INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

U·M·I

University Microfilms International
A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
313/761-4700 800/521-0600

Order Number 9307664

Computation of polynomial invariants of finite groups

McShane, Janet Marie, Ph.D.

The University of Arizona, 1992

U·M·I

300 N. Zeeb Rd.
Ann Arbor, MI 48106

COMPUTATION OF POLYNOMIAL INVARIANTS OF FINITE GROUPS

by

Janet Marie McShane

A Dissertation Submitted to the Faculty of the

DEPARTMENT OF MATHEMATICS

In Partial Fulfillment of the Requirements
For the Degree of

DOCTOR OF PHILOSOPHY

In the Graduate College

THE UNIVERSITY OF ARIZONA

1 9 9 2

THE UNIVERSITY OF ARIZONA
GRADUATE COLLEGE

As members of the Final Examination Committee, we certify that we have read the dissertation prepared by Janet Marie McShane

entitled Computation of Polynomial Invariants of Finite Groups

and recommend that it be accepted as fulfilling the dissertation requirement for the Degree of Doctor of Philosophy

Larry C Grove	30 Oct 92
Dr. Larry Grove	Date
Paul Fan	10/30/92
Dr. Paul Fan	Date
David Gay	10/30/92
Dr. David Gay	Date
Hermann Flaschka	10/30/92
Dr. Hermann Flaschka	Date
Theodore Laetsch	10/30/92
Dr. Theodore Laetsch	Date

Final approval and acceptance of this dissertation is contingent upon the candidate's submission of the final copy of the dissertation to the Graduate College.

I hereby certify that I have read this dissertation prepared under my direction and recommend that it be accepted as fulfilling the dissertation requirement.

Larry C Grove	30 Oct 92
Dissertation Director Dr. Larry Grove	Date

STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at The University of Arizona and is deposited in the University Library to be made available to borrowers under rules of the Library.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgement of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the head of the major department or the Dean of the Graduate College when in his or her judgement the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

SIGNED: Janet Marie McShane

ACKNOWLEDGEMENTS

To my advisor, Larry Grove, go my deepest thanks. You opened my eyes to the world of group theory and invariant theory. You shared your knowledge with me and in so doing enabled me to find the knowledge hidden within myself. Your support, enthusiasm, patience, and confidence in me, made it possible for me to achieve this - and I thank you.

To all my other professors at the University of Arizona a word of thanks for all your help and encouragement.

To all my colleagues at NAU - to those of you who encouraged me to return to school, to those of you who sat through my lectures when I first started studying invariant theory, to those of you who made it possible for me to be gone for a number of years, and to everyone - I truly appreciate your support and encouragement over the years.

To Professor Neubüser and M. Schönert and everyone else at RWTH - a very special thanks. My time at RWTH was invaluable and enabled me to pull all the pieces together.

To Gregor Kemper whose correspondence and Maple expertise were especially helpful.

To Ted for showing me that applied math has important real life applications -to Kathleen for instructing me in the world of sports - to Hannah for listening and a place to stay - to Lisa for the many talks, midnight runs to the Circle K and for being there at the very end - to Lynne for a special soul connection - I thank you all.

To Cliff, Nancy and Mark - faithful friends - little did you know that the year I spent with you would launch me on my way.

To Barb T. - thanks for entering my life again and sharing all these trials and tribulations with me.

To my n.s.f.o.c. in Flagstaff - your belief in me and what I was doing helped me make it through. To Kathy - thanks for always being there and being so positive. To Sybil - thanks for being 'so close' with an open door policy and a couch and an ear that got me through many a night. And to Ann, who has been with me in this process from the very beginning, your support has been invaluable and the late night talks, fixing the ills of the world, helped me keep my perspective through it all. Thanks.

To all my siblings, in-laws, nieces and nephews – though you understood little of what I was doing or why, nonetheless you were always supportive and your presence and lives added some balance to mine.

To my father - for always being there - a special thanks.

And finally - to John. Getting a PhD has enriched my life - and one of the reasons is because I found such a wonderful friend in you. Thanks for always listening and caring, for all the advice and support, for believing in me, and for enriching my life.

DEDICATION

To my mother Rita, who is always with me, and to Misty.

TABLE OF CONTENTS

TABLE OF CONTENTS – Continued

ABSTRACT

If G is a finite subgroup of $GL(n, K)$, K a field of characteristic 0, it is well known that the algebra $\mathcal{I}$ of polynomial invariants of G is Cohen–Macaulay. Consequently $\mathcal{I}$ has a subalgebra $\mathcal{J}$ of Krull dimension n so that $\mathcal{I}$ is a free $\mathcal{J}$–module of finite rank. A sequence $(f_1, \ldots, f_n; g_1, \ldots, g_m)$ of homogeneous invariants is a Cohen–Macaulay (or CM) basis if $\mathcal{J} = K[f_1, \ldots, f_n]$ and $\{g_1, \ldots, g_m\}$ is a basis for $\mathcal{I}$ as a $\mathcal{J}$–module. This dissertation discusses an algorithm, and an implementation using the systems GAP and Maple, for the calculation of CM–bases.

1. INTRODUCTION TO INVARIANT THEORY

The study of the invariant theory of finite groups has been an important part of group theory for over a century, dating back at least to fundamental work of D. Hilbert and E. Noether. The fundamental problem of invariant theory of finite groups is to determine or characterize the algebra of invariants. A survey of the classical approach to this subject can be found in Burnside's *Theory of Groups of Finite Order* [4]. There have been significant applications of invariant theory to such diverse areas as combinatorics, algebraic geometry, coding theory, physics, and chemistry. Recent surveys of some of this work have been given by Stanley [29] and Sloane [26].

We begin this chapter with some basic notation that will be used throughout. We will define what we mean by an invariant of a finite group and look at some basic ideas involving invariants.

1.1 Basics

Let K be a field of characteristic 0 and let V be a vector space of dimension n over K. The dual space of V, $V^* = Hom(V, K)$, also has dimension n. If $\{v_1, \ldots, v_n\}$ is a basis for V then V^* has a corresponding dual basis $\{x_1, \ldots, x_n\}$ characterized by the fact that $x_i(v_j) = \delta_{ij}$ for all i and j.

Let $\mathcal{F}$ be the algebra of all functions from V to K with pointwise operations. We will denote by $\mathcal{P}$ the subalgebra of $\mathcal{F}$ generated by $\{x_1, \ldots, x_n\}$. If $\alpha = (a_1, \ldots, a_n)$, where each $a_i \in \mathbb{N}$, $X = (x_1, \ldots, x_n)$, and $X^\alpha = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, then elements of $\mathcal{P}$ will be finite sums of the form $\sum c_\alpha X^\alpha$, $c_\alpha \in K$. We will call the elements of $\mathcal{P}$

polynomial functions. The generators $\{x_1, \ldots, x_n\}$ of $\mathcal{P}$ are basis dependent, but in fact $\mathcal{P}$ is generated by V^* and thus $\mathcal{P}$ is independent of the basis $\{v_1, \ldots, v_n\}$.

Let $K[z_1, \ldots, z_n]$ be a polynomial algebra over K with distinct commuting indeterminates $z_1, \ldots, z_n$. The function $\theta : K[z_1, \ldots, z_n] \to \mathcal{P}$ determined by $\theta(z_i) = x_i$ is actually a K-isomorphism since K is an infinite field. Since $K[z_1, \ldots, z_n]$ and $\mathcal{P}$ are isomorphic this is the reason we call the elements of $\mathcal{P}$ polynomial functions. We will write $\mathcal{P} = K[x_1, \ldots, x_n]$ and we carry over to $\mathcal{P}$ some of the standard concepts connected with polynomials. These include the facts that we call X^α a *monomial* and the *degree* of X^α is $|\alpha| = \sum_i^n a_i$. Note that a monomial is restricted to having 1 as its coefficient from K. A polynomial of the form cX^α, for arbitrary $c \neq 0$ in K, will be called a *term.* The degree of a term cX^α will simply be the degree of X^α.

Each $f \in \mathcal{P}, f \neq 0$, can be written uniquely as a sum of terms with distinct monomials. The *degree* (relative to $x_1, \ldots, x_n$) of any $f \in \mathcal{P}, f \neq 0$, is the maximum of the degrees of its terms. If $f = 0$ then, by convention, the degree of f is d for every $d \in \mathbb{N}$.

A polynomial function $f \in \mathcal{P}$ is called *homogeneous* of degree d if all its terms have degree d or if $f = 0$.

If $d \in \mathbb{N}$ then we define $\mathcal{P}_d$ to be the set of all homogeneous polynomials of degree d. Each $\mathcal{P}_d$ is a subspace of the K-vector space $\mathcal{P}$ and we have $\mathcal{P} = \mathcal{P}_0 \oplus \mathcal{P}_1 \oplus \mathcal{P}_2 \oplus \ldots$. The subspace $\mathcal{P}_0$ consists of the constant functions and we identify $\mathcal{P}_0$ with K. Note that $\mathcal{P}_1 = V^*$, the dual space.

Let $GL(V)$ represent the group of all nonsingular linear transformations of V. If $T \in GL(V)$ define an action of T on $\mathcal{P}$ as follows:

$$\text{If } f \in \mathcal{P},\ v \in V \text{ then } (Tf)(v) = f(T^{-1}v).$$

Note that if $f \in \mathcal{P}$ then $Tf \in \mathcal{P}$ and that $T\mathcal{P}_d = \mathcal{P}_d$ for each degree d.

The following proposition makes it clear why the inverse appears in the above definition of the action of T on f.

Proposition 1.1.1 *If $S, T \in GL(V)$ and $f \in \mathcal{P}$, then $(ST)f = S(Tf)$.*

Proof. If $v \in V$ then $((ST)f)(v) = f((ST)^{-1}v) = f(T^{-1}S^{-1}v) = (Tf)(S^{-1}v) = (S(Tf))(v)$. So $(ST)f = S(Tf)$. △

Proposition 1.1.2 *If $T \in GL(V)$ and $f, g \in \mathcal{P}$, then $T(fg) = (Tf)(Tg)$.*

Proof. If $v \in V$ then we have $(T(fg))(v) = (fg)(T^{-1}v) = f(T^{-1}v)g(T^{-1}v) = (Tf)(v)(Tg)(v)$. Thus $T(fg) = (Tf)(Tg)$. △

If $T : V \to V$ is a linear transformation recall that its *adjoint* transformation $T^* : V^* \to V^*$ is defined by $T^*(\phi) = \phi \circ T$ (composition of functions) for all $\phi \in V^*$. If $S : V \to V$ is another linear transformation then $(TS)^*\phi = \phi \circ (TS) = \phi \circ T \circ S = (T^*\phi) \circ S = (S^*T^*)\phi$, so $(TS)^* = S^*T^*$.

Now if $T \in GL(V)$ we can define the corresponding *contragredient transformation* which acts on V^* *via* the composition of the adjoint with the inverse. That is, the *contragredient* $\tilde{T}$ is defined by $\tilde{T} = (T^{-1})^*$. Note that if $f \in V^*$ then $(\tilde{T}f)(v) = (T^{-1})^* f(v) = f(T^{-1}v)$. Thus the action of T on $\mathcal{P}$ defined above is an extension to $\mathcal{P}$ of the contragredient action on the dual space.

In view of the isomorphism of $\mathcal{P}$ with $K[z_1, \ldots, z_n]$ we write $f = f(x_1, \ldots, x_n)$ for each $f \in \mathcal{P}$, and then in fact $f(v)$ is just $f(x_1(v), \ldots, x_n(v))$ for all $v \in V$.

Now since we will be dealing with finite groups of matrices we need to know how the action of T on $\mathcal{P}$ is carried out *via* a representing matrix. A small example will help make this clear.

Consider the transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined *via* $Tv_1 = v_2$ and $Tv_2 = -v_1 - v_2$, where $v_1 = e_1$ and $v_2 = e_2$ (the standard basis for $\mathbb{R}^2$). Thus T is represented by the matrix $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ and T^{-1} is represented by the matrix $A^{-1} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$. One can easily show that then $\tilde{T}x_1 = -x_1 + x_2$ and $\tilde{T}x_2 = -x_1$ and thus the representing matrix for $\tilde{T}$ on V^* is $\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ which just happens to be $(A^{-1})^t$ (the transpose of A^{-1}).

Now if we write (x_1, x_2) to represent the list of generators for $\mathcal{P}$ then the product

$$(x_1, x_2)\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = (-x_1 + x_2, -x_1) \qquad (*)$$

tells us that Tf will simply be the function f with the change of variables $x_1 \mapsto -x_1 + x_2$ and $x_2 \mapsto -x_1$. Or taking transposes in equation $(*)$ we have

$$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -x_1 + x_2 \\ -x_1 \end{pmatrix}.$$

Thus, for example, if $f = 3x_1x_2$ then $Tf = f(-x_1 + x_2, -x_1) =$ $3(-x_1 + x_2)(-x_1) = 3x_1^2 - 3x_1x_2$.

A polynomial f is an *invariant* for a group $G \leq GL(V)$ if $Tf = f$ for all T in G. The algebra of all polynomial invariants of G will be denoted by $\mathcal{I} = \mathcal{I}_G$.

For a finite group $G \leq GL(V)$ define $\mathcal{M}_G = \mathcal{M} : \mathcal{P} \to \mathcal{P}$ *via* $\mathcal{M}f = |G|^{-1}\sum\{Tf : T \in G\}$. The polynomial $\mathcal{M}f$ is the *mean* or *average* of the G-transforms of f. The linear transformation $\mathcal{M}$ is sometimes called the *Reynolds Operator*. Note that $\mathcal{M}\,\mathcal{P}_d \subseteq \mathcal{P}_d$ for each d.

For a simple example consider $G = C_3$ with generator T represented by $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ and the polynomial $f = 3x_1x_2$. We saw earlier that $Tf = 3x_1^2 - 3x_1x_2$. Similarly $T^2f = -3x_1x_2 + 3x_2^2$ and therefore

$$\mathcal{M}f = \frac{1}{3}(3x_1x_2 + 3x_1^2 - 3x_1x_2 - 3x_1x_2 + 3x_2^2)$$

$$= x_1^2 - x_1x_2 + x_2^2.$$

Note that the polynomial above, $f = 3x_1x_2$, is not an invariant of C_3. However, $\mathcal{M}f = x_1^2 - x_1x_2 + x_2^2$ is an invariant of C_3. The next proposition proves this fact for a general polynomial f.

Proposition 1.1.3 *Suppose $G \leq GL(V)$ is finite. Then*

(a) if $f \in \mathcal{P}$ then $\mathcal{M}f \in \mathcal{I}$,

(b) $\mathcal{M}$ restricts to the identity map on $\mathcal{I}$ and $\mathcal{M}^2 = \mathcal{M}$, and

(c) if $f \in \mathcal{P}$ and $g \in \mathcal{I}$ then $\mathcal{M}(fg) = (\mathcal{M}f)g$.

In particular $\mathcal{M}$ is a projection from $\mathcal{P}$ onto $\mathcal{I}$.

Proof. (a) If $S \in G$ then $S\mathcal{M}f = |G|^{-1}\sum\{STf : T \in G\} = \mathcal{M}f$ since ST ranges over all elements of G as T does. Thus $\mathcal{M}f \in \mathcal{I}$.

(b) If $f \in \mathcal{I}$ then $\mathcal{M}f = |G|^{-1}\sum\{Tf : T \in G\} = |G|^{-1}\sum\{f : T \in G\} = |G|^{-1}|G|f = f$. Thus $\mathcal{M}$ acts as the identity map on $\mathcal{I}$. Given any $g \in \mathcal{P}, \mathcal{M}^2g = \mathcal{M}(\mathcal{M}g) = \mathcal{M}g$ since $\mathcal{M}g \in \mathcal{I}$.

(c) $\mathcal{M}(fg) = |G|^{-1}\sum\{Tfg : T \in G\} = |G|^{-1}\sum\{(Tf)(Tg) : T \in G\} = |G|^{-1}\sum\{(Tf)g : T \in G\} = |G|^{-1}\sum\{Tf : T \in G\}g = (\mathcal{M}f)g.$ △

Corollary 1.1.4 *$\mathcal{M}$ restricts to a projection from $\mathcal{P}_d$ onto $\mathcal{I}_d$ for each degree d.*

Let us continue with the example C_3 from above. If we take other monomials and apply the Reynolds Operator to them we will obtain other invariants of the group C_3. The set $B = \{f_1, f_2, f_3\}$, with $f_1 = x_1^2 - x_1x_2 + x_2^2$, $f_2 = x_1^2x_2 - x_1x_2^2$, and $f_3 = x_1^3 - 3x_1x_2^2 + x_2^3$, was obtained by averaging various monomials and in

some cases multiplying through by a suitable constant. This set, besides being a set of invariants of C_3, has the special property that *any* invariant of C_3 can be written as a polynomial in f_1, f_2, and f_3. Such a set B is called an *integrity basis*; we will discuss this concept further in Chapter 3.

Since there are only two indeterminates and the set B contains 3 elements then there must exist an algebraic dependence relation among the polynomials in B. Such a dependence relation is called a *syzygy*. For this particular set B one can verify that $f_1^3 - 9f_2^2 + 3f_2f_3 - f_3^2 = 0$ is a syzygy, and in fact, all other syzygies of invariants of C_3 can be derived from this one. We will discuss sygyzies in more detail in Chapter 3.

1.2 The Molien Series

If G is a finite subgroup of $GL(V)$, with algebra $\mathcal{I}$ of invariants, then the *Molien series* of G is a formal power series $\Phi(t) = \Phi_G(t)$ whose coefficients are the K–dimensions of the homogeneous parts $\mathcal{I}_d$ of $\mathcal{I}$, *i.e.*

$$\Phi(t) = \sum_{d=0}^{\infty} (dim_K \mathcal{I}_d) t^d.$$

An elegant theorem of T. Molien, first published in 1897 ([22]), which shows that the Molien series is in fact a rational function of t, provides a means of calculating the series and has important theoretical ramifications as well.

Theorem 1.2.1 (Molien's Theorem) *If G is a finite subgroup of $GL(V)$ then its Molien series is*

$$\Phi(t) = |G|^{-1} \sum \{det(1 - tT)^{-1} : T \in G\}.$$

We will prove a slightly more general version of the theorem below.

Let us write $charpol_T(t)$ for the characteristic polynomial $det(T - t1)$ of a linear transformation T of V. Note that if $T \in GL(V)$ then $det(1 - tT^{-1}) = (det\, T^{-1}) \cdot charpol_T(t)$, so the summands in Molien's theorem can be written as $(det\, T)/charpol_T(t)$. If $cl(T_1), \ldots, cl(T_k)$ are the distinct conjugacy classes in G then Molien's theorem can be rewritten as

$$\Phi(t) = |G|^{-1} \sum_{i=1}^{k} \frac{|cl(T_i)| det\, T_i}{charpol_{T_i}(t)},$$

which is a convenient form for calculation.

For example, for the group C_3 we have

$$\Phi(t) = \frac{1}{3}\left(\frac{1}{(1-t)^2} + \frac{2}{t^2+t+1}\right)$$

$$= \frac{1+t^3}{(1-t^2)(1-t^3)}$$

$$= 1 + t^2 + 2t^3 + t^4 + 2t^5 + 3t^6 + 2t^7 + 3t^8 + 4t^9 + 3t^{10} + 4t^{11} + \cdots.$$

It will be useful to generalize slightly the notion of polynomial invariant. Suppose λ is a linear K–character of G, *i.e.* a homomorphism from G to the multiplicative group K^*. Then $f \in \mathcal{P}$ is called a *semi–invariant* relative to λ, or a *λ–invariant*, if $Tf = \lambda(T)f$ for all $T \in G$. Thus a λ-invariant is an ordinary invariant if and only if λ is the *principal character* 1_G, which maps every $T \in G$ to $1 \in K$.

For a small example consider D_3, the dihedral group of order 6, generated by T_1 represented by $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ and T_2 represented by $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$. Let $f = -x_1^3 + 3x_1x_2^2 - x_2^3$ and define λ by $\lambda(T) = det\, T$. It is easy to check that $Tf = f$ for

$T = 1$, T_1, T_1^2 which all have determinant 1 and $Tf = -f$ for $T = T_2$, T_1T_2, $T_1^2T_2$ which all have determinant -1. Thus f is a λ–invariant of D_3.

The set $\mathcal{I}^{(\lambda)}$ of all λ–invariants of G is clearly a K–subspace of $\mathcal{P}$. It is in fact an $\mathcal{I}$–submodule, for if $f \in \mathcal{I}$ and $g \in \mathcal{I}^{(\lambda)}$ then $T(fg) = (Tf)(Tg) = \lambda(T)fg$, all $T \in G$.

The module of λ–invariants has a vector space decomposition

$$\mathcal{I}^{(\lambda)} = \mathcal{I}_0^{(\lambda)} \oplus \mathcal{I}_1^{(\lambda)} \oplus \mathcal{I}_2^{(\lambda)} \oplus \cdots ,$$

where $\mathcal{I}_d^{(\lambda)}$ is the subspace of homogeneous λ–invariants of degree d (including 0). In the language that will be developed in the next chapter $\mathcal{I}^{(\lambda)}$ is a *graded* $\mathcal{I}$–module.

As for ordinary invariants we define the *Molien series* of $\mathcal{I}^{(\lambda)}$ to be the formal power series

$$\Phi^{(\lambda)}(t) = \sum_{d=0}^{\infty} (dim_K \mathcal{I}_d^{(\lambda)}) t^d.$$

For each dimension d the action of G on the subspace $\mathcal{P}_d$ provides a representation ρ_d of G, the so-called *symmetrized* dth *power* of the contragredient representation of G on V^*. Denote the character of the representation ρ_d by ψ_d. Thus if for each $S \in GL(V)$ we write $tr_d S$ for the trace of the transformation induced by S on $\mathcal{P}_d$, then we have $\psi_d(T) = tr_d T$ for all $T \in G$.

For the proof of the next proposition see [9], page 112.

Proposition 1.2.2 *If* $T \in GL(V)$ *then*

$$\sum_{d=0}^{\infty} (tr_d T^{-1}) t^d = det(1 - tT)^{-1}.$$

The representation ρ_d of G is equivalent, by Maschke's theorem (see *e.g.* [8], page 262), to a direct sum of irreducible representations. If λ is a linear character

of G, as above, then the K–dimension of $\mathcal{I}_d^{(\lambda)}$ is simply the multiplicity of the representation with character λ as a constituent of that direct sum, and it is a standard result from character theory (*e.g.* [8] again) that the multiplicity is equal to the inner product of λ with the character ψ_d of ρ_d, *i.e.*

$$(\lambda, \psi_d) = |G|^{-1} \sum \{\lambda(T)\psi_d(T^{-1}) : T \in G\}.$$

With these ideas in hand we may state and prove the above-mentioned generalization of Molien's theorem.

Theorem 1.2.3 *If G is a finite subgroup of $GL(V)$ and λ is a linear K-character of G then the Molien series of $\mathcal{I}^{(\lambda)}$ is*

$$\Phi^{(\lambda)}(t) = |G|^{-1} \sum \{\lambda(T) det(1 - tT)^{-1} : T \in G\}.$$

Proof. We apply the remarks above and Proposition 1.2.2:

$$\begin{aligned}
\Phi^{(\lambda)}(t) &= \sum_{d=0}^{\infty} (dim_K \mathcal{I}_d^{(\lambda)}) t^d = \sum_{d=0}^{\infty} (\lambda, \psi_d) t^d \\
&= \sum_{d=0}^{\infty} |G|^{-1} \sum_{T \in G} \lambda(T)\psi_d(T^{-1}) t^d \\
&= |G|^{-1} \sum_{T \in G} \lambda(T) \sum_{d=0}^{\infty} (tr_d T^{-1}) t^d \\
&= |G|^{-1} \sum_{T \in G} \lambda(T) det(1 - tT)^{-1}.
\end{aligned}$$

△

Of course Molien's theorem (1.2.1) is obtained by choosing $\lambda = 1_G$.

The following consequence of Theorem 1.2.3 will be useful in Chapter 3.

Proposition 1.2.4 *If λ is the linear character of G defined by $\lambda(T) = det\, T$, then*

$$\Phi(1/t) = (-t)^n \Phi^{(\lambda)}(t).$$

Proof. We begin by applying Molien's theorem; note that in its statement we may replace each T by T^{-1}:

$$\Phi(1/t) = |G|^{-1} \sum_{T \in G} \frac{1}{det(1 - t^{-1}T^{-1})}$$

$$= |G|^{-1} \sum_{T \in G} \frac{1}{det(t^{-1}T^{-1})det(tT - 1)}$$

$$= |G|^{-1} t^n \sum_{T \in G} \frac{det\, T}{(-1)^n det(1 - tT)}$$

$$= (-t)^n \Phi^{(\lambda)}(t).$$

△

2. COMMUTATIVE ALGEBRA

In this chapter we develop some basic concepts of commutative algebra, including graded algebras and modules, regular sequences, systems of parameters, and Cohen-Macaulay modules. These ideas will ultimately provide a very useful description of the structure of the algebra of invariants of a finite group.

2.1 Graded Algebras and Modules

As usual, K is a field of characteristic zero and $\mathbb{N}$ is the semigroup of natural numbers.

A K–algebra A (always assumed to be associative, commutative, and with 1) is said to have a *grading* if it has a vector space direct sum decomposition

$$A = \bigoplus \{A_d : d \in \mathbb{N}\}$$

such that $A_0 = K$ and $A_i A_j \subseteq A_{i+j}$ for all $i, j \in \mathbb{N}$. Strictly speaking this defines an algebra with an $\mathbb{N}$-*grading*; other gradings exist (*e.g.* with $\mathbb{N}$ replaced by $\mathbb{Z}$ or by $\mathbb{N}^k$) but this is the only type of concern to us here.

A *graded K–algebra* is a finitely generated K–algebra A with a grading.

An obvious example is the polynomial algebra $A = \mathcal{P} = K[x_1, \ldots, x_n]$, with A_d the subspace of homogeneous polynomials of degree d for each d. This example motivates much of the terminology that applies to graded algebras in general.

Note that a graded algebra must be Noetherian by the Hilbert Basis Theorem.

In general, an element a in an algebra A with a grading is said to be *homogeneous* if $a \in A_d$ for some d, in which case the *degree* of a is d and we write $deg(a) = d$. We call A_d the dth *homogeneous part* of A. Note in particular that

$deg(0) = d$ for every $d \in \mathbb{N}$, a seeming ambiguity that will be more convenient than confusing.

It will be convenient at times to be able to refer to the homogeneous parts A_d of A with d possibly negative. Our convention will be that $A_d = 0$ if $0 > d \in \mathbb{Z}$.

Every $a \neq 0$ in A can be written uniquely as $a = a_1 + \cdots + a_k$ for some k, with $0 \neq a_i \in A_{d_i}$ and $d_1 < d_2 < \cdots < d_k$. The summands a_i are called the *homogeneous components* of a.

If S is any subset of an algebra A with a grading we will write $Homog(S)$ to denote the set of all homogeneous elements in S.

An ideal $\mathfrak{a} \subseteq A$ is called *homogeneous* if for each nonzero $a \in \mathfrak{a}$ every homogeneous component of a is also in $\mathfrak{a}$. Note, for example, that if $f_1, f_2, \ldots, f_m$ are homogeneous in $\mathcal{P}$ and $\mathfrak{a} = \langle f_1, f_2, \ldots, f_m \rangle$ then $\mathfrak{a}$ is a homogeneous ideal. In fact, it is easy to verify that an ideal $\mathfrak{a}$ of A is homogeneous if and only if $\mathfrak{a}$ is generated by a set of homogeneous elements of A.

The proof of the next proposition is straightforward and is omitted.

Proposition 2.1.1 *If $\mathfrak{a}$ is a homogeneous ideal in an algebra A with a grading, then $A/\mathfrak{a}$ has a natural grading,* via $(A/\mathfrak{a})_d = (A_d + \mathfrak{a})/\mathfrak{a}$.

The *spectrum* of a commutative ring A, denoted by $Spec(A)$, is the set of all prime ideals in A.

If A is an algebra with a grading we will write A^+ for the ideal $\oplus\{A_d : d \geq 1\}$, often called the *irrelevant ideal* of A. Note that $A^+ \in Spec(A)$, and in fact A^+ is a maximal ideal in A.

We will consider various notions of dimension later; vector space dimension will always be denoted by dim_K.

Proposition 2.1.2 *Suppose A is a K-algebra with a grading, $A = \oplus_{d=0}^{\infty} A_d$, and that A^+ is generated by a finite subset $\{a_1, \ldots, a_m\}$ of $Homog(A^+)$. Then $A = K[a_1, \ldots, a_m]$, and in particular A is finitely generated, hence is a graded K-algebra.*

Proof. We will show that $A = K[a_1, \ldots, a_m]$ by showing inductively that each $A_d \subseteq K[a_1, \ldots, a_m]$ for all $d \in \mathbb{N}$. It is clear if $d = 0$, so assume $d > 0$. Say $deg(a_i) = d_i$, with all $d_i \geq 1$. If $a \in A_d$ we may write $a = \sum_{i=1}^{m} b_i a_i$ where we may assume each b_i is homogeneous, so $deg(b_i) = d - d_i$. Thus $A_d = \sum_i A_{d-d_i} a_i$. By induction $A_{d-d_i} \subseteq K[a_1, \ldots, a_m]$. Therefore $A_d \subseteq K[a_1, \ldots, a_m]$ and thus $A = K[a_1, \ldots, a_m]$. Δ

Corollary 2.1.3 *If A is a graded K-algebra, then $dim_K(A_d)$ is finite for all $d \in \mathbb{N}$.*

Proof. It follows from the proposition that each A_d has finite K-dimension since there are only finitely many monomial expressions of the form $\prod_i a_i^{e_i}$ that have degree d. Δ

If A is a graded K-algebra and $B \subseteq A$ then B is a *graded subalgebra* if B is itself a graded algebra and $B_d = B \cap A_d$. For example, $\mathcal{I}$, the ring of polynomial invariants of a finite group, is a graded subalgebra of $\mathcal{P}$, the ring of polynomials. It is not immediately obvious that $\mathcal{I}$ is finitely generated, but it will be proved in Chapter 3.

Proposition 2.1.4 *Suppose B is a graded subalgebra of A, $\mathfrak{a}$ is a homogeneous ideal in B and $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_m \in Spec(A)$. If*

$$Homog(\mathfrak{a}) \subseteq \mathfrak{p}_1 \cup \mathfrak{p}_2 \cup \cdots \cup \mathfrak{p}_m$$

then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.

