(I)$ when it is convenient to do so.

Lemma 7.7. *Let $\{f_1, \ldots, f_r\} \subset k[d_I]$ and suppose that the $\text{LM}(f_i)$ are distinct and non-zero. Let $\lambda_i \in k$ for $i = 1, \ldots, r$. Then*
  (1) $\text{LM}(\sum_{i=1}^r \lambda_i f_i) = \min\{\text{LM}(f_i) \mid \lambda_i \neq 0\}$.
  (2) *The f_i are linearly independent.*

Proof. The first assertion is clear. The second follows from the first since $\sum \lambda_i f_i = 0$ implies that $0 = \text{LM}(\sum \lambda_i f_i) = \min\{\text{LM}(f_i) \mid \lambda_i \neq 0\}$, so all the λ_i must be 0. $\square$

Lemma 7.8. *If $f, m \in k[d_I]$ and m is a monomial, then $\text{LM}(mf) = m \, \text{LM}(f)$.*

Definition 7.9. [soc] Recall that the socle of a kG-module M, denoted by $\text{soc} \, M$, is the sum of the irreducible submodules.

The socle has the following well-known properties.

Lemma 7.10. *Let G be a finite group and let M and N be kG-modules. Then*
  (1) *If $\text{soc} \, M = 0$ then $M = 0$.*
  (2) *If $f : M \to N$ is injective on $\text{soc} \, M$ then it is injective.*
  (3) *If G is a p-group then $\text{soc} \, M$ is just the submodule of invariants, M^G.*

The next lemma is also well known.

Lemma 7.11. *Let G be a finite group, $H \leq G$ and let M be a kH-module. Then $(\text{Ind}_H^G M)^G = \{\sum_{g \in G/H} g \otimes m \mid m \in M^H\} \cong M^H$, by the morphism $m \mapsto \sum_{g \in G/H} g \otimes m$, $m \in M^H$.*

Proof. We concentrate on the equality, since the isomorphism is clear. Certainly the right hand side is contained in the left hand side. Fix a set of representatives $\{g_i\}$ for G/H with $g_1 = 1$, so any $x \in \text{Ind}_H^G M$ can be written uniquely as $\sum_{i=1}^{|G/H|} g_i \otimes m_i$ for some $m_i \in M$.

If x is invariant under H then m_1 must be invariant under H and if x is invariant under g_i then $g_i \otimes m_i = g_i(1 \otimes m_1) = g_i \otimes m_1$, so $m_i = m_1$. Thus if x is invariant under G it must have the form claimed. $\square$

Notation 7.12. [supp X] Let X be a graded kU_I-submodule of $T(I)$, so soc $X \subseteq k[d_I]$. We write supp X for $\{\mathrm{LM}(x) \mid x \in \mathrm{soc}\, X,\, x \neq 0\}$.

Lemma 7.13. *Suppose that for each $m \in \mathrm{supp}\, X$ we are given an element $s_m \in \mathrm{soc}\, X$ with $\mathrm{LM}(s_m) = m$. Then $\{s_m \mid m \in \mathrm{supp}\, X\}$ is a basis for $\mathrm{soc}\, X$.*

Proof. $\{s_m \mid m \in \mathrm{supp}\, X\}$ is a linearly independent set by 7.7. To see that this set spans soc X, fix a degree r (in order to make soc X_r finite-dimensional) and let $s \in \mathrm{soc}\, X_r$ be outside the span of $\{s_m\}$ with $\mathrm{LM}(s)$ maximal. Then there is a $c \in k$ such that $s - c s_{\mathrm{LM}(s)}$ has a higher least monomial and is also outside the span of $\{s_m\}$, a contradiction. $\qquad\square$

Lemma 7.14. *If X and Y are graded submodules of $T(I)$ then*
  (1) $\mathrm{supp}(X \cap Y) \subseteq \mathrm{supp}\, X \cap \mathrm{supp}\, Y$.
  (2) *If $\mathrm{supp}\, X \cap \mathrm{supp}\, Y = \varnothing$ then $X + Y$ is a direct sum and $\mathrm{supp}(X + Y) = \mathrm{supp}\, X \amalg \mathrm{supp}\, Y$.*

Proof. Since $\mathrm{soc}(X \cap Y) = \mathrm{soc}\, X \cap \mathrm{soc}\, Y$, (1) follows from the definition of supp.

  To prove (2), note that X and Y are linearly independent by part (1) and Lemma 7.10. Now the result follows from 7.7(1). $\qquad\square$

Lemma 7.15. *Let $\{X_i \mid i = 1, \ldots, r\}$ be graded submodules of $T(I)$ with $\mathrm{supp}\, X_i$ pairwise disjoint. Then the sum of the X_i is direct.*

Proof. We prove by induction on r that $\sum_{i=1}^{r} X_i$ is direct and that $\mathrm{supp}(\sum_{i=1}^{r} X_i) = \amalg_{i=1}^{r} \mathrm{supp}\, X_i$. The case $r = 1$ is vacuous, and the case $r = 2$ is Lemma 7.14.

  The general case follows by applying the case $r = 2$ to the modules $\sum_{i=1}^{r-1} X_i$ and X_r. $\qquad\square$

  Suppose that $X \subseteq T(I)$ is a U_I-submodule and $D \subseteq d_I$. Then $k[D] \cdot X$ is also a kU_I-submodule of $T(I)$.

Notation 7.16. [Propagation] When the multiplication map $k[d_K] \otimes_k X \to T(I)$ is an injection we say that X is *propagated* by d_K, and we call $k[d_K] \cdot X$ the *propagation* of X by d_K.

Lemma 7.17. *The support of the propagation of X by d_K is $k[d_K] \cdot \mathrm{supp}\, X$.*

Proof. Apply Lemma 7.8. $\qquad\square$

Lemma 7.18. *Let $X \subseteq T(I)_m$ be a kG-submodule and let d be a monomial of $k[d_I]$ of degree M. Suppose that $d \cdot X$ has a complement $Y \subseteq T(I)_{m+M}$. Then X has a complement $Y' \subseteq T(I)_m$. If $\mathrm{supp}(d \cdot X) \cap \mathrm{supp}\, Y = \varnothing$ then Y' can be chosen to satisfy $\mathrm{supp}\, X \cap \mathrm{supp}\, Y' = \varnothing$.*

Proof. By hypothesis we have $(d \cdot X) \oplus Y = T(I)_{m+M}$; there is a projection $\pi \colon T(I)_{m+M} \to d \cdot X$ corresponding to this decomposition with $\ker \pi = Y$. Then the map $d^{-1} \cdot \pi(d \cdot (\ ))$ on $T(I)_m$ is idempotent with image X, so we can take $Y' = \ker \pi(d \cdot (\ ))$.

  To prove the last claim, note that if $x \in \mathrm{supp}\, X \cap \mathrm{supp}\, Y'$ then $d \cdot x \in \mathrm{supp}(d \cdot X) \cap \mathrm{supp}\, Y = \varnothing$, a contradiction. $\qquad\square$

Lemma 7.19. *Suppose that X_i and Y_i are graded kU_I-submodules of $T(I)$ such that $T(I) = X_i \oplus Y_i$ for $i = 1, \ldots, m$, such that*
  (1) $\mathrm{supp}\, X_i \cap \mathrm{supp}\, X_j = \varnothing$ *when $i \neq j$ and*

(2) $\operatorname{supp} T(I) = \operatorname{supp} X_i \amalg \operatorname{supp} Y_i$ *for each i.*

Then

(1) $T(I) = (\oplus_{i=1}^m X_i) \oplus (\cap_{i=1}^m Y_i)$ *as kU_I-modules and*
(2) $\operatorname{supp} T(I) = (\amalg_{i=1}^m \operatorname{supp} X_i) \amalg \operatorname{supp}(\cap_{i=1}^m Y_i)$.

Proof. It is sufficient to prove this degree by degree, so we may restrict our attention to $T(I)_r$. Using the given conditions we see that $\operatorname{supp} T(I)_r = (\amalg_{i=1}^m \operatorname{supp}(X_i)_r) \amalg (\cap_{i=1}^m \operatorname{supp}(Y_i)_r)$. (This is just a statement about sets.) So the sum of the modules $\cap_{i=1}^m (Y_i)_r, (X_1)_r, \ldots, (X_m)_r$ is direct, by 7.15.

Writing codim for the codimension of a subspace of $T(I)_r$, we have

$$\operatorname{codim} \cap_{i=1}^m (Y_i)_r \le \sum_{i=1}^m \operatorname{codim}(Y_i)_r = \sum_{i=1}^m \dim(X_i)_r.$$

So, by dimension-counting, $T(I)_r = (\sum_{i=1}^m (X_i)_r) + (\cap_{i=1}^m (Y_i)_r)$ for each degree r, proving (1). Part (2) now follows from 7.14(2). $\square$

8. POINCARÉ SERIES LEMMAS

Notation 8.1. [PS] If $Y = \oplus_{n \in \mathbb{Z}} Y_n$ is a graded k-module, finite dimensional in each degree, then we define its Poincaré series to be the formal power series in t defined by $\operatorname{PS}(Y) = \sum_{n \in \mathbb{Z}} (\dim Y_n) t^n$. (In some contexts this is traditionally called the Hilbert series instead.)

Lemma 8.2. *The propagation of the X by d_K (in 7.16) has Poincaré series* $\left(\prod_{k \in K} \frac{1}{1 - t^{\deg d_k}} \right) \cdot \operatorname{PS}(X)$.

Proof. By the definition of propagation, it is isomorphic to $k[d_K] \otimes X$. $\square$

Lemma 8.3. *Let W be a graded submodule of $T(I)$, and let $X_1, \ldots, X_r$ be graded submodules of W such that*

$$\operatorname{PS}(X_1) + \cdots + \operatorname{PS}(X_r) = \operatorname{PS}(W) \quad \text{and} \quad \operatorname{supp}(X_i) \cap \operatorname{supp}(X_j) = \varnothing \text{ when } i \ne j.$$

Then W is the direct sum of the submodules $X_1, \ldots, X_r$.

Proof. The sum of the X_i is direct, by 7.15, and $\sum \dim X_i = \dim W$ in each degree by hypothesis. $\square$

Definition 8.4. $[\gamma(t)]$ Let $\gamma(t) = 1 + t + \cdots + t^{q-1}$.

Definition 8.5. $[\kappa_a^{(n-i)}]$ Let $\kappa_a^{(n-i)}$ be the coefficient of t^a in the formal power series $\frac{\gamma(t)^{n-i}}{1-t} = \sum_{a \ge 0} \kappa_a^{(n-i)} t^a$.

Lemma 8.6. *If $a \ge (n-i)(q-1)$ then $\kappa_a^{(n-i)} = q^{n-i}$.*

Proof. Multiplying out the denominator in 8.5 we have $\gamma(t)^{n-i} = \kappa_0^{(n-i)} + \sum_{a \ge 1} (\kappa_a^{(n-i)} - \kappa_{a-1}^{(n-i)}) t^a$.

But $\gamma(t)^{(n-i)}$ is a polynomial of degree $(q-1)(n-i)$, so we must have $\kappa_a^{(n-i)} = \kappa_{a-1}^{(n-i)}$ for $a > (q-1)(n-i)$ and also $\gamma(t)^{n-i} = \kappa_0^{(n-i)} + \sum_{a=1}^{(q-1)(n-1)} (\kappa_a^{(n-i)} - \kappa_{a-1}^{(n-i)}) t^a$. Setting $t = 1$ gives $q^{n-i} = \kappa_0^{(n-i)} + \sum_{a=1}^{(q-1)(n-1)} (\kappa_a^{(n-i)} - \kappa_{a-1}^{(n-i)}) = \kappa_{(q-1)(n-i)}^{(n-i)}$. $\square$

Lemma 8.7. *If $\vec{a} \in S_J(I)$ then $\kappa_{a_k}^{(n-k)} = q^{n-k}$ for each $k \in K$.*

Proof. Just combine 8.6, 5.18 and 5.14. □

Lemma 8.8. *We have $\mathrm{PS}(T(I)) = \sum_{\vec{a} \in P(I)} \prod_{i \in I} \kappa_{a_i}^{(n-i)} \prod_{i \in I} t^{q^{|I^{<i}|}a_i}$.*

Proof. It follows from Definition 6.1 that

$$\mathrm{PS}(T(I)) = \prod_{i \in I} \left(\frac{1}{1 - t^{\deg d_i}} \right) \cdot \prod_{l=1}^{n} (1 + t + \cdots + t^{\deg d_l - 1}).$$

We study the second part of the product and find that, since $\deg(d_l) = q^{|I^{<l}|}$,

$$1 + t + \cdots + t^{\deg d_l - 1} = \prod_{a=0}^{|I^{<l}| - 1} \gamma(t^{q^a}) = \prod_{i \in I^{<l}} \gamma(t^{q^{|I^{<i}|}}).$$

We also have

$$\prod_{l=1}^{n} \prod_{i \in I^{<l}} \gamma(t^{q^{|I^{<i}|}}) = \prod_{i \in I} \prod_{l=i+1}^{n} \gamma(t^{q^{|I^{<i}|}}) = \prod_{i \in I} \gamma(t^{q^{|I^{<i}|}})^{n-i}.$$

Returning to our expression for $\mathrm{PS}(T(I))$, i.e. restoring the first product, we have

$$\mathrm{PS}(T(I)) = \prod_{i \in I} \frac{\gamma(t^{|I^{<i}|})^{n-i}}{1 - t^{|I^{<i}|}} = \prod_{i \in I} \sum_{a_i \geq 0} \kappa_{a_i}^{(n-i)} t^{|I^{<i}|a_i},$$

by the definition of κ (8.5), completing the proof. □

9. ASSEMBLY

In this section we state and prove the key ingredients (9.1, 9.4, 9.5) for the proof by induction on $|I|$ of Theorem 10.1. Here we use the Trace Lemma (16.1): the key application is in Proposition 9.4. This lemma is the only result from Sections 11 through 16 that we need to prove our Structure Theorem (10.1).