Proof. Relabel, if necessary, so that $Homog(\mathfrak{a}) \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_k$ but $Homog(\mathfrak{a})$ is not contained in any union of $k-1$ of the $\mathfrak{p}_i$'s. If $k = 1$ then we are finished, so assume that $k > 1$ and choose $a_j \in (Homog(\mathfrak{a}) \cap \mathfrak{p}_j) \setminus \cup\{\mathfrak{p}_i : i \neq j, 1 \leq i \leq k\}$, for each j, $1 \leq j \leq k$. Since all $\mathfrak{p}_i$ are prime ideals, then all powers of each a_j are also elements of $(Homog(\mathfrak{a}) \cap \mathfrak{p}_j) \setminus \cup\{\mathfrak{p}_i : i \neq j, 1 \leq i \leq k\}$, so we may assume that all a_j have the same degree. Set $a = a_1^{k-1} + \prod\{a_i : 2 \leq i \leq k\} \in Homog(\mathfrak{a})$. Then $a \notin \mathfrak{p}_1$, or else $\prod_2^k a_i \in \mathfrak{p}_1$ and so $a_i \in \mathfrak{p}_1$ for some $i \neq 1$, which is a contradiction. Likewise $a \notin \mathfrak{p}_j$ for $j \geq 2$ or else $a_1 \in \mathfrak{p}_j$, also a contradiction. Thus $k = 1$ and the proposition is proved. $\triangle$

If A is a graded K–algebra and M is a unitary (left) A–module we say that M is a *graded A–module* if there are K–subspaces M_d, $d \in \mathbb{N}$, such that $M = \oplus\{M_d : d \in \mathbb{N}\}$, and $A_i M_j \subseteq M_{i+j}$ for all $i, j \in \mathbb{N}$. Elements of M_d are said to be *homogeneous* of *degree* d, and each $x \neq 0$ in M can be written uniquely as a sum of *homogeneous components*, just as for graded algebras.

Also, as for algebras, we will write $Homog(S)$ to denote the set of all homogeneous elements in any subset S of a graded module, and agree that $M_d = 0$ if $0 > d \in \mathbb{Z}$.

An A-submodule N of M is called *homogeneous*, or a *graded* submodule, if for each nonzero $x \in N$ every homogeneous component of x is also in N. Just as for homogeneous ideals in graded algebras it is easy to verify that a submodule N is homogeneous if and only if it is generated (as a submodule) by a set of homogeneous elements of M. Note that a homogeneous submodule N is itself a graded module with $N_d = N \cap M_d$ for all $d \in \mathbb{N}$.

Proposition 2.1.5 *If N is a homogeneous submodule of a graded A-module M, then M/N is naturally a graded A-module,* via $(M/N)_d = (M_d + N)/N$.

If A is a graded K–algebra we will write ${}_A\mathcal{M}$ for the class of all finitely generated graded A–modules. If $M \in {}_A\mathcal{M}$ then M is a Noetherian module since A is Noetherian and M is finitely generated.

Proposition 2.1.6 *If $M \in {}_A\mathcal{M}$, then $dim_K(M_d)$ is finite for all $d \in \mathbb{N}$.*

Proof. Choose a finite set $\{x_1, \ldots, x_k\}$ of homogeneous generators for M, say with $deg(x_i) = d_i$. As in the proof of Proposition 2.1.2, we can conclude $M_d = \sum_{i=1}^{k} A_{d-d_i} x_i$, for all $d \in \mathbb{N}$. By that proposition each A_{d-d_i} has a finite set of K–generators and therefore so has M_d. Δ

The next proposition is presumably well known, but we were unable to find it in the literature.

Proposition 2.1.7 *Suppose $M \in {}_A\mathcal{M}$, N is a homogeneous submodule and N has a complementary submodule L',* i.e. *$M = N \oplus L'$. Then N has a homogeneous complement L.*

Proof. Let x be any homogeneous element in M, say $x \in M_d$. Write $x = n_x + l'_x$ with $n_x \in N$ and $l'_x \in L'$. Then write $n_x = n'_x + n''_x$ with $n'_x \in N_d$. Since all homogeneous components of n''_x are of degrees different from d, and $x = n'_x + n''_x + l'_x$ then $x - n'_x = n''_x + l'_x \in M_d$. Set $l_x = x - n'_x = n''_x + l'_x \in M_d$ and define L to be the submodule of M generated by $\{l_x : x \in Homog(M)\}$, a homogeneous submodule. Observe that $x = n'_x + l_x \in N + L$ for all homogeneous $x \in M$. Therefore $M = N + L$.

Suppose $N \cap L \neq 0$. Since N and L are both homogeneous there is some $v \in N \cap L, v \neq 0$, say with $deg\ v = d$. Since $v \in L$, we may write $v = \sum_{i=1}^{k} a_i l_i$ with $a_i \in A$ and l_i a generator for L. We may assume $deg(a_i l_i) = d$ for all i. Then

each l_i can be written, as above, as $l_i = y_i - n_i' = n_i'' + l_i'$, where $y_i \in M_{d_i}$, $n_i' \in N_{d_i}$, and $l_i'' \in L'$. Thus each l_i is of degree d_i. Therefore $v = \sum_{i=1}^{k} a_i(n_i'' + l_i'')$ so

$$v - \sum_{i=1}^{k} a_i n_i'' = \sum_{i=1}^{k} a_i l_i' \in N \cap L'.$$

Since $N \cap L' = 0$ then $v = \sum_{i=1}^{k} a_i n_i''$. But all homogeneous components of $a_i n_i''$ are of degree different from $deg\, a_i + d_i = d = deg\, v$ which is a contradiction. Thus $N \cap L = 0$ and $M = N \oplus L$. △

2.2 Associated Primes

If $M \in {}_A\mathcal{M}$, write $\mathcal{Z}(M)$ for the set of zero-divisors on M in A, *i.e.* $\mathcal{Z}(M)$ is the set of all elements $a \in A$ such that $ax = 0$ for some $x \neq 0$ in M.

If $M \in {}_A\mathcal{M}$ and $\emptyset \neq S \subseteq M$ then the *annihilator* of S is $Ann(S) = \{a \in A: aS = 0\}$, which is clearly an ideal in A. Note that $\mathcal{Z}(M) = \cup\{Ann(x): 0 \neq x \in M\}$.

If $M \in {}_A\mathcal{M}$ and $\mathfrak{p} \in Spec(A)$ we say that $\mathfrak{p}$ is *associated with* M if $\mathfrak{p} = Ann(x)$ for some $x \neq 0$ in M. We will write $Assoc(M)$ for $\{\mathfrak{p} \in Spec(A): \mathfrak{p}$ is associated with $M\}$. Note that $Assoc(M) = \emptyset$ if $M = 0$.

There is a nice relationship between $\mathcal{Z}(M)$ and $Assoc(M)$ as given by the following proposition.

Proposition 2.2.1 *Suppose* $0 \neq M \in {}_A\mathcal{M}$. *Then*

i) if $\mathfrak{p}$ *is a maximal element in* $\mathcal{F} = \{Ann(x): 0 \neq x \in M\}$ *then* $\mathfrak{p} \in Assoc(M)$, *so in particular* $Assoc(M) \neq \emptyset$, *and*

ii) $\mathcal{Z}(M) = \cup\{\mathfrak{p}: \mathfrak{p} \in Assoc(M)\}$.

Proof. i) Note that $\mathcal{F} \neq \emptyset$ since $M \neq 0$. By the maximum condition for Noetherian rings there is a maximal element $Ann(x_0)$ in $\mathcal{F}$. Set $\mathfrak{p} = Ann(x_0)$. We must

show that $\mathfrak{p}$ is prime. Suppose $ab \in \mathfrak{p}$ but $b \notin \mathfrak{p}$. Then $(ab)x_0 = 0$ but $bx_0 \neq 0$. Thus $a \in Ann(bx_0)$. But $Ann(bx_0) \supseteq Ann(x_0) = \mathfrak{p}$, so $Ann(bx_0) = Ann(x_0)$ by the maximality of $Ann(x_0)$ in $\mathcal{F}$. Thus $a \in \mathfrak{p}$ and $\mathfrak{p}$ is prime.

ii) That $\cup\{\mathfrak{p}: \mathfrak{p} \in Assoc(M)\} \subseteq \mathcal{Z}(M)$ is clear from the definition. If $a \in \mathcal{Z}(M)$, choose $x \in M, x \neq 0$, so that $ax = 0$. Since $Ann(x) \in \mathcal{F}$, we may choose a maximal element $\mathfrak{p} \in \mathcal{F}$, with $\mathfrak{p} \supseteq Ann(x)$. Then $\mathfrak{p} \in Assoc(M)$ by i), and $a \in \mathfrak{p}$. Thus $a \in \cup\{\mathfrak{p}: \mathfrak{p} \in Assoc(M)\}$. Δ

Suppose $M, N \in {}_A\mathcal{M}$ and $\varphi \in Hom_A(M, N)$. If there exists $k \in \mathbb{N}$ such that $\varphi(M_i) \subseteq N_{i+k}$ for all $i \in \mathbb{N}$, then we say that φ is *homogeneous* of *degree* k . An example that often occurs is if we choose $a \neq 0$ in A_k and define $\varphi: M \to M$ *via* $\varphi(x) = ax$. Note that inclusion maps and quotient maps are homogeneous of degree 0.

Proposition 2.2.2 *If $M, N \in {}_A\mathcal{M}$ and $\varphi: M \to N$ is homogeneous then ker φ and Im φ are graded submodules.*

The ideals in $Assoc(M)$ are actually homogeneous ideals as shown by the next proposition.

Proposition 2.2.3 *If $M \in {}_A\mathcal{M}$ and $\mathfrak{p} \in Assoc(M)$ then $\mathfrak{p}$ is a homogeneous ideal and there exists $x \in Homog(M)$ such that $\mathfrak{p} = Ann(x)$.*

Proof. Choose $y \neq 0$ in M such that $\mathfrak{p} = Ann(y)$. Choose $a \in \mathfrak{p}$; thus $ay = 0$. Write $y = \sum_{i=0}^{k} y_i$, $y_i \in M_i$, $y_k \neq 0$ (so deg $y = k$). Also write $a = \sum_{i=0}^{l} a_i$, $a_i \in A_i$, $a_l \neq 0$. Then $0 = ay = a_0y_0 + (a_0y_1 + a_1y_0) + (a_0y_2 + a_1y_1 + a_2y_0) + \cdots + a_ly_k$. Thus $a_ly_k = 0$ (only term in M_{l+k}). Next $0 = a_{l-1}y_k + a_ly_{k-1}$ so $0 = a_{l-1}a_ly_k + a_l^2y_{k-1}$ so $a_l^2y_{k-1} = 0$. Then we get $a_l^3y_{k-2} = 0$ from the next degree down, etc. Thus

$a_l^{k+1} y_j = 0$ for all j, *i.e.* $a_l^{k+1} \in Ann(y) = \mathfrak{p}$, prime, so $a_l \in \mathfrak{p}$. Then $a - a_l$ has lower degree and is in $\mathfrak{p}$; inductively all $a_i \in \mathfrak{p}$, so $\mathfrak{p}$ is homogeneous.

Now take any homogeneous element $b \in \mathfrak{p}$. Then $0 = by = \sum_{i=0}^{k} by_i$; the summands have different degrees so $by_i = 0$ for all i. Thus $\mathfrak{p} \subseteq \cap_0^k Ann(y_i)$. Also, if $c \in \cap_0^k Ann(y_i)$ then clearly $cy = 0$, $c \in Ann(y) = \mathfrak{p}$. Therefore $\mathfrak{p} = \cap_o^k Ann(y_i)$. But then $\mathfrak{p} = Ann(y_j)$, some j, since $\mathfrak{p}$ is prime. Set $x = y_j$. $\triangle$

We wish to show that the set $Assoc(M)$ is finite. To do this we need the following four propositions.

Proposition 2.2.4 *Suppose* $M \in {}_A\mathcal{M}$. *If* $\mathfrak{p} \in Spec(A)$ *then* $\mathfrak{p} \in Assoc(M)$ *if and only if there is a graded submodule* $N \leq M$ *with* N *isomorphic to* $A/\mathfrak{p}$.

Proof. ($\Rightarrow$) Say $\mathfrak{p} = Ann(x)$, for some $x \in Homog(M)$. Define $\phi: A \to M$ *via* $\phi(a) = ax$, an A-homomorphism. Set $N = Im\ \phi \leq M$, a graded submodule by Proposition 2.2.2, and note that $ker\ \phi = \{a \in A: ax = 0\} = Ann(x) = \mathfrak{p}$. Therefore $A/\mathfrak{p} \cong N$.

($\Leftarrow$) Suppose $\theta: A/\mathfrak{p} \to N \leq M$ is an isomorphism. Define $\phi: A \to M$ *via* $\phi(a) = \theta(a + \mathfrak{p})$. Clearly ϕ is an A-homomorphism with $ker\ \phi = \mathfrak{p}$ and $Im\ \phi = N$. Set $x = \phi(1)$. Thus if $a \in A$ then $ax = 0$ if and only if $0 = a\phi(1) = \phi(a)$ if and only if $a \in \mathfrak{p}$. Therefore $\mathfrak{p} = Ann(x)$ and so $\mathfrak{p} \in Assoc(M)$. $\triangle$

Proposition 2.2.5 *Suppose* A *is a graded* K*-algebra and* $\mathfrak{p} \in Spec(A)$. *If* $\overline{b} = b + \mathfrak{p}$ *is non-zero in* $A/\mathfrak{p}$, *then* $Ann_A(\overline{b}) = \mathfrak{p}$. *In particular,* $Assoc(A/\mathfrak{p}) = \{\mathfrak{p}\}$.

Proof. If $a \in A$ then since $\mathfrak{p}$ is prime and $b \notin \mathfrak{p}$ we have $a\overline{b} = a(b+\mathfrak{p}) = ab+\mathfrak{p} = \mathfrak{p}$ if and only if $a \in \mathfrak{p}$. $\triangle$

Proposition 2.2.6 *If $M \in {}_A\mathcal{M}$ and $N \leq M$ is a graded submodule then*

$$Assoc(N) \subseteq Assoc(M) \subseteq Assoc(N) \cup Assoc(M/N).$$

Proof. The first inclusion is clear.

Take $\mathfrak{p} \in Assoc(M)$. We may assume $\mathfrak{p} \notin Assoc(N)$ or else there is nothing to prove. Thus $\mathfrak{p} = Ann(x)$ for some $x \in M \setminus N$. By Proposition 2.2.4 and its proof we have $A/\mathfrak{p} \cong Ax \leq M$ and by Proposition 2.2.5 if $b \in A \setminus \mathfrak{p}$ then $Ann(b + \mathfrak{p}) = Ann(bx) = \mathfrak{p}$. Thus if $0 \neq bx \in Ax \cap N$ then $\mathfrak{p} = Ann(bx) \in Assoc(N)$, contrary to our assumption. Thus $Ax \cap N = 0$. Therefore $a(x + N) = ax + N = N$ if and only if $ax \in N$ if and only if $ax = 0$ if and only if $a \in \mathfrak{p}$. Thus $Ann(x + N) = \mathfrak{p}$ and $\mathfrak{p} \in Assoc(M/N)$. △

Proposition 2.2.7 *If $M \in {}_A\mathcal{M}$ then M has a chain of submodules*

$$0 = M^{(0)} \leq M^{(1)} \leq M^{(2)} \leq \cdots \leq M^{(k)} = M,$$

with each $M^{(i)}/M^{(i-1)}$ isomorphic to $A/\mathfrak{p}_i$ for some $\mathfrak{p}_i \in Spec(A)$.

Proof. If $M \neq 0$ choose $\mathfrak{p}_1 \in Assoc(M)$. By Proposition 2.2.4 there is a submodule $M^{(1)} \cong A/\mathfrak{p}_1$. If $M^{(1)} \neq M$ then we choose $\mathfrak{p}_2 \in Assoc(M/M^{(1)})$ and obtain a submodule $M^{(2)}/M^{(1)} \cong A/\mathfrak{p}_2$.. Continue, and obtain an ascending chain $M^{(1)} \leq M^{(2)} \leq \cdots$ with the desired quotients. Since M is Noetherian the chain must terminate with some $M^{(k)} = M$. △

Theorem 2.2.8 *If $M \in {}_A\mathcal{M}$ then $Assoc(M)$ is finite.*

Proof. Apply Propositions 2.2.5, 2.2.6, and 2.2.7 to see that $Assoc(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ where $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are the primes that appear in 2.2.7. △

If $M \in {}_A\mathcal{M}$ and $k \in \mathbb{N}$, set $M^{[k]} = \oplus\{M_i : i \geq k\}$. For example, $A^{[1]} = A^+$.

Proposition 2.2.9 *If $M \in {}_A\mathcal{M}$, then there exist $k \in \mathbb{N}$ and $a \in Homog(A^+)$ such that $a \notin \mathcal{Z}(M^{[k]})$.*

Proof. Set $N = \{x \in M : A^+x = 0\}$, a finitely generated submodule of M. Since $A^+N = 0$, N is a finitely generated A/A^+ module. But $A/A^+ \cong K$ so N is a finite dimensional K–vector space. Thus there is a $k \in \mathbb{N}$ such that $N \cap M^{[k]} = 0$. In particular $A^+ \notin Assoc(M^{[k]})$. If $M^{[k]} = 0$ then any $a \in Homog(A^+)$ will do since then $\mathcal{Z}(M^{[k]}) = \emptyset$. If $M^{[k]} \neq 0$ apply Proposition 2.1.4 to $Assoc(M^{[k]})$ and conclude that $Homog(A^+) \not\subseteq \cup\{\mathfrak{p} : \mathfrak{p} \in Assoc(M^{[k]})\}$. But $\cup\{\mathfrak{p} : \mathfrak{p} \in Assoc(M^{[k]})\} = \mathcal{Z}(M^{[k]})$ by Proposition 2.2.1 and thus there is an $a \in Homog(A^+)$ with $a \notin \mathcal{Z}(M^{[k]})$. $\triangle$

The next proposition can be viewed as a graded version of Nakayama's Lemma.

Proposition 2.2.10 *Suppose $M \in {}_A\mathcal{M}$, $0 \neq a \in Homog(A^+)$, and $aM = M$. Then $M = 0$.*

Proof. Assume $M \neq 0$ and let $k = min\{i : M_i \neq 0\}$. Thus $M = M^{[k]}$. If $deg(a) = m > 0$ then $M = aM \subseteq M^{[k+m]}$, which is a proper submodule, and we have a contradiction. $\triangle$

The next few results will be needed in the section on dimension theory.

Proposition 2.2.11 *Suppose that $\{x_1, \ldots, x_n\}$ is a set of generators for $M \in {}_A\mathcal{M}$, and that $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in A with $\mathfrak{a} \supseteq Ann(M)$ and $\mathfrak{b}M \subseteq \mathfrak{a}M$. Then $\mathfrak{b}^n \subseteq \mathfrak{a}$.*

Proof. Choose any $b_1, b_2, \ldots, b_n \in \mathfrak{b}$. Then $b_i x_i \in \mathfrak{b}M \subseteq \mathfrak{a}M$ so there are $a_{ij} \in \mathfrak{a}$ such that

$$b_i x_i = \sum_j a_{ij} x_j. \qquad (*)$$

If $B = B(b_1, \ldots, b_n)$ is the $n \times n$ matrix over $\mathfrak{a}$ with ij entry $a_{ij} - b_i \delta_{ij}$ and X is the column vector $(x_1, \ldots, x_n)^T$ then by $(*)$ $BX = 0$. If $adj(B)$ denotes the classical

adjoint of B, *i.e.* the transposed matrix of cofactors, then $adj(B)\cdot B = (det\ B)\cdot I$, so $0 = adj(B)\cdot B\cdot X = (det\ B)\cdot X$. If we set $b = det\ B$ then $bx_i = 0$ for all i. Thus $b \in Ann(M) \subseteq \mathfrak{a}$. But expansion of $det\ B$ shows that $b_1 b_2 \ldots b_n \in \mathfrak{a}$ so $\mathfrak{b}^n \subseteq \mathfrak{a}$. $\triangle$

Corollary 2.2.12 *If $M \in {}_A\mathcal{M}$, M has n generators and $a \in A$, then*

$$(Ann(M/aM))^n \subseteq \langle a\rangle + Ann(M) \subseteq Ann(M/aM).$$

Proof. Take $\mathfrak{a} = \langle a\rangle + Ann(M) \supseteq Ann(M)$. Let $\mathfrak{b} = Ann(M/aM)$. If $c \in \mathfrak{b}$ then $cM \subseteq aM$ and so $\mathfrak{b}M \subseteq aM$. Clearly $aM \subseteq \mathfrak{a}M$ and so $\mathfrak{b}M \subseteq \mathfrak{a}M$. Therefore by the proposition $\mathfrak{b}^n \subseteq \mathfrak{a}$.

The second inclusion is obvious. $\triangle$

We define the *support* of a module M, denoted $Supp(M)$, to be $\{\mathfrak{p} \in Spec(A)$: $\mathfrak{p} \supseteq Ann(M)\}$. Note that $Assoc(M) \subseteq Supp(M)$.

Proposition 2.2.13 *Suppose $M \in {}_A\mathcal{M}$, $\mathfrak{p} \in Spec(A)$ and $a \in Homog(A^+)$. Then $\mathfrak{p} \in Supp(M/aM)$ if and only if $\mathfrak{p} \supseteq \langle a\rangle + Ann(M)$.*

Proof. Say $\{x_1, \ldots, x_n\} \subseteq M$ is a generating set for M. If $\mathfrak{p} \supseteq \langle a\rangle + Ann(M)$ then $(Ann(M/aM))^n \subseteq \mathfrak{p}$ by the Corollary above, and so $Ann(M/aM) \subseteq \mathfrak{p}$ since $\mathfrak{p}$ is prime. The converse is clear since $\langle a\rangle + Ann(M) \subseteq Ann(M/aM) \subseteq \mathfrak{p}$. $\triangle$

If $\mathfrak{a}$ is an ideal in a commutative ring A then $\mathfrak{p} \in Spec(A)$ is said to be *minimal over* $\mathfrak{a}$ if $\mathfrak{p} \supseteq \mathfrak{a}$ and $\mathfrak{p}$ is minimal in that respect, *i.e.* if $\mathfrak{q} \in Spec(A)$ and $\mathfrak{a} \subseteq \mathfrak{q} \subseteq \mathfrak{p}$ then $\mathfrak{q} = \mathfrak{p}$.

Proposition 2.2.14 *If $\mathfrak{a}$ is a proper ideal in a commutative ring A then there is some $\mathfrak{p} \in Spec(A)$ that is minimal over $\mathfrak{a}$.*

The proof of Proposition 2.2.14 is an easy application of Zorn's Lemma.

Proposition 2.2.15 *If $M \in {}_A\mathcal{M}$ and $\mathfrak{p} \in Spec(A)$ is minimal over $Ann(M)$, then $\mathfrak{p} \in Assoc(M)$.*

Proof.(McAdam, [21]) Let $\{x_1, \ldots, x_n\}$ be a set of generators for M. Then $Ann(M) = \cap_1^n Ann(x_i) \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime there is an x_i such that $\mathfrak{p} \supseteq Ann(x_i)$. Since A is Noetherian we may choose $x \in M$ so that $\mathfrak{c} = Ann(x)$ is maximal in the set of annihilators of elements within $\mathfrak{p}$. Suppose $ab \in \mathfrak{c}$ but $a \notin \mathfrak{c}$ and $b \notin \mathfrak{c}$. Then $\mathfrak{c} \subset \langle \mathfrak{c}, b \rangle \subseteq Ann(ax)$, so $Ann(ax) \not\subseteq \mathfrak{p}$ by the maximality of $\mathfrak{c}$. Choose $c \in Ann(ax) \setminus \mathfrak{p}$. Then $\mathfrak{c} \subset \langle \mathfrak{c}, a \rangle \subseteq Ann(cx)$, so $Ann(cx) \not\subseteq \mathfrak{p}$. Choose $d \in Ann(cx) \setminus \mathfrak{p}$. Then $cdx = 0$, so $cd \in Ann(x) \subseteq \mathfrak{p}$, a contradiction since $\mathfrak{p}$ is prime. Thus $\mathfrak{c} = Ann(x)$ is prime, and hence $Ann(x) = \mathfrak{p} \in Assoc(M)$. Δ

Proposition 2.2.16 *If $M \in {}_A\mathcal{M}$ and $\mathfrak{q} \in Supp(M)$ then there is some $\mathfrak{p} \in Assoc(M)$ with $\mathfrak{p} \subseteq \mathfrak{q}$.*

Proof. By Proposition 2.2.14 we may choose $\mathfrak{p} \subseteq \mathfrak{q}$ with $\mathfrak{p}$ minimal over $Ann(M)$ and apply Proposition 2.2.15. Δ

2.3 Regular Sequences

If $M \in {}_A\mathcal{M}$ and $a \in A$ is not a zero-divisor on M then we say that a is *regular* on M. A sequence $(a_1, a_2, \ldots, a_k)$ of elements in A, with each $a_i \in Homog(A^+)$, is called an *M–regular sequence* if a_i is regular on $M/\langle a_1, a_2, \ldots, a_{i-1} \rangle M$ for $1 \leq i \leq k$.

The definition of regular sequence often appears in the literature with the added condition that $\langle a_1, a_2, \ldots, a_k \rangle M \neq M$. In the present context that condition is equivalent with the requirement that all a_i be homogeneous of positive degree.

Proposition 2.3.1 *Suppose* $M \in {}_A\mathcal{M}$ *and* (a,b) *is an* M*-regular sequence. Then* $a \notin \mathcal{Z}(M/bM)$.

Proof. We prove the proposition by contradiction. Suppose $y + bM \neq 0$ in M/bM but $ay + bM = 0$ in M/bM, *i.e.* $y \notin bM$ but $ay \in bM$, say $ay = bx$ for some $x \in M$. Thus $bx + aM = 0$ in M/aM. But $b \notin \mathcal{Z}(M/aM)$ and thus $x \in aM$ *via* $x = az$ for some $z \in M$. Thus $ay = bx = baz$ and so $a(y - bz) = 0$. But $a \notin \mathcal{Z}(M)$, so $y = bz \in bM$, which is a contradiction. $\triangle$

Corollary 2.3.2 *If* (a,b) *is* M*-regular then* (b,a) *is* M*-regular if and only if* $b \notin \mathcal{Z}(M)$.

Proposition 2.3.3 *If* $M \in {}_A\mathcal{M}$ *and* (a,b) *is* M*-regular, then* (b,a) *is* M*-regular.*

Proof. Let $N = \{y \in M : by = 0\}$, the kernel of the map $x \mapsto bx$ from M to M. Then N is a graded submodule. If $y \in N$ then $by + aM = 0$ in M/aM. But $b \notin \mathcal{Z}(M/aM)$, so $y \in aM$, say $y = az$, for some $z \in M$. Thus $0 = by = abz$ and $bz = 0$ since $a \notin \mathcal{Z}(M)$. Therefore $z \in N$ also, and since $y \in N$ was arbitrary, we have $aN = N$. Therefore $N = 0$ by Proposition 2.2.10, so $b \notin \mathcal{Z}(M)$. Thus (b,a) is M-regular by Corollary 2.3.2. $\triangle$

Proposition 2.3.4 *If* $\mathfrak{a}, \mathfrak{b}$ *are ideals in* A *and* $M \in {}_A\mathcal{M}$ *then* $(M/\mathfrak{a}M)\big/\mathfrak{b}(M/\mathfrak{a}M)$ *is* A*-isomorphic with* $M/(\mathfrak{a}+\mathfrak{b})M$.

Proof. Note first that $\mathfrak{b}(M/\mathfrak{a}M) = (\mathfrak{b}M + \mathfrak{a}M)/(\mathfrak{a}M) = (\mathfrak{a}+\mathfrak{b})M/\mathfrak{a}M$. Therefore

$$\frac{M/\mathfrak{a}M}{\mathfrak{b}(M/\mathfrak{a}M)} = \frac{M/\mathfrak{a}M}{(\mathfrak{a}+\mathfrak{b})M/\mathfrak{a}M} \cong \frac{M}{(\mathfrak{a}+\mathfrak{b})M}$$

by a standard isomorphism theorem. $\triangle$

Proposition 2.3.5 *Suppose* $M \in {}_A\mathcal{M}$ *and* $a_1, \ldots, a_k \in Homog(A^+)$. *Then* $(a_1, \ldots, a_k)$ *is* M*-regular if and only if* $(a_1, \ldots, a_i)$ *is* M*-regular and* $(a_{i+1}, \ldots, a_k)$ *is* $(M/\langle a_1, \ldots, a_i\rangle M)$*-regular for* $1 \leq i \leq k$.

Proof. If $1 \leq j \leq i$ it is immediate from the definition that a_{j+1} is regular on $M/\langle a_1, \ldots, a_j\rangle M$. If $i+1 \leq j < k$ set $\mathfrak{a} = \langle a_1, \ldots, a_i\rangle$ and $\mathfrak{b} = \langle a_{i+1}, \ldots, a_j\rangle$, and apply Proposition 2.3.4 to see that a_{j+1} is regular on $M/(\mathfrak{a}+\mathfrak{b})M$ if and only if it is regular on $(M/\mathfrak{a}M)\big/\mathfrak{b}(M/\mathfrak{a}M)$. △

Corollary 2.3.6 *If* $M \in {}_A\mathcal{M}$, $(a_1, \ldots, a_k)$ *is* M*-regular, and* $1 \leq i < k$, *then* $(a_1, \ldots, a_{i+1}, a_i, \ldots, a_k)$, *with* a_i *and* a_{i+1} *interchanged, is also* M*-regular.*

Proof. First we apply Proposition 2.3.5 twice to see that $(a_1, \ldots, a_{i-1})$ is an M–regular sequence, (a_i, a_{i+1}) is an $(M/\langle a_1, \ldots, a_{i-1}\rangle M)$–regular sequence and $(a_{i+2}, \ldots, a_k)$ is an $(M/\langle a_1, \ldots, a_{i+1}\rangle M)$–regular sequence. Next apply Proposition 2.3.3 to see that (a_{i+1}, a_i) is also $(M/\langle a_1, \ldots, a_{i-1}\rangle M)$–regular. Finally apply Proposition 2.3.5 (the converse) twice to see that $(a_1, \ldots, a_{i+1}, a_i, \ldots, a_k)$ is M–regular. △

Theorem 2.3.7 *If* $M \in {}_A\mathcal{M}$ *and* $(a_1, a_2, \ldots, a_n)$ *is* M*-regular, then any permutation of* $(a_1, a_2, \ldots, a_n)$ *is also* M*-regular.*

Proof. (See [16]) Apply the corollary above; any permutation is a product of adjacent transpositions. △

Proposition 2.3.8 *If* A *is a graded* K*-algebra and* $(a_1, \ldots, a_m)$ *is an* A*-regular sequence then* $\{a_1, \ldots, a_m\}$ *is algebraically independent.*

Proof.(See [10]) Define a map ϕ from a polynomial algebra $K[y_1, \ldots, y_m]$ to A *via* $\phi: y_i \mapsto a_i$, $1 \leq i \leq m$. It will suffice to prove by induction on m that ϕ is one-to-one.

If $m = 1$ write $a = a_1$ and $y = y_1$, and suppose that $f \in ker\,\phi$. We may assume that f is of minimal degree in $ker\,\phi$, and write $f(y) = c_0 + c_1 y + \cdots + c_k y^k$, so $0 = f(a) = c_0 + c_1 a + \cdots + c_k a^k$. Thus $c_i a^i = 0$, for all i. Therefore $f = 0$.

Suppose that $m > 1$, and assume the result for regular sequences of length $m-1$ or less. Set $A' = A/\langle a_1 \rangle$. Then $(a_2, \ldots, a_m)$ is A'–regular by Proposition 2.3.5, or equivalently $(\overline{a}_2, \ldots, \overline{a}_m)$ is A'–regular (in A'). By induction the map $\overline{\phi} : y_i \to \overline{a}_i$, $2 \leq i \leq m$, is one-to-one from $B = K[y_2, \ldots, y_m]$ to A'. Suppose though that $0 \neq F \in ker\ \phi$. We may view F as being in $B[y_1]$, and write $F = \sum_{j \geq 0} g_j y_1^j$, each $g_j \in B$, and we have $0 = \sum_j a_1^j g_j(a_2, \ldots, a_m)$. Let s be minimal so that $g_s \neq 0$ in B. Then $0 = a_1^s \sum_{j \geq s} a_1^{j-s} g_j(a_2, \ldots, a_m)$, and hence $\sum_{j \geq s} a_1^{j-s} g_j(a_2, \ldots, a_m) = 0$, either because $s = 0$ or else because a_1 is regular on A. But then modulo $\langle a_1 \rangle$ we have $g_s(\overline{a}_2, \ldots, \overline{a}_m) = 0$, and $g_s \in ker(\overline{\phi})$, a contradiction. $\triangle$

The following useful proposition was suggested by David Surowski.

Proposition 2.3.9 *Suppose C is a graded subalgebra of a graded algebra A and $a \in Homog(A^+)$. If $M \in {}_A\mathcal{M}$, a is regular on M, and M/aM is a free C-module then M is a free $C[a]$-module.*

Proof. By Proposition IV.2.10 of [8] we may write $M = aMv \oplus N'$ with N' a free C–module. Note that aM is a homogeneous submodule, so by Proposition 2.1.7 there is a homogeneous C–submodule N with $M = aM \oplus N$. We will show inductively that $M = \oplus_{i=0}^{\infty} a^i N$. First note that $M_0 \subseteq N$ since $deg\, a > 0$. Assume inductively that $M_j \subseteq \sum_{i=0}^{\infty} a^i N$ if $j < k$ and consider M_k. Take $x \in M_k$ and write

$x = ax' + y \in aM \oplus N$ with $deg\, ax' = deg\, y = deg\, x = k$. Note that $deg\, x' < k$ (since $deg\, a > 0$) so $x' \in \sum_i a^i N$ and therefore $x = ax' + y \in \sum_{i=0}^{\infty} a^i N$. Thus $M_k \subseteq \sum_{i=0}^{\infty} a^i N$, hence $M = \sum_{i=0}^{\infty} a^i N$.

To see that the sum is direct suppose that $\sum_{i=0}^{\infty} a^i y_i = 0$ (with finitely many nonzero summands). Then $y_0 = -\sum_{i=1}^{\infty} a^i y_i \in aM \cap N = 0$ and $y_0 = 0$. Thus $a(\sum_{i=0}^{\infty} a^{i-1} y_i) = 0$ and therefore $\sum_{i=0}^{\infty} a^{i-1} y_i = 0$ since a is regular on M, hence $y_1 = 0$. Repeat the argument to see that all $y_i = 0$. Thus $M = \oplus_0^{\infty} a^i N$.

Since N is a free C–module ($N \cong M/aM$), we can choose a C–basis $\{y_\delta : \delta \in D\}$ for N (not necessarily finite). Therefore $M = \oplus_{i=0}^{\infty} a^i N = \oplus_i a^i (\oplus \{Cy_\delta : \delta \in D\}) = \oplus_\delta (\oplus_i Ca^i) y_\delta = \oplus_\delta C[a] y_\delta$. Thus $\{y_\delta\}$ is a $C[a]$–basis for M and M is a free $C[a]$–module. △

Theorem 2.3.10 *Suppose that $M \in {}_A\mathcal{M}$, $(a_1, \ldots, a_m)$ is M–regular, and $B = K[a_1, \ldots, a_m]$. Then M is a free B–module.*

Proof. We apply induction on m. The result is trivial if $m = 0$; for $m = 1$ apply Proposition 2.3.9 with $a = a_1$ and $C = K$. Take $m > 1$ and assume the result for regular sequences of length $m - 1$. Set $M' = M/a_1 M$. By Proposition 2.3.5 the sequence $(a_2, \ldots, a_m)$ is M'–regular, so by induction M' is a free $K[a_2, \ldots, a_m]$–module. Apply Proposition 2.3.9 again, with $a = a_1$ and $C = K[a_2, \ldots, a_m]$, conclude that M is a free $C[a_1]$–module, and observe that $C[a_1] = K[a_1, \ldots, a_m] = B$. △

An M–regular sequence $(a_1, \ldots, a_n)$ is *maximal* if it cannot be extended to a longer M–regular sequence, *i.e.* if every $a \in Homog(A^+)$ acts as a zero divisor on $M/\sum_1^n a_i M$. Lengths of maximal M–regular sequences will play a role in applications to invariant theory, and the next theorem will be useful.

Theorem 2.3.11 (Northcott and Rees) *Suppose* $0 \neq M \in {}_A\mathcal{M}$. *Then any two maximal* M*–regular sequences have the same length.*

Proof.(See [19]) Choose a maximal M–regular sequence $(a_1, \ldots, a_n)$ that is as short as possible; we show by induction that every maximal M–regular sequence has length n. If $n = 0$ then $A^+ = \mathcal{Z}(M)$ and every M–regular sequence is empty. Thus suppose $n > 0$. It will suffice to show that if $(b_1, \ldots, b_n)$ is M–regular then $\mathcal{Z}(M/\sum_1^n b_i M) \supseteq Homog(A^+)$ so that $(b_1, \ldots, b_n)$ can't be extended to a longer M–regular sequence.

If $n = 1$ then $Homog(A^+) \subseteq \mathcal{Z}(M/a_1M)$, so $A^+ \in Assoc(M/a_1M)$ by Propositions 2.1.4 and 2.2.1. Thus $A^+ = Ann(\overline{x})$,where $\overline{x} = x + a_1M$ for some $x \in M$. Therefore $A^+x \subseteq a_1M$ and in particular $b_1x = a_1x'$ for some $x' \in M$. Note that $x' \notin b_1M$, for if $x' = b_1y$, $y \in M$ then $b_1x = a_1x' = a_1b_1y$ and $x = a_1y$ since $b_1 \notin \mathcal{Z}(M)$. But then $\overline{x} = 0$ which is a contradiction since $Ann(\overline{x}) = A^+$. Now $a_1A^+x' = A^+a_1x' = A^+b_1x \subseteq a_1b_1M$ since $A^+x \subseteq a_1M$ and so $A^+x' \subseteq b_1M$ (since $a_1 \notin \mathcal{Z}(M)$). Thus $A^+ = Ann(\overline{x}')$, where $\overline{x}' = x' + b_1M \in M/b_1M$. Therefore $A^+ \in Assoc(M/b_1M)$, $\mathcal{Z}(M/b_1M) = A^+$ and b_1 is a maximal M–regular sequence.

Now take $n > 1$ and assume the result for modules with shorter maximal M–regular sequences. Write $K^{(i)} = M/\sum_{j=1}^i a_jM$, $L^{(i)} = M/\sum_{j=1}^i b_jM$, $0 \leq i \leq n-1$. Choose $c \in Homog(A^+)$ such that $c \notin \cup_0^{n-1}\mathcal{Z}(K^{(i)})$ and $c \notin \cup_0^{n-1}\mathcal{Z}(L^{(i)})$ (this is possible by Proposition 2.1.4 since each $\mathcal{Z}(K^{(i)})$ and each $\mathcal{Z}(L^{(i)})$ is a finite union of prime ideals, none of them being A^+). Thus both $(a_1, \ldots, a_{n-1}, c)$ and $(b_1, \ldots, b_{n-1}, c)$ are M–regular. Apply Theorem 2.3.7 to see that $(c, a_1, \ldots, a_{n-1})$ and $(c, b_1, \ldots, b_{n-1})$ are M–regular.

Now observe that $(a_1, \ldots, a_{n-1}, c)$ is maximal M–regular since both (a_n) and (c) are maximal $K^{(n-1)}$–regular (by the case $n = 1$ above). Thus $(c, a_1, \ldots, a_{n-1})$ is also

maximal M–regular (note: any rearrangement of a maximal M–regular sequence is also maximal). Now $(a_1, \ldots, a_{n-1})$ and $(b_1, \ldots, b_{n-1})$ are both M/cM–regular and $(a_1, \ldots, a_{n-1})$ is maximal so by induction $(b_1, \ldots, b_{n-1})$ is maximal M/cM–regular. Therefore $(c, b_1, \ldots, b_{n-1})$ is maximal M–regular and so is $(b_1, \ldots, b_{n-1}, c)$. But now compare $(b_1, \ldots, b_{n-1}, c)$ with $(b_1, \ldots, b_n)$ as was done for $(a_1, \ldots, a_n)$ and $(a_1, \ldots, a_{n-1}, c)$ (again use the case $n = 1$), and conclude finally that $(b_1, , \ldots, b_n)$ is maximal. Δ

2.4 Dimension Theory

In this section we consider three seemingly rather different notions of dimension for graded modules and show that they coincide.

When we speak of a *chain* $\mathfrak{p}_0 \subset \mathfrak{p}_1 \cdots \subset \mathfrak{p}_n$ of prime ideals of a ring in this section we mean explicitly that all the inclusions are proper. We say that the chain has *length* n (thus the length is the number of proper inclusions). The chain can be viewed either as *ascending* from $\mathfrak{p}_0$ to $\mathfrak{p}_n$, or *descending* from $\mathfrak{p}_n$ to $\mathfrak{p}_0$.

If A is a commutative ring then A has *finite Krull dimension* n if there is a chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \cdots \subset \mathfrak{p}_n$ of prime ideals of length n in A, but there is no chain of length $n + 1$. In that case we write $dim(A) = n$. If there are chains of length n for every $n \in \mathbb{N}$ we say that A has *infinite* Krull dimension, and write $dim(A) = \infty$.

Although examples exist of Noetherian rings having infinite Krull dimension, we shall see later that $dim(A)$ is finite for every graded K–algebra.

For some examples, note first that if $A = K$, a field, then $dim(A) = 0$ since $\mathfrak{p} = 0$ is the only prime ideal in A. If A is an integral domain then 0 is a prime ideal, so it is clear that A can have Krull dimension 0 only if there are no other prime ideals, so in that case $dim(A) = 0$ if and only if A is a field. There are,

however, rings of Krull dimension 0 that are not fields. The smallest example is $A = \mathbb{Z}_2 \oplus \mathbb{Z}_2$; any (ring) direct sum of two or more fields provides a similar example.

For an easy but nontrivial example of a graded K–algebra of Krull dimension 0 set $A = K[x]/\langle x^2 \rangle$ and note that $Spec(A) = \{A^+\} = \{A_1\}$.

If A is an integral domain in which every non-zero prime ideal is maximal (but A is not a field) then clearly $dim(A) = 1$. For example, $dim(\mathbb{Z}) = 1$, and among graded K–algebras, $dim(K[x]) = 1$. For the same reason, if A is any PID, or more generally, a Dedekind domain, then $dim(A) = 1$.

If $A = \mathcal{P} = K[x_1, \ldots, x_n]$, set $\mathfrak{p}_0 = 0$ and $\mathfrak{p}_i = \langle x_1, \ldots, x_i \rangle$ for $1 \leq i \leq n$ (thus $\mathfrak{p}_n = A^+$). Then $A/\mathfrak{p}_i \cong K[x_{i+1}, \ldots, x_n]$, an integral domain, so each $\mathfrak{p}_i$ is prime. Thus since $\mathfrak{p}_0 \subset \mathfrak{p}_1 \cdots \subset \mathfrak{p}_n$ it follows that $dim(A) \geq n$. We shall show later in this section that in fact $dim(A) = n$.

In order to extend the notion of dimension to A–modules we extend it first to ideals in A.

If $\mathfrak{a}$ is an ideal in A, define $dim(\mathfrak{a})$ to be the Krull dimension of the quotient ring $A/\mathfrak{a}$. Since prime ideals in $A/\mathfrak{a}$ are all of the form $\mathfrak{p}/\mathfrak{a}$ where $\mathfrak{p}$ is a prime ideal in A and $\mathfrak{p} \supseteq \mathfrak{a}$ we see that $dim(\mathfrak{a})$, if finite, is the maximal length of chains $\mathfrak{p}_0 \subset \mathfrak{p}_1 \cdots \subset \mathfrak{p}_n$ in A for which $\mathfrak{a} \subseteq \mathfrak{p}_0$. If $\mathfrak{a}$ happens to be prime then any such chain of maximal length must of course begin with $\mathfrak{p}_0 = \mathfrak{a}$. Thus if $\mathfrak{p}$ is prime in A then $dim(\mathfrak{p})$ (again if finite) is the maximal length of chains $\mathfrak{p} = \mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ ascending from $\mathfrak{p}$.

Suppose now for the rest of the section that A is a graded K–algebra.

If $0 \neq M \in {}_A\mathcal{M}$ define the *dimension* of M, denoted by $dim(M)$, to be $dim(Ann(M))$, *i.e.* the Krull dimension of $A/Ann(M)$. If the Krull dimension of A is n, finite, then clearly $dim(M) \leq n$.

Proposition 2.4.1 *If $M, N \in {}_A\mathcal{M}$ and N is a homomorphic image of M then $dim(N) \leq dim(M)$.*

Proof. Since N is a homomorphic image of M then $Ann(M) \subseteq Ann(N)$ and thus $dim(N) \leq dim(M)$. △

Proposition 2.4.2 *If $0 \neq M \in {}_A\mathcal{M}$ and $dim(M)$ is finite then*

$$dim(M) = max\ \{dim(\mathfrak{p}) : \mathfrak{p} \in Assoc(M)\}.$$

Proof. Say $dim(M) = n$ and suppose $\mathfrak{p}_0 \subset \mathfrak{p}_1 \cdots \subset \mathfrak{p}_n$ is a maximal ascending chain with $Ann(M) \subset \mathfrak{p}_0$. Then $\mathfrak{p}_0 \in Supp(M)$ and consequently $\mathfrak{p}_0 \in Assoc(M)$ by Proposition 2.2.16 and the maximality of the chain. △

Corollary 2.4.3 *If $M \in {}_A\mathcal{M}$ and N is a graded submodule then $dim(N) \leq dim(M)$.*

Proof. Apply the proposition and Proposition 2.2.6. △

We have looked at the first notion of dimension for a graded module and some properties of $dim(M)$. We now wish to set the stage in order to define the next idea of dimension of a graded module.

If $M \in {}_A\mathcal{M}$ then, by Proposition 2.1.6, $dim_K(M_i)$ is finite for all $i \in \mathbb{N}$. Thus we can define the *Hilbert function* $H_M : \mathbb{N} \to \mathbb{N}$ *via* $H_M(i) = dim_K(M_i)$. Then the *Poincaré series* of M is defined to be the formal power series

$$\Phi_M(t) = \sum_{i=0}^{\infty} H_M(i) t^i.$$

For example, if $M = A = \mathcal{I}$, the algebra of invariants for some finite group G, then $\Phi_M(t)$ is the Molien series.

The following proposition develops a relationship between homogeneous maps, Hilbert functions and Poincaré series.

Proposition 2.4.4 *Suppose that* $0 \to L \xrightarrow{\varphi} M \xrightarrow{\theta} N \to 0$ *is an exact sequence in* ${}_A\mathcal{M}$, *and that* φ *and* θ *are homogeneous of degrees* l *and* m, *respectively. Then*

$$H_L(i) - H_M(i+l) + H_N(i+l+m) = 0 \qquad (*)$$

for all $i \in \mathbb{N}$, *and consequently*

$$t^{l+m}\ \Phi_L(t) - t^m \Phi_M(t) + \Phi_N(t) = 0.$$

Proof. Since φ and θ are homogeneous they restrict to K–linear maps on homogeneous parts and give us exact sequences

$$0 \to L_i \to M_{i+l} \to N_{i+l+m} \to 0.$$

The result $(*)$ now follows from elementary linear algebra. If we multiply $(*)$ by t^{i+l+m} and sum from $i = -(l+m)$ to ∞ we obtain the final result about Poincaré series. Δ

The proposition extends easily to longer exact sequences. For example, if $0 \to L \xrightarrow{\varphi} M \xrightarrow{\theta} N \xrightarrow{\psi} P \to 0$ is exact in ${}_A\mathcal{M}$ and φ, θ, and ψ are homogeneous of degrees l, m, and n, respectively, then

$$H_L(i) - H_M(i+l) + H_N(i+l+m) - H_P(i+l+m+n) = 0$$

for all $i \in \mathbb{N}$, and consequently

$$t^{l+m+n}\ \Phi_L(t) - t^{m+n}\Phi_M(t) + t^n \Phi_N(t) - \Phi_P(t) = 0.$$

The following theorem gives a closed form representation of the Poincaré series as a rational function.

Theorem 2.4.5 (Hilbert-Serre) *Suppose* $A = K[a_1, \ldots, a_m]$, *where each* $a_i \in Homog(A^+)$ *with* $\deg a_i = d_i$, *and* $M \in {}_A\mathcal{M}$. *Then there exists* $f(t) \in \mathbb{Z}[t]$ *such that*

$$\Phi_M(t) = \frac{f(t)}{\prod\{1 - t^{d_i} : 1 \leq i \leq m\}}.$$

Proof. We prove the theorem by induction on m.

If $m = 0$ then $A = K$ so then M is a finitely generated (and therefore finite dimensional) K–vector space. In that case, $\Phi_M(t) \in \mathbb{Z}[t]$.

Assume then that $m > 0$, and assume that the result is true for $m-1$ generators. Set $a = a_m$, and define $\phi: M \to M$ *via* $\phi(x) = ax$ for all $x \in M$. Thus ϕ is homogeneous of degree d_m. Set $N = ker\ \phi$ and $L = Im\ \phi$ which, by Proposition 2.2.2, are graded submodules of M. The sequence $0 \to N \to M \xrightarrow{\phi} M \to M/L \to 0$ is exact, so by Proposition 2.4.4

$$t^{d_m}\Phi_N(t) - t^{d_m}\Phi_M(t) + \Phi_M(t) - \Phi_{M/L}(t) = 0.$$

Thus

$$\Phi_M(t) = \frac{\Phi_{M/L}(t) - t^{d_m}\Phi_N(t)}{1 - t^{d_m}}.$$

Observe that $a \in Ann(N)$ and $a \in Ann(M/L)$ so N and M/L are $A/\langle a\rangle$-modules, and that $A/\langle a\rangle$ has $m-1$ generators $\overline{a}_1, \ldots, \overline{a}_{m-1}$. Thus by induction each of $\Phi_N(t)$ and $\Phi_{M/L}(t)$ is a polynomial in $\mathbb{Z}[t]$ divided by $\prod\{1 - t^{d_i} : 1 \leq i \leq m-1\}$, and the result follows. $\triangle$

For any $M \in {}_A\mathcal{M}$ define $d(M)$ to be the minimal $m \in \mathbb{N}$ for which it is possible to write $\Phi_M(t)$ as in Theorem 2.4.5. This is our second notion of dimension for a graded module – it is sometimes called the *Hilbert dimension.*

The following proposition will be useful in relating $d(M)$ to the other notions of dimension.

Proposition 2.4.6 *Suppose* $0 \neq M \in {}_A\mathcal{M}$ *and* $a \in Homog(A^+) \setminus \mathcal{Z}(M)$. *Then for some power* a^k *we have* $d(M/a^kM) \leq d(M) - 1$.

Proof. For any power a^k we can apply Proposition 2.4.4 and thus obtain $\Phi_{M/a^kM}(t)$ $= (1 - t^{dk})\Phi_M(t)$ where $d = deg(a)$. Write

$$\Phi_M(t) = \frac{f(t)}{\prod_1^m (1 - t^{d_i})}$$

minimally as in Theorem 2.4.5, so $m = d(M)$. Then choose k so that the smallest d_i divides dk. Therefore $(1-t^{d_i})$ divides $(1-t^{dk})$ algebraically and $(1-t^{dk})/(1-t^{d_i}) = g(t) \in \mathbb{Z}[t]$. Thus

$$\Phi_{M/a^kM}(t) = \frac{g(t)f(t)}{\prod_{j \neq i}(1 - t^{d_j})},$$

and $d(M/a^kM) \leq m - 1$. △

We are now ready to define the third notion of dimension for a graded module.

By Proposition 2.1.2, if $a_1, \ldots, a_m$ is a set of homogeneous generators for A^+ then $A = K[a_1, \ldots, a_m]$. Thus by the definition of ${}_A\mathcal{M}$ any $M \in {}_A\mathcal{M}$ is a finitely generated $K[a_1, \ldots, a_m]$–module.

If $M \in {}_A\mathcal{M}$ define $s(M)$ to be the *minimal* $k \in \mathbb{N}$ such that there are $a_1, \ldots, a_k \in Homog(A^+)$ with M a finitely generated $K[a_1, \ldots, a_k]$–module. For example, $s(M) = 0$ if and only if $dim_K M$ is finite.

Proposition 2.4.7 *If* $M \in {}_A\mathcal{M}$ *and* N *is a graded submodule then* $s(N) \leq s(M)$.

Proof. Say that $s(M) = m$ and choose $a_1, \ldots, a_m \in Homog(A^+)$ so that M is a finitely generated B–module, $B = K[a_1, \ldots, a_m]$. Since B is Noetherian M is a Noetherian B–module, and hence the B–submodule N is finitely generated, *i.e.* $s(N) \leq m$. △

The following two propositions will help us relate $d(M)$ to $s(M)$.

Proposition 2.4.8 *If $M \in {}_A\mathcal{M}$, $a_1, \ldots, a_n \in Homog(A^+)$ and M/a_nM is finitely generated over $K[a_1, \ldots, a_{n-1}]$, then M is finitely generated over $K[a_1, \ldots, a_n]$.*

Proof. Choose $u_1, \ldots, u_r \in Homog(M)$ such that $\overline{u}_1, \ldots, \overline{u}_r$ generate M/a_nM over $K[a_1, \ldots, a_{n-1}]$. Let N be the $K[a_1, \ldots, a_n]$-submodule of M generated by $u_1, \ldots, u_r$. If $N = M$ we are finished. If not, choose $u \in Homog(M \setminus N)$ of minimal degree. Write $\overline{u} = \sum_1^r z_i \overline{u}_i$ where $z_i \in Homog(K[a_1, \ldots, a_{n-1}])$. Thus $u - \sum_1^r z_i u_i \in a_nM$, say $u = \sum_1^r z_i u_i + a_n v$, with $v \in Homog(M)$. We may assume that $deg\, z_i u_i = deg\, z_i + deg\, u_i = deg\, u$, for $1 \leq i \leq r$. Hence $deg\, a_n + deg\, v = deg\, u$. Thus $deg\, v < deg\, u$ since $a_n \in A^+$. Since u was chosen to have minimal degree in $Homog(M \setminus N)$ then $v \in N$. But then also $u = \sum z_i u_i + a_n v \in N$, which is a contradiction. Δ

Theorem 2.4.9 *Suppose $M \in {}_A\mathcal{M}$ with $d(M) = m$. Then there are $a_1, a_2, \ldots, a_m \in Homog(A^+)$ such that M is a finitely generated module over $K[a_1, \ldots, a_m]$. Therefore $s(M) \leq d(M)$.*

Proof. We prove the theorem by induction on m. If $m = 0$ then $\Phi_M(t) \in \mathbb{Z}[t]$ so M has finite K-dimension and we are finished. Take $m > 0$ and assume the result for any $N \in {}_A\mathcal{M}$ such that $d(N) \leq m - 1$. Apply Proposition 2.2.9 to obtain $a \in Homog(A^+) \setminus \mathcal{Z}(M^{[k]})$ for some $k \geq 0$. By Proposition 2.4.6 we may assume that $d(M^{[k]}/aM^{[k]}) \leq d(M^{[k]}) - 1$. Since $\Phi_{M^{[k]}}(t)$ and $\Phi_M(t)$ differ by a polynomial and likewise for $\Phi_{M^{[k]}/aM^{[k]}}(t)$ and $\Phi_{M/aM}(t)$ it follows that $d(M^{[k]}) = d(M)$ and $d(M^{[k]}/aM^{[k]}) = d(M/aM)$. By induction there exist $a_1, \ldots, a_{m-1} \in Homog(A^+)$ such that M/aM is a finitely generated $K[a_1, \ldots, a_{m-1}]$-module. Now apply Proposition 2.4.8 with $a_m = a$ and conclude that M is a finitely generated $K[a_1, \ldots, a_m]$-module. Δ

We have looked at three different notions of dimension for a graded module M, namely $dim(M)$, $d(M)$, and $s(M)$. We will now show, as mentioned at the outset of this section, that the three notions coincide.

Theorem 2.4.10 (The Dimension Theorem) *If* $0 \neq M \in {}_A\mathcal{M}$ *then* $d(M) = s(M) = dim(M)$.

Proof.(See [27]) By Theorem 2.4.9 $s(M) \leq d(M)$. If $s(M) = m$, then there exist $a_1, \ldots, a_m \in Homog(A^+)$ so that if we set $B = K[a_1, \ldots, a_m]$ then $M \in {}_B\mathcal{M}$. Now apply Theorem 2.4.5 with A replaced by B to see that $d(M) \leq m = s(M)$. Thus $s(M) = d(M)$.

Consider an increasing chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ of prime ideals of A, with $Ann(M) \subseteq \mathfrak{p}_0$. We will show that $n \leq d(M)$ by induction on $d(M)$. If $d(M) = 0$ then $dim_K(M)$ is finite and so $Ann(M)$ contains all homogeneous elements of sufficiently high degree. Thus there is a k such that $(A^+)^k \subseteq Ann(M) \subseteq \mathfrak{p}_0$, and $A^+ \subseteq \mathfrak{p}_0$ since $\mathfrak{p}_0$ is prime. Therefore $A^+ = \mathfrak{p}_0$, since A^+ is maximal, so $n = 0$ and we have that $dim(M) = 0 = d(M)$. Assume then that $d(M) > 0$. Since the prime ideal $\mathfrak{p}_0$ contains $Ann(M)$, it must contain an element of $Assoc(M)$ by Proposition 2.2.16. We may as well assume that $\mathfrak{p}_0 \in Assoc(M)$, say *via* $\mathfrak{p}_0 = Ann(x)$, with $x \in Homog(M)$. The submodule $N = Ax$ of M is isomorphic with $A/\mathfrak{p}_0$ and by Proposition 2.2.5 $Assoc(N) = \{\mathfrak{p}_0\}$. If $n = 0$ there is nothing to prove. Thus we assume $n \geq 1$ and choose $b \in Homog(\mathfrak{p}_1 \setminus \mathfrak{p}_0)$. By Proposition 2.2.1 $b \notin \mathcal{Z}(N)$, so by Proposition 2.4.6 we may assume that $d(N/bN) < d(N)$. Note that $N/bN = Ax/bAx$ so $Ann(N/bN) = \{a \in A : aAx \subseteq bAx\}$. Thus if $a \in Ann(N/bN)$ then $ax = ba'x$ for some $a' \in A$. Therefore $(a - ba')x = 0$ and since $x \neq 0$ then $a - ba' \in Ann(x) = \mathfrak{p}_0$. Thus we have $a \in ba' + \mathfrak{p}_0 \subseteq Ab + \mathfrak{p}_0$ and $Ann(N/bN) \subseteq Ab + \mathfrak{p}_0$. Conversely, $(Ab + \mathfrak{p}_0)Ax \subseteq bAx$, since $\mathfrak{p}_0 = Ann(x)$, so

$Ab + \mathfrak{p}_0 \subseteq Ann(N/bN)$. Therefore $Ann(N/bN) = Ab + \mathfrak{p}_0$. Note in particular that $Ann(N/bN) \subseteq \mathfrak{p}_1$, so we have the chain

$$Ann(N/bN) \subseteq \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$$

and since $d(N/bN) < d(N)$ we have $d(N/bN) < d(N) = s(N) \leq s(M) = d(M)$. Thus by induction we have $n - 1 \leq d(N/bN)$. Therefore $n \leq d(N) \leq d(M)$. Since the original increasing chain was arbitrary the above is also true for a maximal increasing chain and thus we have $dim(M) \leq d(M)$.

Finally let us show that $s(M) \leq dim(M)$ by induction on $dim(M)$. If $dim(M) = 0$ then since A^+ is a prime ideal containing $Ann(M)$ and A^+ does contain an element of $Assoc(M)$ we have $Assoc(M) = \{A^+\}$. Thus the only prime ideal of the form $Ann(x)$ for $0 \neq x \in M$ is A^+ and consequently $Assoc(M^{[k]}) = \{A^+\}$ for any nonzero $M^{[k]}$. Thus if $M^{[k]} \neq 0$ then $\mathcal{Z}(M^{[k]}) = A^+$ by Proposition 2.2.1. Apply Proposition 2.2.9 to conclude that there is a k such that $M^{[k]} = 0$ and so $dim_K(M)$ is finite, thus $d(M) = s(M) = 0 = dim(M)$. Next take M with $dim(M) > 0$ and assume the inequality for $N \in {}_A\mathcal{M}$ with $dim(N) < dim(M)$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the minimal elements in $Assoc(M)$, so clearly no $\mathfrak{p}_i$ is equal to A^+ since $dim(M) > 0$. By Proposition 2.1.4 there exists $b \in Homog(A^+)$ but $b \notin \cup_1^r \mathfrak{p}_i$. Since $b \in Ann(M/bM)$ we have $Ann(M/bM) \not\subseteq \mathfrak{p}_i, 1 \leq i \leq r$. However, it is clear that $Ann(M) \subseteq Ann(M/bM)$ and it follows that $dim(M/bM) < dim(M)$, so by induction $s(M/bM) \leq dim(M/bM)$. Now apply Proposition 2.4.8 to obtain $s(M) \leq s(M/bM) + 1 \leq dim(M/bM) + 1 \leq dim(M)$. Δ

Corollary 2.4.11 *The full polynomial algebra $\mathcal{P}$ has dimension n.*

Proof. Since $\mathcal{P}$ is finitely generated over $K[x_1, \ldots, x_n] = \mathcal{P}$ we have $s(\mathcal{P}) \leq n$. It was observed on page 37 that $dim(\mathcal{P}) \geq n$. Δ

Proposition 2.4.12 *If* $M \in {}_A\mathcal{M}$ *and* $0 \neq b \in Homog(A^+)$ *then* $dim(M) \geq dim(M/bM) \geq dim(M) - 1$.