Proposition 9.1. *Let $X_1, \ldots, X_r$ be kU_I-submodules of $T(I)$ that are obtained via propagation (7.16), i.e. there are finite-dimensional kU_I-submodules $\bar{X}_1, \ldots, \bar{X}_r$ and subsets D_i of d_I such that X_i is the propagation $k[D_i] \cdot \bar{X}_i \cong k[D_i] \otimes \bar{X}_i$. Suppose also that*

    (1) $\mathrm{supp}\, X_i \cap \mathrm{supp}\, X_j = \varnothing$ *if $i \neq j$ and*
    (2) *there is a polynomial $F \in \mathbb{Z}[t]$ such that $F + \mathrm{PS}(X_1) + \cdots + \mathrm{PS}(X_r) = \mathrm{PS}(T(I))$.*

Then there is a kU_I-submodule $B \subset T(I)$ such that

    (1) $\mathrm{PS}(B) = F$,
    (2) $\mathrm{supp}\, B$ *is the complement of $\cup_i \mathrm{supp}\, X_i$ in $\mathrm{supp}(T(I))$ and*
    (3) $T(I)$ *is the direct sum of the submodules $B, X_1, \ldots, X_r$.*

Proof. Since F is a polynomial, its coefficients are zero in sufficiently large degrees. Therefore, the coefficients of t^a in $\sum_{i=1}^{r} \mathrm{PS}(X_i)$ and in $\mathrm{PS}(T(I))$ are the same for sufficiently large powers of t. By 8.3, it follows that $T(I)$ is the direct sum $X_1 \oplus \cdots \oplus X_r$ in large degrees.

By 7.18, the X_i are *individually* summands in all degrees, with complements Y_i such that $\mathrm{supp}\, X_i \cap \mathrm{supp}\, Y_i = \varnothing$. We can therefore apply 7.19 to see that the X_i are simultaneously

summands, i.e. their direct sum is a summand. We write B for the complement of $\oplus X_i$ in $T(I)$ and note that conclusion 2 of 7.19 implies that B satisfies conclusion 2 of the present proposition. From hypothesis 2 it is immediate that B satisfies conclusion 1. By construction, B satisfies conclusion 3, so we have completed the proof. $\square$

The least element of K will always be denoted by k_1.

Definition 9.2. $[G(I, J), G(J)]$ For $J \subsetneq I$ let

$$G(I, J) = \prod_{k_1 < i \leq n,\ i \notin J} \frac{\theta(x_i; I^{<i})}{\theta(x_i; J^{<i})}.$$

We will often write just $G(J)$ when I is understood.

Note that $G(I, J)$ is a polynomial, since $\theta(x_i; J^{<i})$ divides $\theta(x_i; I^{<i})$ from the definition.

Definition 9.3. [Tr] As usual, if G is a finite group, $H < G$ and M is a kG-module then $\mathrm{Tr}_{G/H} : M^H \to M^G$ is the map $m \mapsto \sum_{g \in G/H} gm$. If $H = 1$ we write just Tr_G.

The proof of the next proposition depends on the Trace Lemma, which will eventually be proved in Section 16. (We ignore the sign in equation (1).)

First we define $h_i = \theta(x_i; J^{<i})$, so $S^{U_J} = k[h_1, \ldots, h_n]$, by Proposition 4.6.

Lemma (Trace Lemma, 16.1). *If $\vec{a} \in P(J)$ is $S_J(J)$-k_1-compatible then*

(1) $$\mathrm{Tr}_{U_I/U_J} \left[G(I, J) \cdot h_J^{\vec{a}} \right] = \pm d_K^{\lambda(J, \vec{a})} d_J^{\vec{a}} + x,$$

where $x \in H(d_K^{\lambda(J, \vec{a})} d_J^{\vec{a}}, k[d_I])$. Furthermore,

(2) $$\mathrm{Tr}_{U_I/U_J} \left[G(I, J) \cdot H(h_J^{\vec{a}}, k[h_J]) \right] \subset H(d_K^{\lambda(J, \vec{a})} d_J^{\vec{a}}, k[d_I]).$$

Proposition 9.4. *Let $T(I)$ be the kU_I-submodule of the polynomial ring S defined in Section 6, and suppose that B is a U_J-submodule of $T(J)$ with $\mathrm{supp}\, B = S_J(J)$. Then there are U_I-submodules $\bar{X}_J(I)$ and $X_J(I)$ of $T(I)$ such that*

(1) $\bar{X}_J(I) = \bigoplus_{g \in U_I/U_J} g \cdot G(I, J) \cdot B$, *which is isomorphic to $\mathrm{Ind}_{U_J}^{U_I} B$ (but with a change of grading),*
(2) $X_J(I) \cong k[d_K] \otimes \bar{X}_J(I)$,
(3) $\mathrm{supp}\, \bar{X}_J(I) = \bar{S}_J(I)$ *and* $\mathrm{supp}\, X_J(I) = S_J(I)$, *and*
(4) $\mathrm{PS}(X_J(I)) = \mathrm{PS}(B) \cdot [U_I : U_J] \cdot \prod_{k \in K} \left(\frac{1}{1 - t^{\deg d_k}} \right) \cdot t^{\deg G(I, J)}$.

Notice that, since B is a U_J-submodule, $\mathrm{supp}\, B$ is calculated with respect to $k[h_1, \ldots, h_n]$, but $\mathrm{supp}\, \bar{X}_J(I)$ and $\mathrm{supp}\, X_J(I)$ are calculated with respect to $k[d_1, \ldots d_n]$.

Proof. We define a map $\rho \colon \mathrm{Ind}_{U_J}^{U_I} B \to T(I)$ using the inclusion $T(J) \subseteq T(I)$, (6.6); if $g \otimes b \in \mathrm{Ind}_{U_J}^{U_I} B = kU_I \otimes_{kU_J} B$ then we set $\rho(g \otimes b) = g \cdot (G(I, J) \cdot b)$. (Note that the first dot is the group action and the second dot multiplication of polynomials.) This map is well defined since $G(I, J)$ is U_J-invariant.

We claim that ρ is injective; by 7.10, it suffices to show that ρ is injective on the socle and $\mathrm{soc}\, \mathrm{Ind}_{U_J}^{U_I} B = (\mathrm{Ind}_{U_J}^{U_I} B)^{U_I} = \{ \sum_{g \in U_I/U_J} g \otimes b \mid b \in B^{U_J} \} \cong \mathrm{soc}\, B$, by 7.11. We need to show that the map that takes $(\sum_{g \in U_I/U_J} g) \otimes b$ to $\mathrm{Tr}_{U_I/U_J}[G(I, J) \cdot b]$ is injective. By hypothesis, $\mathrm{supp}\, B = S_J(J)$, so there is a basis $\{ b(\vec{a}) \mid \vec{a} \in S_J(J) \}$ for $\mathrm{soc}\, B$ with

$\text{LM}(b(\vec{a})) = h_J^{\vec{a}}$ and hence a basis $\{(\sum_{g \in U_I/U_J} g) \otimes b(\vec{a}) \mid \vec{a} \in S_J(J)\}$ for $\text{soc Ind}_{U_J}^{U_I} B$ with $\text{LM}(b(\vec{a})) = h_J^{\vec{a}}$.

By the Trace Lemma (16.1), the least monomial of

$$\rho\Big(\sum_{g \in U_I/U_J} g \otimes b(\vec{a}) \Big) = \text{Tr}_{U_I/U_J}[G(I,J) \cdot b(\vec{a})] \quad \text{is} \quad d_K^{\vec{\lambda}(J,\vec{a})} d_J^{\vec{a}}.$$

In particular, for different $\vec{a}$ the least monomials are distinct so, by 7.13, we have shown that the given basis of $\text{soc Ind}_{U_J}^{U_I} B$ is mapped to a linearly independent set in $T(I)$. It follows that ρ is injective and we have therefore produced a module $\bar{X}_J(I) = \rho(\text{Ind}_{U_J}^{U_I} B) \subset T(I)$, with the socle having a basis with least terms as specified above.

By the construction of $\bar{X}_J(I)$ it follows that

$$\text{supp } \bar{X}_J(I) = \{d_K^{\vec{\lambda}(J,\vec{a})} d_J^{\vec{a}} \mid \vec{a} \in S_J(J)\}$$

and, by 5.7 this is equal to $\{d_I^{\vec{a}} \mid \vec{a} \in \bar{S}_J(I)\}$.

Consider the multiplication map $k[d_K] \otimes \bar{X}_J(I) \to T(I)$ and denote its image by $X_J(I)$. Clearly

$$\text{supp } X_J(I) = \{d_K^{\vec{b}} d_I^{\vec{a}} \mid \vec{b} \in P(K), \vec{a} \in \bar{S}_J(I)\},$$

so $\text{supp } X_J(I) = S_J(I)$ by 5.6. Also $\text{soc}(k[d_K] \otimes \bar{X}_J(I)) = k[d_K] \otimes \text{soc } \bar{X}_J(I)$, which has a basis consisting of elements $m \otimes b$, where m is a monomial in $k[d_K]$ and b is from our basis for B. The images of these have distinct least monomials, so the multiplication map is injective by the same argument as was used for ρ.

To see that (4) holds, note that $\text{PS}(\bar{X}_J(I)) = t^{\deg G(I,J)}[U_I : U_J] \cdot PS(B)$, and that the extra factor in condition (4) comes from the propagation of $\bar{X}_J(I)$ by $k[d_K]$ using 8.2. $\quad\square$

Corollary 9.5. *With the hypotheses of Proposition 9.4, if we have in addition*

$$\text{PS}(B) = \sum_{\vec{a} \in S_J(J)} \prod_{j \in J} \kappa_{a_j}^{(n-j)} t^{q^{|J^{<j}|} a_j},$$

then we may refine conclusion (4) to state that

$$\text{PS}(X_J(I)) = \sum_{\vec{a} \in S_J(I)} \prod_{i \in I} \kappa_{a_i}^{(n-i)} t^{q^{|I^{<i}|} a_i}.$$

To give the proof of Corollary 9.5 we require several lemmas, which we state now.

Definition 9.6. $[\nu(J,j,k)]$ Let

$$\nu(J,j,k) = \begin{cases} (q-1)q^{|(J^{<j})^{>k}|} & \text{if} \quad k < j \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 9.7. *We have* $\psi(J^{>k}, \vec{a}) = \sum_{j \in J} \nu(J,j,k) a_j$.

Proof. By definition of ψ (5.3), $\psi(J^{>k}, \vec{a}) = (q-1) \sum_{j \in J^{>k}} q^{|(J^{>k})^{<j}|}$. $\quad\square$

Lemma 9.8. *We have* $\deg h_j = \deg d_j - \sum_{k \in K} \deg d_k^{\nu(J,j,k)}$.

Proof. Observe that $\deg h_j = q^{|J^{<j}|}$ and $\deg d_j = q^{|I^{<j}|}$. By the definition of ν (9.6), we have

$$\sum_{k \in K} \deg d_k^{\nu(J,j,k)} = \sum_{k \in K^{<j}} q^{|I^{<k}|}(q-1)q^{|(J^{<j})^{>k}|}.$$

It is easily verified that, for $k < j$, $I^{<k} \amalg (J^{<j})^{>k} = J^{<j} \amalg K^{<k}$ and it follows that

$$\sum_{k \in K} \deg d_k^{\nu(J,j,k)} = \sum_{k \in K^{<j}} q^{|J^{<j} \cup K^{<k}|}(q-1) = \sum_{u=|J^{<j}|}^{|I^{<j}|-1} q^u(q-1) = q^{|I^{<j}|} - q^{|J^{<j}|}.$$

$\square$

Lemma 9.9. *We have* $\deg G(I,J) = \prod_{k \in K} \deg d_k^{\mu(J,k)}$.

Proof. A direct proof is possible, but it is easier to apply the Trace Lemma (16.1) with $\vec{a} = 0$ and note that $\lambda(J,0,k) = \mu(J,k)$ (see 5.4). Thus the degree of $\mathrm{Tr}_{U_I/U_J} G(I,J)$ is the right hand side of the equation of the lemma. Since $G(I,J)$ is homogeneous, this must be $\deg G(I,J)$. $\square$

Proof of Corollary 9.5. To simplify this proof, instead of powers of t in the Poincaré series we will write invariants, where each invariant d is meant to stand for $t^{\deg d}$.

Using conclusion (4) of Proposition 9.4 and the expression for PS(B) in the hypothesis, we obtain:

$$PS(X_J(I)) = \sum_{\vec{a} \in S_J(J)} \left[\left(\prod_{j \in J} \kappa_{a_j}^{(n-j)} \right) \cdot h_J^{\vec{a}} \cdot [U_I : U_J] \cdot \left(\prod_{k \in K} \frac{1}{1-d_k} \right) \cdot t^{\deg G(I,J)} \right].$$

Using 9.9 we can replace $t^{\deg G(I,J)}$ by $\prod_{k \in K} d_k^{\mu(J,k)}$ and by 9.8 we can replace h_j by $d_j \prod_{k \in K} d_k^{-\nu(J,j,k)}$. (All that this means is that the degrees are the same.) We know from the definition of the groups that $[U_I : U_J] = |U_K| = \prod_{k \in K} q^{n-k}$. We can also write $\prod_{k \in K} \frac{1}{1-d_k} = \sum_{\vec{b} \in P(K)} d_K^{\vec{b}}$. Therefore we have:

$$PS(X_J(I)) = \sum_{\vec{a} \in S_J(J)} \left[\prod_{j \in J} \kappa_{a_j}^{(n-j)} \cdot \prod_{j \in J}(d_j \prod_{k \in K} d_k^{-\nu(J,j,k)})^{a_j} \cdot \prod_{k \in K} q^{n-k} \cdot \sum_{\vec{b} \in P(K)} d_K^{\vec{b}} \cdot \prod_{k \in K} d_k^{\mu(J,k)} \right].$$

But $\prod_{j \in J} d_k^{-\nu(J,j,k)a_j} = d_k^{\sum_{j \in J} -\nu(J,j,k)a_j} = d_k^{-\psi(J^{>k},\vec{a})}$, by 9.7, and combining this with $d_k^{\mu(J,k)}$ and $d_k^{b_k}$ we obtain $d_k^{b_k+\lambda(J,\vec{a},k)}$.