Proof. Clearly $dim(M) \geq dim(M/bM)$. Say that $dim(M) = m$. If $dim(M/bM) \leq m-2$ then there exists $a_1, \ldots, a_{m-2} \in A$ such that M/bM is finitely generated as a $K[a_1, \ldots, a_{m-2}]$-module. But then M is finitely generated as a module over $K[a_1, \ldots a_{m-2}, b]$ by Proposition 2.4.8, so $dim(M) = s(M) \leq m-1$, which is a contradiction. Δ

Corollary 2.4.13 *If* $M \in {}_A\mathcal{M}$ *and* $a \in Homog(A^+) \setminus \mathcal{Z}(M)$, *then* $dim(M/aM) = dim(M) - 1$.

Proof. By Proposition 2.4.6 there is some $k \in \mathbb{N}$ such that $dim(M/a^kM) \leq dim(M) - 1$. But M/aM is a homomorphic image of M/a^kM, so $dim(M/aM) \leq dim(M/a^kM)$. Thus $dim(M) - 1 \leq dim(M/aM) \leq dim(M/a^kM) \leq dim(M) - 1$, and all are equal. Δ

2.5 Integral Extensions

Recall that if R is a subring of S then $a \in S$ is *integral* over R if there is a nonzero monic polynomial $f(t) \in R[t]$ with $f(a) = 0$. If every $a \in S$ is integral over R then S is called an *integral extension* of R.

Proposition 2.5.1 *If* A *is a graded* K*-algebra and* B *is a graded subalgebra, then* A *is integral over* B *if and only if* A *is a finitely generated* B*-module.*

Proof. ($\Rightarrow$) Choose $a_1, \ldots, a_n \in A$ so that $A = K[a_1, \ldots, a_n]$. Each a_i is integral over B, so for some $k_i > 0$ in $\mathbb{N}$ we may write $a_i^{k_i} = \sum_{j=0}^{k_i-1} b_{ij} a_i^j$, all $b_{ij} \in B$, so $a_i^{k_i} \in \sum_{j=0}^{k_i-1} a_i^j B$. It follows that $A = \sum_{i=1}^{n} \sum_{j=0}^{k_i-1} a_i^j B$.

($\Leftarrow$) This is immediate from c) $\Rightarrow$ a) in Proposition VI.4.3 of [8], setting $S = M = A$ and $R = B$. Δ

Proposition 2.5.2 *If A is a graded K-algebra and B is a graded subalgebra with A integral over B, then $dim(B) = dim(A)$.*

Proof. Say $dim(B) = m = s(B)$. Then there are $c_1, \ldots, c_m \in B$ so that B is a finitely generated C-module, $C = K[c_1, \ldots, c_m]$. Thus B is integral over C by Proposition 2.5.1, and consequently A is integral over C by transitivity. Applying Proposition 2.5.1 again we see that A is a finitely generated C-module, hence $dim(A) = s(A) \leq m$, and $m \leq s(A)$ by Proposition 2.4.7. Δ

The next theorem is due in essence to Hilbert (see [12]); there is an ungraded version due to E. Noether (see *e.g.* [20], page 262).

Theorem 2.5.3 (Normalization) *If A is a graded K-algebra of dimension n then there are algebraically independent elements $b_1, \ldots, b_n \in Homog(A^+)$ such that A is integral over the graded subalgebra $B = K[b_1, \ldots, b_n]$.*

Proof. Let $a_1, \ldots, a_s \in Homog(A^+)$ be a set of generators for A, so $A = K[a_1, \ldots, a_s]$. If $a_1, \ldots, a_s$ are algebraically independent then $s = n$ by Corollary 2.4.11 and we may take $B = A$. Suppose then that they are dependent. The proof will proceed by replacing sets of generators by certain K-linear combinations of the generators, so to maintain homogeneity it will be necessary that all generators be of the same degree. To that end we may first replace each a_i by a power of itself, say $a_i^{m_i}$, the power being just sufficient so that all $a_i^{m_i}$ are of degree $LCM(deg\, a_i : 1 \leq i \leq s)$. Clearly then A is integral over $K[a_1^{m_1}, \ldots, a_s^{m_s}]$, so we may (and shall) simply assume at the outset that all a_i are of the same degree.

Choose a homogeneous polynomial $F \neq 0$ such that $F(a_1, \ldots, a_s) = 0$, say with $deg\, F = d$. Since K is infinite we may choose $\beta_1, \ldots, \beta_{s-1} \in K$ so that $F(\beta_1, \ldots, \beta_{s-1}, 1) \neq 0$. Set $c_i = a_i - \beta_i a_s$, $1 \leq i \leq s-1$. Then

$$0 = F(a_1, \ldots, a_s) = F(c_1 + \beta_1 a_s, \ldots, c_{s-1} + \beta_{s-1} a_s, a_s),$$

which can be expanded as $a_s^d F(\beta_1, \ldots, \beta_{s-1}, 1)$ + terms of lower degree in a_s having coefficients from $K[c_1, \ldots, c_{s-1}]$. Therefore a_s is integral over $K[c_1, \ldots, c_{s-1}]$, as is each $a_i = c_i + \beta_i a_s$, $1 \leq i \leq s-1$, and hence A is integral over $K[c_1, \ldots, c_{s-1}]$. Proceed inductively to obtain, eventually, $b_1, \ldots, b_r$ algebraically independent in $Homog(A^+)$, where $b_1, \ldots, b_r$ are K–linear combinations of $a_1, \ldots, a_s$, such that A is integral over $B = K[b_1, \ldots, b_r]$. Note finally that B has dimension r, so $r = n$ by Proposition 2.5.2. Δ

2.6 Systems of Parameters

Suppose $M \in {}_A\mathcal{M}$ with $dim(M) = s(M) = n$ and suppose $\{a_1, \ldots, a_n\} \subseteq Homog(A^+)$ with M a finitely generated $K[a_1, \ldots, a_n]$–module. Then $\{a_1, \ldots, a_n\}$ is called a *system of parameters* for M.

Proposition 2.6.1 *Suppose* $0 \neq M \in {}_A\mathcal{M}, a \in Homog(A^+) \setminus \mathcal{Z}(M)$ *and* $\{a_1, \ldots, a_{n-1}\}$ *is a system of parameters for* M/aM. *Then* $\{a_1, \ldots, a_{n-1}, a\}$ *is a system of parameters for* M.

Proof. By Proposition 2.4.8 M is finitely generated over $K[a_1, \ldots, a_{n-1}, a]$ so we have that $s(M) \leq n$. Note that $Ann(M) \subseteq Ann(M/aM)$. On the other hand $a \in Ann(M/aM)$ but $a \notin \mathfrak{p}$ for any $\mathfrak{p} \in Assoc(M)$ since $a \notin \mathcal{Z}(M)$. If $\mathfrak{r}$ is any prime ideal with $\mathfrak{r} \supseteq Ann(M/aM)$ then, by Proposition 2.2.16, there is a

$\mathfrak{q} \in Assoc(M/aM)$ with $\mathfrak{q} \subseteq \mathfrak{r}$, and then there is a $\mathfrak{p} \in Assoc(M)$ with $\mathfrak{p} \subseteq \mathfrak{q}$, but $\mathfrak{p} \not\supseteq Ann(M/aM)$. Thus we have $dim(M) > dim(M/aM) = s(M/aM) = n-1$, so $dim(M) = s(M) = n$ and $\{a_1, \ldots, a_{n-1}, a\}$ is a system of parameters. $\triangle$

Note that Proposition 2.6.1 gives us another proof of the fact that $dim(M) = dim(M/aM) + 1$.

Recall that a sequence $(a_1, a_2, \ldots, a_k)$ of elements from $Homog(A^+)$ is called M–regular if $a_1 \notin \mathcal{Z}(M)$, $a_2 \notin \mathcal{Z}(M/a_1M)$, ... , and $a_k \notin \mathcal{Z}(M/\sum_{i=1}^{k-1} a_iM)$.

Proposition 2.6.2 *If $0 \neq M \in {}_A\mathcal{M}$ and $(a_1, \ldots, a_k)$ is an M–regular sequence then $\{a_1, \ldots, a_k\}$ is contained in a system of parameters for M.*

Proof. For $i = 0, \ldots, k$ set $N^{(i)} = \sum_{j=1}^{i} a_jM$ and $M^{(i)} = M/N^{(i)}$. By the standard homomorphism theorem we have $M^{(i)} \cong M^{(i-1)}/a_iM^{(i-1)}$ for $1 \leq i \leq k$. Choose a system of parameters $a_{k+1}, \ldots, a_m$ for $M^{(k)}$. Since $M^{(k)} \cong M^{(k-1)}/a_kM^{(k-1)}$ and $a_k \notin \mathcal{Z}(M^{(k-1)})$ we can apply Proposition 2.6.1 to see that $a_k, a_{k+1}, \ldots, a_m$ is a system of parameters for $M^{(k-1)}$. Inductively, $a_i, \ldots, a_m$ is a system of parameters for $M^{(i-1)}$ for each i and in particular $a_1, a_2, \ldots, a_m$ is a system of parameters for $M^{(0)} = M$. $\triangle$

Corollary 2.6.3 *The length k of any M–regular sequence is less than or equal to $dim(M)$.*

Proposition 2.6.4 *Suppose B is a graded subalgebra of $A, a \in Homog(A^+)$, and $M \in {}_A\mathcal{M}$. Then M is a finitely generated $B[a]$–module if and only if M/aM is a finitely generated B–module.*

Proof. ($\Rightarrow$) If $x_1, \ldots, x_k \in M$ generate M over $B[a]$ then it is easy to see that $\overline{x}_1, \ldots, \overline{x}_k$ generate M/aM over B.

($\Leftarrow$) Since M is graded we may choose $\overline{x}_1, \ldots, \overline{x}_k$ in M/aM that generate M/aM over B, where $x_1, \ldots, x_k$ are homogeneous in M. To see that $x_1, \ldots, x_k$ generate M over $B[a]$ it is sufficient to show that each $x \in Homog(M)$ is a $B[a]$-combination of $x_1, \ldots, x_k$. We use induction on $deg(x)$. If $deg(x) < deg(a)$ write $\overline{x} = \sum_i b_i \overline{x}_i$, with $b_i \in B$, and so $x - \sum_1^k b_i x_i \in aM$. We may assume that $deg(b_i x_i) = deg(x)$ for $1 \leq i \leq k$ and thus $x = \sum b_i x_i$ since all terms are of degree less than $deg(a)$. In general, write $\overline{x} = \sum_1^k b_i \overline{x}_i$ and say $x - \sum_1^k b_i x_i = ay$, for some $y \in Homog(M)$. Since $deg(y) = deg(x) - deg(a) < deg(x)$, then by induction $y = \sum_1^k g_i(a) x_i$, with $g_i(a) \in B[a]$, and therefore $x = \sum_1^k (b_i + a g_i(a)) x_i$. $\triangle$

Proposition 2.6.5 *Suppose that $M \in {}_A\mathcal{M}$, $dim(M) = m$, and that $a_1, \ldots, a_m \in Homog(A^+)$. Then $\{a_1, \ldots, a_m\}$ is a system of parameters for M if and only if $dim(M/\sum_1^m a_i M) = 0$.*

Proof. ($\Rightarrow$) M is finitely generated as a $K[a_1, \ldots, a_m]$-module. Apply Proposition 2.6.4 ($\Rightarrow$) m times to see that $M/\sum_1^m a_i M$ is a finitely generated K-module (*i.e.* a finite dimensional K-vector space). But then $dim(M/\sum_1^m a_i M) = 0$ by Theorem 2.4.10.

($\Leftarrow$) We have $dim(M/\sum_1^m a_i M) = 0$ if and only if $dim_K(M/\sum a_i M)$ is finite if and only if $M/\sum a_i M$ is a finitely generated K-module. Apply Proposition 2.6.4 ($\Leftarrow$) m times to see that M is a finitely generated $K[a_1, \ldots, a_m]$-module, *i.e.* that $\{a_1, \ldots, a_m\}$ is a system of parameters. $\triangle$

Corollary 2.6.6 *If $M \in {}_A\mathcal{M}$, $dim(M) = m$ and $a_1, \ldots, a_m \in Homog(A^+)$ then $\{a_1, \ldots, a_m\}$ is a system of parameters for M if and only if $dim(M/\sum_1^j a_i M) = m - j$, $0 \leq j \leq m$.*

Proof. Propositions 2.4.12 and 2.6.4. △

Recall from Proposition 2.4.2 that if $0 \neq M \in {}_A\mathcal{M}$ then $dim(M) = max\{dim(\mathfrak{p})$: $\mathfrak{p} \in Assoc(M)\}$. It is possible though to have $\mathfrak{q} \in Assoc(M)$ with $dim(\mathfrak{q}) < dim(M)$.

Example

Set $A = K[x,y,z]/\langle xy, yz\rangle$ and take $M = A$. Then $dim(A) = 2$, *e.g.* since its Poincaré series is $\Phi(t) = (1 + t - t^2)/(1-t)^2$. The prime ideal $\mathfrak{p} = \langle \overline{x}, \overline{z}\rangle$ is in $Assoc(M)$ since it is $Ann(\overline{y})$. However the chain $\mathfrak{p} \subset A^+$ is maximal, so $dim(\mathfrak{p}) = 1$.

If $M \in {}_A\mathcal{M}$ define the *span* of M to be

$$Span(M) = dim(M) - min\{dim(\mathfrak{p}): \mathfrak{p} \in Assoc(M)\}.$$

Proposition 2.6.7 *If* $M \in {}_A\mathcal{M}$ *and* $a \in Homog(A^+) \setminus \mathcal{Z}(M)$, *then* $Span(M) \leq Span(M/aM)$.

Proof. We know, by Corollary 2.4.13, that $dim(M/aM) = dim(M) - 1$. Say $dim(M) = m$ and $Span(M) = s$. Choose $\mathfrak{p} \in Assoc(M)$ such that $s = m - dim(\mathfrak{p})$ and say $\mathfrak{p} = Ann(y)$, with $y \in M$. Note that $\cap_{n=1}^{\infty} a^n M = 0$, since $deg(a) > 0$, so there is some $k \in \mathbb{N}$ such that $y \in a^k M \setminus a^{k+1}M$. Say $y = a^k z$, where $z \in M$ but $z \notin aM$. But then $a^k \mathfrak{p} z = \mathfrak{p} y = 0$, so $\mathfrak{p} z = 0$ since $a \notin \mathcal{Z}(M)$. Thus for $z + aM \in M/aM$ we have $\mathfrak{p} \subseteq (Ann(z + aM))$. Choose $\mathfrak{p}' \in Assoc(M/aM)$ so that $\mathfrak{p}' \supseteq Ann(z + aM)$ (proof of Proposition 2.2.1). Thus $\mathfrak{p}' \supseteq \mathfrak{p}$ and since $a \in Ann(M/aM)$ but $a \notin \mathfrak{p}$ (by (ii) of Proposition 2.2.1), then $\mathfrak{p} \subset \mathfrak{p}'$. Therefore $dim(\mathfrak{p}') < dim(\mathfrak{p}) = m - s$. Conclude that $Span(M/aM) \geq dim(M/aM) - dim(\mathfrak{p}') \geq dim(M) - 1 - (m - s - 1) = s = Span(M)$. △

2.7 Cohen–Macaulay Modules

The maximum length of an M–regular sequence is called the *depth* of M, so $depth(M) \leq dim(M)$ by Proposition 2.6.3. We say that M is a *Cohen–Macaulay module* if $depth(M) = dim(M)$, or equivalently if there is an M–regular sequence which is a system of parameters for M. As a consequence, if $(a_1, \ldots, a_n)$ is a system of parameters, then M is a free $K[a_1, \ldots, a_n]$–module (see Theorem 2.3.10).

A graded algebra A is called *Cohen–Macaulay* if $M = A$ is Cohen–Macaulay as an A–module.

Perhaps the most obvious example is $\mathcal{P} = K[x_1, \ldots, x_n]$, since $(x_1, \ldots, x_n)$ is clearly both a regular sequence and a system of parameters. We shall see in the next chapter that the subalgebra $\mathcal{I}$ of invariants of a finite subgroup of $GL_n(K)$ is also Cohen–Macaulay in all cases.

Proposition 2.7.1 *If* $0 \neq M \in {}_A\mathcal{M}$ *then* $Span(M) \leq dim(M) - depth(M)$.

Proof. Say $depth(M) = k$ and choose a maximal M–regular sequence $(a_1, \ldots, a_k)$. Thus $Homog(A^+) \subseteq \mathcal{Z}(M/\sum_{i=1}^{k} a_i M)$ (by maximality) and consequently $A^+ \in Assoc(M/\sum_{i=1}^{k} a_i M)$ by Propositions 2.1.4 and 2.2.1(ii). But A^+ is a maximal ideal and $dim(A^+) = 0$ so

$$Span(M/\sum_{i=1}^{k} a_i M) = dim(M/\sum_{i=1}^{k} a_i M) - 0 = dim(M) - k$$

by Corollary 2.6.6. Now apply Proposition 2.6.7 k times to conclude that $Span(M)$ $\leq dim(M) - k = dim(M) - depth(M)$. Δ

Corollary 2.7.2 *If* $M \in {}_A\mathcal{M}$ *is Cohen–Macaulay then* $dim(\mathfrak{p}) = dim(M)$ *for all* $\mathfrak{p} \in Assoc(M)$.

Proof. By the Proposition $Span(M) = 0$, and therefore $dim(\mathfrak{p}) = dim(M)$ for all $\mathfrak{p} \in Assoc(M)$. Δ

Thus, for example, the algebra in the example preceding Proposition 2.6.7 is *not* Cohen–Macaulay.

The following proposition gives a partial converse to Corollary 2.4.13.

Proposition 2.7.3 *Suppose* $0 \neq M \in {}_A\mathcal{M}$, $Span(M) = 0$ *and* $a \in Homog(A^+)$ *with* $dim(M/aM) = dim(M) - 1$. *Then* $a \notin \mathcal{Z}(M)$.

Proof. If $a \in \mathcal{Z}(M)$ then $a \in \mathfrak{p}$ for some $\mathfrak{p} \in Assoc(M)$ by Proposition 2.2.1. But then $\langle a \rangle + Ann(M) \subseteq \mathfrak{p}$ and therefore, by Proposition 2.2.13, $Ann(M/aM) \subseteq \mathfrak{p}$. Thus $dim(M/aM) \geq dim(\mathfrak{p}) = dim(M)$ since $Span(M) = 0$, which is a contradiction. Δ

Proposition 2.7.4 *If* $0 \neq M \in {}_A\mathcal{M}$ *is Cohen–Macaulay and* $a \in Homog(A^+)$, $a \notin \mathcal{Z}(M)$, *then* M/aM *is also Cohen–Macaulay.*

Proof. Extend (a) to a maximal M–regular sequence $(a_1, a_2, \ldots, a_m)$ with $a_1 = a$, where $m = dim(M)$ by Theorem 2.3.11. Then $dim(M/a_1M) = m - 1$ and $(a_2, \ldots, a_m)$ is M/a_1M–regular. Also $dim(M/\sum_1^m a_iM) = 0$ and $\{a_1, \ldots, a_m\}$ is a system of parameters for M. Thus $(a_2, \ldots, a_m)$ is both a system of parameters for M/a_1M and is M/a_1M–regular, so M/a_1M is Cohen–Macaulay. Δ

Theorem 2.7.5 *If* $M \in {}_A\mathcal{M}$ *is Cohen–Macaulay then every system of parameters is* M*–regular, and conversely every maximal* M*–regular sequence is a system of parameters.*

Proof. Let $\{a_1, a_2, \ldots, a_m\}$ be a system of parameters for M. Then $dim(M/a_1M) = m - 1$ (by Corollary 2.6.6) and $a_1 \notin \mathcal{Z}(M)$ by Proposition 2.7.3. But now M/a_1M is Cohen–Macaulay by Proposition 2.7.4 and $\{a_2, \ldots, a_m\}$ is a system of parameters for M/a_1M. Thus $(a_2, \ldots, a_m)$ is an M/a_1M–regular sequence by induction, and therefore $(a_1, \ldots, a_m)$ is M–regular.

The converse is an immediate consequence of Theorem 2.3.11 and Proposition 2.6.2. Δ

Example

Let $A = K[x^4, x^3y, xy^3, y^4] \subseteq K[x, y]$, and let B be the subalgebra $K[x^4, y^4]$. Since $(x^3y)^4 = (x^4)^3y^4$ and $(xy^3)^4 = x^4(y^4)^3$ it is clear that A is integral over B, and hence A is a finitely generated B–module. It follows that$\{x^4, y^4\}$ is a system of parameters for A, and hence $dim(A) = 2$. Of course x^4 is regular on A, since A is an integral domain, but $y^4 \cdot (x^3y)^2 = x^6y^6 = (xy^3)^2 \cdot x^4 \in \langle x^4 \rangle$ (but $(x^3y)^2 \notin \langle x^4 \rangle$), so y^4 is a zero–divisor on $A/\langle x^4 \rangle$. Thus (x^4, y^4) is *not* A–regular, and A is not Cohen–Macaulay.

Suppose now that A is a Cohen–Macaulay algebra of dimension n. Choose a system of parameters $\{b_1, \ldots, b_n\} \subseteq Homog(A^+)$ and denote by B the graded subalgebra $K[b_1, \ldots, b_n]$. Then A is a finitely generated free B–module by Theorem 2.3.10, and we may choose a B–module basis $\{c_1, \ldots, c_m\} \subseteq Homog(A)$. Thus $A = \bigoplus_{i=1}^{m} c_iB$, and each $a \in A$ has a unique expression as

$$a = \sum_{i=1}^{m} c_i h_i(b_1, \ldots, b_n)$$

for some polynomials $h_i \in \mathcal{P}$.

The sequence $(b_1, \ldots, b_n; c_1, \ldots, c_m)$ is called a *Cohen–Macaulay basis*, or *CM–basis*, for A. The elements $b_1, \ldots, b_n$ are called *free generators* and $c_1, \ldots, c_m$ are

called *transient generators*; they have also been called *primary* and *secondary* generators, or *generators* and *separators.*

If $d_i = \deg b_i$, $1 \leq i \leq n$, and $e_i = \deg c_i$, $1 \leq i \leq m$, then since $\{c_1, \ldots, c_m\}$ is a B–module basis for A and the set $\{b_1, \ldots, b_n\}$ is algebraically independent (Proposition 2.3.8) it is clear that the set

$$\mathcal{B}_d = \{c_i b_1^{k_{i1}} \cdots b_n^{k_{in}} : e_i + \sum_j k_{ij} d_j = d, \text{ all } k_{ij} \in \mathbb{N},\ 1 \leq i \leq m\}$$

is a K–basis for the homogeneous part A_d of A.

On the other hand, if the rational function $(\sum_{i=1}^m t^{e_i}) / \prod_{j=1}^n (1 - t^{d_j})$ is expanded to a power series about $t = 0$ then by inspection the coefficient of t^d is the total number of ways that it is possible to choose i, $1 \leq i \leq m$, and then to choose integers $k_{ij} \in \mathbb{N}$ so that $e_i + \sum_j k_{ij} d_j = d$. In other words, the coefficient of t^d is equal to the cardinality of $\mathcal{B}_d$, and we have proved the next proposition.

Proposition 2.7.6 *Suppose that A is a Cohen–Macaulay algebra and $(b_1, \ldots, b_n; c_1, \ldots, c_m)$ is a CM–basis for A, with $\deg b_i = d_i$, $\deg c_j = e_j$. Then the Poincaré series of A is*

$$\Phi(t) = \frac{t^{e_1} + \cdots + t^{e_m}}{(1 - t^{d_1}) \cdots (1 - t^{d_n})}.$$

For the simplest of examples note that $(x_1, \ldots, x_n; 1)$ is a CM–basis for the polynomial algebra $\mathcal{P} = K[x_1, \ldots, x_n]$, so its Poincaré series is

$$\Phi(t) = \frac{1}{(1-t)^n} = \sum_{d=0}^{\infty} \binom{n+d-1}{d} t^d.$$

3. BACK TO INVARIANT THEORY

3.1 Classical Finiteness Theorems

Recall that $\mathcal{P}$ is the algebra of polynomial functions and $\mathcal{I}$ is the ring of all polynomial invariants of a finite group G.

An *integrity basis* for a group $G \leq GL(V)$ is a set $\{f_1, f_2, \ldots, f_m\}$ of invariants with the property that every invariant of G is a polynomial in $f_1, \ldots, f_m$, *i.e.* $\mathcal{I} = K[f_1, \ldots, f_m]$.

Theorem 3.1.1 (D. Hilbert [11], 1890) *Every finite subgroup G of $GL(V)$ has an integrity basis,* i.e. *there exist $\{f_1, \ldots, f_m\} \subseteq \mathcal{I} = \mathcal{I}(G)$ such that $\mathcal{I} = K[f_1, \ldots, f_m]$. The basis elements f_i may be chosen to be homogeneous of positive degree.*

Proof. Set $\mathfrak{a} = \mathcal{P}\mathcal{I}^+$, the ideal in $\mathcal{P}$ generated by $Homog(\mathcal{I}^+)$. By the Hilbert Basis Theorem $\mathfrak{a}$ is finitely generated, so there are $f_1, \ldots, f_m \in Homog(\mathcal{I}^+)$ such that $\mathfrak{a} = \langle f_1, \ldots, f_m \rangle_{\mathcal{P}}$. Let us show that $\langle f_1, \ldots, f_m \rangle_{\mathcal{I}} = \mathcal{I}^+$. The inclusion left to right is clear. If $g \in \mathcal{I}^+$ we may write $g = \sum_i h_i f_i$ for some h_i's in $\mathcal{P}$. But then $g = \mathcal{M}\, g = \sum_i (\mathcal{M}\, h_i) f_i \in \langle f_1, \ldots, f_m \rangle_{\mathcal{I}}$, as required. Now we may apply Proposition 2.1.2 and conclude that $\mathcal{I} = K[f_1, \ldots, f_m]$. Δ

Corollary 3.1.2 *The algebra $\mathcal{I}$ of invariants is a graded subalgebra of $\mathcal{P}$.*

Note that the theorem and its proof are totally non–constructive. An integrity basis is shown to exist but no information is provided as to how the f_i's might be constructed, nor is there any information regarding the number m of elements

in the basis or bounds for their degrees. This is the aspect of the Hilbert Basis Theorem that has been called "*theology, not mathematics*". The next theorem might be viewed as an improvement, in that bounds for m and the degrees are provided, and the proof indicates means for constructing the basis elements.

Theorem 3.1.3 (E. Noether [23], 1916) *If $G \leq GL(V)$ is finite, with $|G| = \gamma$ and $\dim V = n$, then G has an integrity basis $\{f_1, \ldots, f_m\}$, with $m \leq \binom{n+\gamma}{n}$ and $\deg f_i \leq \gamma$ for all i.*

Proof. Write $G = \{T_1, \ldots, T_\gamma\}$. Let $u_1, \ldots, u_n$ be another set of indeterminates and write $U = (u_1, \ldots, u_n)$ as in Chapter 1. For $k \in \mathbb{N}$ and $\alpha = (a_1, \ldots, a_n) \in \mathbb{N}^n$ write $\binom{k}{\alpha}$ for the multinomial coefficient $\binom{k}{a_1, \ldots, a_n}$.

Set $y_i = (T_i x_1)u_1 + (T_i x_2)u_2 + \cdots + (T_i x_n)u_n$, $1 \leq i \leq \gamma$. If $k \in \mathbb{N}$ consider y_i^k expanded as a product of k factors:

$$y_i^k = [(T_i x_1)u_1 + \cdots + (T_i x_n)u_n]^k$$

$$= \sum\{\binom{k}{\alpha}(\prod_{j=1}^{n}(T_i x_j)^{a_j})U^\alpha : \alpha \in \mathbb{N}^n,\ |\alpha| = k.\}$$

Write s_k for the *power sum* $y_1^k + \cdots + y_\gamma^k$. Thus

$$s_k = \sum_{i=1}^{\gamma}\sum\{\binom{k}{\alpha}(\prod_{j=1}^{n}(T_i x_j)^{a_j})U^\alpha : |\alpha| = k\}$$

$$= \sum\{\binom{k}{\alpha}[\sum_{i=1}^{\gamma}\prod_{j=1}^{n}(T_i x_j)^{a_j}]U^\alpha : |\alpha| = k\}$$

$$= \sum\{\binom{k}{\alpha}J_\alpha U^\alpha : |\alpha| = k\}$$

where $J_\alpha = J_\alpha(X) = \sum_{i=1}^{\gamma} \prod_{j=1}^{n} (T_i x_j)^{a_j}$. Clearly $J_\alpha \in \mathcal{I}$, and $deg\, J_\alpha = |\alpha|$.

Every s_k for $k > \gamma$ is a polynomial in $s_1, s_2, \ldots, s_\gamma$ (see *e.g.* [8], page 276). Each s_k expands as above and if $1 \leq k \leq \gamma$ then the J_α's in the expansion have $|\alpha| \leq \gamma$. For $k > \gamma$ write $s_k = h(s_1, \ldots, s_\gamma)$ for some polynomial h and compare coefficients of the monomials U^α to see that each J_β, $|\beta| > k$ is a polynomial in various J_α's with $|\alpha| \leq \gamma$.

Now take any $f \in \mathcal{I}_d$ and write $f = \sum\{c_\alpha X^\alpha : |\alpha| = d\}$. Then

$$f = \mathcal{M}f = \sum_{|\alpha|=d} c_\alpha \mathcal{M}(X^\alpha)$$

$$= \sum_{|\alpha|=d} c_\alpha \frac{1}{\gamma} \sum_{i=1}^{\gamma} (T_i x_1)^{a_1} \ldots (T_i x_n)^{a_n}$$

$$= \sum_{|\alpha|=d} \frac{c_\alpha}{\gamma} J_\alpha.$$

It follows that $\{J_\alpha : |\alpha| \leq \gamma\}$ is an integrity basis.

To bound the size of the basis we need to count the $\alpha \in \mathbb{N}^n$ with $|\alpha| \leq \gamma$. That number is well known to be $\binom{n+\gamma}{n}$ (see *e.g.* Exercises 7.8 and 7.9 of [9]). $\triangle$

Recall that classically a *symmetric polynomial* in indeterminates $(z_1, \ldots, z_\gamma)$ is a polynomial $g = g(z_1, \ldots, z_\gamma)$ that is an invariant of the symmetric group $Sym(\gamma)$, *i.e.* g is unchanged under any permutation of $(z_1, \ldots, z_\gamma)$.

Proposition 3.1.4 *If $G = \{T_1, \ldots, T_\gamma\} \leq GL(V)$, $g = g(z_1, \ldots, z_\gamma)$ is a symmetric polynomial, and $h \in \mathcal{P}$, then $g(T_1 h, \ldots, T_\gamma h) \in \mathcal{I}(G)$.*

Proof. This is clear since for any $S \in G$ the sequence $(ST_1 h, \ldots, ST_\gamma h)$ is a permutation of $(T_1 h, \ldots, T_\gamma h)$. $\triangle$

Proposition 3.1.5 *If $G \leq GL(V)$ is finite then the polynomial algebra $\mathcal{P}$ is an integral ring extension of $\mathcal{I}$,* i.e. *every $f \in \mathcal{P}$ satisfies $p(f) = 0$ for some nonzero monic polynomial $p(t) = p_f(t) \in \mathcal{I}[t]$.*

Proof. If $G = \{T_1, \ldots, T_\gamma\}$ set $p(t) = \prod_{i=1}^{\gamma}(t - T_i f)$; $p(t)$ is clearly monic, and $p(f) = 0$ since one of the T_i is 1. When the product is expanded the coefficients of p are ($\pm$) elementary symmetric polynomials in $T_1 f, \ldots, T_\gamma f$, so $p(t) \in \mathcal{I}[t]$ by Proposition 3.1.4. $\triangle$

Corollary 3.1.6 *$dim(\mathcal{I}) = dim(\mathcal{P})$.*

Proof. Apply Proposition 2.5.2. $\triangle$

3.2 $\mathcal{I}$ is Cohen-Macaulay

The main result of this section, Theorem 3.2.1, is more recent in origin than those of the previous section, having first been proved by M. Hochster and J. Eagon in 1971. The proof given below is based on ideas suggested by H. Terao.

Theorem 3.2.1 (See [14]) *The algebra $\mathcal{I}$ of invariants of a finite group $G \leq GL(V)$ is a Cohen–Macaulay algebra.*

Proof. Since $dim\,\mathcal{I} = n$ (by Corollary 3.1.6) it will suffice to produce an $\mathcal{I}$–regular sequence of length n. We first find a $\mathcal{P}$–regular sequence of elements from $Homog(\mathcal{I}^+)$. To begin we may choose any nonzero $f_1 \in Homog(\mathcal{I}^+)$, since $\mathcal{P}$ is an integral domain. If $(f_1, \ldots, f_i)$ is $\mathcal{P}$–regular, with $i < n$ and all $f_j \in Homog(\mathcal{I}^+)$, set $M = \mathcal{P}/\langle f_1, \ldots, f_i\rangle \in {}_{\mathcal{P}}\mathcal{M}$, and suppose $Assoc(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$. By Proposition 2.6.2 $\{f_1, \ldots, f_i\}$ is contained in a system of parameters for $\mathcal{P}$, and so $dim\, M =$

$n - i > 0$ by Corollary 2.6.6. Since $dim\,\mathcal{I} = dim\,\mathcal{P} = n$ we have $dim(\mathcal{P}\mathcal{I}^+) = 0$. Thus we cannot have $\mathcal{I}^+ \subseteq \mathfrak{p}_i$ for any i, and hence $Homog(\mathcal{I}^+) \not\subseteq \cup_{i=1}^{k} \mathfrak{p}_i = \mathcal{Z}(M)$ by Proposition 2.1.4. Thus we may choose $f_{i+1} \in Homog(\mathcal{I}^+) \setminus \mathcal{Z}(M)$ and the sequence $(f_1, \ldots, f_i, f_{i+1})$ is $\mathcal{P}$–regular. By induction then there is a $\mathcal{P}$–regular sequence $(f_1, \ldots, f_n)$ from $Homog(\mathcal{I}^+)$.

To complete the proof we show inductively that each subsequence $(f_1, \ldots, f_i)$ is in fact $\mathcal{I}$–regular, $1 \leq i \leq n$. The case $i = 1$ is clear, so suppose for some i with $1 < i < n$ that $(f_1, \ldots, f_i)$ is $\mathcal{I}$–regular, but that f_{i+1} is a zero divisor on $\mathcal{I}/\langle f_1, \ldots, f_i \rangle_{\mathcal{I}}$. Thus there is some $g \in \mathcal{I} \setminus \langle f_1, \ldots, f_i \rangle_{\mathcal{I}}$ such that $gf_{i+1} \in \langle f_1, \ldots, f_i \rangle_{\mathcal{I}} \subseteq \langle f_1, \ldots, f_i \rangle_{\mathcal{P}}$. However f_{i+1} *is* regular on $\mathcal{P}/\langle f_1, \ldots, f_i \rangle_{\mathcal{P}}$, so $g \in \langle f_1, \ldots, f_i \rangle_{\mathcal{P}}$, say *via* $g = \sum_{j=1}^{i} h_j f_j$, $h_j \in \mathcal{P}$. But then

$$g = \mathcal{M}g = \sum_j (\mathcal{M}h_j) f_j \in \langle f_1, \ldots, f_i \rangle_{\mathcal{I}},$$

a contradiction, and the proof is complete. $\triangle$

Since $\mathcal{I}$ is a Cohen-Macaulay algebra of dimension n it has a CM–basis, *i.e.* a sequence $(f_1, \ldots, f_n; g_1, \ldots, g_m)$ of elements of $Homog(\mathcal{I}^+)$ such that

$$\mathcal{I} = \bigoplus_{i=1}^{m} g_i K[f_1, \ldots, f_n],$$

and in particular every invariant $f \in \mathcal{I}$ can be expressed uniquely in the form $f = \sum_i g_i h_i(f_1, \ldots, f_n)$ for some $h_1, \ldots, h_m \in \mathcal{P}$. Since $\mathcal{I}_0 = K$ we may (and shall) always choose g_1 to be the constant polynomial 1.

Recall from Chapter 2 that $f_1, \ldots, f_n$ are called *free* and $g_1, \ldots, g_m$ *transient* generators for $\mathcal{I}$. In accordance with the notation introduced there we denote the degrees of the generators by $d_i = deg\, f_i$ and $e_i = deg\, g_i$, and we further assume the generators labeled so that

$$d_1 \leq \cdots \leq d_n; \quad e_1 \leq \cdots \leq e_m.$$

Proposition 3.2.2 (See [15]) *If* $(f_1,\ldots,f_n;g_1,\ldots,g_m)$ *is a CM-basis for* $\mathcal{I}$ *then*

$$m=\frac{d_1\cdots d_n}{|G|}.$$

Proof. We have 2 expressions for the Molien series $\Phi(t)$ as a rational function – from Molien's Theorem 1.2.1 and from Proposition 2.7.6. Thus we have

$$\frac{1}{|G|}\sum_{T\in G}\frac{detT}{charpol_T(t)}=\frac{t^{e_1}+\cdots+t^{e_m}}{(1-t^{d_1})\cdots(1-t^{d_n})}.$$

Multiply both sides of the equation by $(1-t)^n$. On the right hand side all factors $1-t$ cancel, leaving a product of polynomials $1+t+\cdots+t^{d_i-1}$ in the denominator. On the left hand side the only $T\in G$ having eigenvalue 1 with multiplicity n is $T=1$; in all other summands fewer than n of the factors $1-t$ cancel. When all cancellations have been completed set $t=1$ and obtain $|G|^{-1}=m/\prod_i d_i$. $\triangle$

Next we determine a bound, established by G. Kempf and R. Stanley in 1979 (see [18] and [29]) for the degrees of the transient generators. The bound will be used in the implementation of the algorithm of Chapter 5.

Proposition 3.2.3 *Denote by* λ *the linear character of* G *defined by* $\lambda(T)=detT$, *all* $T\in G$, *and let* μ *be the minimal degree of (nonzero)* λ*-invariants of* G. *If* $(f_1,\ldots,f_n;g_1,\ldots,g_m)$ *is a CM-basis for* $\mathcal{I}$ *then*

$$e_m=\sum_{i=1}^{n}d_i-n-\mu.$$

Proof. Combining Propositions 1.2.4 and 2.7.6 we have

$$(-t)^n\Phi^{(\lambda)}(t)=\Phi(1/t)$$

$$=\frac{t^{-e_1}+\cdots+t^{-e_m}}{(1-t^{-d_1})\cdots(1-t^{-d_n})}$$

$$= \frac{t^{\Sigma d_i}(-1)^n \sum t^{-e_i}}{(1-t^{d_1})\cdots(1-t^{d_n})}.$$

Comparing lowest degree terms we obtain

$$\mu + n = \sum_i d_i - e_m.$$

Δ

Corollary 3.2.4 *The highest degree e_m of a transient generator in a CM-basis for $\mathcal{I}$ satisfies $e_m \leq \sum_{i=1}^{n} d_i - n$; equality holds if and only if $G \leq SL(V)$.*

A very classical result of invariant theory is the calculation of the invariants of the *alternating group*, $Alt(n)$. Let us now look at $Alt(n)$ and see how Propositions 3.2.2 and 3.2.3 relate to $\mathcal{I}_{Alt(n)}$.

In Chapter 1 we defined an action of T on $\mathcal{P}$ where $T \in GL(V)$. We now wish to talk about the action of ϕ on $\mathcal{P}$ where $\phi \in Sym(n)$. The same definition will work if we view the permutation ϕ as a permutation matrix.

Recall that the *elementary symmetric polynomials* σ_i, in the indeterminates $x_1, \ldots, x_n$, are defined by $\sigma_i = \sum\{x_{j_1}x_{j_2}\cdots x_{j_i} : j_1 < \cdots < j_i \in \mathbb{N}\}$. All of the elementary symmetric polynomials are invariants of the *symmetric group* $Sym(n)$ and in fact the set $\{\sigma_1, \ldots, \sigma_n\}$ is an integrity basis for $\mathcal{I}_{Sym(n)}$. This is the Fundamental Theorem of Symmetric Polynomials.

Define $\delta = \delta(x_1, \ldots, x_n)$ to be $\delta = \Pi\{(x_i - x_j) : 1 \leq j < i \leq n\}$. Note that δ has degree $(n^2 - n)/2$. Clearly $\delta \in \mathcal{I}_{Alt(n)}$ but $\phi\delta = -\delta$ for every $\phi \in Sym(n) \setminus Alt(n)$.

We claim that $(\sigma_1, \ldots, \sigma_n; 1, \delta)$ is a CM-basis for $\mathcal{I}_{Alt(n)}$ (*i.e.* if $f \in \mathcal{I}_{Alt(n)}$ then $f = f_1(\sigma_1, \ldots, \sigma_n) + \delta \cdot f_2(\sigma_1, \ldots, \sigma_n)$ for some $f_1, f_2 \in \mathcal{P}$). The sequence $(\sigma_1, \ldots, \sigma_n)$ is an $\mathcal{I}_{Alt(n)}$-regular sequence and thus $\sigma_1, \ldots, \sigma_n$ are free generators for $\mathcal{I}_{Alt(n)}$. By Proposition 3.2.2 the number of transient generators m is equal to

$(1 \cdot 2 \cdot 3 \cdots n)/(n!/2)$ which is 2, corresponding to the transient generators 1 and δ. Also by Corollary 3.2.4, since $Alt(n) \leq SL(V)$, the highest degree of a transient generator is

$$e_m = \sum_{i=1}^{n} d_i - n = \sum_{i=1}^{n} i - n = (n(n+1))/2 - n = (n^2 - n)/2$$

which is exactly the degree of δ. Clearly, then $\mathcal{I}$ is the direct sum of $K[\sigma_1, \ldots, \sigma_n]$ and $\delta \cdot K[\sigma_1, \ldots, \sigma_n]$, and $(\sigma_1, \ldots, \sigma_n; 1, \delta)$ is a CM–basis for $Alt(n)$.

In general, recall that we can write the Molien Series $\Phi(t)$ as a rational function in the form

$$\Phi(t) = \frac{\sum_{i=1}^{m} t^{e_i}}{\prod_{j=1}^{n}(1 - t^{d_i})}$$

where $d_i = \deg f_i$, $e_i = \deg g_i$, n is the number of free generators and m is the number of transient generators. The f_i's are algebraically independent. However, if $m > 1$ then the set $\{f_1, \ldots, f_n; g_2, \ldots, g_m\}$ is algebraically dependent, *i.e.* there exists a nonzero polynomial h such that $h(f_1, \ldots, f_n, g_2, \ldots, g_m) = 0$. We call this polynomial h a *syzygy* . The syzygies form an ideal S in $\mathcal{I}$.

If $\mathcal{I}$ has a CM–basis $(f_1, \ldots, f_n; 1, g_2, \ldots, g_m)$ then every $f \in \mathcal{I}$ can be uniquely represented as $f = \sum_1^m g_i p_i(f_1, \ldots, f_n)$. Take any pair $g_j, g_k, k \geq j \geq 2$. Then $g_j g_k \in \mathcal{I}$ so $g_j g_k = \sum_1^m g_i p_i(f_1, \ldots, f_n)$ and $g_j g_k - \sum_1^m g_i p_i(f_1, \ldots, f_n) = 0$ and thus we have obtained a syzygy. In fact, if we define $h(u_1, \ldots, u_n, v_1, \ldots v_m) = v_j v_k - \sum_1^m v_i p_i(u_1, \ldots, u_n)$ then the set of all h's of this form will be a generating set for the syzygies.

For an example, consider the Klein four group V_4 generated by $a = (12)$ and $b = (34)$. The Molien Series for this group can be written as

$$\Phi(t) = \frac{1 + t + t^2}{(1-t)(1-t^2)^2(1-t^3)}.$$

One possible CM–basis for this group consists of

$$f_1 = x_1 + x_2, \quad f_2 = x_1^2 + x_2^2, \quad f_3 = x_3^2 + x_4^2, \quad f_4 = x_3^3 + x_4^3;$$

$$g_1 = 1, \quad g_2 = x_3 + x_4, \quad g_3 = x_3 x_4.$$

To find the generators for the syzygies we simply take all products of the form $g_j g_k$, $k \geq j \geq 2$. Thus we have

$$g_2^2 = f_3 + 2g_3, \qquad g_2 g_3 = -f_4 + f_3 g_2, \qquad g_3^2 = (1/2)(f_3^2 - f_4 g_2 + f_3 g_3).$$

For another example, consider again the group $Alt(n)$. The Molien Series for $Alt(n)$ can be written as

$$\Phi(t) = \frac{1 + t^{(n^2-n)/2}}{\prod_{i=1}^{n}(1 - t^i)}.$$

We saw earlier that $(\sigma_1, \ldots, \sigma_n; 1, \delta)$ is a CM–basis for $\mathcal{I}_{Alt(n)}$. Since $\delta^2 \in \mathcal{I}_{Sym(n)}$ we can express δ^2 uniquely in terms of $\sigma_1, \ldots, \sigma_n$. For example if $n = 2$ then $\delta^2 = \sigma_1^2 - 4\sigma_2$. In general, there exists $p \in \mathcal{P}$ such that $\delta^2 = p(\sigma_1, \ldots, \sigma_n)$ and we set $\ell = y^2 - p \in K[x_1, \ldots, x_n, y]$ so that $\ell(\sigma_1, \ldots, \sigma_n, \delta) = 0$. Note that p is the classical formula for the generic discriminant, *i.e.* the discriminant of the *generic polynomial* of degree n, $P(y) = \prod_{i=1}^{n}(y - x_i) = y^n - \sigma_1 y^{n-1} + \cdots \pm \sigma_n$.

The polynomial ℓ is a basic syzygy for $Alt(n)$ in the following sense (see [31]): if $k \in K[x_1, \ldots, x_n, y]$ with $k(\sigma_1, \ldots, \sigma_n, \delta) = 0$ then $\ell | k$.

To see this view k and ℓ as elements in $\mathcal{P}[y]$, *i.e* polynomials in y with polynomials in $x_1, \ldots, x_n$ as coefficients. Divide k by ℓ getting quotient and remainder $q(y), r(y) \in \mathcal{P}[y]$ and with $deg_y r(y) \leq 1$. Say $r(y) = A + By$, with $A, B \in K[x_1, \ldots, x_n]$, so $k(y) = q(y)\ell(y) + A + By$. Substitute δ for y and $\sigma_1, \ldots, \sigma_n$ for $x_1, \ldots, x_n$ and get $0 = k(\sigma_1, \ldots, \sigma_n, \delta) = q(\delta)\ell(\sigma_1, \ldots, \sigma_n, \delta) + A + B\delta$, or

$$A(\sigma_1, \ldots, \sigma_n) + \delta B(\sigma_1, \ldots, \sigma_n) = 0. \quad (*)$$

Apply any $\phi \in Sym(n) \setminus Alt(n)$ to $(*)$ and get

$$A(\sigma_1, \ldots, \sigma_n) - \delta\ B(\sigma_1, \ldots, \sigma_n) = 0. \quad (**)$$

Add $(*)$ and $(**)$ and conclude that $A(\sigma_1, \ldots, \sigma_n) = 0$, and hence also that $B(\sigma_1, \ldots, \sigma_n) = 0$. But $\{\sigma_1, \ldots, \sigma_n\}$ is an algebraically independent set of polynomials. Thus A and B are in fact both the zero polynomial, *i.e.* $r(y) = 0$. Therefore $\ell | k$.

Thus the ideal of syzygies of $Alt(n)$ is generated by ℓ, *i.e.* $S =< \ell >$.

4. POLYNOMIALS

We gather in this chapter some notions pertaining to polynomial algebras that are oriented toward the calculation of polynomial invariants for finite groups in the next chapter.

We assume as usual that K is a field of characteristic 0, and write $\mathcal{P} = K[x_1, \ldots, x_n]$.

4.1 Monomial Orders

Recall from Chapter 1 that a *monomial* in $\mathcal{P}$ is a power product $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, with each $a_i \in \mathbb{N}$. It is convenient notationally to write that monomial as X^α, where X serves as a reminder of the (ordered) list $x_1, \ldots, x_n$ of indeterminates and $\alpha = (a_1, \ldots, a_n) \in \mathbb{N}^n$. The notation provides an isomorphism $\alpha \leftrightarrow X^\alpha$ between the (additive) semigroup $\mathbb{N}^n$ and the (multiplicative) semigroup $\operatorname{Mon} \mathcal{P}$ of all monomials in $\mathcal{P}$.

Recall also that a monomial is restricted to having 1 as its coefficient from K, and that a polynomial of the form cX^α, with $c \neq 0$ in K, is called a *term*. These conventions are of course not completely standard, but they are also not unusual.

If $\alpha = (a_1, \ldots, a_n) \in \mathbb{N}^n$ then $|\alpha| = \sum_1^n a_i$ is the degree of the monomial X^α.

An ideal I in $\mathcal{P}$ is called a *monomial ideal* if it is generated by some set of monomials.

Proposition 4.1.1 *Suppose $I = \langle X^\alpha : \alpha \in A \subseteq \mathbb{N}^n \rangle$ is a monomial ideal in $\mathcal{P}$. If $f \in \mathcal{P}$ then $f \in I$ if and only if every term of f is divisible by some X^α, $\alpha \in A$.*

Proof. This is clear since every $f \in I$ can be written as a finite sum of the form $\sum_i f_i X^{\alpha_i}$, $f_i \in \mathcal{P}, \alpha_i \in A$. Δ

Proposition 4.1.2 *If I is an ideal in $\mathcal{P}$ then I is a monomial ideal if and only if every term of each $f \in I$ is also in I.*

Proof. If the latter condition holds then I is generated by the set of monomials of the terms of its elements. The converse follows from Proposition 4.1.1. Δ

It will be useful to impose various orderings on $\mathrm{Mon}\,\mathcal{P}$ so as to determine canonical expressions for polynomials in general, by analogy, for example, with writing a polynomial of one variable in order of descending powers of the variable. In view of the isomorphism mentioned above we may describe orderings either for $\mathbb{N}^n$ or for $\mathrm{Mon}\,\mathcal{P}$.

Recall that an order relation $>$ on a set S is called a *total* order if it satisfies a **trichotomy law**, *i.e.* given any pair α, $\beta \in S$ then exactly one of $\alpha > \beta$, $\alpha = \beta$, or $\beta > \alpha$ must hold. Given an order $>$ we will, as is customary, sometimes write $\alpha \geq \beta$ to mean that either $\alpha > \beta$ or $\alpha = \beta$.

A total order relation $>$ on $\mathbb{N}^n$ will be called a *monomial order* if it satisfies two further requirements, *viz.*

i) $\alpha \geq 0$, all $\alpha \in \mathbb{N}^n$, and

ii) if $\alpha > \beta$ then $\alpha + \gamma > \beta + \gamma$ for all $\gamma \in \mathbb{N}^n$.

As mentioned, the most familiar example occurs when $n = 1$ and $>$ is the usual order on $\mathbb{N}$, resulting in $x^k > x^l$ in $\mathrm{Mon}\,\mathcal{P}$ if and only if $k - l$ is a positive integer.

We present four further examples, although the list could be expanded indefinitely. In all cases it is easy to verify that the required conditions for a monomial order are satisfied, so the details are omitted.

1) *(Lexicographic)* Say that $\alpha >_l \beta$ if the left-most nonzero entry of $\alpha - \beta = (a_1 - b_1, \ldots, a_n - b_n)$ is positive. Thus *e.g.* $x_1 >_l x_2 >_l \cdots >_l x_n$, and $x^2y >_l xy^{17}$. This order is often referred to as *dictionary order*, for obvious reasons.

2) *(Graded lexicographic)* Say that $\alpha >_{gl} \beta$ if

a) $|\alpha| > |\beta|$, or if

b) $|\alpha| = |\beta|$ and $\alpha >_l \beta$.

Thus the order is determined first by higher degree, then ties are broken lexicographically. For example, $y^3 >_{gl} x^2$ and $xy^2z^3 >_{gl} xyz^4$.

3) *(Graded reverse lexicographic)* Say that $\alpha >_{grl} \beta$ if

a) $|\alpha| > |\beta|$, or if

b) $|\alpha| = |\beta|$ and $\alpha - \beta$ has right-most nonzero entry negative.

Note for example that $xz >_{gl} y^2$, but $y^2 >_{grl} xz$ since $(0,2,0) - (1,0,1) = (-1,2,-1)$.

4) *(Graded inverse lexicographic)* Say that $\alpha >_{gil} \beta$ if

a) $|\alpha| > |\beta|$, or if

b) $|\alpha| = |\beta|$ and $\beta >_l \alpha$.

We remark that the graded inverse lexicographic order is the default for certain functions in the computer algebra system *Maple* [5].

Proposition 4.1.3 *If $X^\alpha \mid X^\beta$ in $Mon\mathcal{P}$ then $\beta \geq \alpha$ for any monomial order $>$.*

Proof. We have $\beta = \gamma + \alpha$ for some γ, and $\gamma \geq 0$, so $\beta = \gamma + \alpha \geq 0 + \alpha = \alpha$. $\triangle$

Proposition 4.1.4 *Every monomial order $>$ on $Mon\mathcal{P}$ is a well-ordering,* i.e. *every nonempty subset of $Mon\mathcal{P}$ has a smallest element.*

Proof. If $>$ is not a well-ordering then there is an infinite properly descending chain $\alpha_1 > \alpha_2 > \cdots$ in $\mathbb{N}^n$. Define ideals $I_k = \langle X^{\alpha_1}, \ldots, X^{\alpha_k} \rangle$ in $\mathcal{P}$, $1 \leq k \in \mathbb{N}$. Let us show that $X^{\alpha_{k+1}} \notin I_k$ for each k. If $X^{\alpha_{k+1}} \in I_k$ then $X^{\alpha_m} \mid X^{\alpha_{k+1}}$ for some $m \leq k$ by Proposition 4.1.1, say $X^{\alpha_m} X^{\gamma} = X^{\alpha_{k+1}}$, *i.e.* $\alpha_m + \gamma = \alpha_{k+1}$ in $\mathbb{N}^n$. But since $\alpha_m > \alpha_{k+1}$ and $\gamma > 0$ we have also that $\alpha_m + \gamma > \alpha_{k+1} + \gamma > \alpha_{k+1} + 0 = \alpha_{k+1}$, a contradiction. Now, however, the increasing chain $\{I_k\}$ of ideals is incompatible with the fact that $\mathcal{P}$ is Noetherian, and the proof is complete. Δ

We assume for the remainder of this section that some fixed monomial order has been chosen for Mon $\mathcal{P}$. Unless otherwise specified all illustrative examples will use graded lexicographic order.

If $f \neq 0$ in $\mathcal{P}$ is written (uniquely) as a sum of terms, $f = \sum_\alpha c_\alpha X^\alpha$, with $0 \neq c_\alpha \in K$, and with the monomials X^α appearing in decreasing order, then the first term, say $c_\gamma X^\gamma$, that occurs is called the *leading term* of f, c_γ is the *leading coefficient*, and X^γ is the *leading monomial*. We will denote them respectively as $\ell t\, f$, $\ell c\, f$, and $\ell m\, f$. A nonzero polynomial is called *monic* if its leading coefficient is 1. Needless to say the definitions depend very much on the choice of monomial order.

4.2 Gröbner Bases

If S is any subset of $\mathcal{P}$ define $\ell m\, S$ to be the set of leading monomials of elements of S. Then $\langle \ell m\, S \rangle$ is called the *monomial ideal* corresponding to S.

If $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq \mathcal{P}$ and $I = \langle \mathcal{F} \rangle$, then clearly $\langle \ell m\, \mathcal{F} \rangle \subseteq \langle \ell m\, I \rangle$. The reverse inclusion may, however, fail.

For an example take $f_1 = xy - y + 1$, $f_2 = x^2 - x$, and set $\mathcal{F} = \{f_1, f_2\}$, $I = \langle \mathcal{F} \rangle$. Thus $\langle \ell m\, \mathcal{F} \rangle = \langle xy, x^2 \rangle$, and every element of $\langle \ell m\, \mathcal{F} \rangle$ has degree at least

2. Note, however, that $xf_1 - yf_2 = x \in I$, so $x \in \langle \ell m\, I \rangle$ but $x \notin \langle \ell m\, \mathcal{F} \rangle$.

Now a very important definition. If I is a nonzero ideal in $\mathcal{P}$, then a finite set $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq \mathcal{P}$ is a *Gröbner basis* (or a *standard basis*) for I if

i) $\mathcal{F}$ is a basis for I, *i.e.* $\langle \mathcal{F} \rangle = I$, and

ii) $\langle \ell m\, \mathcal{F} \rangle = \langle \ell m\, I \rangle$.

We will write *$\mathcal{G}$-basis* to denote a Gröbner basis. The concept of Gröbner basis is an important tool in dealing with polynomials, for example, using them we can develop an effective test for ideal membership. The notion was first introduced by Hironaka, who called it a standard basis, in 1964 (see [13]), then independently in 1965 by Buchberger [2], who called it a Gröbner basis in honor of his dissertation adviser for the Ph.D. degree at Innsbruck.

Proposition 4.2.1 *If $\mathcal{F}$ is a finite set of monomials in $\mathcal{P}$ and $I = \langle \mathcal{F} \rangle$, then $\mathcal{F}$ is a $\mathcal{G}$-basis for I.*

Proof. Obviously $\ell m\, \mathcal{F} = \mathcal{F}$, and $\langle \ell m\, I \rangle = I$ follows easily from Proposition 4.1.2, so $\langle \ell m\, \mathcal{F} \rangle = \langle \mathcal{F} \rangle = I = \langle \ell m\, I \rangle$. △

Although the definition above is straightforward, it is generally difficult to decide on the basis of the definition whether or not a set $\mathcal{F}$ actually *is* a $\mathcal{G}$-basis for an ideal I, and furthermore it begs the question of the existence of a $\mathcal{G}$-basis for a given ideal. It will be convenient to develop some conditions equivalent with the definition that will allow an effective determination, and will in fact lead to an algorithm for the construction of $\mathcal{G}$-bases.

We begin by describing a generalization to $\mathcal{P}$ of the usual division algorithm for polynomials in one indeterminate. Given $g \in \mathcal{P}$ the idea is to divide g not just by another polynomial f, but by a "divisor sequence" $\mathcal{F} = (f_1, \ldots, f_m)$ of nonzero

polynomials from $\mathcal{P}$. The desired result is a "quotient sequence" $(q_1, \ldots, q_m)$ and a "remainder" r from $\mathcal{P}$, with $g = \sum_i q_i f_i + r$, and either $r = 0$ or else no term of r is divisible by any $\ell m\, f_i$.

We outline below the steps for one such algorithm. In practice it is carried out in a manner very much analogous to the familiar "long division" process for the case of one variable. The Boolean variable LTRM (when true) indicates *"leading term removed"*.

For a more leisurely exposition, with several illustrative examples, see Chapter 2 of [6].

A Division Algorithm for $\mathcal{P}$

1. *Input:* $g \in \mathcal{P}$ and a divisor sequence $\mathcal{F} = (f_1, \ldots, f_m)$ from $\mathcal{P}$.

2. *Initialize:* $q_1 := 0, \ldots, q_m := 0; r := 0; h := g$.

3. While $h \neq 0$ do

   $i := 1$

   $LTRM :=$ false

   while $i \leq m$ and not $LTRM$ do

      if $\ell m\, f_i \mid \ell m\, h$ then

         $q_i := q_i + \ell t\, h / \ell t\, f_i$

         $h := h - (\ell t\, h / \ell t\, f_i) \cdot f_i$

         $LTRM :=$ true

      else

         $i := i + 1$

if not $LTRM$ then

$$r := r + \ell t\, h$$

$$h := h - \ell t\, h.$$

4. *Output:* $q_1, \ldots, q_m$ and r, with $g = \sum_i q_i f_i + r$ and $r = 0$ or no term of r divisible by any $\ell m\, f_i$.

We remark that the algorithm is guaranteed to terminate by Proposition 4.1.4, since at each pass h is replaced by a polynomial whose leading monomial is lower in the order.

For a given divisor sequence $\mathcal{F} = (f_1, \ldots, f_m)$ from $\mathcal{P}$ and polynomial $g \in \mathcal{P}$ denote by $r_{\mathcal{F}}(g)$ the remainder r obtained from the division algorithm upon division of g by $\mathcal{F}$.