Now set $\alpha_k = b_k + \lambda(J,\vec{a},k)$ for $k \in K$. We combine this with $\vec{a}$ to form a new vector $\vec{\alpha} \in P(I)$. The condition $b_k \geq 0$ for $k \in K$ now becomes $\alpha_k \geq \lambda(J,\vec{\alpha},k)$, which is $\mathrm{IE}_{J,k}$ for $\vec{\alpha}$, and the condition $\vec{a} \in S_J(J)$ yields $\mathrm{IE}_{J,j}$ for $j \in J$.

Thus $\sum_{\vec{a} \in S_J(J)} \sum_{\vec{b} \in P(K)}$ can be replaced by $\sum_{\vec{\alpha} \in S_J(I)}$ and we obtain:

$$PS(X_J(I)) = \sum_{\vec{\alpha} \in S_J(I)} \left[\left(\prod_{j \in J} \kappa_{a_j}^{(n-j)} \right) \cdot \left(\prod_{k \in K} q^{n-k} \right) \cdot d_I^{\vec{\alpha}} \right].$$

But, since $\vec{\alpha} \in S_J(I)$, we can apply 8.7 to replace $\prod_{k \in K} q^{n-k}$ by $\prod_{k \in K} \kappa_{\alpha_k}^{(n-k)}$ and combine it with the other κ-term to obtain $\prod_{i \in I} \kappa_{\alpha_i}^{(n-i)}$.

All that remains is to replace the d_i by powers of t. $\square$

10. The Main Theorem

We can now put all of this together to prove the promised Structure Theorem.

Theorem 10.1. *For all $I \subseteq \{1, \ldots, n-1\}$ there is a direct sum decomposition as graded kU_I-modules $T(I) \cong \oplus_{J \subseteq I} X_J(I)$, where*

(1) $X_J(I) \cong k[d_k \mid k \in K] \otimes \bar{X}_J(I)$ *by the multiplication map,*
(2) $\bar{X}_J(I) = \bigoplus_{g \in U_I/U_J} g \cdot G(I, J) \cdot X_J(J)$, *which is isomorphic to* $\mathrm{Ind}_{U_J}^{U_I} X_J(J)$ *(but with a change of grading),*
(3) $\mathrm{supp}\, \bar{X}_J(I) = \bar{S}_J(I)$ *and* $\mathrm{supp}\, X_J(I) = S_J(I)$,
(4) $\mathrm{PS}(X_J(I)) = \sum_{\vec{a} \in S_J(I)} \prod_{i \in I} \kappa_{a_i}^{(n-i)} t^{q^{|I^{<i}|} a_i}$.

Proof. We prove the theorem by induction on $t = |I|$, the number of rows. Let $J \subsetneq I$, so that U_J is a group with fewer than t rows. By induction, we may apply the Theorem to U_J and obtain a direct sum decomposition of $T(J)$ and, in particular, a finite-dimensional submodule $X_J(J)$. Applying Proposition 9.4 and Corollary 9.5, we obtain a submodule $X_J(I) \subseteq T(I)$ with the properties required by the statement of the Theorem. It remains to exhibit the module $X_I(I)$.

By Proposition 5.10 the complement of $\cup_{J \subsetneq I} S_J(I)$ in $P(I)$ is $S_I(I)$ and since, by 8.8,

$$\mathrm{PS}(T(I)) = \sum_{\vec{a} \in P(I)} \prod_{i \in I} \kappa_{a_i}^{(n-i)} t^{q^{|I^{<i}|} a_i},$$

it follows that

$$\mathrm{PS}(T(I)) - \sum_{J \subsetneq I} \mathrm{PS}(X_J(I)) = \sum_{\vec{a} \in S_I(I)} \kappa_{a_i}^{(n-i)} t^{q^{|I^{<i}|} a_i}.$$

Now set

$$F = \sum_{\vec{a} \in S_I(I)} \kappa_{a_i}^{(n-i)} t^{q^{|I^{<i}|} a_i}$$

and apply Proposition 9.1 to obtain a module B. We set $X_I(I) = B$ and note that, by construction, $X_I(I)$ has the properties required, by the statement of the present theorem. $\square$

Combining this with 6.4 we obtain the Main Theorem of the Introduction 1.1.

11. Overview of the Trace Lemmas

Our aim in the next part of the paper is to prove the Trace Lemma (16.1), which will complete the proof of Theorem 10.1. In order to prove this lemma, we start with an elementary fact about finite fields (12.3), which can be considered as computing a trace over the additive group of k. Since we can obtain the group U_K over which we must compute a trace by repeated extensions by groups isomorphic to k^+, we can perform a proof by induction.

More explicitly, the group U_K can be written as a product $U_{\{k_1\}} \cdot U_{\{k_2\}} \cdots U_{\{k_{|K|}\}}$, breaking it up row by row. We refer to the result for $U_{\{k_i\}}$ as the "One-Row" Trace Lemma (15.3). In order to obtain this we need a result for groups with one row having only m positions with nonzero entries, which we call the "m-Step" Lemma (15.2). The key point

in the proof of the m-Step Lemma is the induction step, or "One-Step" Lemma (14.1). This is where almost all of the bookkeeping is concentrated.

Once the proof of the One-Row Trace Lemma is complete, we must do a second induction to prove the "m-Row" Lemma (16.2). This lemma follows in a completely formal way from the One-Row Lemma, and the Trace Lemma (16.1), which is our ultimate goal, is a special case of the m-Row Lemma.

The reader should note that the only result in Sections 12 to 16 that is used in any other part of the paper is the Trace Lemma itself (16.1). Furthermore, the extra bookkeeping (starting in Lemma 12.18) required to get the sign in the Trace Lemma is not necessary for our application.

In principle, the traces we need can be calculated by the elegant method of [17], but the change of basis required seems difficult to formulate explicitly.

Now we fix the notation for the invariants of all the different groups that we will consider. We start with the invariants of U_J, which are denoted by h's. As we move to larger groups, we move the letters used to denote the invariants down the alphabet, so that g's denote invariants of $U_{J \cup \{k_1\}}$, f's denote invariants of $U_{J \cup K^{\leq k_{m-1}}}$, e's denote invariants of $U_{J \cup K^{\leq k_m}}$, and d's denote invariants of U_I (consistently with 4.5). To summarize:

Definition 11.1. $[d_i, e_i, f_i, g_i, h_i]$ For given $k_m \in K$, let $h_i = \theta(x_i; J^{<i})$, $g_i = \theta(x_i; (J \cup \{k_1\})^{<i})$, $f_i = \theta(x_i; (J \cup K^{\leq k_{m-1}})^{<i})$, $e_i = \theta(x_i; (J \cup K^{\leq k_m})^{<i})$, $d_i = \theta(x_i; I^{<i})$.

By Proposition 4.6, the d_i, e_i, f_i, g_i, and h_i are algebraically independent and generate the invariant rings of the groups U_I, $U_{J \cup K^{\leq k_m}}$, $U_{J \cup K^{\leq k_{m-1}}}$, $U_{J \cup \{k_1\}}$, and U_J, i.e.:

$$
\begin{aligned}
S^{U_I} &= k[d_1, \ldots, d_n] & S^{U_{J \cup \{k_1\}}} &= k[g_1, \ldots, g_n] \\
S^{U_{J \cup K^{\leq k_m}}} &= k[e_1, \ldots, e_n] & S^{U_J} &= k[h_1, \ldots, h_n] \\
S^{U_{J \cup K^{\leq k_{m-1}}}} &= k[f_1, \ldots, f_n].
\end{aligned}
$$

We also need some basic subgroups, from which the other groups are built.

Notation 11.2. $[A(x_i, x_j)]$ $A(x_i, x_j)$ is the subgroup of U_n consisting of matrices with just one non-zero off-diagonal entry in position (i, j). (Mnemonic: **A**dd $\mathbf{x_i}$ to $\mathbf{x_j}$.)

Thus $A(x_i, x_j) = \{a_{ij}(\lambda) \mid \lambda \in k\}$ (see §4).

12. Trace Lemmas

Many of the results in this section are well known.

Notation 12.1. $[\theta(y, x)]$ We write $\theta(y, x)$ for $\prod_{\lambda \in k}(y + \lambda x)$. (This is just a slight variation on the definition of θ in 4.4.)

Lemma 12.2. θ has the following properties:
  (1) $\theta(y, x) = y^q - y x^{q-1}$,
  (2) $\theta(v; I) = 0$ if v is a linear combination of the x_i for $i \in I$,
  (3) $\theta(t; I)$ is linear in t over k,
  (4) $\theta(t; I) = \theta(\theta(t; I - \{i\}), \theta(x_i; I - \{i\}))$ for $i \in I$.

Proof. (1) The expression $y^q - y x^{q-1}$ vanishes whenever $y = \lambda x$, $\lambda \in k$, so must be divisible by $\theta(y, x)$. But both expressions have the same degree and the same coefficient of y^q, so must be equal.

(2) This is clear from the definition.

We prove (3) and (4) together by induction on the size of I. If $I = \{i\}$ then $\theta(t; I) = \theta(t, x_i)$, so (3) is true by (1) and (4) is clear from the definitions. If $|I| > 1$ then it follows from the induction hypothesis that $\theta(\theta(t; I - \{i\}), \theta(x_i; I - \{i\}))$ is linear in t. Suppose that $t = v + \lambda x_i$, where v is a linear combination of $\{x_j \mid j \in I - \{i\}\}$. Then

$$\theta(\theta(t; I-\{i\}), \theta(x_i; I-\{i\})) = \theta(\theta(v; I-\{i\}), \theta(x_i; I-\{i\}))+\lambda\theta(\theta(x_i; I-\{i\}), \theta(x_i; I-\{i\})),$$

and we see that the right hand side is zero using property (2). So $\theta(\theta(t; I - \{i\}), \theta(x_i; I - \{i\}))$ is divisible by all expressions $t - v - \lambda x_i$, hence by $\theta(t; I)$. Since both expressions have the same degree and the same coefficient of $t^{q^{|I|}}$, they must be equal. $\qquad\square$

Lemma 12.3. *If $i > 0$, then*

$$\sum_{\lambda \in k} \lambda^i = \begin{cases} 0 & i \not\equiv 0 \mod q - 1, \\ -1 & i \equiv 0 \mod q - 1. \end{cases}$$

Proof. Let ω be a generator of the cyclic multiplicative group $\mathbb{F}_q^\times$, so $\sum_{\lambda \in k} \lambda^i = \sum_{j=1}^{q-1} \omega^{ij}$. If $i \equiv 0 \mod q - 1$, then $\omega^i = 1$ so this sum is -1. Otherwise we sum the geometric series to obtain $\omega^i(1 - \omega^{i(q-1)})(1 - \omega^i)^{-1} = 0$. $\qquad\square$

Definition 12.4. $[\mathrm{Tr}_{A(x,y)}]$ Let R be a commutative k-algebra without zero-divisors, and let $\mathrm{Tr}_{A(x,y)}\colon R[x, y] \to R[x, y]$ be the function defined by $f \mapsto \sum_{\lambda \in k} f(x, y + \lambda x)$ for $f \in R[x, y]$. This extends to the field of fractions of $R[x, y]$.

Observe that this definition is consistent with Definition 9.3 and Notation 11.2 if we regard $A(x, y)$ as the additive group of k and let it act on $R[x, y]$ in such a way that $\lambda \in k$ sends $x \mapsto x$ and $y \mapsto y + \lambda x$.

Lemma 12.5. *Let $f \in R[x, y]$ and write*

$$f(x, y + h) = a_0(x, y) + a_1(x, y)h + a_2(x, y)h^2 + \cdots$$

in $R[x, y, h]$, where $a_i(x, y) \in R[x, y]$. Then

$$\mathrm{Tr}_{A(x,y)} f = -[a_{q-1}(x, y)x^{q-1} + a_{2(q-1)}(x, y)x^{2(q-1)} + a_{3(q-1)}(x, y)x^{3(q-1)} + \cdots]$$

Proof. Note that $\mathrm{Tr}_{A(x,y)} f = qa_0(x, y) + a_1(x, y)(\sum_{\lambda \in k} \lambda)x + a_2(x, y)(\sum_{\lambda \in k} \lambda^2)x^2 + \cdots$, and apply 12.3. $\qquad\square$

Lemma 12.6. *We have*

$$\mathrm{Tr}_{A(x,y)} y^i = \begin{cases} 0, & i < q - 1 \\ -x^{q-1}, & i = q - 1 \end{cases}$$

Proof. Use the binomial expansion for $(y + h)^i$ and 12.5. $\qquad\square$

Lemma 12.7. *Let $\langle u, v \rangle \subseteq R[u, v]$ denote the k-vector space spanned by u and v. If $f \in R[y]$, $\phi\colon \langle u, v \rangle \to R$ is linear over k and $\mathrm{Tr}_{A(x,y)} f = g(x, y)$ then*

$$\mathrm{Tr}_{A(u,v)} f(\phi(v)) = g(\phi(u), \phi(v)).$$

Proof. $\mathrm{Tr}_{A(u,v)} f(\phi(v)) = \sum_{\lambda \in k} f(\phi(v + \lambda u)) = \sum_{\lambda \in k} f(\phi(v) + \lambda\phi(u)) = g(\phi(u), \phi(v)).$ $\qquad\square$

Lemma 12.8. $\mathrm{Tr}_{A(x,y)}\, \theta(y; I)^i = 0$ *if* $i < q - 1$, *while* $\mathrm{Tr}_{A(x,y)}\, \theta(y; I)^{q-1} = -\theta(x; I)^{q-1}$.