Proposition 4.2.2 *Suppose that $I \neq 0$ is an ideal in $\mathcal{P}$ and that $\mathcal{F} = \{f_1, \ldots, f_m\}$ is a $\mathcal{G}$-basis for I. Form divisor sequences $\mathcal{F}_1$ and $\mathcal{F}_2$ that are permutations of $\mathcal{F}$. Take any $g \in \mathcal{P}$ and use the division algorithm above to divide g by $\mathcal{F}_1$ and by $\mathcal{F}_2$, obtaining remainders r_1 and r_2. Then $r_1 = r_2$.*

Proof. If $r_1 \neq r_2$ then $0 \neq r_1 - r_2 \in I$, and $\ell m(r_1 - r_2)$ is either one of the monomials of r_1 or of r_2, so it is not divisible by $\ell m\, f_i$ for any i. But $\mathcal{F}$ is a $\mathcal{G}$–basis , so *every* $\ell m\, f$, for every nonzero $f \in I$, is divisible by some $\ell m\, f_i$ by Proposition 4.1.1. Thus we have a contradiction, and $r_1 = r_2$. Δ

Because of Proposition 4.2.2 we have a well-defined notion of remainder $r_{\mathcal{F}}(g)$ of a polynomial g upon division by a $\mathcal{G}$–basis $\mathcal{F}$, independent of the ordering of $\mathcal{F}$ as a sequence. This remainder is sometimes referred to as the *normal form*, or the *reduction*, of g relative to $\mathcal{F}$.

If $\mathcal{F}$ is not a $\mathcal{G}$–basis for some ideal then the result of Proposition 4.2.2 may well fail; it is in fact easy to find examples of sets $\mathcal{F}$ for which permuted divisor sequences formed from $\mathcal{F}$ result in totally different remainders. It should perhaps be remarked that even if $\mathcal{F}$ is a $\mathcal{G}$–basis the quotients q_i produced by the division algorithm may (in fact usually do) change upon permutations of divisor sequences.

Proposition 4.2.3 *Suppose $I \neq 0$ is an ideal in $\mathcal{P}$ and $\mathcal{F} = \{f_1, \ldots, f_m\}$ is a $\mathcal{G}$–basis for I. If $g \in \mathcal{P}$ then $g \in I$ if and only if $r_{\mathcal{F}}(g) = 0$.*

Proof. ($\Leftarrow$) For some set $\{q_i\}$ of quotients we have $g = \sum_i q_i f_i \in I$.
($\Rightarrow$) Since $\mathcal{F}$ is a $\mathcal{G}$–basis and $g \in I$ we have $\ell m\, g \in \langle \ell m\, I \rangle = \langle \ell m\, \mathcal{F} \rangle$, so $\ell m\, g$ is divisible by some $\ell m\, f_i$ by Proposition 4.1.1. In the division algorithm g (renamed as h) is replaced by $h - cX^\alpha f_i$, for some c and α, which is also in I. Thus the condition $\ell m\, f_i \mid \ell m\, h$ holds true for some i at every stage of the algorithm, and r never receives $\ell t\, h$, *i.e.* r remains 0. $\triangle$

Because of Proposition 4.2.3 the division algorithm provides an effective test for ideal membership, provided we have a $\mathcal{G}$–basis for the ideal.

If $f, g \in \mathcal{P}$ are both nonzero define their *S-polynomial* (S for *syzygy*) to be

$$S(f,g) = (\ell c\, g)X^\alpha f - (\ell c\, f)X^\beta g,$$

where $X^\alpha \ell m\, f = X^\beta \ell m\, g$, with $|\alpha|$ and $|\beta|$ minimal in that respect. In plain language we multiply each of f and g minimally so the leading terms agree, then subtract to cancel them. Note that in fact $X^\alpha = LCM(\ell m\, f, \ell m\, g)/\ell m\, f$ and $X^\beta = LCM(\ell m\, f, \ell m\, g)/\ell m\, g$.

For example take $f = x^3 - 2xy + 3x$ and $g = 2x^2y - 3xy^2 + 6y$. Then $S(f,g) = 2yf - xg = 3x^2y^2 - 4xy^2$.

Observe that $S(f,f) = 0$, $S(g,f) = -S(f,g)$, and $S(af,bg) = abS(f,g)$ if $a,b \in K$. An easy calculation shows that if $\gamma, \delta \in \mathbb{N}^n$ then $S(X^\gamma f, X^\delta g) = X^\epsilon S(f,g)$, where $X^\epsilon = LCM(X^\gamma \ell m\, f, X^\delta \ell m\, g)/LCM(\ell m\, f, \ell m\, g)$.

The next proposition, which is easy but rather technical, indicates in terms of S–polynomials how leading terms can cancel in a combination of polynomials all having the same leading monomial.

Proposition 4.2.4 *Suppose $p_1, \ldots, p_k \in \mathcal{P}$, $\alpha \in \mathbb{N}^n$, and $\ell t\, p_i = a_i X^\alpha$ for all i. Set $f = \sum_{i=1}^k c_i p_i$, $c_i \in K$, and suppose that $\ell m\, f < X^\alpha$. Then there are coefficients $b_j \in K$ so that $f = \sum_{j=1}^{k-1} b_j S(p_j, p_{j+1})$.*

Proof. Set $q_i = a_i^{-1} p_i$, all i, so each q_i is monic, with $\ell t\, q_i = X^\alpha$, and $S(q_i, q_{i+1}) = q_i - q_{i+1} = (a_i a_{i+1})^{-1} S(p_i, p_{i+1})$. Since $\ell m\, f < X^\alpha$ we must have $\sum_{i=1}^k c_i a_i = 0$. Observe now that $f = \sum_i c_i p_i = c_1 a_1 (q_1 - q_2) + (c_1 a_1 + c_2 a_2)(q_2 - q_3) + \cdots + (c_1 a_1 + \cdots + c_{k-1} a_{k-1})(q_{k-1} - q_k)$, the last summand being correct since $c_1 a_1 + \cdots + c_{k-1} a_{k-1} = -c_k a_k$. Thus we may set $b_j = (c_1 a_1 + \cdots + c_j a_j)/(a_j a_{j+1})$, all j, and conclude that $f = \sum_{j=1}^{k-1} b_j S(p_j, p_{j+1})$. $\triangle$

The next theorem provides a characterization of Gröbner bases that is very important for computational purposes.

Theorem 4.2.5 (Buchberger) *Suppose $\mathcal{F} = (f_1, \ldots, f_m)$, with all $f_i \in \mathcal{P}$, and $I = \langle \mathcal{F} \rangle$. Then $\mathcal{F}$ is a $\mathcal{G}$-basis for I if and only if $r_{\mathcal{F}}(S(f_i, f_j)) = 0$ for all i and j.*

Proof. (See [6]; also see [1]) ($\Rightarrow$) Since $S(f_i, f_j) \in I$ we have $r_{\mathcal{F}}(S(f_i, f_j)) = 0$ by Proposition 4.2.3.

($\Leftarrow$) If $0 \neq f \in I$ we must show that $\ell m\, f \in \langle \ell m\, \mathcal{F} \rangle$. Since $f \in I$ we may write

$$f = \sum_i (\sum_j a_{ij} X^{\alpha_{ij}}) f_i \quad (*)$$

for some polynomials $\sum_j a_{ij}X^{\alpha_{ij}} \in \mathcal{P}$. Denote by γ the maximum exponent that occurs in the leading monomials of the summands $(\sum_j a_{ij}X^{\alpha_{ij}})f_i$; we may assume that the expression $(*)$ for f has been chosen so that γ is minimal. Observe that if $X^\gamma = \ell m\, f$ then $\ell m\, f \in \langle \ell m\, \mathcal{F}\rangle$ and the theorem is proved. Suppose then that $X^\gamma > \ell m\, f$, so that in $(*)$ some cancellation of leading terms has occurred. Write $f = g + h$, where g includes precisely those summands $(\sum_j a_{ij}X^{\alpha_{ij}})f_i$ having leading monomial X^γ and the leading monomials of the corresponding summands of h are lower in the order. Since the leading terms of g must cancel we may apply Proposition 4.2.4 and express g as a K–linear combination of S–polynomials of the form $S = S(X^{\alpha_{ij}}f_i, X^{\alpha_{kl}}f_k)$, which is equal to $X^\beta S(f_i, f_k)$ for some $\beta \in \mathbb{N}^n$ (depending on i, j, k, and l), as observed on page 73. Since $X^{\alpha_{ij}}f_i$ and $X^{\alpha_{kl}}f_k$ both have leading monomial X^γ, S must have a smaller leading monomial, as must $S(f_i, f_k)$. By assumption we may divide $S(f_i, f_k)$ by $\mathcal{F}$ and express it as $\sum_u q_u f_u$, since the remainder is 0, then multiply by X^β to obtain $S = \sum_u p_u f_u$, and by the nature of the division algorithm each summand $p_u f_u$ has $\ell m(p_u f_u) < X^\gamma$. But then we may replace each of the S-polynomials in the expression for g as a linear combination of them, and the resulting expression of f as $g + h$ contradicts the choice of γ as minimal, proving the theorem. Δ

Note that the condition in Theorem 4.2.5 can be checked in a finite number of steps. Even better, it can be used as the basis for an algorithm that constructs a $\mathcal{G}$–basis from an arbitrary ideal basis, which will now be outlined. The algorithm uses ordered ideal bases so as to be able to use the division algorithm in $\mathcal{P}$, although the ordering is no longer necessary when the process is complete.

Buchberger's Algorithm

1. *Input:* $\mathcal{F} = (f_1, \ldots, f_m) \subseteq \mathcal{P}$ [an ordered basis for the ideal I].

2. $\mathcal{G} := \mathcal{F}$, $t := 0$.

3. Repeat

   $t := t + 1$

   $H_t := \mathcal{G}$

   for $p \neq q$ in H_t do

   $r := r_{H_t}(S(p, q))$

   if $r \neq 0$ then $\mathcal{G} := \mathit{Append}(\mathcal{G}, r)$

   until $\mathcal{G} = H_t$.

4. *Output:* $\mathcal{G}$, a $\mathcal{G}$–basis for I.

It should be pointed out immediately that the algorithm as presented is in a very crude and inefficient form, chiefly to make clear its basic simplicity. It has been implemented many times, and versions are present in all the major computer algebra systems, in all cases with many refinements.

Note that *if* the process terminates then the resulting set $\mathcal{G}$ is guaranteed to be a $\mathcal{G}$–basis for I by Theorem 4.2.5.

If the process has not terminated after the $t^{\underline{th}}$ pass it is because it has produced some $r \in \mathcal{G} \setminus H_t$. Observe that then $\ell m\, r \notin \langle \ell m\, H_t \rangle$, for otherwise $\ell m\, r$ would be divisible by $\ell m\, f$ for some $f \in H_t$ by Proposition 4.1.1, and hence it should have been removed by the division algorithm. Thus as the process continues it

produces an ascending chain $\langle \ell m\, H_1 \rangle \subset \langle \ell m\, H_2 \rangle \subset \cdots$ of monomial ideals, and it must eventually terminate since $\mathcal{P}$ is Noetherian.

We have proved the next theorem.

Theorem 4.2.6 *If $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq \mathcal{P}$ and $I = \langle \mathcal{F} \rangle$ then $\mathcal{F}$ can be enlarged to a $\mathcal{G}$-basis $\mathcal{G}$ for I.*

A small example is in order; most of the details will be suppressed. Take $f_1 = xy - y + 2$, $f_2 = x^2 - x$, $\mathcal{F} = \{f_1, f_2\}$, and $I = \langle \mathcal{F} \rangle$, with graded lex order as usual. We set $H_1 = \mathcal{G} = \mathcal{F}$ and find that $r = r_{H_1}(S(f_1, f_2)) = 2x \neq 0$, so we set $f_3 = 2x$ and $\mathcal{G}$ becomes $\{f_1, f_2, f_3\}$, as does H_2. Next we find that $r = r_{H_2}(S(f_1, f_3)) = -2y+4 \neq 0$, we set $f_4 = -2y+4$ and $\mathcal{G} = H_3 = \{f_1, f_2, f_3, f_4\}$. Now, however, we find that $r = 0$ for all pairs f_i, f_j in H_3, so $\mathcal{G} = \{f_1, f_2, f_3, f_4\}$ is a $\mathcal{G}$–basis for I.

One drawback to the algorithm as above is that it tends to produce unnecessarily large $\mathcal{G}$-bases, but we shall see that it is not particularly difficult to remove superfluous elements.

Proposition 4.2.7 *Suppose $\mathcal{F}$ is a $\mathcal{G}$-basis for the ideal I in $\mathcal{P}$, $p \in \mathcal{F}$, and $\ell m\, p \in \langle \ell m(\mathcal{F} \setminus \{p\}) \rangle$. Then $\mathcal{F} \setminus \{p\}$ is also a $\mathcal{G}$-basis for I.*

Proof. Since $J = \langle \ell m(\mathcal{F} \setminus \{p\}) \rangle$ is a monomial ideal and $\ell m\, p \in J$ there is some $q \in \mathcal{F} \setminus \{p\}$ such that $\ell m\, q \,|\, \ell m\, p$. Thus their S–polynomial is $s = S(p, q) = ap - bX^\alpha q$ for some $a, b \in K$ and $\alpha \in \mathbb{N}^n$. Since $\mathcal{F}$ is a $\mathcal{G}$–basis $r_{\mathcal{F}}(s) = 0$ by Theorem 4.2.5. But $\ell m\, p > \ell m\, s$, so the result of the division algorithm is $s = \sum_i q_i f_i$, with $f_i \in \mathcal{F}$. However, the only f_i that appear must have $\ell m\, f_i \leq \ell m\, s < \ell m\, p$, and in particular p is not among them. Thus $p = a^{-1}(s + bX^\alpha q) \in \langle \mathcal{F} \setminus \{p\} \rangle$, and $\mathcal{F}' = \langle \mathcal{F} \setminus \{p\} \rangle$ is

an ideal basis for I. Clearly $\langle \ell m\, \mathcal{F}' \rangle = \langle \ell m\, \mathcal{F} \rangle = \langle \ell m\, I \rangle$, so $\mathcal{F}'$ is in fact a $\mathcal{G}$–basis for I. Δ

Note that the question of membership of $\ell m\, p$ in $\langle \ell m(\mathcal{F} \setminus \{p\}) \rangle$ is easily answered *via* Propositions 4.2.1 and 4.2.3.

Repeated application of Proposition 4.2.7 will produce a $\mathcal{G}$–basis $\mathcal{F}$ for I that is *minimal*, in the sense that $\ell m\, p \notin \langle \ell m(\mathcal{F} \setminus \{p\}) \rangle$ for all $p \in \mathcal{F}$. A minimal $\mathcal{G}$–basis $\mathcal{F}$ with leading coefficients adjusted so that every $p \in \mathcal{F}$ is monic is called a *reduced* $\mathcal{G}$–basis. Computer algebra systems typically produce reduced $\mathcal{G}$–bases.

To continue the example from above observe that $\ell m\, f_1 = \frac{1}{2} y f_3$ so $\ell m\, f_1 \in \langle \ell m(\mathcal{F} \setminus \{f_1\}) \rangle$, and likewise $\ell m\, f_2 \in \langle \ell m\, f_3, \ell m\, f_4 \rangle$, so $\{f_3, f_4\}$ is a $\mathcal{G}$–basis. The corresponding reduced $\mathcal{G}$–basis is $\{x, y - 2\}$.

The final proposition in this section is now a triviality; nevertheless it will prove useful in the next section.

Proposition 4.2.8 *If I is a nonzero ideal in $\mathcal{P}$ then $1 \in I$* (i.e. *$I = \mathcal{P}$*) *if and only if $\{1\}$ is a reduced $\mathcal{G}$–basis for I.*

4.3 Applications

We develop in this section some procedures depending on $\mathcal{G}$–bases that will be needed for the algorithm of Chapter 5.

If R is a commutative ring and I is an ideal in R recall that the *radical* of I is $rad\, I = \{r \in R : r^k \in I \text{ for some } k > 0 \text{ in } \mathbb{N}\}$.

Let us write $\overline{K}$ for an algebraic closure of the field K. If $\mathcal{F}$ is a set of polynomials in $\mathcal{P}$ then an *algebraic zero* of $\mathcal{F}$ is a point $c = (c_1, \ldots, c_n) \in \overline{K}^n$ for which $f(c) = 0$, all $f \in \mathcal{F}$. The *variety* of $\mathcal{F}$, denoted $Var(\mathcal{F})$, is the set of all algebraic zeros of

$\mathcal{F}$. Note that $Var(\mathcal{F}) = Var(\langle\mathcal{F}\rangle) = Var(rad\,\langle\mathcal{F}\rangle)$, and that if $\mathcal{F}_1 \subseteq \mathcal{F}_2$ then $Var(\mathcal{F}_1) \supseteq Var(\mathcal{F}_2)$.

We state next the celebrated *Hilbert Nullstellensatz*; for a proof see [20], page 33.

Theorem 4.3.1 *Suppose $\mathcal{F} \subseteq \mathcal{P}$ and $I = \langle\mathcal{F}\rangle$.*

i) If $Var(\mathcal{F}) = \emptyset$ then $1 \in I$.

ii) If $f \in \mathcal{P}$ and $f(c) = 0$ for all $c \in Var(\mathcal{F})$ then $f \in rad\,I$.

As an application of the Nullstellensatz the next theorem provides a testable characterization of elements in the radical of an ideal in $\mathcal{P}$.

Theorem 4.3.2 *Suppose $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq \mathcal{P}$, $I = \langle\mathcal{F}\rangle$, and $f \in \mathcal{P}$. Introduce a new indeterminate y, set $g = 1 - yf$, and set $\mathcal{F}' = \mathcal{F} \cup \{g\}$. Then $f \in rad\,I$ if and only if $1 \in \langle\mathcal{F}'\rangle \subseteq K[x_1, \ldots, x_n, y]$.*

Proof. ($\Rightarrow$) Say $f^k = \sum_i g_i f_i$, where $1 \leq k \in \mathbb{N}$; let us show that $Var(\mathcal{F}') = \emptyset$. Suppose $c = (c_1, \ldots, c_{n+1}) \in \overline{K}^{n+1}$ and that $f_i(c) = 0$, all $f_i \in \mathcal{F}$. Then also $f^k(c) = 0$, so $f(c) = 0$. But then $g(c) = 1 - c_{n+1}f(c) = 1 \neq 0$. Thus $1 \in \langle\mathcal{F}'\rangle$ by the Nullstellensatz.

($\Leftarrow$) Write $1 = \sum_i p_i(X, y)f_i + q(X, y)(1 - yf)$ for some p_i, $q \in K[X, y]$, and substitute $y = 1/f$ (in the field $K(X, y)$) to obtain $1 = \sum_i p_i(X, 1/f)f_i$. Multiply through by a sufficient power f^k to clear all denominators, obtaining $f^k = \sum_i h_i(X)f_i \in I$, hence $f \in rad(I)$. Δ

With Theorem 4.3.2 and Proposition 4.2.8 in hand the following test should be clear.

Test for Radical Containment

Given: $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq \mathcal{P}$ and $f \in \mathcal{P}$. Set $I = \langle \mathcal{F} \rangle$, let y be a new indeterminate, set $g = 1 - yf$, $\mathcal{F}' = \mathcal{F} \cup \{g\}$, and $Y = (x_1, \ldots, x_n, y)$. Then $f \in rad(I)$ if and only if $\{1\}$ is a reduced $\mathcal{G}$–basis for $\langle \mathcal{F}' \rangle$ relative to Y.

Theorem 4.3.3 *Suppose* $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq Homog(\mathcal{P}^+)$. *Then* $Var(\mathcal{F}) = \{0\}$ *if and only if* $rad\langle \mathcal{F} \rangle = \mathcal{P}^+$.

Proof. ($\Leftarrow$) Set $g_i = x_i \in rad\langle \mathcal{F} \rangle$, $1 \leq i \leq n$, and note that if $c = (c_1, \ldots, c_n) \in Var(\mathcal{F})$ then $g_i(c) = c_i = 0$, all i, *i.e.* $c = 0$.

($\Rightarrow$) It will suffice to show that each x_j is in $rad\langle \mathcal{F} \rangle$, since it is clear that $rad\langle \mathcal{F} \rangle \subseteq \mathcal{P}^+$. Let y be a new indeterminate, set $g = 1 - yx_j$, and set $\mathcal{F}' = \mathcal{F} \cup \{g\} \subseteq K[X, y]$. Any algebraic zero of $\mathcal{F}$ in $\overline{K}^{n+1}$ has the form $c = (0, \ldots, 0, c_{n+1})$, and then $g(c) = 1 - c_{n+1} \cdot 0 = 1$, so $Var(\mathcal{F}') = \emptyset$. By the Nullstellensatz $1 \in \langle \mathcal{F}' \rangle$, so we may write $1 = \sum_i p_i(X, y) f_i + q(X, y)(1 - yx_j)$ for some p_i, $q \in K[X, y]$. Substitute $y = 1/x_j$ (in the field $K(X, y)$) to obtain $1 = \sum_i p_i(X, 1/x_j) f_i$. Multiply through by a sufficient power x_j^k to clear all denominators, obtaining $x_j^k = \sum_i h_i(X) f_i \in \langle \mathcal{F} \rangle$, hence $x_j \in rad(\langle \mathcal{F} \rangle)$. $\triangle$

There is a small point to be made here that is not deep, but is slightly subtle, concerning the field of definition. The condition $Var(\mathcal{F}) = \{0\}$ in Theorem 4.3.3 depends not on K but, by the very definition of $Var(\mathcal{F})$, on the algebraic closure $\overline{K}$. Thus by the equivalence in the theorem the same is true for the condition

$rad\langle\mathcal{F}\rangle = \mathcal{P}^+$. Thus in determining whether that condition holds there is no loss of generality if the field is assumed to be algebraically closed.

Proposition 4.3.4 (See [3]) *Suppose that $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq \mathcal{P}$ is a $\mathcal{G}$-basis for $I = \langle\mathcal{F}\rangle$. Let V be the K-vector space $\mathcal{P}/I$, and write $\overline{f}$ for each element $f + I \in V$. Set $\mathcal{B} = \{\overline{u}: u \in Mon\mathcal{P}$ and $\ell m\, f_i \not| \, u,\ 1 \leq i \leq m\}$. Then $\mathcal{B}$ is a basis for V.*

Proof. The fact that $\mathcal{B}$ spans V is an easy consequence of the fact that $\overline{f} = \overline{r_{\mathcal{F}}(f)}$ for all $f \in \mathcal{P}$. Suppose that $\sum_i c_i\overline{u_i} = 0$ for some $c_i \in K$, $\overline{u_i} \in \mathcal{B}$. Thus $g = \sum_i c_i u_i \in I$, so $r_{\mathcal{F}}(g) = 0$ by Proposition 4.2.3. On the other hand it is clear from the definition of $\mathcal{B}$ and the nature of the division algorithm that $r_{\mathcal{F}}(g) = g$, since no $\ell m\, f_j$ divides any u_i, so $g = 0$, *i.e.* all $c_i = 0$. Δ

Corollary 4.3.5 *The K-dimension of $\mathcal{P}/I$ is finite if and only if for each i, $1 \leq i \leq n$, there is some $p \in \mathcal{F}$ and some $k_i \in \mathbb{N}$ with $\ell m\, p = x_i^{k_i}$.*

Proof. ($\Rightarrow$) If no power of x_i occurs as $\ell m\, p$, $p \in \mathcal{F}$, then the set $\{\overline{x_i^l}: l \in \mathbb{N}\}$ is linearly independent by the Proposition.
($\Leftarrow$) If $u \in \mathrm{Mon}\,\mathcal{P}$ and $\overline{u} \in \mathcal{B}$ then u must have the form $\prod x_i^{l_i}$, with all $l_i < k_i$, so $\mathcal{B}$ is finite. Δ

Note that the condition in the corollary must be independent of the choice of monomial order, since $dim_K\, \mathcal{P}/I$ does not depend on the order.

Theorem 4.3.6 *Suppose $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq \mathcal{P}$ and $I = \langle\mathcal{F}\rangle$. If $dim_K(\mathcal{P}/I)$ is finite then $Var(\mathcal{F})$ is a finite set.*

Proof. Let $\mathcal{G}$ be a $\mathcal{G}$-basis for I relative to lexicographic order, and note that $Var(\mathcal{G}) = Var(\mathcal{F})$. By Corollary 4.3.5 there are elements $p_i \in \mathcal{G}$ with $\ell m\, p_i = x_i^{k_i}$,

$1 \leq i \leq n$. All monomials in the terms of p_n must then be powers of x_n, since they must be $\leq x_n^{k_n}$ lexicographically, *i.e.* p_n must be a polynomial in x_n alone. Similarly, p_{n-1} is a polynomial in x_{n-1} and x_n, and in general p_j is a polynomial in $x_j, \ldots, x_n$. But now there are only finitely many solutions (for x_n) to $p_n = 0$, and for each of these in turn there are only finitely many solutions (for x_{n-1}) to $p_{n-1} = 0$, *etc.* The result follows. Δ

Corollary 4.3.7 *Suppose* $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq Homog(\mathcal{P}^+)$ *and* $I = \langle \mathcal{F} \rangle$, *a homogeneous ideal. If* $dim_K(\mathcal{P}/I)$ *is finite then* $Var(\mathcal{F}) = \{0\}$.

Proof. By the Theorem $Var(\mathcal{F})$ is finite. If $a \neq 0$ in $\overline{K}^n$ were in $Var(\mathcal{F})$, and if $c \in \overline{K}$, then $f(ca) = c^{deg\, f} f(a) = 0$, all $f \in \mathcal{F}$, so $Var(\mathcal{F})$ would be infinite. Δ

Although it won't be needed here it should be remarked that the converse of Theorem 4.3.6 is also true; one source for a proof is [7].

If I is a proper homogeneous ideal in $\mathcal{P}$ we say that I has *full radical* if $rad\, I = \mathcal{P}^+$.

The next test is now a consequence of Theorem 4.3.3 and Corollaries 4.3.5 and 4.3.7.

Test for Full Radical

Suppose $\mathcal{F} \subseteq \mathcal{P}^+$ is a $\mathcal{G}$–basis for a homogeneous ideal I in $\mathcal{P}$. If for each i, $1 \leq i \leq n$, there is some $p \in \mathcal{F}$ and some $k_i \in \mathbb{N}$ with $\ell m\, p = x_i^{k_i}$, then I has full radical, *i.e.* $rad\, I = \mathcal{P}^+$.

4.4 Module Membership

In this section we discuss how to determine whether a given polynomial is an element of a module generated by some set of polynomials.

Let $f_1, \ldots, f_n$ be a system of parameters and $B = K[f_1, \ldots, f_n]$. Consider the B–module $C = \sum_{i=1}^{k} g_i\, B$, where the g_i's are homogeneous polynomials, and suppose $f \in \mathcal{P}$, f homogeneous. We wish to determine whether $f \in C$.

If $f \in C$ then f can be written as a sum of terms of the form $c_i g_i f_1^{a_1} \cdots f_n^{a_n}$, where $\sum a_j + deg\ g_i = deg\ f$.

We therefore determine all such terms of the appropriate degree, form their sum and write the result as a combination of monomials in $x_1, \ldots, x_n$. It is then a matter of equating the coefficients of the right hand side with the coefficients of f. This will give us a system of linear equations over K. If this system has a solution then $f \in C$ and if there is no solution then we know that $f \notin C$. A small example will make this clear.

Let $f_1 = x_1 + x_2 + x_3 + x_4$, $f_2 = x_1^2 + x_2^2 + x_3^2 + x_4^2$, $f_3 = x_1x_2 + x_3x_4$, $f_4 = x_1x_3 + x_2x_4$, $g_1 = 1$, and $g_2 = x_1^3 + x_2^3 + x_3^3 + x_4^3$. Suppose we want to check whether $f = 6x_1x_2x_3 + 6x_1x_2x_4 + 6x_1x_3x_4 + 6x_2x_3x_4$ is in $C = \sum_{i=1}^{2} g_i K[f_1, f_2, f_3, f_4]$. Then we need to determine whether we can write

$$f = 1 \cdot p_1(f_1, f_2, f_3, f_4) \ + \ g_2 \cdot p_2(f_1, f_2, f_3, f_4). \qquad (*)$$

Since the degree of 1 is zero $p_1(f_1, f_2, f_3, f_4)$ must have degree 3 and since the degree of g_2 is three $p_2(f_1, f_2, f_3, f_4)$ must have degree 0. Thus

$$p_1 = c_1(f_1^3) + c_2(f_1f_2) + c_3(f_1f_3) + c_4(f_1f_4) \qquad \text{and} \qquad p_2 = c_5,$$

for coefficients c_i to be determined if f is to be in C.

Substitute into (∗), gather like terms, and equate coefficients to obtain the following system of linear equations.

$$\begin{array}{rcrcrcrcl}
c_1 & + & c_2 & & & & + & c_5 & = 0 \\
3c_1 & + & c_2 & + & c_3 & & & & = 0 \\
3c_1 & + & c_2 & & & + & c_4 & & = 0 \\
3c_1 & + & c_2 & & & & & & = 0 \\
6c_1 & & & + & c_3 & + & c_4 & & = 6
\end{array}$$

This system has a unique solution, namely, $c_1 = 1$, $c_2 = -3$, $c_3 = 0$, $c_4 = 0$, $c_5 = 2$. Thus $f = g_1 \cdot (f_1^3 - 3f_1f_2) + 2g_2 \in C$.

5. CALCULATING INVARIANTS

Our goal in this final chapter is an algorithm for the calculation of CM–bases for the algebra of invariants of a finite subgroup of $GL(V)$ and an implementation of the algorithm.

5.1 Invariants and Geometry

We begin by tying together some ideas from Chapters 3 and 4 connecting the algebra of invariants with varieties and radicals. As always G is a finite subgroup of $GL(V)$ and $\mathcal{I} \subseteq \mathcal{P}$ is its algebra of polynomial invariants.