Proof. Apply 12.6 and 12.7 with $\theta(\cdot; I)$ as $\phi \colon k\langle x, y \rangle \to R$. $\qquad\square$

Lemma 12.9. *In the field of fractions of* $k[x, y]$,

$$\mathrm{Tr}_{A(x,y)}\, \frac{1}{y} = \frac{-x^{q-1}}{\theta(y, x)}.$$

Proof. Note that $\mathrm{Tr}_{A(x,y)}\, \dfrac{1}{y} = \dfrac{1}{\theta(y,x)}\, \mathrm{Tr}_{A(x,y)}\, \dfrac{\theta(y,x)}{y} = \mathrm{Tr}_{A(x,y)}(y^{q-1} - x^{q-1})$ and use 12.6.
$\qquad\square$

Lemma 12.10. *If* $l, t \notin I$, $l \neq t$ *then in the field of fractions of* $k[x_1, \ldots, x_n]$ *we have*

$$\mathrm{Tr}_{A(x_t, x_l)}\, \frac{1}{\theta(x_l; I)} = \frac{-\theta(x_t; I)^{q-1}}{\theta(x_l; I \cup \{t\})}.$$

Proof. Use Lemmas 12.9 and 12.7 with $\theta(\cdot; I)$ as $\phi \colon k\langle x_t, x_l \rangle \to R$ to obtain

$$\mathrm{Tr}_{A(x_t, x_l)}\, \frac{1}{\theta(x_l; I)} = \frac{-\theta(x_t; I)^{q-1}}{\theta(\theta(x_l; I); \theta(x_t; I))}.$$

By 12.2(4), this is equal to the form claimed. $\qquad\square$

Lemma 12.11. *Write* B *for the group of automorphisms of* $k[x, y]$ *given by* $y \mapsto \mu y + \lambda x$, $x \mapsto x$, $\mu, \lambda \in k$, $\mu \neq 0$. *Then the invariant ring* $k[x, y]^B$ *is* $k[x, \theta(y, x)^{q-1}]$.

Proof. First note that $B = A \rtimes C$, where $C \cong k^\times$ is the subgroup for which $\lambda = 0$ and A is the subgroup with $\mu = 1$. Now notice that $k[x, y]^A = k[x, \theta(y, x)]$ has a basis $\{x^i \theta(y, x)^j \mid i \geq 0, j \geq 0\}$ consisting of eigenvectors for the action of C. The invariant ring $k[x, \theta(y, x)]^C$ is the $+1$ eigenspace, which is just $k[x, \theta(y, x)^{q-1}]$. Alternatively, use the method of 4.6 or of [7] 3.7.5. $\qquad\square$

Lemma 12.12. $\mathrm{Tr}_{A(x,y)}((x^{q-1} - y^{q-1})^a) = x^{(q-1)a} + \theta(y, x)^{q-1} P(x, \theta(y, x)^{q-1})$, *for some polynomial* P *in two variables.*

Proof. Notice that y^{q-1} is already invariant under $y \mapsto \mu y$ for $\mu \in k$, $\mu \neq 0$. So, in the notation of 12.11, $\mathrm{Tr}_A((x^{q-1} - y^{q-1})^a)$ is B-invariant and lies in $k[x, \theta(y, x)^{q-1}]$.

Regarding $\mathrm{Tr}_{A(x,y)}((x^{q-1} - y^{q-1})^a)$ as a polynomial in x and $\theta(y, x)^{q-1}$ it suffices to check that the coefficient of $x^{(q-1)a}$ is 1. Since we are checking a polynomial identity, we can set $y = 0$, so $\theta(y, x) = 0$ also. We have

$$[\mathrm{Tr}_A((x^{q-1} - y^{q-1})^a)]|_{y=0} = \sum_{\lambda \in k}(x^{q-1} - (\lambda x)^{q-1})^a$$

$$= x^{(q-1)a} + \sum_{\lambda \in k^\times}(x^{q-1} - \lambda^{q-1} x^{q-1})^a$$

$$= x^{(q-1)a},$$

and the coefficient of $x^{(q-1)a}$ is indeed 1. $\qquad\square$

Lemma 12.13. *If* $l, t \notin I$ *then, for some polynomial* P,

$$\mathrm{Tr}_{A(x_t, x_l)}\, [\theta(x_t; I \cup \{l\})^a] = \theta(x_t; I)^{qa} + \theta(x_l; I \cup \{t\})^{q-1} \cdot \theta(x_t; I)^a \cdot P(\theta(x_t; I), \theta(x_l; I \cup \{t\})^{q-1}).$$

Proof. First observe that, by Lemma 12.2 parts (1) and (4), $\theta(x_t; I \cup \{l\})^a = \theta(x_t; I)^a[\theta(x_t; I)^{q-1} - \theta(x_l; I)^{q-1}]^a$. Now $\theta(x_t; I)$ is invariant under $A(x_t, x_l)$ so, by 12.12 and 12.7,

$$\mathrm{Tr}_{A(x_t,x_l)}\left[\theta(x_t; I \cup \{l\})^a\right] =$$
$$\theta(x_t; I)^a[\theta(x_t; I)^{(q-1)a} + \theta(\theta(x_l; I), \theta(x_t; I))^{q-1} \cdot P(\theta(x_t; I), \theta(\theta(x_l; I), \theta(x_t; I))^{q-1})].$$

But $\theta(\theta(x_l; I), \theta(x_t; I)) = \theta(x_l, I \cup \{t\})$, by 12.2(4). $\qquad\square$

Lemma 12.14. *Let* $1 \le k, l \le n - 1$ *but* $k, l \notin I$. *Then* $\theta(x_l; I \cup \{k\}) \cdot \theta(x_k; I) = -\theta(x_l; I) \cdot \theta(x_k; I \cup \{l\})$.

Proof.

$$\begin{aligned}
\theta(x_l; I \cup \{k\}) \cdot \theta(x_k; I) &= \left[\theta(x_l; I)^q - \theta(x_k; I)^{q-1}\theta(x_l; I)\right] \cdot \theta(x_k; I) \quad \text{by Lemma 12.2(4)} \\
&= \theta(x_l; I) \cdot \left[\theta(x_l; I)^{q-1}\theta(x_k; I) - \theta(x_k; I)^q\right] \\
&= -\theta(x_l; I)\theta(x_k; I \cup \{l\}) \qquad\qquad \text{by Lemma 12.2(4).}
\end{aligned}$$

$\qquad\square$

Recall from 11.1 that $h_i = \theta(x_i; J^{<i})$, $g_i = \theta(x_i; (J \cup \{k_1\})^{<i})$.

Lemma 12.15. *If* $l \notin J$ *then*

$$\mathrm{Tr}_{A(x_{k_1}, x_l)} \frac{1}{h_l} = \frac{-\theta(x_{k_1}; J^{<(l+1)})^{q-1}}{g_l}.$$

Proof. Apply Lemma 12.10. $\qquad\square$

Notation 12.16. $[\tilde{J}]$ Let $\tilde{J}$ denote $J^{>k_1}$.

Lemma 12.17 (Theta Lemma). $\theta(x_{k_1}; J^{<l})$ *is an element of* $k[h_{k_1}, h_{\tilde{J}<l}]$. *As an element of* $k[h_1, \ldots, h_n]$, *its least term is* $h_{k_1}^{q^{|\tilde{J}^{<l}|}}$.

Proof. We prove the result by induction on $|\tilde{J}^{<l}|$. If $|\tilde{J}^{<l}| = 0$ then $\theta(x_{k_1}; J^{<l}) = h_{k_1}$, so the initial case is clear. To prove the induction step, let j be the largest number in $\tilde{J}^{<l}$ and apply Lemma 12.2 parts (1) and (4) to get the equation

$$\theta(x_{k_1}; J^{<l}) = \theta(x_{k_1}; J^{<l} - \{j\})^q - \theta(x_j; J^{<l} - \{j\})^{q-1} \cdot \theta(x_{k_1}; J^{<l} - \{j\}).$$

By the induction hypothesis, we have an expression $\theta(x_{k_1}; J^{<l} - \{j\}) = h_{k_1}^{q^{|\tilde{J}^{<l}|-1}} + f$, where $f \in k[h_{k_1}, h_{\tilde{J}<l - \{j\}}]$ is a polynomial with $\deg_{h_{k_1}} f < q^{|\tilde{J}^{<l}|-1}$. In any case, $\theta(x_j; J^{<l} - \{j\}) = h_j$. Thus we can write $\theta(x_{k_1}; J^{<l}) = (h_{k_1}^{q^{|\tilde{J}^{<l}|-1}} + f)^q - h_j^{q-1}(h_{k_1}^{q^{|\tilde{J}^{<l}|-1}} + f) = h_{k_1}^{q^{|\tilde{J}^{<l}|}} + f^q - h_j^{q-1}h_{k_1}^{q^{|\tilde{J}^{<l}|-1}} - h_j^{q-1}f$.

Because of the condition on $\deg_{h_{k_1}} f$, we see that $h_{k_1}^{q^{|\tilde{J}^{<l}|}}$ is the least term of the last expression, and this proves the lemma. $\qquad\square$

Lemma 12.18 ((a,b)-Lemma). *Let* $l \in \tilde{J}$. *If* $a < b$ *then*

(1) $\mathrm{Tr}_{A(x_{k_1}, x_l)}\left[h_l^a \theta(x_{k_1}; J^{<l+1})^b\right] = (-1)^a g_l^a \theta(x_{k_1}; J^{<l})^{a+q(b-a)} \pmod{g_l^{a+1} k[g_{k_1}, h_{\tilde{J}<l}, g_l]}$.

If, instead, $a \ge b$ *then, for some polynomial* Q,

(2) $\mathrm{Tr}_{A(x_{k_1}, x_l)}\left[h_l^a \theta(x_{k_1}; J^{<l+1})^b\right] = g_l^b \theta(x_{k_1}; J^{<l})^b \cdot Q(g_l, \theta(x_{k_1}; J^{<l}))$.

Proof. Since $l > k_1$ we have, by Lemma 12.14, that $h_l \cdot \theta(x_{k_1}; J^{<(l+1)}) = -g_l \cdot \theta(x_{k_1}; J^{<l})$.
    Case 1: $a < b$. From the observation above, we have

$$\text{Tr}_{A(x_{k_1}, x_l)}\left[h_l^a \theta(x_{k_1}; J^{<(l+1)})^b\right] = (-1)^a g_l^a \theta(x_{k_1}; J^{<l})^a \text{Tr}_{A(x_{k_1}, x_l)}\left[\theta(x_{k_1}; J^{<(l+1)})^{b-a}\right],$$

and now we use Lemma 12.13 to obtain

$$(-1)^a g_l^a \theta(x_{k_1}; J^{<l})^a \left[\theta(x_{k_1}; J^{<l})^{q(b-a)} + g_l^{q-1}\theta(x_{k_1}; J^{<l})^{b-a} P(\theta(x_{k_1}; J^{<l}), g_l^{q-1})\right].$$

We know that $\theta(x_{k_1}; J^{<l}) \in k[h_{k_1}, h_{\tilde{j}<l}]$ by 12.17 and $g_{k_1} = h_{k_1}$ from the definitions.
    Case 2: $a \geq b$. From the observation again, we get

$$\begin{aligned}
\text{Tr}_{A(x_{k_1}, x_l)}\left[h_l^a \theta(x_{k_1}; J^{<(l+1)})^b\right] &= (-1)^b g_l^b \theta(x_{k_1}; J^{<l})^b \text{Tr}_{A(x_{k_1}, x_l)}\left[h_l^{a-b}\right] \\
&= g_l^b \theta(x_{k_1}; J^{<l})^b Q(g_l, \theta(x_{k_1}; J^{<l})).
\end{aligned}$$

The last step perhaps requires a little explanation, even though the reason it works is quite general. Consider the action of $A(x_{k_1}, x_l)$ on $k[h_l, \theta(x_{k_1}; J^{<l})]$. This has the effect $h_l \mapsto h_l + \lambda\theta(x_{k_1}; J^{<l})$, where $\lambda \in k$. The invariant subring under this action is $k[g_l, \theta(x_{k_1}; J^{<l})]$, and so $\text{Tr}_{A(x_{k_1}, x_l)}[h_l^{a-b}] = Q(g_l, \theta(x_{k_1}; J^{<l}))$ for some polynomial Q (which is possibly 0). $\qquad\square$

13. Preparations for the One-Step Lemma

The purpose of this section is to set up some notation that will be used for the One-Step Lemma (14.1) and establish some simple properties of this notation.

Definition 13.1. $[G(I, J)_l]$ For $l = k_1 + 1, \ldots, n + 1$, let

$$G(I, J)_l = \prod_{k_1 < i < l,\; i \notin J} \frac{\theta(x_i; I^{<i})}{\theta(x_i; J^{<i})} \prod_{l \leq i \leq n,\; i \notin J} \frac{\theta(x_i; I^{<i})}{\theta(x_i; J^{<i} \cup \{k_1\})}.$$

We will usually write just $G(J)$ for short, since I will not vary.

Lemma 13.2. $G(J)_{n+1} = G(J)$ and $G(J)_{k_1+1} = G(J \cup \{k_1\})$

Lemma 13.3. *For $l > k_1$ both $G(J)_l$ and g_l are $A(x_{k_1}, x_l)$-invariant.*

Notation 13.4. $[w_{l,i},\; w_{l,X}]$ Let $w_{l,i} = h_i$ if $i < l$ and $w_{l,i} = g_i$ if $i \geq l$.
    For $X \subseteq \{1, \ldots, n\}$, we write $w_{l,X}$ for the set $\{w_{l,i} \mid i \in X\}$ and for $X \subseteq Y$ and $\vec{a} \in P(Y)$ we write $w_{l,X}^{\vec{a}}$ for $\prod_{i \in X} w_{l,i}^{a_i}$.

Lemma 13.5. *If $l \notin J$ then*

(1) $\theta(x_{k_1}; J^{<l+1}) = \theta(x_{k_1}; J^{<l})$ is $A(x_{k_1}, x_l)$-invariant   (3) $G(J)_{l+1} = G(J)_l \frac{g_l}{h_l}$
(2) $w_{l+1,\tilde{J}}^{\vec{a}} = w_{l,\tilde{J}}^{\vec{a}}$ is $A(x_{k_1}, x_l)$-invariant   (4) $\tilde{J}^{\geq l} = \tilde{J}^{\geq l+1}$ and $\tilde{J}^{<l} = \tilde{J}^{<l+1}$

Lemma 13.6. *If $l \in J$ then*

(1) $w_{l+1,\tilde{J}}^{\vec{a}} = w_{l,\tilde{J}}^{\vec{a}}(\frac{h_l}{g_l})^{a_l}$ (3) $G(J)_{l+1} = G(J)_l$
(2) $w_{l,\tilde{J}}^{\vec{a}}$ is $A(x_{k_1}, x_l)$-invariant

Lemma 13.7. *If $l \notin J$, $l > k_1$ then*

$$G(J)_{l+1}\theta(x_{k_1}; J^{<l+1})^{f(l+1)}w_{l+1,\tilde{J}}^{\vec{a}} = G(J)_l g_l w_{l,\tilde{J}}^{\vec{a}} \cdot \frac{\theta(x_{k_1}; J^{<l+1})^{f(l+1)}}{h_l},$$

and everything on the right hand side before the dot is $A(x_{k_1}, x_l)$-invariant.

Proof. Apply Lemmas 13.5 and 13.3. □

Lemma 13.8. *If $l \in J, l > k_1$ then*

$$G(J)_{l+1}\theta(x_{k_1}; J^{<l+1})^{f(l+1)}w_{l+1,\tilde{J}}^{\vec{a}} = G(J)_l w_{l,\tilde{J}}^{\vec{a}}\frac{1}{g_l^{a_l}} \cdot h_l^{a_l}\theta(x_{k_1}; J^{<l+1})^{f(l+1)},$$

and everything on the right hand side before the dot is $A(x_{k_1}, x_l)$-invariant.

Proof. Apply Lemmas 13.6 and 13.3. □

The One-Step Lemma will compute certain traces up to an error term which lies in a certain ideal $R_l(\vec{a})$ over which we have some control. We now define this ideal.

Remark 13.9. In reading the following definition, recall that $h_{k_1} = g_{k_1}$ and also the ordering on elements of $P(I)$ (7.2).

If $\vec{a} \in P(J)$ and $J' \subset J$ we will write $\vec{a}_{J'} \in P(J')$ for the obvious restriction, and sometimes just $\vec{a}$ when no confusion is likely to arise. We will also on occasion extend $\vec{a}$ by 0 to give a vector $\vec{a}_0 \in P(J \cup \{k_1\})$.

Definition 13.10. Given $k_1, \tilde{J}$, $\vec{a} \in P(\tilde{J})$ and l such that $k_1 < l \leq n + 1$ and $f(l) \geq 0$, we write $R_l(\vec{a})$ for the k-subspace of $k[g_{k_1}, w_{l,\tilde{J}}]$ spanned by elements of the form

$$(1) \qquad\qquad g_{k_1}^c w_{l,\tilde{J}}^{\vec{v}} \quad \text{where} \quad \vec{v} \in P(\tilde{J}), \quad \vec{v}_{\tilde{j} \geq l} > \vec{a}_{\tilde{j} \geq l}, \quad \text{and} \quad c \geq 0,$$

and elements of the form

$$(2) \qquad g_{k_1}^d \theta(x_{k_1}; J^{<l})^{f(l)} w_{l,\tilde{J}}^{\vec{v}} \quad \text{where} \quad \vec{v}_{\tilde{j} \geq l} = \vec{a}_{\tilde{j} \geq l}, \quad \vec{v}_{\tilde{j} < l} > \vec{a}_{\tilde{j} < l}, \quad \text{and} \quad d \geq 0.$$

Thus $R_l(\vec{a})$ depends implicitly on k_1 and $\tilde{J}$, although they do not appear in the notation.

Remark 13.11. The extreme cases $l = n + 1$ and $l = k_1 + 1$ are of special interest in the above definition.

By definition, $R_{n+1}(\vec{a})$ is spanned by elements of types 1 and 2. If $l = n+1$ then $\tilde{J}^{\geq l}$ is empty and thus $\vec{v}_{\tilde{j} \geq l} = \vec{a}_{\tilde{j} \geq l}$. In particular, $\vec{v}_{\tilde{j} \geq l} > \vec{a}_{\tilde{j} \geq l}$ is impossible and so there are *no* elements of type 1. As for the elements of type 2, $f(n + 1) = 0$ (5.24) and $g_{k_1} = h_{k_1}$ and so $R_{n+1}(\vec{a})$ is the ideal in $k[h_{k_1}, h_{\tilde{j}}]$ generated by monomials with exponent vector greater than $\vec{a}_0$. In other words, $R_{n+1}(\vec{a}) = H(\vec{a}_0, k[h_{k_1}, h_{\tilde{j}}])$, (see 7.4).

If $l = k_1 + 1$ then $\tilde{J}^{<k_1+1}$ is empty and $\vec{v}_{\tilde{j} < k_1+1} > \vec{a}_{\tilde{j} < k_1+1}$ is impossible. It follows that there are no elements of type 2. Similarly, this means that $R_{k_1+1}(\vec{a})$ is the ideal in $k[g_{k_1}, g_{\tilde{j}}]$ generated by monomials with exponent vector greater than $\vec{a}_{\tilde{j}}$. That is, $R_{k_1+1}(\vec{a}) = H(\vec{a}_0, k[g_{k_1}, g_{\tilde{j}}])$.

Lemma 13.12. $R_l(\vec{a})$ *is an ideal in* $k[g_{k_1}, w_{l,\tilde{j}}]$.

Proof. In order to prove that a sub-vector-space of $k[g_{k_1}, w_{l,\tilde{j}}]$ is an ideal, it is enough to show that the subspace is closed under multiplication by g_{k_1} and $w_{l,i}$ for $i \in \tilde{J}$.

First we show that the span of the elements of type 1 forms an ideal. Let $g_{k_1}^c w_{l,\tilde{j}}^{\vec{v}}$ be an element of type 1 in $R_l(\vec{a})$, so $\vec{v}_{\tilde{j} \geq l} > \vec{a}_{\tilde{j} \geq l}$. Consider the product of this element with each of the following:

(1) g_{k_1}: The product is again an element of type 1 in $R_l(\vec{a})$.
(2) h_i, $i < l$: Write $\vec{v}'$ for the exponent vector of $w_{l,\tilde{j}}^{\vec{v}} \cdot h_i$. Then $\vec{v}'_{\tilde{j} \geq l} = \vec{v}_{\tilde{j} \geq l} > \vec{a}_{\tilde{j} \geq l}$ and so the product is still an element of type 1 in $R_l(\vec{a})$.
(3) g_i, $i \geq l$: Write $\vec{v}'$ for the exponent vector of $w_{l,\tilde{j}}^{\vec{v}} \cdot g_i$. Then $\vec{v}'_{\tilde{j} \geq l} > \vec{v}_{\tilde{j} \geq l} > \vec{a}_{\tilde{j} \geq l}$ and so the product is still an element of type 1 in $R_l(\vec{a})$.

Thus we have shown that the elements of type 1 form an ideal in $k[g_{k_1}, w_{l,\tilde{j}}]$.

Now let $g_{k_1}^d \theta(x_{k_1}; J^{<l})^{f(l)} w_{l,\tilde{j}}^{\vec{v}}$ be an element of type 2. We have the conditions $\vec{v}_{\tilde{j} \geq l} = \vec{a}_{\tilde{j} \geq l}$, $\vec{v}_{\tilde{j} < l} > \vec{a}_{\tilde{j} < l}$. Consider the product of this element with each of the following:

(1) g_{k_1}: The product is again an element of type 2 in $R_l(\vec{a})$.
(2) h_i, $i < l$: Write $\vec{v}'$ for the exponent vector of $w_{l,\tilde{j}}^{\vec{v}} \cdot h_i$. Then $\vec{v}'_{\tilde{j} \geq l} = \vec{v}_{\tilde{j} \geq l} = \vec{v}_{\tilde{j} \geq l}$ and $\vec{v}'_{\tilde{j} < l} > \vec{v}_{\tilde{j} < l} > \vec{a}_{\tilde{j} \geq l}$ so the product is still an element of type 2.
(3) g_i, $i \geq l$: This is the only tricky part. Write $\vec{v}'$ for the exponent vector of $w_{l,\tilde{j}}^{\vec{v}} \cdot g_i$. Then $\vec{v}'_{\tilde{j} \geq l} > \vec{v}_{\tilde{j} \geq l} = \vec{a}_{\tilde{j} \geq l}$ and so $w_{l,\tilde{j}}^{\vec{v}} \cdot g_i$ is an element of type 1 in $R_l(\vec{a})$. We have already shown that the span of the elements of type 1 forms an ideal in $k[g_{k_1}, w_{l,\tilde{j}}]$. By the Theta Lemma (12.17), $\theta(x_{k_1}; J^{<l}) \in k[g_{k_1}, w_{l,\tilde{j}}]$. Hence the product $g_{k_1}^d \theta(x_{k_1}; J^{<l})^{f(l)} w_{l,\tilde{j}}^{\vec{v}'}$ is a linear combination of elements of type 1 and therefore lies in $R_l(\vec{a})$.

$\square$

14. THE ONE-STEP LEMMA

Lemma 14.1 (One-Step Lemma). *Let $\vec{a} \in P(\tilde{J})$ be $S_J(J)$-$(l-1)$-compatible and $k_1 < l \leq n$. Then we have*

(1) $\mathrm{Tr}_{A(x_{k_1}, x_l)} \left[G(J)_{l+1} \theta(x_{k_1}; J^{<l+1})^{f(l+1)} w_{l+1, \tilde{j}}^{\vec{a}} \right] = G(J)_l \left[(-1)^\sigma \theta(x_{k_1}; J^{<l})^{f(l)} w_{l, \tilde{j}}^{\vec{a}} + x \right],$

where $x \in R_l(\vec{a})$ and $\sigma = 1$ if $l \notin J$, $\sigma = a_l$ if $l \in J$. Furthermore,

(2) $\mathrm{Tr}_{A(x_{k_1}, x_l)} \left[G(J)_{l+1} R_{l+1}(\vec{a}) \right] \subseteq G(J)_l R_l(\vec{a}).$

Notice that both $f(l)$ and $f(l+1)$ are non-negative, by 5.28.

Proof of the One-Step Lemma. Formula (1). In this part we compute a trace up to an element of $R_l(\vec{a})$. We divide the calculation into two cases, according to whether $l \in J$ or not.

Case $l \notin J$. By Lemma 13.7, it is enough to compute:

$$\mathrm{Tr}_{A(x_{k_1},x_l)}\ \frac{\theta(x_{k_1};J^{<l+1})^{f(l+1)}}{h_l} = -\frac{\theta(x_{k_1};J^{<l+1})^{f(l+1)+q-1}}{g_l} \quad \text{by Lemma 12.15}$$

$$= -\frac{\theta(x_{k_1};J^{<l})^{f(l)}}{g_l} \quad \text{by Lemmas 5.24 and 13.5(1).}$$

Thus $\mathrm{Tr}_{A(x_{k_1},x_l)}\left[G(J)_{l+1}\theta(x_{k_1};J^{\leq l+1})^{f(l+1)}w_{l+1,\tilde{J}}^{\vec{a}}\right] = -G(J)_l\theta(x_{k_1};J^{<l})^{f(l)}w_{l,\tilde{J}}^{\vec{a}}$ exactly, with no error term.

Case $l \in J$. By Lemma 13.8, we need to compute $\mathrm{Tr}_{A(x_{k_1},x_l)}\left[h_l^{a_l}\theta(x_{k_1};J^{<l+1})^{f(l+1)}\right]$.

Since $\vec{a}$ is $S_J(J)$-$(l-1)$-compatible, 5.27 applies and we know that $f(l+1) > a_l$. So from the first part of the (a,b)-Lemma (12.18(1)), the required trace is equal to $(-1)^{a_l}g_l^{a_l}\theta(x_{k_1};J^{<l})^{a_l+q(f(l+1)-a_l)} + g_l^{a_l+1}X$, where $X \in k[g_{k_1},w_{l,\tilde{J}}]$.

Now we apply 5.24 to simplify the exponent; we obtain $(-1)^{a_l}g_l^{a_l}\theta(x_{k_1};J^{<l})^{f(l)} + g_l^{a_l+1}X$ and so

$$\mathrm{Tr}_{A(x_{k_1},x_l)}\left[G(J)_{l+1}\theta(x_{k_1};J^{<l+1})^{f(l+1)}w_{l+1,\tilde{J}}^{\vec{a}}\right]$$
$$= G(J)_l\left[(-1)^{a_l}\theta(x_{k_1};J^{<l})^{f(l)}w_{l,\tilde{J}}^{\vec{a}} + w_{l,\tilde{J}}^{\vec{a}}g_lX\right].$$

To complete this part of the proof, we must show that $w_{l,\tilde{J}}^{\vec{a}}g_lX \in R_l(\vec{a})$. Note that the power of g_l in the monomial $w_{l,\tilde{J}}^{\vec{a}}g_l$ is greater than a_l, so $w_{l,\tilde{J}}^{\vec{a}}g_l$ is a generating element of $R_l(\vec{a})$ of type 1. In particular, $w_{l,\tilde{J}}^{\vec{a}}g_l \in R_l(\vec{a})$. Since $X \in k[g_{k_1},w_{l,\tilde{J}}]$ and $R_l(\vec{a})$ is an ideal in this ring (13.12), $w_{l,\tilde{J}}^{\vec{a}}g_lX \in R_l(\vec{a})$.