Proposition 5.1.1 *If $\mathcal{J} = \langle \mathcal{I}^+ \rangle_{\mathcal{P}}$, the ideal in $\mathcal{P}$ generated by $Homog(\mathcal{I}^+)$, then $rad\,\mathcal{J} = \mathcal{P}^+$, and consequently $Var(\mathcal{I}^+) = \{0\}$.*

Proof. Clearly $rad\,\mathcal{J} \subseteq \mathcal{P}^+$. If $f \in \mathcal{P}^+$ then as in the proof of Proposition 3.1.5 we have

$$f^\gamma = \sum_k (-1)^{k+1} \sigma_k(T_1 f, \ldots, T_\gamma f) f^{\gamma-k} \in \mathcal{J},$$

where $\gamma = |G|$ and the σ_k are the elementary symmetric polynomials. Thus $f \in rad\,\mathcal{J}$, and $Var(\mathcal{I}^+) = \{0\}$ by Theorem 4.3.3. △

Theorem 5.1.2 *If $\mathcal{F} = \{f_1, \ldots, f_k\} \subseteq Homog(\mathcal{I}^+)$ set $B = K[f_1, \ldots, f_k] \subseteq \mathcal{I}$. Then $\mathcal{I}$ is a finitely generated B-module if and only if $Var(\mathcal{F}) = \{0\}$.*

Proof. (See [17]) ($\Rightarrow$) Recall that $\mathcal{I}$ is integral over B by Proposition 2.5.1. If $g \in \mathcal{I}$ is homogeneous of degree d let

$$g^m + b_{m-1} g^{m-1} + \cdots + b_1 g + b_0 = 0, \qquad (*)$$

all $b_i \in B$, be an integrality relation for g over B of minimal degree m. Let us show that every b_i has zero constant term. For each $b \in B$ and $\ell \in \mathbb{N}$ write $(b)_\ell$ for the degree ℓ component of b. If some b_j had nonzero constant term c_j then considering the terms of degree jd in $(*)$ we would have

$$c_j g^j + (b_{j-1})_d g^{j-1} + \cdots + (b_1)_{(j-1)d} g + (b_0)_{jd} = 0,$$

with each coefficient in B since B is graded. Dividing by c_j we contradict the minimality of m. It now follows from $(*)$ that any algebraic zero $v \in \overline{K}^n$ of $\mathcal{F}$ is a zero of each b_i, hence of g^m, and hence of g. Thus $Var(\mathcal{F}) \subseteq Var(\mathcal{I}^+)$, which is $\{0\}$ by Proposition 5.1.1.

$(\Leftarrow)$ Let $\mathcal{J} = \langle \mathcal{F} \rangle_{\mathcal{P}}$, so $rad\, \mathcal{J} = \mathcal{P}^+$ by Theorem 4.3.3. It is an elementary fact (see *e.g.* [24], page 83) that $(\mathcal{I}^+)^d \subseteq (\mathcal{P}^+)^d \subseteq \mathcal{J}$ for some $d \in \mathbb{N}$. By Theorem 3.1.1 there is an integrity basis $\{h_1, \ldots, h_r\} \subseteq Homog(\mathcal{I}^+)$ for $\mathcal{I}$, so $\mathcal{I} = K[h_1, \ldots, h_r]$. Denote by μ the maximum of the degrees of the h_i and set $m = d\mu$. If $\ell \geq m$ and $g \in \mathcal{I}_\ell$ then g is a K–linear combination of monomials $h_1^{a_1} \cdots h_r^{a_r}$, with $\sum_i a_i \geq d$, so $g \in (\mathcal{I}^+)^d \subseteq \mathcal{J}$, *i.e.* $\mathcal{I}^{[m]} \subseteq \mathcal{J}$ (recall that $\mathcal{I}^{[m]}$ denotes $\oplus_{d \geq m} \mathcal{I}_d$). Let $\{g_1, \ldots, g_s\}$ be a K–basis for $\oplus_{d=0}^{m-1} \mathcal{I}_d$. We will show that $\mathcal{I} = \sum_j g_j B$ by showing inductively that each $\mathcal{I}_\ell \subseteq \sum_j g_j B$. Of course $\oplus_{d=0}^{m-1} \mathcal{I}_d \subseteq \sum_j g_j B$, which is more than enough to start the induction. If $g \in \mathcal{I}_\ell$, with $\ell \geq m$, then as shown above $g \in \mathcal{J}$, and we may write $g = \sum_i p_i f_i$, with each p_i homogeneous in $\mathcal{P}$. Thus $g = \mathcal{M} g = \sum_i (\mathcal{M} p_i) f_i$, and each $q_i = \mathcal{M} p_i$ has degree $\ell - deg\, f_i < \ell$, so by induction each $q_i \in \sum_j g_j B$, and hence $g \in \sum_j g_j B$. $\triangle$

5.2 The Algorithm

In this section we give an algorithm for finding a Cohen-Macaulay basis for the invariant algebra $\mathcal{I}$ of a finite group $G \leq GL_n(K)$. The algorithm first determines a sequence $\mathcal{F} = (f_1, \ldots, f_n)$ of free generators and then a sequence $\mathcal{G} = (g_1, \ldots, g_m)$ of transient generators. Thus we will be able to express $\mathcal{I}$ as a free B-module, where $B = K[f_1, \ldots, f_n]$, *i.e.* $\mathcal{I} = \sum_{i=1}^{m} g_i B$ as noted at the end of Chapter 2.

By Proposition 1.1.3 the average of a polynomial is an invariant. Thus we can use the set of averaged monomials as a source of invariants. We start with a set of monomials, average them one by one, and check to see whether each average increases the radical and thus qualifies as a new generator. We do this by using the test for radical containment discussed in Chapter 4. When we have at least n generators we check whether we have full radical by using the test for full radical, also discussed in Chapter 4. This part of the algorithm is based on a paper of Sturmfels and White (see [30]).

Once we have a set of free generators we continue to average monomials and check whether each average is contained in the module over B (as above) with basis those transients previously obtained. For that we use the test for module membership discussed in Chapter 4.

The algorithm follows.

An Algorithm for Finding a CM–basis

1. *Input:* Elements of a finite group $G \leq GL_n(K)$ and degrees for free generators.

2. *Initialize:* $\mathcal{F} := [\,]$, $g_1 := 1$, $\mathcal{G} := [g_1]$, $h := 1$, $i := 0$.

3. *Repeat:* $i := i + 1$ and generate monomial $M[i]$ until average$(M[i]) \neq 0$ *and* average$(M[i]) \notin Rad\langle \mathcal{F} \rangle$.

4. $\mathcal{F} := \mathcal{F} \cup \{\text{average}(M[i])\}$.

   If $|\mathcal{F}| < n$ go to 3.

   If $|\mathcal{F}| \geq n$ *and* $Rad\langle \mathcal{F} \rangle \neq \mathcal{P}^+$ go to 3.

5. If $|\mathcal{F}| > n$ then for j from $|\mathcal{F}|$ to 1 by -1 do

   if $f_j \in Rad\langle \mathcal{F} \setminus \{f_j\} \rangle$ then $\mathcal{F} := \mathcal{F} \setminus \{f_j\}$.

6. If $|\mathcal{F}| > n$ then normalize to obtain $|\mathcal{F}| = n$.

7. Determine the number $m = |G|^{-1} \prod_{i=1}^{n} deg\ f_i$ of transient generators, the degrees of the transients, and the number of transients of each degree.

8. $i := 1$.

9. If $h = m$ go to 12.

10. If average$(M[i]) \notin \sum_{j=1}^{h} g_j K[f_1, \ldots, f_n]$ then

    $h := h + 1$;

    $g_h :=$ average$(M[i])$;

    $\mathcal{G} := \mathcal{G} \cup \{g_h\}$.

11. $i := i + 1$; go to 9.

12. *Output:* $(\mathcal{F}; \mathcal{G})$, a CM–basis for G.

Why does the algorithm give a Cohen–Macaulay basis for G? First of all, the set $\mathcal{F}$ of free generators that is obtained has cardinality n and it gives us full

radical, *i.e.* $Rad\langle\mathcal{F}\rangle = \mathcal{P}^+$. Thus $Var(\mathcal{F}) = \{0\}$ and $\mathcal{I}$ is a finitely generated $K[f_1,\ldots,f_n]$–module by Theorem 5.1.2. Thus $\mathcal{F}$ is a system of parameters, as required.

Once we have the set of free generators we then determine the number of transient generators, as well as the degree of each. A transient generator, g_i, is only added if it is of the correct degree and if it is not contained in the module over B with basis $(g_1, g_2, \ldots, g_{i-1})$. We are guaranteed at the end that our output is a CM–basis since it has the correct Molien series.

Occasionally we may need more than n generators to obtain full radical. When this happens we carry out Step 5 of the algorithm and try to obtain the correct number of free generators. If after carrying out Step 5 we still have more than n generators then we must normalize to obtain the correct number.

The normalization algorithm is based on the proof of Theorem 2.5.3. The basic idea is to form n random linear combinations of the generators which give full radical. However, in order to maintain homogenity we must first transform the sequence of generators into a sequence of polynomials all of whose degrees are the same. This is easily done by finding the least common multiple of the degrees of the generators and then raising each generator to the appropriate power to achieve that degree; the radical of the generated ideal is unchanged.

The normalization algorithm follows.

Normalization Algorithm

1. *Input*: $\mathcal{H} := \{h_1,\ldots,h_k\}$, $n :=$ dim.

2. *Initialize*: $\mathcal{H}^* := \{\}$.

3. *Determine*: m:= *lcm* of the degrees of h_i's.

4. For i from 1 to k do

$$h_i^* := (h_i)^{m/deg\ h_i};$$

$$\mathcal{H}^* := \mathcal{H}^* \cup \{h_i^*\}.$$

5. $\mathcal{L} := \{\}$.

For i from 1 to n do

$$\ell_i := a_{i1}h_1^* + a_{i2}h_2^* + \cdots + a_{ik}h_k^*$$

(a random linear combination of h_i^*s)

$$\mathcal{L} := \mathcal{L} \cup \{\ell_i\}.$$

6. If $\mathcal{L}$ does not give full radical go to 5.

7. $\mathcal{F} := \mathcal{L}$.

5.3 Implementing the Algorithm

It should be noted first that the algorithm as currently implemented requires that the field be restricted to the rational numbers. The algorithm is in fact correct for any field of characteristic zero but the implementation uses the *Maple* software package and currently this package has some difficulties with polynomial algebra involving irrational coefficients.

The algorithm as presented in Section 2 is very basic and somewhat redundant. When one actually implements the algorithm there are a number of steps that can be taken to make the algorithm more efficient. We discuss some of these strategies here.

In Step 1 we input the elements of a finite group $G \leq GL_n(K)$. In our implementation we find generators for the finite group G and use the software package

GAP [25] to generate all the elements of the group (see Appendix A for the GAP program 'gengroup'). These elements are then written to a file and in Step 1 *Maple* simply reads this file.

In Step 1 we also input the degrees for the free generators. For certain groups we know the degrees of the free generators. However for many groups we do not have this information. We can always use the numbers $1, 2, \ldots, \gamma$, where γ is the order of the group, as possible degrees for the free generators. For large groups this tends to entail checking many more monomials than needed. We can often simplify this step by looking at a rational form of the Molien series.

Recall that if $(f_1, \ldots, f_n; g_1, \ldots, g_m)$ is a CM–basis for a finite group G then the Molien series can be represented as

$$\Phi(t) = \frac{\sum_{i=1}^{m} t^{e_i}}{\prod_{j=1}^{n}(1 - t^{d_i})},$$

where e_i = degree g_i, d_j = degree f_j. Thus by first computing some form of the Molien series as a rational function we can get an idea of what the possible degrees of the free generators might be. Knowing this we may then consider only monomials of those degrees. If our conjecture of the possible degrees is incorrect (*e.g.* if we leave out the degree of a free generator) then the algorithm will tell us that we have only a partial CM–basis .

It should be noted here that not all rational forms of the Molien series correspond to Cohen-Macaulay bases. Later we will look at an example that illustrates a rational form of the Molien series that does not correspond to a CM–basis .

Working with only a few degrees for monomials tends to improve the time of the algorithm, especially when we are dealing with larger groups.

Different monomials may have the same average. Thus if we have already checked whether a particular average is in the radical of the ideal generated by

the previous f's we do not wish to waste time by checking this again if the same average should re–appear. To prevent this we keep track of all nonzero averages.

If Step 6 is implemented, then we need to apply the normalization algorithm (see above). The implementation of this algorithm can also be simplified. We start with a set H that contains $k > n$ basic invariants which give full radical. We then form a new set H^* which contains k invariants all of the same degree. In Step 5 of the normalization algorithm we form a new set $\mathcal{L}$ which contains n polynomials, each a random linear combination of the k elements in H^*. At this point we check to see whether or not $\mathcal{L}$ gives full radical. Checking whether a set gives full radical is very computer intensive to begin with and since the degrees of the elements of $\mathcal{L}$ have been increased to be equal it takes even more time. To simplify this, when we actually find l_i's, rather than taking a random linear combination of all k elements of H^*, instead we randomly pick two elements of H^* and then randomly either add or subtract them. We do this n times and then check whether we have full radical. If so, the result is our set $\mathcal{F}$ of free generators. If not, then we form a new set $\mathcal{L}$ and try again. It should be noted here that we know of no examples where the normalization algorithm is ever needed.

In Step 7 we determine the number of transient generators m where $m = |G|^{-1} \prod_{i=1}^{n} deg\ f_i$. We determine the degrees of the transient generators and the number of each degree by using the rational form of the Molien series. We calculate the Molien series and multiply it by the polynomial $\prod_{i=1}^{n}(1-t^{d_i})$ where the d_i's are the degrees of the free generators. This gives us the polynomial $t^{e_1}+t^{e_2}+\cdots+t^{e_m}$ from which we can casily determine the degrees e_i of the transient generators and the number of each degree.

Step 8 of the algorithm sets the counter i back to one. Thus once we have our

set $\mathcal{F}$ of free generators and are ready to work on finding the set $\mathcal{G}$ of transient generators, we start again with the very first monomial. We can save considerable time here by noticing two things. First, any g will be a nonzero average of a monomial and second, it cannot be an f. Thus, instead of starting all over with monomials we simply first check whether any of the nonzero averages (that are not f's) are g's. If we have checked all of these and yet do not have the correct number of transient generators then we continue to generate and average monomials but only from the point where we left off when determining the free generators and we only look at those degrees that correspond to degrees of g's found in Step 7.

In Step 10 we begin to find the transient generators. To do this we need to check whether the average of a monomial is an element of $\sum_{j=1}^{h} g_j K[f_1, \ldots, f_n]$ where the g_j's are the transient generators found thus far. Recall that the f_i's and g_j's are all homogeneous polynomials. Thus to determine the module membership of the average of a monomial we simply need to determine whether there is a solution to a system of linear equations as discussed in Chapter 4. If there is no solution when we try to solve the system of equations then the polynomial we are checking is added as a new transient generator.

As stated in the algorithm, we continue to check averaged monomials as possible transient generators until we have the correct number of transient generators. When this happens then we have a Cohen–Macaulay basis.

See Appendix C for a copy of the program 'CMbasis' which is an implementation of the algorithm in *Maple* and Appendix D for a sample of the output of the program.

5.4 Examples

Example 1 - $C_2 \times C_4$

We mentioned in Section 3 that not all rational forms of the Molien series correspond to Cohen-Macaulay bases. Let us look at an example illustrating this.

Consider the group $C_2 \times C_4$ generated by

$$a = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

If we calculate the Molien series for this group we get

$$\Phi(t) \;=\; 1 + 4t^2 + 11t^4 + 24t^6 + 45t^8 + 76t^{10} + \cdots \;=\; \frac{1+t^4}{(1-t^2)^4}.$$

One would be tempted to say therefore that the group should have a CM–basis that consists of 4 free generators all of degree two and 2 transient generators, 1 of degree zero and 1 of degree four. However, this is not the case. Although the coefficient 4 of t^2 in the Molien series tells us that there are 4 independent invariants of degree 2, no sequence of 4 degree 2 invariants gives full radical. A sequence $\mathcal{F}$ of free generators is $\mathcal{F} = (x_1^2,\ x_2^2,\ x_3^2 + x_4^2,\ x_3^4 + x_4^4)$ and we have 3 f's of degree two and 1 of degree four. The rational form of the Molien series corresponding to this situation is

$$\Phi(t) = \frac{1 + t^2 + t^4 + t^6}{(1-t^2)^3(1-t^4)}.$$

We therefore should have 4 g's; 1 of degree zero, 1 of degree two, 1 of degree four and 1 of degree six. A CM–basis is

$$(f_1 = x_1^2,\ f_2 = x_2^2,\ f_3 = x_3^2 + x_4^2,\ f_4 = x_3^4 + x_4^4;$$

$$g_1 = 1,\ g_2 = x_1x_2,\ g_3 = x_3^3x_4 - x_3x_4^3,\ g_4 = x_1x_2x_3^3x_4 - x_1x_2x_3x_4^3).$$

Example 2 - Quaternions

Due to the order in which the f's are obtained we may need more than n f's to achieve full radical. If this happens then our sequence of f's is algebraically dependent and cannot be a sequence of free generators. We must then implement Step 5 of the algorithm and try to see whether we can eliminate some f's and still maintain full radical. An example for which this happens is the degree 4 representation of the quaternion group of order 8 generated by

$$a = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

The Molien series for this group is

$$\Phi(t) \;=\; 1 + 2t^2 + 11t^4 + 20t^6 + 45t^8 + \cdots \;=\; \frac{1 + 6t^4 + t^8}{(1-t^2)^2(1-t^4)^2}.$$

After completing Step 4 of the algorithm the sequence of generators which gives full radical is

$$\mathcal{F} = (x_1^2 + x_2^2 + x_3^2 + x_4^2,\ x_1x_4 + x_2x_3,\ x_1^4 + x_2^4 + x_3^4 + x_4^4,$$

$$x_1^3x_2 - x_1x_2^3 - x_3^3x_4 + x_3x_4^3,\ x_1^3x_3 - x_1x_3^3 - x_2^3x_4 + x_2x_4^3).$$

However, in Step 5 we eliminate $x_1^4 + x_2^4 + x_3^4 + x_4^4$ and thus obtain

$$\mathcal{F} = (x_1^2 + x_2^2 + x_3^2 + x_4^2,\ \ x_1x_4 + x_2x_3,\ x_1^3x_2 - x_1x_2^3 - x_3^3x_4 + x_3x_4^3,$$

$$x_1^3x_3 - x_1x_3^3 - x_2^3x_4 + x_2x_4^3)$$

which has the correct number of f's. We then go on to obtain a CM-basis that has 4 free generators and 8 transient generators.

CM-basis

$f_1 = x_1^2 + x_2^2 + x_3^2 + x_4^2$, $f_2 = x_1x_4 + x_2x_3$, $f_3 = x_1^3x_2 - x_1x_2^3 - x_3^3x_4 + x_3x_4^3$,

$f_4 = x_1^3x_3 - x_1x_3^3 - x_2^3x_4 + x_2x_4^3$; $g_1 = 1$, $g_2 = x_1^4 + x_2^4 + x_3^4 + x_4^4$,

$g_3 = x_1^2x_2x_3 + x_1x_2^2x_4 + x_1x_3^2x_4 + x_2x_3x_4^2$, $g_4 = x_1^2x_3x_4 - x_1x_2x_3^2 + x_1x_2x_4^2 - x_2^2x_3x_4$,

$g_5 = x_1^2x_2x_4 - x_1x_2^2x_3 + x_1x_3x_4^2 - x_2x_3^2x_4$, $g_6 = x_1^2x_3^2 + x_2^2x_4^2$,

$g_7 = x_1^2x_2^2 + x_3^2x_4^2$, $g_8 = x_1^8 + x_2^8 + x_3^8 + x_4^8$

Example 3 - C_3

In calculating a CM–basis for a finite group both the representation and its dimension are crucial. As might be expected, different dimensions, and therefore different representations, can give very different bases. For example, consider the cyclic group C_3. We will compare a 2-dimensional, a 3-dimensional, and a 5-dimensional representation of C_3.

C_3 - 2 Dimensional

Generator: $a = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, the companion matrix of $1 + x + x^2$.

Molien series:

$$\Phi(t) = \frac{1 + t^3}{(1 - t^2)(1 - t^3)}$$

CM-basis

$f_1 = x_1^2 - x_1x_2 + x_2^2$, $f_2 = x_1^2x_2 - x_1x_2^2$; $g_1 = 1$, $g_2 = x_1^3 - 3x_1x_2^2 + x_2^3$

C_3 - 3 Dimensional

Generator: $a = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, the permutation representation of a 3–cycle.

Molien series:

$$\Phi(t) = \frac{1 + t^3}{(1 - t)(1 - t^2)(1 - t^3)}$$

CM-basis

$f_1 = x_1 + x_2 + x_3, \quad f_2 = x_1^2 + x_2^2 + x_3^2, \quad f_3 = x_1^3 + x_2^3 + x_3^3;$

$g_1 = 1, \quad g_2 = x_1^2 x_3 + x_1 x_2^2 + x_2 x_3^2$

The following 5–dimensional representation of C_3 is the direct sum of the 2–dimensional and 3–dimensional representations above.

C_3 - 5 Dimensional

Generator: $a = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$

Molien series:

$$\Phi(t) = \frac{1 + 2t^2 + 6t^3 + 2t^4 + t^6}{(1-t)(1-t^2)^2(1-t^3)^2}$$

CM-basis

$f_1 = x_3 + x_4 + x_5, \quad f_2 = x_1^2 - x_1 x_2 + x_2^2, \quad f_3 = x_3^2 + x_4^2 + x_5^2,$

$f_4 = x_1^2 x_2 - x_1 x_2^2, \quad f_5 = x_3^3 + x_4^3 + x_5^3; \quad g_1 = 1,$

$g_2 = x_1 x_3 - x_1 x_4 + x_2 x_4 - x_2 x_5, \quad g_3 = x_1 x_5 - x_2 x_5 + x_2 x_3 - x_1 x_4,$

$g_4 = x_1^3 - 3x_1^2 x_2 + x_2^3, \quad g_5 = x_4 x_1^2 - 2x_4 x_1 x_2 + x_4 x_2^2 + x_2^2 x_5 + x_1^2 x_3,$

$g_6 = x_1^2 x_5 - 2x_1 x_2 x_5 + x_2^2 x_5 + x_3 x_2^2 + x_4 x_1^2, \quad g_7 = x_1 x_4^2 - x_2 x_4^2 + x_2 x_5^2 - x_1 x_3^2,$

$g_8 = x_4 x_1 x_5 - x_2 x_4 x_5 + x_2 x_5 x_3 - x_1 x_3 x_4, \quad g_9 = x_3^2 x_5 + x_3 x_4^2 + x_4 x_5^2,$

$g_{10} = x_1^2 x_3 x_5 - x_1 x_2 x_3 x_4 - x_1 x_2 x_3 x_5 + x_1 x_2 x_4 x_5 + x_2^2 x_3 x_4,$

$g_{11} = x_1^2 x_3^2 - x_1 x_2 x_3^2 - x_1 x_2 x_4^2 + x_1 x_2 x_5^2 + x_2^2 x_4^2,$

$g_{12} = x_1^3 x_3^2 x_5 - x_1^2 x_2 x_3^2 x_5 + x_1^2 x_2 x_3 x_4^2 - 2x_1 x_2^2 x_3 x_4^2 - x_1 x_2^2 x_4 x_5^2 + x_2^3 x_3 x_4^2$

Example 4 - Sym(4)

In the previous example we saw how representations of different dimensions give very different CM–bases. It is also true that different representations (in the same dimension) can give very different CM–bases.

The group $Sym(4)$ has exactly two inequivalent irreducible 3–dimensional representations. Note that the representations of the groups are not very different in appearance and yet the CM–bases are very different.

The first representation is a reflection representation and thus there are no nontrivial transient generators (see *e.g.* [28]).

Generators: $a = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}$ and $b = \begin{pmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Molien series:

$$\Phi(t) = \frac{1}{(1-t^2)(1-t^3)(1-t^4)}$$

CM–basis

$f_1 = x_1^2 - x_1x_2 + x_2^2 - x_2x_3 + x_3^2, \quad f_2 = x_1^2x_2 - x_1x_2^2 + x_2^2x_3 - x_2x_3^2,$

$f_3 = x_1^4 - 2x_1^3x_2 + 3x_1^2x_2^2 - 2x_1x_2^3 + x_2^4 - 2x_2^3x_3 + 3x_2^2x_3^2 - 2x_2x_3^3 + x_3^4; \quad g_1 = 1$

The second representation is not a reflection representation and requires one nontrivial transient generator of degree 9.

Generators: $a = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}$ and $b = \begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$

Molien series:

$$\Phi(t) = \frac{1+t^9}{(1-t^2)(1-t^4)(1-t^6)}$$

CM-basis

$f_1 = x_1^2 - x_1x_2 + x_2^2 - x_2x_3 + x_3^2,$

$f_2 = x_1^4 - 2x_1^3x_2 + 3x_1^2x_2^2 - 2x_1x_2^3 + x_2^4 - 2x_2^3x_3 + 3x_2^2x_3^2 - 2x_2x_3^3 + x_3^4,$

$f_3 = 2x_1^6 - 6x_1^5x_2 + 15x_1^4x_2^2 - 20x_1^3x_2^3 + 15x_1^2x_2^4 - 6x_1x_2^5 + 2x_2^6 - 6x_2^5x_3 + 15x_2^4x_3^2 - 20x_2^3x_3^3 + 15x_2^2x_3^4 - 6x_2x_3^5 + 2x_3^6;$

$g_1 = 1,$

$g_2 = 2x_1^7x_2^2 - 4x_1^7x_2x_3 - 7x_1^6x_2^3 + 14x_1^6x_2^2x_3 + 5x_1^5x_2^4 - 4x_1^5x_2^3x_3 - 18x_1^5x_2^2x_3^2 + 12x_1^5x_2x_3^3 + 5x_1^4x_2^5 - 25x_1^4x_2^4x_3 + 45x_1^4x_2^3x_3^2 - 30x_1^4x_2^2x_3^3 - 7x_1^3x_2^6 + 26x_1^3x_2^5x_3 - 30x_1^3x_2^4x_3^2 + 30x_1^3x_2^2x_3^4 - 12x_1^3x_2x_3^5 + 2x_1^2x_2^7 - 7x_1^2x_2^6x_3 + 30x_1^2x_2^4x_3^3 - 45x_1^2x_2^3x_3^4 + 18x_1^2x_2^2x_3^5 + 7x_1x_2^6x_3^2 - 26x_1x_2^5x_3^3 + 25x_1x_2^4x_3^4 + 4x_1x_2^3x_3^5 - 14x_1x_2^2x_3^6 + 4x_1x_2x_3^7 - 2x_2^7x_3^2 + 7x_2^6x_3^3 - 5x_2^5x_3^4 - 5x_2^4x_3^5 + 7x_2^3x_3^6 - 2x_2^2x_3^7$

Example 5 - Irreducible Weyl Groups

The examples thus far have been very small groups. What happens when one applies the algorithm to larger groups? For a nice set of examples consider the irreducible Weyl groups A_4, B_4, D_4, and F_4. The groups B_4, D_4, and F_4 all have faithful orthogonal rational representations of degree 4; A_4, however, does not, so for A_4 we have used the natural root representation. These are all reflection representations and thus a CM–basis for each will consist of a set of free generators along with $g_1 = 1$. We look at each of these groups and for A_4, B_4, and D_4 also their rotation subgroups. In each case, the order of the rotation subgroup is one-half the order of the group and thus by 3.2.2 the CM–basis for the rotation subgroup will be the CM–basis for the group with one additional transient generator. The rotation subgroup for F_4 requires a transient generator of degree 24 which causes memory problems for *Maple* and thus is presently beyond the scope of the implementation.