This completes the proof of the first formula; we now turn to the second one.

Formula (2). There are two types of traces, corresponding to the two types of generators of $R_l(\vec{a})$.

Type 1. The first type is $\mathrm{Tr}_{A(x_{k_1},x_l)}\left[G(J)_{l+1}g_{k_1}^c w_{l+1,\tilde{J}}^{\vec{v}}\right]$ for $\vec{v}_{\tilde{J}\geq l+1} > \vec{a}_{\tilde{J}\geq l+1}$.

The calculation splits into two cases, depending on whether $l \in J$ or not.

Type 1, $l \notin J$. If $l \notin J$ we apply Lemmas 13.3 and 13.5 and obtain:

$$\mathrm{Tr}_{A(x_{k_1},x_l)}\left[G(J)_{l+1}g_{k_1}^c w_{l+1,\tilde{J}}^{\vec{v}}\right] = \mathrm{Tr}_{A(x_{k_1},x_l)}\left[G(J)_l\frac{g_l}{h_l}g_{k_1}^c w_{l+1,\tilde{J}}^{\vec{v}}\right]$$
$$= G(J)_l g_l g_{k_1}^c w_{l,\tilde{J}}^{\vec{v}}\,\mathrm{Tr}_{A(x_{k_1},x_l)}\frac{1}{h_l}.$$

By 12.15, $\mathrm{Tr}_{A(x_{k_1},x_l)}\frac{1}{h_l} = \frac{-\theta(x_k;J^{\leq l})^{q-1}}{g_l}$, so

$$\mathrm{Tr}_{A(x_{k_1},x_l)}\left[G(J)_l\frac{g_l}{h_l}g_{k_1}^c w_{l+1,\tilde{J}}^{\vec{v}}\right] = -G(J)_l g_{k_1}^{c+q-1}w_{l,\tilde{J}}^{\vec{v}}.$$

Since $\tilde{J}^{\geq l} = \tilde{J}^{\geq l+1}$ we have $\vec{v}_{\tilde{J}\geq l} > \vec{a}_{\tilde{J}\geq l}$ and therefore $g_{k_1}^{c+q-1}w_{l,\tilde{J}}^{\vec{v}} \in R_l(\vec{a})$.

Type 1, $l \in J$. If $l \in J$ we apply Lemma 13.6 and get:

$$\mathrm{Tr}_{A(x_{k_1}, x_l)}\left[G(J)_{l+1} g_{k_1}^c w_{l+1, \tilde{J}}^{\vec{v}} \right] = G(J)_l g_{k_1}^c \frac{w_{l, \tilde{J}}^{\vec{v}}}{g_l^{v_l}} \mathrm{Tr}_{A(x_{k_1}, x_l)} h_l^{v_l}.$$

Note that $\frac{w_{l, \tilde{J}}^{\vec{v}}}{g_l^{v_l}}$ is a polynomial (13.4), which contains $g_{\tilde{j} \geq l+1}^{\vec{v}}$ as a factor. Since $g_{k_1}^c w_{l+1, \tilde{J}}^{\vec{v}}$ is of type 1 in $R_{l+1}(\vec{a})$ by hypothesis, it follows that $\vec{v}_{\tilde{j} \geq l+1} > \vec{a}_{\tilde{j} \geq l+1}$ and hence that $g_{\tilde{j} \geq l+1}^{\vec{v}}$ is an element of $R_l(\vec{a})$ of type 1. Since $R_l(\vec{a})$ is an ideal in $k[g_{k_1}, w_{l, \tilde{J}}]$ (13.12), $\frac{w_{l, \tilde{J}}^{\vec{v}}}{g_l^{v_l}} \in R_l(\vec{a})$.

Now we have to study the trace of $h_l^{v_l}$. We apply the (a, b)-Lemma (12.18) with $a = v_l$, $b = 0$ to conclude that $\mathrm{Tr}_{A(x_{k_1}, x_l)} h_l^{v_l}$ lies in $k[g_l, \theta(x_{k_1}; J^{<l})]$, which in turn is contained in $k[h_{k_1}, h_{\tilde{j} < l}, g_l]$ by the Theta Lemma (12.17). Now $k[h_{k_1}, h_{\tilde{j} < l}, g_l] \subset k[g_{k_1}, w_{l, \tilde{J}}]$ and, since $R_l(\vec{a})$ is an ideal in $k[g_{k_1}, w_{l, \tilde{J}}]$ (13.12), the product $g_{k_1}^c \frac{w_{l, \tilde{J}}^{\vec{v}}}{g_l^{v_l}} \mathrm{Tr}_{A(x_{k_1}, x_l)} h_l^{v_l}$ lies in $R_l(\vec{a})$.

Type 2. The second type of trace is $\mathrm{Tr}_{A(x_{k_1}, x_l)}\left[G(J)_{l+1} g_{k_1}^d \theta(x_{k_1}; J^{<l+1})^{f(l+1)} w_{l+1, \tilde{J}}^{\vec{v}} \right]$, where $\vec{v}_{\tilde{j} \geq l+1} = \vec{a}_{\tilde{j} \geq l+1}$ but $\vec{v}_{\tilde{j} < l+1} > \vec{a}_{\tilde{j} < l+1}$.

Type 2, $l \notin J$. Since $l \notin J$ we can apply Lemma 13.5 and get

$$\mathrm{Tr}_{A(x_{k_1}, x_l)}\left[G(J)_{l+1} g_{k_1}^d \theta(x_{k_1}; J^{<l+1})^{f(l+1)} w_{l+1, \tilde{J}}^{\vec{v}} \right]$$

$$= \mathrm{Tr}_{A(x_{k_1}, x_l)}\left[G(J)_l \frac{g_l}{h_l} g_{k_1}^d \theta(x_{k_1}; J^{<l})^{f(l+1)} w_{l, \tilde{J}}^{\vec{v}} \right]$$

$$= G(J)_l g_{k_1}^d g_l w_{l, \tilde{J}}^{\vec{v}} \mathrm{Tr}_{A(x_{k_1}, x_l)} \frac{\theta(x_{k_1}; J^{<l})^{f(l+1)}}{h_l} \qquad \text{by Lemmas 13.3 and 13.5}$$

$$= -G(J)_l g_{k_1}^d g_l w_{l, \tilde{J}}^{\vec{v}} \frac{\theta(x_{k_1}; J^{<l})^{f(l+1)+q-1}}{g_l} \qquad \text{by Lemma 12.15}$$

$$= -G(J)_l g_{k_1}^d \theta(x_{k_1}; J^{<l})^{f(l)} w_{l, \tilde{J}}^{\vec{v}} \qquad \text{by Lemma 5.24.}$$

Since we started with an element of type 2 in $R_{l+1}(\vec{a})$, $\vec{v}_{\tilde{j} \geq l+1} = \vec{a}_{\tilde{j} \geq l+1}$ and $\vec{v}_{\tilde{j} < l+1} > \vec{a}_{\tilde{j} < l+1}$. In view of 13.5(4), this gives us the same two conditions on $\vec{v}$ and $\vec{a}$ but with $l+1$ replaced by l. Thus the trace lies in $G(J)_l R_l(\vec{a})$.

Type 2, $l \in J$. Using Lemmas 13.3 and 13.6 we reduce the problem to computing

$$G(J)_l g_{k_1}^d \frac{w_{l, \tilde{J}}^{\vec{v}}}{g_l^{v_l}} \mathrm{Tr}_{A(x_{k_1}, x_l)}\left[h_l^{v_l} \theta(x_{k_1}; J^{<l+1})^{f(l+1)} \right].$$

Recall that $\frac{w_{l, \tilde{J}}^{\vec{v}}}{g_l^{v_l}}$ is a polynomial (13.4).

The problem now splits into two cases again, depending on whether $v_l < f(l+1)$ or not.

Type 2, $l \in J$, $v_l < f(l+1)$. The computation here is analogous to that for Formula 1, $l \in J$.

We need to compute

$$\mathrm{Tr}_{A(x_{k_1}, x_l)} \left[h_l^{v_l} \theta(x_{k_1}; J^{<l+1})^{f(l+1)} \right].$$

Since $f(l+1) > v_l$, the first part of the (a,b)-Lemma (12.18(1)) tells us that the required trace is

$$(-1)^{v_l} \left[g_l^{v_l} \theta(x_{k_1}; J^{<l})^{v_l + q(f(l+1) - v_l)} + g_l^{v_l+1} X \right],$$

where $X \in k[g_{k_1}, w_{l,\tilde{J}}]$. Returning to the original trace computation, we have shown that

$$\mathrm{Tr}_{A(x_{k_1}, x_l)} \left[G(J)_{l+1} \theta(x_{k_1}; J^{<l+1})^{f(l+1)} g_{k_1}^d w_{l+1, \tilde{J}}^{\vec{v}} \right]$$
$$= \pm G(J)_l g_{k_1}^d \left[w_{l, \tilde{J}}^{\vec{v}} \theta(x_{k_1}; J^{<l})^{v_l + q(f(l+1) - v_l)} + w_{l, \tilde{J}}^{\vec{v}} g_l X \right].$$

It is sufficient to show that $w_{l, \tilde{J}}^{\vec{v}} \theta(x_{k_1}; J^{<l})^{v_l + q(f(l+1) - v_l)}$ and $w_{l, \tilde{J}}^{\vec{v}} g_l X$ lie in $R_l(\vec{a})$. We start with the easy case, $w_{l, \tilde{J}}^{\vec{v}} g_l X$.

If $\vec{v}'$ is the exponent vector of $w_{l, \tilde{J}}^{\vec{v}} g_l$, we have immediately that $v_l' > v_l \geq a_l$ and hence that $\vec{v}'_{\tilde{j} \geq l} > \vec{a}_{\tilde{j} \geq l}$. This implies that $w_{l, \tilde{J}}^{\vec{v}} g_l$ is an element of $R_l(\vec{a})$ of type 1. Since $X \in k[g_{k_1}, w_{l, \tilde{J}}]$ and $R_l(\vec{a})$ is an ideal in this ring (13.12), $w_{l, \tilde{J}}^{\vec{v}} g_l X \in R_l(\vec{a})$.

To see that the term $w_{l, \tilde{J}}^{\vec{v}} \theta(x_{k_1}; J^{<l})^{v_l + q(f(l+1) - v_l)}$ lies in $R_l(\vec{a})$ is slightly trickier. There are two possibilities: first, that $v_l > a_l$ and second, that $v_l = a_l$ but also $\vec{v}_{\tilde{j} < l} > \vec{a}_{\tilde{j} < l}$.

If $v_l > a_l$ then $w_{l, \tilde{j}}^{\vec{v}}$ satisfies the definition of an element of type 1 in $R_l(\vec{a})$. By the Theta Lemma (12.17), $\theta(x_{k_1}; J^{<l}) \in k[g_{k_1}, w_{l, \tilde{j}}]$, and $R_l(\vec{a})$ is an ideal in this ring (13.12), so $w_{l, \tilde{j}}^{\vec{v}} \theta(x_{k_1}; J^{<l})^{v_l + q(f(l+1) - v_l)} \in R_l(\vec{a})$.

Now suppose that $v_l = a_l$, but also $\vec{v}_{\tilde{j} < l} > \vec{a}_{\tilde{j} < l}$. By 5.24, $w_{l, \tilde{j}}^{\vec{v}} \theta(x_{k_1}; J^{<l})^{v_l + q(f(l+1) - v_l)} = w_{l, \tilde{j}}^{\vec{v}} \theta(x_{k_1}; J^{<l})^{f(l)}$, which is an element of $R_l(\vec{a})$ of type 2, so we are done.

Type 2, $l \in J$, $v_l \geq f(l+1)$. Just as in the case $v_l < f(l+1)$, we need to compute $\mathrm{Tr}_{A(x_{k_1}, x_l)} h_l^{v_l} \theta(x_{k_1}; J^{<l+1})^{f(l+1)}$. Since $v_l \geq f(l+1)$, the second part of the (a,b)-Lemma (12.18(2)) shows us that the required trace is $g_l^{f(l+1)} \theta(x_{k_1}; J^{<l})^{f(l+1)} Q$, where $Q \in k[g_{k_1}, \theta(x_{k_1}; J^{<l})]$, which is contained in $k[g_{k_1}, w_{l, \tilde{j}}]$ by the Theta Lemma (12.17). Returning to the original trace computation we have shown that

$$\mathrm{Tr}_{A(x_{k_1}, x_l)} \left[G(J)_{l+1} \theta(x_{k_1}; J^{<l+1})^{f(l+1)} g_{k_1}^d w_{l+1, \tilde{J}}^{\vec{v}} \right]$$
$$= G(J)_l g_{k_1}^d \left[\frac{w_{l, \tilde{J}}^{\vec{v}}}{g_l^{v_l}} g_l^{f(l+1)} \theta(x_{k_1}; J^{<l})^{f(l+1)} Q \right].$$

Again, recall that $\frac{w_{l, \tilde{J}}^{\vec{v}}}{g_l^{v_l}}$ is a polynomial (13.4).

We must now show that $\frac{w_{l, \tilde{J}}^{\vec{v}}}{g_l^{v_l}} g_l^{f(l+1)} \theta(x_{k_1}; J^{<l})^{f(l+1)} Q$ is an element of $R_l(\vec{a})$. First we show that $\frac{w_{l, \tilde{J}}^{\vec{v}}}{g_l^{v_l}} g_l^{f(l+1)} \in R_l(\vec{a})$.

By 5.27, $f(l+1) > a_l$, so if we define $\vec{v}'$ to be the same as $\vec{v}$ except that v_l is replaced by $f(l+1)$, we can write $w_{l,\tilde{J}}^{\vec{v}'} = \frac{w_{l,\tilde{J}}^{\vec{v}}}{g_l^{v_l}} g_l^{f(l+1)}$ and we have $\vec{v}'_{\tilde{J}\geq l} > \vec{a}_{\tilde{J}\geq l}$. This means that $\frac{w_{l,\tilde{J}}^{\vec{v}}}{g_l^{v_l}} g_l^{f(l+1)}$ is an element of $R_l(\vec{a})$ of type 1.

Since $\theta(x_{k_1}; J^{<l})^{f(l+1)}Q \in k[g_l, w_{l,\tilde{J}}]$ and $R_l(\vec{a})$ is an ideal in this ring (13.12), the product $\frac{w_{l,\tilde{J}}^{\vec{v}}}{g_l^{v_l}} g_l^{f(l+1)}\theta(x_{k_1}; J^{<l})^{f(l+1)}Q$ lies in $R_l(\vec{a})$, as we have argued before in this proof. $\qquad\square$

15. THE ONE-ROW TRACE LEMMA

For groups $A, B < C$ we write $C = A \cdot B$ to signify that $C \cong A \times B$ as sets and that the bijection is given by multiplication. This happens if and only if $|C| = |A| \cdot |B|$ and $A \cap B = 1$.

The induction argument in this section is based on the decomposition $U_{\{i\}} = \prod_{j=i+1}^{n} A(x_i, x_j)$ (where $\prod$ signifies repeated $\cdot$).

The next lemma is easy and well known.

Lemma 15.1. *If $C = A \cdot B$ then $\mathrm{Tr}_C = \mathrm{Tr}_A \mathrm{Tr}_B$ and also $\mathrm{Tr}_{C/B} = \mathrm{Tr}_A$ on B-invariants.*

Lemma 15.2 (m-Step Lemma). *Let $\vec{a} \in P(J)$ be $S_J(J)$-$(l-1)$-compatible and $k_1 < l \leq n+1$. Then we have*

(1) $\mathrm{Tr}_{A(x_{k_1},x_l)} \mathrm{Tr}_{A(x_{k_1},x_{l+1})} \cdots \mathrm{Tr}_{A(x_{k_1},x_n)} \left[G(J) \cdot h_J^{\vec{a}} \right]$
$$= G(J)_l h_{J<k_1}^{\vec{a}} \left[(-1)^\tau \theta(x_{k_1}; J^{<l})^{f(l)} w_{l,\tilde{J}}^{\vec{a}} + x \right],$$

where $x \in R_l(\vec{a})$ and $\tau = \tau(l, J, \vec{a}) = n + l + 1 + \sum_{j \in J \geq l}(a_j + 1) \pmod 2$. Furthermore,

(2) $\mathrm{Tr}_{A(x_{k_1},x_l)} \mathrm{Tr}_{A(x_{k_1},x_{l+1})} \cdots \mathrm{Tr}_{A(x_{k_1},x_n)} \left[G(J) \cdot R_{n+1}(\vec{a}) \right] \subseteq G(J)_l R_l(\vec{a}).$

If $l = n+1$ we interpret the left hand side of (1) as $G(J) \cdot h_J^{\vec{a}}$.

Proof. The result is proved by downward induction on l. In the initial case, $l = n+1$, the left hand side is $G(J) \cdot h_J^{\vec{a}}$ and, on the right hand side, $G(J)_{n+1} = G(J)$ by 13.2, $\tau = 0$, $f(l) = 0$ by 5.24 and $w_{n+1,\tilde{J}}^{\vec{a}} = h_J^{\vec{a}}$ by definition (13.4). The latter combines with $h_{J<k_1}^{\vec{a}}$ to give $h_J^{\vec{a}}$, so the two sides are equal when $x = 0$.

The induction step is a formal application of the One-Step Lemma (14.1). $\qquad\square$

Up until now we have always extended $\vec{a} \in P(J)$ to a vector in $P(J \cup \{k_1\})$ by giving it the value 0 on k_1. But now we want it to take the value $\lambda(J, \vec{a}, k_1)$ on k_1. The simplest way to express this is to use monomials and to write $g_{k_1}^{\lambda(J,\vec{a},k_1)} g_J^{\vec{a}}$.

Lemma 15.3. (One-Row Trace Lemma) *Let $\vec{a} \in P(J)$ be $S_J(J)$-k_1-compatible. Then we have*

(1) $\mathrm{Tr}_{U_{\{k_1\}}} \left[G(J) \cdot h_J^{\vec{a}} \right] = G(J \cup \{k_1\}) \left[(-1)^{\tau(k_1+1,J,\vec{a})} g_{k_1}^{\lambda(J,\vec{a},k_1)} g_J^{\vec{a}} + x \right],$

where $x \in H(g_{k_1}^{\lambda(J,\vec{a},k_1)} g_J^{\vec{a}}, k[g_{k_1}, g_J])$ and $\tau = \tau(k_1 + 1, J, \vec{a})$ is as in Lemma 15.2. Furthermore,

(2) $\mathrm{Tr}_{U_{\{k_1\}}} \left[G(J) \cdot H(h_J^{\vec{a}}, k[h_{k_1}, h_J]) \right] \subseteq G(J \cup \{k_1\}) H(g_{k_1}^{\lambda(J,\vec{a},k_1)} g_J^{\vec{a}}, k[g_{k_1}, g_J]).$

Proof of the One-Row Trace Lemma. We just need to interpret the result of the m-Step Lemma (15.2) in the case when $l = k_1 + 1$. We are calculating the correct trace by Lemma 15.1 and the fact that $U_{\{k_1\}} = \prod_{j=k_1+1}^n A(x_{k_1}, x_j)$. Notice also that $G(J)_{k_1+1} = G(J \cup \{k_1\})$ (Lemma 13.2), $h_{J<k_1}^{\vec{a}} = g_{J<k_1}^{\vec{a}}$, $\theta(x_{k_1}; J^{<k_1+1}) = g_{k_1}$ and $f(k_1+1) = \lambda(J, \vec{a}, k_1)$ (by the definition of f (5.23)).

Also $R_{k_1+1}(\vec{a}) = H((\vec{a}_{\tilde{j}})_0, k[g_{k_1}, g_{\tilde{j}}])$ and $R_{n+1}(\vec{a}) = H(\vec{a}_0, k[h_{k_1}, h_{\tilde{j}}])$ (Remark 13.11). The old x (in 15.2) is in $R_{k_1+1}(\vec{a})$, so the new x (in 15.3) is in $h_{J<k_1}^{\vec{a}} R_{k_1+1}(\vec{a}) = H(\vec{a}, k[g_{k_1}, g_J]) = H(g_J^{\vec{a}}, k[g_{k_1}, g_J])$. In fact, it is in $H(g_{k_1}^{\lambda(J,\vec{a},k_1)} g_J^{\vec{a}}, k[g_{k_1}, g_J])$, since there is some j greater than k_1 for which g_j occurs to a higher power than a_j and we are using the lexicographic ordering. $\square$

The λ inside the H-terms is not necessary at this stage, but we want it for use later.

16. THE TRACE LEMMA

In this section we will finally be able to prove the Trace Lemma (16.1), which is a partial calculation of $\mathrm{Tr}_{U_I/U_J} : S^{U_J} \to S^{U_I}$. Recall that the notation in the statement of the result was introduced in Section 7 (7.1, 7.4), in particular the definitions of the invariants d_i, e_i, f_i, g_i, and h_i. We will regard $\lambda(J, \vec{a}, -)$ as a function on K (or some subset), denoted by $\vec{\lambda}(J, \vec{a})$.

Lemma 16.1 (Trace Lemma)**.** *Let $\vec{a} \in P(J)$ be $S_J(J)$-k_1-compatible. Then we have*

(1) $$\mathrm{Tr}_{U_I/U_J} \left[G(J) \cdot h_J^{\vec{a}} \right] = (-1)^{\hat{\tau}} d_K^{\vec{\lambda}(J,\vec{a})} d_J^{\vec{a}} + x,$$

where $x \in H(d_K^{\vec{\lambda}(J,\vec{a})} d_J^{\vec{a}}, k[d_I])$ and $\hat{\tau} = \hat{\tau}(I, J, \vec{a}) = ns + \sum_{k \in K} k + \sum_{j \in J} |K^{<j}|(a_j + 1)$. Furthermore,

(2) $$\mathrm{Tr}_{U_I/U_J} \left[G(J) \cdot H(h_J^{\vec{a}}, k[h_J]) \right] \subseteq H(d_K^{\vec{\lambda}(J,\vec{a})} d_J^{\vec{a}}, k[d_I]).$$

The above result is the special case, $m = |K|$, of the following slightly more general lemma, which is a partial calculation of $\mathrm{Tr}_{U_{J \cup K^{\leq k_m}}/U_J} : S^{U_J} \to S^{U_{J \cup K^{\leq k_m}}}$.

The idea of the proof is that $U_I = U_K \cdot U_J$ and if we write $K = \langle k_1, \ldots, k_{|K|} \rangle$ then $U_K = U_{\{k_{|K|}\}} \cdot U_{\{k_{|K|-1}\}} \cdots U_{\{k_2\}} \cdot U_{\{k_1\}}$. So, using 15.1, we can decompose $\mathrm{Tr}_{U_I/U_J} = \mathrm{Tr}_{U_K}$ as the composition $\mathrm{Tr}_{U_{\{k_{|K|}\}}} \mathrm{Tr}_{U_{\{k_{|K|-1}\}}} \cdots \mathrm{Tr}_{U_{\{k_2\}}} \mathrm{Tr}_{U_{\{k_1\}}}$ and compute the trace bit by bit.

Lemma 16.2. (*m-Row Trace Lemma, $P(m)$*) *Let $\vec{a}$ be $S_J(J)$-k_1-compatible and let $k_m \in K$. Then we have*

(1) $$\mathrm{Tr}_{U_{J \cup K^{\leq k_m}}/U_J} \left[G(J) \cdot h_J^{\vec{a}} \right] = G(J \cup K^{\leq k_m}) \cdot \left[(-1)^{\tau^{(m)}} e_{K^{\leq k_m}}^{\vec{\lambda}(J,\vec{a})} e_J^{\vec{a}} + x \right],$$

where $x \in H(e_{K^{\leq k_m}}^{\vec{\lambda}(J,\vec{a})} e_J^{\vec{a}}, k[e_{K^{\leq k_m}}, e_J])$ and $\tau^{(m)} = \sum_{i=1}^m \tau(k+1, J, \vec{a})$. Furthermore,

(2) $$\mathrm{Tr}_{U_{J \cup K^{\leq k_m}}/U_J} \left[G(J) \cdot H(h_J^{\vec{a}}, k[h_J]) \right] \subset G(J \cup K^{\leq k_m}) \cdot H(e_{K^{\leq k_m}}^{\vec{\lambda}(J,\vec{a})} e_J^{\vec{a}}, k[e_{K^{\leq k_m}}, e_J]).$$

We prove the m-Row Trace Lemma by induction on m. Of course, all that we actually need to prove is that $P(m-1) \Rightarrow P(m)$, since $P(1)$ is the One-Row Trace Lemma. Here we record what we need to show for the induction step of the proof of Lemma 16.2, which is a partial calculation of $\mathrm{Tr}_{U_{\{k_m\}}} = \mathrm{Tr}_{U_{J \cup K^{\leq k_m}}/U_{J \cup K^{\leq k_{m-1}}}} : S^{U_{J \cup K^{\leq k_{m-1}}}} \to S^{U_{J \cup K^{\leq k_m}}}$.

Lemma 16.3. $(P(m-1) \Rightarrow P(m))$ *Let $\vec{a}$ be $S_J(J)$-k_1-compatible. Then*

(1) $\mathrm{Tr}_{U_{\{k_m\}}} \left[G(J \cup K^{\leq k_{m-1}}) \cdot f_{K^{\leq k_{m-1}}}^{\vec{\lambda}(J,\vec{a})} f_J^{\vec{a}} \right] = G(J \cup K^{\leq k_m}) \cdot \left[(-1)^{\tau(k_m+1,J,\vec{a})} e_{K^{\leq k_m}}^{\vec{\lambda}(J,\vec{a})} e_J^{\vec{a}} + x \right],$

where $x \in H(e_{K^{\leq k_m}}^{\vec{\lambda}(J,\vec{a})} e_J^{\vec{a}}, k[e_{K^{\leq k_m}}, e_J])$. Furthermore,

(2) $\mathrm{Tr}_{U_{\{k_m\}}} \left[G(J \cup K^{\leq k_{m-1}}) \cdot H(f_{K^{\leq k_{m-1}}}^{\vec{\lambda}(J,\vec{a})} f_J^{\vec{a}}, k[f_{K^{\leq k_{m-1}}}, f_J]) \right] \subseteq$

$$G(J \cup K^{\leq k_m}) \cdot H(e_{K^{\leq k_m}}^{\vec{\lambda}(J,\vec{a})} e_J^{\vec{a}}, k[e_{K^{\leq k_m}}, e_J]).$$

Finally,
(3) $P(m-1)$, *1, and 2 together imply $P(m)$.*

Proof of Lemma 16.2. Use induction on m: Lemma 15.3 is the initial case and Lemma 16.3 is the induction step. $\square$

Proof of Lemma 16.3. For convenience, we write $K' = K^{\leq k_{m-1}}$ and $K'' = K^{\leq k_m}$.
   To prove part 1 we use the One-Row Trace Lemma (15.3), with J replaced by $J \cup K'$. In order to apply this lemma we must verify that $f_{K'}^{\vec{\lambda}(J,\vec{a})} f_J^{\vec{a}}$ is $S_{J \cup K'}(J \cup K')$-compatible. This is true by Lemma 5.31. We may therefore conclude that

$$\mathrm{Tr}_{U_{\{k_m\}}} \left[G(J \cup K') \cdot f_{K'}^{\vec{\lambda}(J,\vec{a})} f_J^{\vec{a}} \right] =$$

$$G(J \cup K'') \cdot \left[(-1)^{\tau(k_m+1,J \cup K',\vec{\alpha})} e_{k_m}^{\lambda(J \cup K',\vec{\alpha},k_m)} e_{K'}^{\vec{\lambda}(J,\vec{a})} e_J^{\vec{a}} + x \right],$$

where $\vec{\alpha} \in P(J \cup K')$ is the exponent vector associated to the monomial $f_{K'}^{\vec{\lambda}(J,\vec{a})} f_J^{\vec{a}}$, and $x \in H(e_{k_m}^{\lambda(J,\vec{a},k_m)} e_{K'}^{\vec{\lambda}(J,\vec{a})} e_J^{\vec{a}}, k[e_{K''}, e_J])$.
   Observe that $\lambda(J \cup K', \vec{\alpha}, k_m) = \lambda(J, \vec{\alpha}, k_m)$ by Lemma 5.30. Also observe that $\tau(k_m + 1, J \cup K', \vec{\alpha}) = \tau(k_m + 1, J, \vec{a})$ by definition of τ (15.2).
   Up to a change of notation, we have now proved Part 1 of Lemma 16.3.
   Part 2 of Lemma 16.3 is likewise an application of the One-Row Trace Lemma. We apply Lemma 15.3(2), with J replaced by $J \cup K'$ and k_1 replaced by k_m. This gives the desired equation.
   The proof of part 3 is easy and therefore left to the reader. $\square$

17. Consequences

Perhaps the most surprising corollary is the following result.

Theorem 17.1. *For any finite group G acting on S, only a finite number of (isomorphism types of) indecomposable kG-modules can occur as a summand of S.*

Proof. First we deal with the case of a p-group P, so we may assume that $P \subseteq U_n$. Taking the statement of the Main Theorem 10.1 and restricting it to P, we see that any indecomposable summand must be a summand of some $\mathrm{Res}_P^{U_n} \mathrm{Ind}_{U_J}^{U_n} X_J(J)$. Since there are only finitely many possible J and each $X_J(J)$ is finite, the result follows for P.
   For general G, let P be a Sylow p-subgroup of G. Then, as kG-modules, S is a summand of $\mathrm{Ind}_P^G \mathrm{Res}_P^G S$ and the result follows from the one for P. $\square$

Given a finite group G, let A be an abelian group (often $\mathbb{Z}$). We will consider an additive homomorphism $\chi : a_k(G) \to A$ from the Green ring to A, that is a function on the isomorphism classes of finite dimensional kG-modules with values in A which is additive on direct sums.

For any $\mathbb{Z}$-graded kG-module M, finite dimensional in each degree, the Poincaré series relative to χ is $\mathrm{PS}_\chi(M,t) = \sum_{n \in \mathbb{Z}} \chi(M_n) t^n$.

Interesting possibilities for χ include the dimension of the invariants or coinvariants, $\dim H^n(G,-)$ or the multiplicity of a given indecomposable kG-module as a summand. We can even take the identity function $\mathrm{id} : a_k(G) \to a_k(G)$, in which case $\mathrm{PS}_{\mathrm{id}}(M,t)$ expresses the isomorphism class of M.

Theorem 17.2. *For any p-group P acting on S, the Poincaré series relative to χ has the form*

$$\mathrm{PS}_\chi(S,t) = \frac{f(t)}{\prod_{i=1}^n (1 - t^{q^{i-1}})},$$

where $f(t)$ is a polynomial of degree at most $\frac{q^n-1}{q-1} - n$.

If we can calculate $\mathrm{PS}_\chi(S,t)$ in degrees up to and including $\frac{q^n-1}{q-1} - n$ then we know it in all degrees.

Proof. We may assume that $P \subseteq U_n$. By the Main Theorem (10.1) with $I = \{1, \ldots, n-1\}$,

(A) $$S \cong k[d_n] \otimes T(I) \cong \bigoplus_{J \subseteq I} k[d_k | k \in (I-J) \cup \{n\}] \otimes \bar{X}_J(I),$$

as kP-modules. Applying PS_χ we find that

$$\mathrm{PS}_\chi(S,t) = \sum_{J \subseteq I} \frac{\mathrm{PS}_\chi(\bar{X}_J(I),t)}{\prod_{i \in (I-J) \cup \{n\}} (1 - t^{q^{i-1}})}.$$

If we put each term over the common denominator $\prod_{i=1}^n (1 - t^{q^{i-1}})$ then the numerator becomes $\mathrm{PS}_\chi(\bar{X}_J(I),t) \prod_{j \in J} (1 - t^{q^{j-1}})$; this is bounded as required, by 5.21 and 5.22.

The last claim comes from the observation that $f(t) = \mathrm{PS}_\chi(S,t) \prod_{i=1}^n (1 - t^{q^{i-1}})$, so we can calculate $f(t)$. $\qquad\square$

We can reduce the bound on the degree at the cost of a more complicated formulation.

Theorem 17.3. *If we know the decomposition into indecomposables of S as a kU_I-module in degrees less than or equal to $q^{n-1} - n$ (or even just $\deg_I(\vec{p})$), then we know the decomposition into indecomposables of S in all degrees.*

Proof. We show by induction on $|I|$ that we know all the $X_J(I)$ for $J \subseteq I$; this proves the claim and the case $|I| = 0$ is trivial.

Since we know S as a kU_I-module in the range of degrees given, we certainly know it as a kU_J-module for $J \subset I$ and by induction we know $X_J(J)$ up to isomorphism for $J \subsetneqq I$. But this tells us $X_J(I)$, since the latter is constructed by induction and propagation from the former in the Main Theorem 10.1.

We can now identify $X_I(I)$ up to isomorphism as the remainder since, according to Lemma 5.22, the degree of an element of $X_I(I)$ is bounded by the two expressions given in the statement of the theorem. $\qquad\square$

Describing the ring structure of the invariants is a classical problem.

Theorem 17.4. *For any p-group P acting on S, the invariants S^P are generated as a ring by elements of degree less than or equal to $\frac{q^n-1}{q-1} - n$ if $n \geq 3$, (q if $n = 2$).*

For any group G acting on S, the invariants S^G are generated as a ring by elements of degree less than or equal to $\frac{q^n-1}{q-1}(nq - n - 1)$ if $n \geq 3$, ($2q^2 - q - 2$ if $n = 2$).

Proof. Taking invariants in formula A above we obtain $S^P = \bigoplus_{J \subseteq I} k[d_k | k \in (I - J) \cup \{n\}] \cdot \bar{X}_J(I)^P$. Thus S^P is generated by the d_i and $\bar{X}_J(I)^P$. The degrees of the former are bounded by q^{n-1}. The degrees of the latter are bounded by $\frac{q^n-1}{q-1} - n$, by Lemma 5.21. This is greater unless $n = 2$.

For general G, let P be a Sylow p-subgroup of G. Now $S^G \subseteq S^P$, and is, in fact, a summand as an S^{GL_n}-module. The splitting is given by $|G : P|^{-1} \operatorname{Tr}_P^G$ (where $\operatorname{Tr}_P^G s = \sum_{g \in G/P} gs$).

Thus it suffices to show that S^P is finitely generated as an S^{GL_n}-module by elements of the claimed degree (since S^{GL_n} is generated by the Dickson invariants, which have degree at most $q^n - 1$).

But we have already seen that every $s \in S^P$ can be expressed as $s = \sum_i \lambda_i a_i$ with $\lambda_i \in S^{U_n}$ and $\deg a_i \leq \frac{q^n-1}{q-1} - n$. To finish we note that it is shown in [6] that every $\lambda_i \in S^{U_n}$ can be written as $\sum_j \mu_{i,j} b_{i,j}$ with $\mu_{i,j} \in S^{GL_n}$ and $b_{i,j} \in S^{U_n}$ such that $\deg b_{i,j} \leq nq^n - 2\frac{q^n-1}{q-1}$. So $s = \sum_{i,j} \mu_{i,j} b_{i,j} a_i$ and S^P is generated over S^{GL_n} by elements of the form ba with $\deg a \leq \frac{q^n-1}{q-1} - n$ and $\deg b \leq nq^n - 2\frac{q^n-1}{q-1}$. These have the degrees claimed. $\quad\square$

Of course, it is well known that S^G is finitely generated: it is the explicit bound on the degrees of the generators that is relevant here. For a long time no such a priori bound was known, but recently Derksen and Kemper [7], using forgotten work of Hermann [9], produced the bound

$$(B) \qquad\qquad n(|G| - 1) + |G|^{n \cdot 2^{n-1}+1} \cdot n^{2^{n-1}+1}.$$

It is curious that this bound depends only on the order of the group and not the field, while the bound in Theorem 17.4 depends only on the field and not the group.

For "large" groups the bound in Theorem 17.4 is very much smaller than Derksen and Kemper's bound (B). For example, for U_n, where the best possible bound is q^{n-1}, it is of order q^{n-1} in q, while Derksen and Kemper's bound is roughly of order $(q^{n-1})^{n^2 2^{n-2}}$.

The bound in Theorem 17.4 can be improved if we know that P is contained in some U_I.

18. Index of Notation

Symbol	Definition	Symbol	Definition	Symbol	Definition
k	§4	p, q	§4	S	§4
U_n	§4	I, J, K	4.1	U_I	4.2
$J^{<i}$	4.3	θ	4.4, 12.1	d_i	4.5
μ	5.1	$P(I)$	5.2	ψ	5.3
λ	5.4	$S_J(I)$	5.5	IE, E	5.5
b_i^J	5.15	$\deg_I$	5.19	$f(l)$	5.23
$T(I)$	6.1	$d_I, d_I^{\vec{a}}$	7.1	$H(\vec{a}, k[d_I]), H(\vec{a})$	7.4
LM	7.6	soc	7.9	supp	7.12
PS	8.1	γ	8.4	κ	8.5
$G(I, J)$	9.2	Tr	9.3, 12.4	ν	9.6
d_i, e_i, f_i, g_i, h_i	11.1	$A(x_i, x_j)$	11.2	$\tilde{J}$	12.16
$G(I, J)_l$	13.1	$w_{l,i}, w_{l,X}$	13.4	$R_l(\vec{a})$	13.10

References

[1] Almkvist, G. and Fossum, R.M., *Decompositions of exterior and symmetric powers of indecomposable $\mathbb{Z}/p\mathbb{Z}$-modules in characteristic p and relations to invariants*, in *Séminaire d'Algèbre P. Dubreil*, Lecture Notes in Math. **641** 1-111, Springer, Berlin 1977.

[2] Alperin, J. and Kovacs, L.G., *Periodicity of Weyl modules for $SL(2, q)$*, Jour. Algebra **74** (1982), pp. 52–54.

[3] Bleher, F.M. and Chinberg, T., *Galois structure of homogeneous coordinate rings*, preprint.

[4] Bosma, W., Cannon, J. and Playoust, C., *The Magma algebra system. I. The user language.* Computational algebra and number theory (London, 1993). J. Symbolic Comput. **24** (1997), pp. 235–265.

[5] Bryant, R.M., *Symmetric powers of representations of finite groups*, Jour. Algebra **154** (1993), pp. 416–436.

[6] Campbell, H. E. A. and Hughes, I. P., *The ring of upper triangular invariants as a module over the Dickson invariants*, Math. Ann. **306** (1996), pp. 429–443.

[7] Derksen, H. and Kemper, G., *Computational Invariant Theory*, Encyclopaedia of Mathematical Sciences **130**, Springer-Verlag, Berlin, Heidelberg, New York 2002.

[8] Doty, S.R., *The submodule structure of certain Weyl modules for groups of type A_n*, Jour. Algebra **95** (1985), pp. 373–383.

[9] Hermann, G., *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale* Math. Ann., **95** (1926), pp. 736-788.

[10] Howe, R., *Asymptotics of dimensions of invariants for finite groups*, Jour. Algebra **122** (1989), pp. 374–379.

[11] Karagueuzian, D. B. and Symonds, P. *The module structure of a group action on a polynomial ring.* J. Algebra **218** (1999), pp. 672–692.

[12] Karagueuzian, D. B. and Symonds, P., *The module structure of a group action on a polynomial ring: examples, generalizations, and applications* Centre de Recherches Mathématiques Proceedings and Lecture Notes **35**, 2004, pp. 139–158.

[13] Glover, D.J., *A study of certain modular representations*, Journal of Algebra **51** (1978), pp. 425-275.

[14] Hughes, I. and Kemper, G., *Symmetric powers of modular representations, Hilbert series and degree bounds*, Comm. Algebra **28** (2000) pp. 2059-2080.

[15] Hughes, I. and Kemper, G., *Symmetric powers of modular representations for groups with a Sylow subgroup of prime order*, Jour. Algebra **241** (2001) pp. 759–788.

[16] Mui, H., *Modular invariant theory and cohomology algebras of symmetric groups.* J. Fac. Sci. Univ. Tokyo Sect. IA Math. **22** (1975), pp. 319–369.

[17] Shank, R.J. and Wehlau, D.L., *The transfer in modular invariant theory*, J. Pure Applied Algebra **142** (1999), pp. 63-77.

[18] Symonds, P., *Group actions on polynomial and power series rings*, Pacific J. Math. **195** (2000), pp. 225–230 .

[19] Symonds, P., *Cyclic group actions on polynomial rings*, to appear in Bull. London Math. Soc., or http://www.ma.umist.ac.uk/pas/preprints

[20] Symonds, P., *Structure theorems over polynomial rings*, preprint. http://www.ma.umist.ac.uk/pas/preprints

MATHEMATICS DEPARTMENT, BINGHAMTON UNIVERSITY, P. O. BOX 6000, BINGHAMTON, NEW YORK, 13902-6000
E-mail address: dikran@math.binghamton.edu

SCHOOL OF MATHEMATICS, UNIVERSITY OF MANCHESTER, P.O. BOX 88, MANCHESTER M60 1QD, ENGLAND
E-mail address: Peter.Symonds@manchester.ac.uk