A_4 - Order 120 - Root Representation

Generators:

$$a = \begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$c = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

Molien series:

$$\Phi(t) = \frac{1}{(1-t^2)(1-t^3)(1-t^4)(1-t^5)}$$

CM-basis

$f_1 = x_1^2 - x_1x_2 + x_2^2 - x_2x_3 + x_3^2 - x_3x_4 + x_4^2,$

$f_2 = x_1^2x_2 - x_1x_2^2 + x_2^2x_3 - x_2x_3^2 + x_3^2x_4 - x_3x_4^2,$

$f_3 = x_1^4 - 2x_1^3x_2 + 3x_1^2x_2^2 - 2x_1x_2^3 + x_2^4 - 2x_2^3x_3 + 3x_2^2x_3^2 - 2x_2x_3^3 + x_3^4 - 2x_3^3x_4 + 3x_3^2x_4^2 - 2x_3x_4^3 + x_4^4,$

$f_4 = x_1^4x_2 - 2x_1^3x_2^2 + 2x_1^2x_2^3 - x_1x_2^4 + x_2^4x_3 - 2x_2^3x_3^2 + 2x_2^2x_3^3 - x_2x_3^4 + x_3^4x_4 - 2x_3^3x_4^2 + 2x_3^2x_4^3 - x_3x_4^4;$

$g_1 = 1$

A_4 - Rotation Subgroup - Order 60

Generators: ab, bc, cd

Molien series:

$$\Phi(t) = \frac{1+t^{10}}{(1-t^2)(1-t^3)(1-t^4)(1-t^5)}$$

CM-basis

$f_1,\ f_2,\ f_3,\ f_4,$ and $g_1 = 1$ as above and $g_2 = 6x_1^{10} - 30x_1^9x_2 + 90x_1^8x_2^2 - 42x_1^8x_2x_3 +$
$42x_1^8x_3^2 - 42x_1^8x_3x_4 + 42x_1^8x_4^2 - 180x_1^7x_2^3 + 169x_1^7x_2^2x_3 - 2x_1^7x_2^2x_4 - 171x_1^7x_2x_3^2 +$
$174x_1^7x_2x_3x_4 - 168x_1^7x_2x_4^2 + 2x_1^7x_3^3 - 3x_1^7x_3^2x_4 - 3x_1^7x_3x_4^2 + 2x_1^7x_4^3 + 270x_1^6x_2^4 - 406x_1^6x_2^3x_3 +$
$7x_1^6x_2^3x_4 + 453x_1^6x_2^2x_3^2 - 426x_1^6x_2^2x_3x_4 + 405x_1^6x_2^2x_4^2 - 87x_1^6x_2x_3^3 + 93x_1^6x_2x_3^2x_4 -$
$72x_1^6x_2x_3x_4^2 - 7x_1^6x_2x_4^3 + 40x_1^6x_3^4 - 80x_1^6x_3^3x_4 + 120x_1^6x_3^2x_4^2 - 80x_1^6x_3x_4^3 + 40x_1^6x_4^4 -$
$306x_1^5x_2^5 + 622x_1^5x_2^4x_3 - 5x_1^5x_2^4x_4 - 745x_1^5x_2^3x_3^2 + 638x_1^5x_2^3x_3x_4 - 627x_1^5x_2^3x_4^2 + 237x_1^5x_2^2x_3^3 -$
$237x_1^5x_2^2x_3^2x_4 + 234x_1^5x_2^2x_3x_4^2 + 9x_1^5x_2^2x_4^3 - 110x_1^5x_2x_3^4 + 216x_1^5x_2x_3^3x_4 - 348x_1^5x_2x_3^2x_4^2 +$
$232x_1^5x_2x_3x_4^3 - 120x_1^5x_2x_4^4 - 4x_1^5x_3^5 + 10x_1^5x_3^4x_4 - 4x_1^5x_3^3x_4^2 - 4x_1^5x_3^2x_4^3 + 10x_1^5x_3x_4^4 -$
$4x_1^5x_4^5 + 270x_1^4x_2^6 - 707x_1^4x_2^5x_3 - 5x_1^4x_2^5x_4 + 1024x_1^4x_2^4x_3^2 - 713x_1^4x_2^4x_3x_4 + 738x_1^4x_2^4x_4^2 -$
$669x_1^4x_2^3x_3^3 + 543x_1^4x_2^3x_3^2x_4 - 588x_1^4x_2^3x_3x_4^2 - 5x_1^4x_2^3x_4^3 + 422x_1^4x_2^2x_3^4 - 540x_1^4x_2^2x_3^3x_4 +$
$843x_1^4x_2^2x_3^2x_4^2 - 526x_1^4x_2^2x_3x_4^3 + 273x_1^4x_2^2x_4^4 - 110x_1^4x_2x_3^5 + 128x_1^4x_2x_3^4x_4 - 242x_1^4x_2x_3^3x_4^2 +$
$208x_1^4x_2x_3^2x_4^3 - 124x_1^4x_2x_3x_4^4 + 10x_1^4x_2x_4^5 + 40x_1^4x_3^6 - 120x_1^4x_3^5x_4 + 273x_1^4x_3^4x_4^2 -$
$346x_1^4x_3^3x_4^3 + 273x_1^4x_3^2x_4^4 - 120x_1^4x_3x_4^5 + 40x_1^4x_4^6 - 180x_1^3x_2^7 + 579x_1^3x_2^6x_3 + 7x_1^3x_2^6x_4 -$
$1020x_1^3x_2^5x_3^2 + 594x_1^3x_2^5x_3x_4 - 627x_1^3x_2^5x_4^2 + 958x_1^3x_2^4x_3^3 - 721x_1^3x_2^4x_3^2x_4 + 786x_1^3x_2^4x_3x_4^2 -$
$5x_1^3x_2^4x_4^3 - 669x_1^3x_2^3x_3^4 + 760x_1^3x_2^3x_3^3x_4 - 1176x_1^3x_2^3x_3^2x_4^2 + 712x_1^3x_2^3x_3x_4^3 - 346x_1^3x_2^3x_4^4 +$
$237x_1^3x_2^2x_3^5 - 326x_1^3x_2^2x_3^4x_4 + 584x_1^3x_2^2x_3^3x_4^2 - 456x_1^3x_2^2x_3^2x_4^3 + 208x_1^3x_2^2x_3x_4^4 - 4x_1^3x_2^2x_4^5 -$
$87x_1^3x_2x_3^6 + 272x_1^3x_2x_3^5x_4 - 596x_1^3x_2x_3^4x_4^2 + 712x_1^3x_2x_3^3x_4^3 - 526x_1^3x_2x_3^2x_4^4 + 232x_1^3x_2x_3x_4^5 -$
$80x_1^3x_2x_4^6 + 2x_1^3x_3^7 - 7x_1^3x_3^6x_4 + 9x_1^3x_3^5x_4^2 - 5x_1^3x_3^4x_4^3 - 5x_1^3x_3^3x_4^4 + 9x_1^3x_3^2x_4^5 - 7x_1^3x_3x_4^6 +$
$2x_1^3x_4^7 + 90x_1^2x_2^8 - 347x_1^2x_2^7x_3 - 2x_1^2x_2^7x_4 + 764x_1^2x_2^6x_3^2 - 391x_1^2x_2^6x_3x_4 + 405x_1^2x_2^6x_4^2 -$
$1020x_1^2x_2^5x_3^3 + 768x_1^2x_2^5x_3^2x_4 - 810x_1^2x_2^5x_3x_4^2 + 9x_1^2x_2^5x_4^3 + 1024x_1^2x_2^4x_3^4 - 1149x_1^2x_2^4x_3^3x_4 +$
$1497x_1^2x_2^4x_3^2x_4^2 - 596x_1^2x_2^4x_3x_4^3 + 273x_1^2x_2^4x_4^4 - 745x_1^2x_2^3x_3^5 + 1093x_1^2x_2^3x_3^4x_4 -$
$1420x_1^2x_2^3x_3^3x_4^2 + 584x_1^2x_2^3x_3^2x_4^3 - 242x_1^2x_2^3x_3x_4^4 - 4x_1^2x_2^3x_4^5 + 453x_1^2x_2^2x_3^6 - 957x_1^2x_2^2x_3^5x_4 +$
$1497x_1^2x_2^2x_3^4x_4^2 - 1176x_1^2x_2^2x_3^3x_4^3 + 843x_1^2x_2^2x_3^2x_4^4 - 348x_1^2x_2^2x_3x_4^5 + 120x_1^2x_2^2x_4^6 - 171x_1^2x_2x_3^7 +$
$459x_1^2x_2x_3^6x_4 - 810x_1^2x_2x_3^5x_4^2 + 786x_1^2x_2x_3^4x_4^3 - 588x_1^2x_2x_3^3x_4^4 + 234x_1^2x_2x_3^2x_4^5 - 72x_1^2x_2x_3x_4^6 -$

$$3x_1^2x_2x_4^7+42x_1^2x_3^8-168x_1^2x_3^7x_4+405x_1^2x_3^6x_4^2-627x_1^2x_3^5x_4^3+738x_1^2x_3^4x_4^4-627x_1^2x_3^3x_4^5+$$
$$405x_1^2x_3^2x_4^6-168x_1^2x_3x_4^7+42x_1^2x_4^8-30x_1x_2^9+132x_1x_2^8x_3-347x_1x_2^7x_3^2+166x_1x_2^7x_3x_4-$$
$$168x_1x_2^7x_4^2+579x_1x_2^6x_3^3-445x_1x_2^6x_3^2x_4+459x_1x_2^6x_3x_4^2-7x_1x_2^6x_4^3-707x_1x_2^5x_3^4+$$
$$800x_1x_2^5x_3^3x_4-957x_1x_2^5x_3^2x_4^2+272x_1x_2^5x_3x_4^3-120x_1x_2^5x_4^4+622x_1x_2^4x_3^5-910x_1x_2^4x_3^4x_4+$$
$$1093x_1x_2^4x_3^3x_4^2-326x_1x_2^4x_3^2x_4^3+128x_1x_2^4x_3x_4^4+10x_1x_2^4x_4^5-406x_1x_2^3x_3^6+800x_1x_2^3x_3^5x_4-$$
$$1149x_1x_2^3x_3^4x_4^2+760x_1x_2^3x_3^3x_4^3-540x_1x_2^3x_3^2x_4^4+216x_1x_2^3x_3x_4^5-80x_1x_2^3x_4^6+169x_1x_2^2x_3^7-$$
$$445x_1x_2^2x_3^6x_4+768x_1x_2^2x_3^5x_4^2-721x_1x_2^2x_3^4x_4^3+543x_1x_2^2x_3^3x_4^4-237x_1x_2^2x_3^2x_4^5+93x_1x_2^2x_3x_4^6-$$
$$3x_1x_2^2x_4^7-42x_1x_2x_3^8+166x_1x_2x_3^7x_4-391x_1x_2x_3^6x_4^2+594x_1x_2x_3^5x_4^3-713x_1x_2x_3^4x_4^4+$$
$$638x_1x_2x_3^3x_4^5-426x_1x_2x_3^2x_4^6+174x_1x_2x_3x_4^7-42x_1x_2x_4^8-2x_1x_3^7x_4^2+7x_1x_3^6x_4^3-5x_1x_3^5x_4^4-$$
$$5x_1x_3^4x_4^5+7x_1x_3^3x_4^6-2x_1x_3^2x_4^7+6x_2^{10}-30x_2^9x_3+90x_2^8x_3^2-42x_2^8x_3x_4+42x_2^8x_4^2-180x_2^7x_3^3+$$
$$169x_2^7x_3^2x_4-171x_2^7x_3x_4^2+2x_2^7x_4^3+270x_2^6x_3^4-406x_2^6x_3^3x_4+453x_2^6x_3^2x_4^2-87x_2^6x_3x_4^3+$$
$$40x_2^6x_4^4-306x_2^5x_3^5+622x_2^5x_3^4x_4-745x_2^5x_3^3x_4^2+237x_2^5x_3^2x_4^3-110x_2^5x_3x_4^4-4x_2^5x_4^5+$$
$$270x_2^4x_3^6-707x_2^4x_3^5x_4+1024x_2^4x_3^4x_4^2-669x_2^4x_3^3x_4^3+422x_2^4x_3^2x_4^4-110x_2^4x_3x_4^5+40x_2^4x_4^6-$$
$$180x_2^3x_3^7+579x_2^3x_3^6x_4-1020x_2^3x_3^5x_4^2+958x_2^3x_3^4x_4^3-669x_2^3x_3^3x_4^4+237x_2^3x_3^2x_4^5-87x_2^3x_3x_4^6+$$
$$2x_2^3x_4^7+90x_2^2x_3^8-347x_2^2x_3^7x_4+764x_2^2x_3^6x_4^2-1020x_2^2x_3^5x_4^3+1024x_2^2x_3^4x_4^4-745x_2^2x_3^3x_4^5+$$
$$453x_2^2x_3^2x_4^6-171x_2^2x_3x_4^7+42x_2^2x_4^8-30x_2x_3^9+132x_2x_3^8x_4-347x_2x_3^7x_4^2+579x_2x_3^6x_4^3-$$
$$707x_2x_3^5x_4^4+622x_2x_3^4x_4^5-406x_2x_3^3x_4^6+169x_2x_3^2x_4^7-42x_2x_3x_4^8+6x_3^{10}-30x_3^9x_4+90x_3^8x_4^2-$$
$$180x_3^7x_4^3+270x_3^6x_4^4-306x_3^5x_4^5+270x_3^4x_4^6-180x_3^3x_4^7+90x_3^2x_4^8-30x_3x_4^9+6x_4^{10}$$

B_4 - Order 384 - Orthogonal Representation

Generators:

$$a=\begin{pmatrix}0&0&1&0\\1&0&0&0\\0&1&0&0\\0&0&0&1\end{pmatrix},\qquad b=\begin{pmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix},\qquad c=\begin{pmatrix}-1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$$

Molien series:

$$\Phi(t)=\frac{1}{(1-t^2)(1-t^4)(1-t^6)(1-t^8)}$$

CM-basis

$f_1 = x_1^2 + x_2^2 + x_3^2 + x_4^2, \quad f_2 = x_1^4 + x_2^4 + x_3^4 + x_4^4, \quad f_3 = x_1^6 + x_2^6 + x_3^6 + x_4^6,$

$f_4 = x_1^8 + x_2^8 + x_3^8 + x_4^8; \quad g_1 = 1$

B_4 - Rotation Subgroup - Order 192

Generators:

$$a = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad c = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Molien series:

$$\Phi(t) = \frac{1 + t^{16}}{(1 - t^2)(1 - t^4)(1 - t^6)(1 - t^8)}$$

CM-basis

$f_1,\ f_2,\ f_3,\ f_4;\ g_1 = 1,$ as above and $g_2 = x_1^7x_2^5x_3^3x_4 - x_1^7x_2^5x_3x_4^3 - x_1^7x_2^3x_3^5x_4 + x_1^7x_2^3x_3x_4^5 + x_1^7x_2x_3^5x_4^3 - x_1^7x_2x_3^3x_4^5 - x_1^5x_2^7x_3^3x_4 + x_1^5x_2^7x_3x_4^3 + x_1^5x_2^3x_3^7x_4 - x_1^5x_2^3x_3x_4^7 - x_1^5x_2x_3^7x_4^3 + x_1^5x_2x_3^3x_4^7 + x_1^3x_2^7x_3^5x_4 - x_1^3x_2^7x_3x_4^5 - x_1^3x_2^5x_3^7x_4 + x_1^3x_2^5x_3x_4^7 + x_1^3x_2x_3^7x_4^5 - x_1^3x_2x_3^5x_4^7 - x_1x_2^7x_3^5x_4^3 + x_1x_2^7x_3^3x_4^5 + x_1x_2^5x_3^7x_4^3 - x_1x_2^5x_3^3x_4^7 - x_1x_2^3x_3^7x_4^5 + x_1x_2^3x_3^5x_4^7$

D_4 - Order 192 - Orthogonal Representation

Generators:

$$a = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad c = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Molien series:

$$\Phi(t) = \frac{1}{(1 - t^2)(1 - t^4)^2(1 - t^6)}$$

CM-basis

$f_1 = x_1^2 + x_2^2 + x_3^2 + x_4^2$, $f_2 = x_1^4 + x_2^4 + x_3^4 + x_4^4$, $f_3 = x_1x_2x_3x_4$,

$f_4 = x_1^6 + x_2^6 + x_3^6 + x_4^6$; $g_1 = 1$

D_4 - Rotation Subgroup - Order 96

Generators:

$$a = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad c = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Molien series:

$$\Phi(t) = \frac{1 + t^{12}}{(1 - t^2)(1 - t^4)^2(1 - t^6)}$$

CM-basis

f_1, f_2, f_3, f_4, and $g_1 = 1$ as above and $g_2 = x_1^6x_2^4x_3^2 + x_1^6x_2^2x_4^4 + x_1^6x_3^4x_4^2 + x_1^4x_2^6x_4^2 + x_1^4x_2^2x_3^6 + x_1^4x_3^2x_4^6 + x_1^2x_2^6x_3^4 + x_1^2x_2^4x_4^6 + x_1^2x_3^6x_4^4 + x_2^6x_3^2x_4^4 + x_2^4x_3^6x_4^2 + x_2^2x_3^4x_4^6$

F_4 - Order 1152 - Orthogonal Representation

Generators:

$$a = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$c = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad d = \frac{1}{2}\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}$$

Molien series:

$$\Phi(t) = \frac{1}{(1 - t^2)(1 - t^6)(1 - t^8)(1 - t^{12})}$$

CM-basis

$f_1 = x_1^2 + x_2^2 + x_3^2 + x_4^2,$

$f_2 = 3x_1^6+5x_1^4x_3^2+5x_1^4x_4^2+5x_1^4x_2^2+5x_1^2x_3^4+30x_1^2x_3^2x_4^2+30x_1^2x_3^2x_2^2+5x_1^2x_4^4+30x_1^2x_4^2x_2^2+$
$5x_1^2x_2^4+3x_3^6+5x_3^4x_4^2+5x_3^4x_2^2+5x_3^2x_4^4+30x_3^2x_4^2x_2^2+5x_3^2x_2^4+3x_4^6+5x_4^4x_2^2+5x_4^2x_2^4+3x_2^6,$

$f_3 = 33x_1^8+28x_1^6x_3^2+28x_1^6x_4^2+28x_1^6x_2^2+70x_1^4x_3^4+420x_1^4x_3^2x_4^2+420x_1^4x_3^2x_2^2+70x_1^4x_4^4+$
$420x_1^4x_4^2x_2^2+70x_1^4x_2^4+28x_1^2x_3^6+420x_1^2x_3^4x_4^2+420x_1^2x_3^4x_2^2+420x_1^2x_3^2x_4^4+2520x_1^2x_3^2x_4^2x_2^2+$
$420x_1^2x_3^2x_2^4+28x_1^2x_4^6+420x_1^2x_4^4x_2^2+420x_1^2x_4^2x_2^4+28x_1^2x_2^6+33x_3^8+28x_3^6x_4^2+28x_3^6x_2^2+$
$70x_3^4x_4^4+420x_3^4x_4^2x_2^2+70x_3^4x_2^4+28x_3^2x_4^6+420x_3^2x_4^4x_2^2+420x_3^2x_4^2x_2^4+28x_3^2x_2^6+33x_4^8+$
$28x_4^6x_2^2+70x_4^4x_2^4+28x_4^2x_2^6+33x_2^8,$

$f_4 = 171x_1^{12}+22x_1^{10}x_3^2+22x_1^{10}x_4^2+22x_1^{10}x_2^2+165x_1^8x_3^4+990x_1^8x_3^2x_4^2+990x_1^8x_3^2x_2^2+$
$165x_1^8x_4^4+990x_1^8x_4^2x_2^2+165x_1^8x_2^4+308x_1^6x_3^6+4620x_1^6x_3^4x_4^2+4620x_1^6x_3^4x_2^2+4620x_1^6x_3^2x_4^4+$
$27720x_1^6x_3^2x_4^2x_2^2+4620x_1^6x_3^2x_2^4+308x_1^6x_4^6+4620x_1^6x_4^4x_2^2+4620x_1^6x_4^2x_2^4+308x_1^6x_2^6+$
$165x_1^4x_3^8+4620x_1^4x_3^6x_4^2+4620x_1^4x_3^6x_2^2+11550x_1^4x_3^4x_4^4+69300x_1^4x_3^4x_4^2x_2^2+11550x_1^4x_3^4x_2^4+$
$4620x_1^4x_3^2x_4^6+69300x_1^4x_3^2x_4^4x_2^2+69300x_1^4x_3^2x_4^2x_2^4+4620x_1^4x_3^2x_2^6+165x_1^4x_4^8+4620x_1^4x_4^6x_2^2+$
$11550x_1^4x_4^4x_2^4+4620x_1^4x_4^2x_2^6+165x_1^4x_2^8+22x_1^2x_3^{10}+990x_1^2x_3^8x_4^2+990x_1^2x_3^8x_2^2+$
$4620x_1^2x_3^6x_4^4+27720x_1^2x_3^6x_4^2x_2^2+4620x_1^2x_3^6x_2^4+4620x_1^2x_3^4x_4^6+69300x_1^2x_3^4x_4^4x_2^2+$
$69300x_1^2x_3^4x_4^2x_2^4+4620x_1^2x_3^4x_2^6+990x_1^2x_3^2x_4^8+27720x_1^2x_3^2x_4^6x_2^2+69300x_1^2x_3^2x_4^4x_2^4+$
$27720x_1^2x_3^2x_4^2x_2^6+990x_1^2x_3^2x_2^8+22x_1^2x_4^{10}+990x_1^2x_4^8x_2^2+4620x_1^2x_4^6x_2^4+4620x_1^2x_4^4x_2^6+$
$990x_1^2x_4^2x_2^8+22x_1^2x_2^{10}+171x_3^{12}+22x_3^{10}x_4^2+22x_3^{10}x_2^2+165x_3^8x_4^4+990x_3^8x_4^2x_2^2+165x_3^8x_2^4+$
$308x_3^6x_4^6+4620x_3^6x_4^4x_2^2+4620x_3^6x_4^2x_2^4+308x_3^6x_2^6+165x_3^4x_4^8+4620x_3^4x_4^6x_2^2+11550x_3^4x_4^4x_2^4+$
$4620x_3^4x_4^2x_2^6+165x_3^4x_2^8+22x_3^2x_4^{10}+990x_3^2x_4^8x_2^2+4620x_3^2x_4^6x_2^4+4620x_3^2x_4^4x_2^6+990x_3^2x_4^2x_2^8+$
$22x_3^2x_2^{10}+171x_4^{12}+22x_4^{10}x_2^2+165x_4^8x_2^4+308x_4^6x_2^6+165x_4^4x_2^8+22x_4^2x_2^{10}+171x_2^{12};$

$g_1 = 1$

Example 6 - D_4 – Root Representation

Earlier we mentioned that the representation plays a crucial role in the *CM*–basis obtained. For a final example let us look again at D_4 in dimension 4 but this time we use the root representation instead of an orthogonal representation.

D_4 - Order 192

Generators:

$$a = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$c = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}$$

Molien series:

$$\Phi(t) = \frac{1}{(1-t^2)(1-t^4)^2(1-t^6)}$$

CM-basis

$f_1 = x_1^2 - x_1x_2 - x_1x_3 - x_1x_4 + x_2^2 + x_3^2 + x_4^2,$

$f_2 = x_1^4 - 2x_1^3x_2 - 2x_1^3x_3 - 2x_1^3x_4 + 3x_1^2x_2^2 + x_1^2x_2x_3 + x_1^2x_2x_4 + 3x_1^2x_3^2 + 4x_1^2x_3x_4 +$
$3x_1^2x_4^2 - 2x_1x_2^3 - x_1x_2^2x_3 - x_1x_2^2x_4 - x_1x_2x_3^2 - x_1x_2x_4^2 - 2x_1x_3^3 - 4x_1x_3^2x_4 - 4x_1x_3x_4^2 -$
$2x_1x_4^3 + x_2^4 + x_2^2x_3^2 + x_2^2x_4^2 + x_3^4 + 4x_3^2x_4^2 + x_4^4,$

$f_3 = x_1^4 - 2x_1^3x_2 - 2x_1^3x_3 - 2x_1^3x_4 + 3x_1^2x_2^2 + x_1^2x_2x_3 + 4x_1^2x_2x_4 + 3x_1^2x_3^2 + x_1^2x_3x_4 +$
$3x_1^2x_4^2 - 2x_1x_2^3 - x_1x_2^2x_3 - 4x_1x_2^2x_4 - x_1x_2x_3^2 - 4x_1x_2x_4^2 - 2x_1x_3^3 - x_1x_3^2x_4 - x_1x_3x_4^2 -$
$2x_1x_4^3 + x_2^4 + x_2^2x_3^2 + 4x_2^2x_4^2 + x_3^4 + x_3^2x_4^2 + x_4^4,$

$f_4 = 3x_1^6 - 9x_1^5x_2 - 9x_1^5x_3 - 9x_1^5x_4 + 15x_1^4x_2^2 + 20x_1^4x_2x_3 + 20x_1^4x_2x_4 + 15x_1^4x_3^2 + 20x_1^4x_3x_4 +$
$15x_1^4x_4^2 - 15x_1^3x_2^3 - 25x_1^3x_2^2x_3 - 25x_1^3x_2^2x_4 - 25x_1^3x_2x_3^2 - 30x_1^3x_2x_3x_4 - 25x_1^3x_2x_4^2 -$

$15x_1^3x_3^3-25x_1^3x_2^2x_4-25x_1^3x_3x_4^2-15x_1^3x_4^3+15x_1^2x_2^4+10x_1^2x_2^3x_3+10x_1^2x_2^3x_4+30x_1^2x_2^2x_3^2+$
$30x_1^2x_2^2x_3x_4+30x_1^2x_2^2x_4^2+10x_1^2x_2x_3^3+30x_1^2x_2x_3^2x_4+30x_1^2x_2x_3x_4^2+10x_1^2x_2x_4^3+15x_1^2x_3^4+$
$10x_1^2x_3^3x_4+30x_1^2x_3^2x_4^2+10x_1^2x_3x_4^3+15x_1^2x_4^4-9x_1x_2^5-5x_1x_2^4x_3-5x_1x_2^4x_4-10x_1x_2^3x_3^2-$
$10x_1x_2^3x_4^2-10x_1x_2^2x_3^3-30x_1x_2^2x_3^2x_4-30x_1x_2^2x_3x_4^2-10x_1x_2^2x_4^3-5x_1x_2x_3^4-30x_1x_2x_3^2x_4^2-$
$5x_1x_2x_4^4-9x_1x_3^5-5x_1x_3^4x_4-10x_1x_3^3x_4^2-10x_1x_3^2x_4^3-5x_1x_3x_4^4-9x_1x_4^5+3x_2^6+5x_2^4x_3^2+$
$5x_2^4x_4^2+5x_2^2x_3^4+30x_2^2x_3^2x_4^2+5x_2^2x_4^4+3x_3^6+5x_3^4x_4^2+5x_3^2x_4^4+3x_4^6;$

$g_1=1$

D_4 - Rotation Subgroup - Order 96

Generators: ab, bc, cd

Molien series:

$$\Phi(t)=\frac{1+t^{12}}{(1-t^2)(1-t^4)^2(1-t^6)}$$

CM-basis

f_1, f_2, f_3, f_4, and $g_1=1$ as above and $g_2=12x_1^{12}-72x_1^{11}x_2-72x_1^{11}x_3-$
$72x_1^{11}x_4+268x_1^{10}x_2^2+464x_1^{10}x_2x_3+308x_1^{10}x_2x_4+268x_1^{10}x_3^2+276x_1^{10}x_3x_4+268x_1^{10}x_4^2-$
$681x_1^9x_2^3-1679x_1^9x_2^2x_3-899x_1^9x_2^2x_4-1679x_1^9x_2x_3^2-1282x_1^9x_2x_3x_4-899x_1^9x_2x_4^2-$
$681x_1^9x_3^3-739x_1^9x_3^2x_4-739x_1^9x_3x_4^2-681x_1^9x_4^3+1291x_1^8x_2^4+3890x_1^8x_2^3x_3+1870x_1^8x_2^3x_4+$
$5310x_1^8x_2^2x_3^2+4218x_1^8x_2^2x_3x_4+1986x_1^8x_2^2x_4^2+3890x_1^8x_2x_3^3+3714x_1^8x_2x_3^2x_4+$
$2382x_1^8x_2x_3x_4^2+1870x_1^8x_2x_4^3+1291x_1^8x_3^4+1334x_1^8x_3^3x_4+1602x_1^8x_3^2x_4^2+1334x_1^8x_3x_4^3+$
$1291x_1^8x_4^4-1864x_1^7x_2^5-6440x_1^7x_2^4x_3-3040x_1^7x_2^4x_4-10416x_1^7x_2^3x_3^2-8944x_1^7x_2^3x_3x_4-$
$3080x_1^7x_2^3x_4^2-10416x_1^7x_2^2x_3^3-11232x_1^7x_2^2x_3^2x_4-6648x_1^7x_2^2x_3x_4^2-3080x_1^7x_2^2x_4^3-$
$6440x_1^7x_2x_3^4-6704x_1^7x_2x_3^3x_4-5976x_1^7x_2x_3^2x_4^2-2656x_1^7x_2x_3x_4^3-3040x_1^7x_2x_4^4-1864x_1^7x_3^5-$
$1856x_1^7x_3^4x_4-2280x_1^7x_3^3x_4^2-2280x_1^7x_3^2x_4^3-1856x_1^7x_3x_4^4-1864x_1^7x_4^5+2099x_1^6x_2^6+$
$7954x_1^6x_2^5x_3+3642x_1^6x_2^5x_4+14321x_1^6x_2^4x_3^2+13310x_1^6x_2^4x_3x_4+4229x_1^6x_2^4x_4^2+16788x_1^6x_2^3x_3^3+$
$20656x_1^6x_2^3x_3^2x_4+12272x_1^6x_2^3x_3x_4^2+2860x_1^6x_2^3x_4^3+14321x_1^6x_2^2x_3^4+17520x_1^6x_2^2x_3^3x_4+$
$16338x_1^6x_2^2x_3^2x_4^2+5352x_1^6x_2^2x_3x_4^3+4229x_1^6x_2^2x_4^4+7954x_1^6x_2x_3^5+8438x_1^6x_2x_3^4x_4+$

$$9472x_1^6x_2x_3^3x_4^2+5016x_1^6x_2x_3^2x_4^3+2582x_1^6x_2x_3x_4^4+3642x_1^6x_2x_4^5+2099x_1^6x_3^6+1906x_1^6x_3^5x_4+$$
$$2717x_1^6x_3^4x_4^2+2188x_1^6x_3^3x_4^3+2717x_1^6x_3^2x_4^4+1906x_1^6x_3x_4^5+2099x_1^6x_4^6-1852x_1^5x_2^7-$$
$$7528x_1^5x_2^6x_3-3216x_1^5x_2^6x_4-14556x_1^5x_2^5x_3^2-13776x_1^5x_2^5x_3x_4-4440x_1^5x_2^5x_4^2-$$
$$18496x_1^5x_2^4x_3^3-25572x_1^5x_2^4x_3^2x_4-16680x_1^5x_2^4x_3x_4^2-2604x_1^5x_2^4x_4^3-18496x_1^5x_2^3x_3^4-$$
$$26744x_1^5x_2^3x_3^3x_4-26988x_1^5x_2^3x_3^2x_4^2-6744x_1^5x_2^3x_3x_4^3-2604x_1^5x_2^3x_4^4-14556x_1^5x_2^2x_3^5-$$
$$18012x_1^5x_2^2x_3^4x_4-23292x_1^5x_2^2x_3^3x_4^2-10716x_1^5x_2^2x_3^2x_4^3-4056x_1^5x_2^2x_3x_4^4-4440x_1^5x_2^2x_4^5-$$
$$7528x_1^5x_2x_3^6-7392x_1^5x_2x_3^5x_4-10968x_1^5x_2x_3^4x_4^2-5624x_1^5x_2x_3^3x_4^3-3888x_1^5x_2x_3^2x_4^4-$$
$$1752x_1^5x_2x_3x_4^5-3216x_1^5x_2x_4^6-1852x_1^5x_3^7-1480x_1^5x_3^6x_4-2424x_1^5x_3^5x_4^2-1876x_1^5x_3^4x_4^3-$$
$$1876x_1^5x_3^3x_4^4-2424x_1^5x_3^2x_4^5-1480x_1^5x_3x_4^6-1852x_1^5x_4^7+1282x_1^4x_2^8+5416x_1^4x_2^7x_3+$$
$$2016x_1^4x_2^7x_4+11488x_1^4x_2^6x_3^2+9828x_1^4x_2^6x_3x_4+3636x_1^4x_2^6x_4^2+14240x_1^4x_2^5x_3^3+$$
$$21492x_1^4x_2^5x_3^2x_4+15852x_1^4x_2^5x_3x_4^2+1600x_1^4x_2^5x_4^3+16460x_1^4x_2^4x_3^4+26200x_1^4x_2^4x_3^3x_4+$$
$$30420x_1^4x_2^4x_3^2x_4^2+6800x_1^4x_2^4x_3x_4^3+1900x_1^4x_2^4x_4^4+14240x_1^4x_2^3x_3^5+21720x_1^4x_2^3x_3^4x_4+$$
$$32720x_1^4x_2^3x_3^3x_4^2+12720x_1^4x_2^3x_3^2x_4^3+3640x_1^4x_2^3x_3x_4^4+1600x_1^4x_2^3x_4^5+11488x_1^4x_2^2x_3^6+$$
$$12420x_1^4x_2^2x_3^5x_4+22020x_1^4x_2^2x_3^4x_4^2+11600x_1^4x_2^2x_3^3x_4^3+6840x_1^4x_2^2x_3^2x_4^4+1932x_1^4x_2^2x_3x_4^5+$$
$$3636x_1^4x_2^2x_4^6+5416x_1^4x_2x_3^7+4564x_1^4x_2x_3^6x_4+8796x_1^4x_2x_3^5x_4^2+5120x_1^4x_2x_3^4x_4^3+$$
$$3080x_1^4x_2x_3^3x_4^4+1932x_1^4x_2x_3^2x_4^5+948x_1^4x_2x_3x_4^6+2016x_1^4x_2x_4^7+1282x_1^4x_3^8+832x_1^4x_3^7x_4+$$
$$1732x_1^4x_3^6x_4^2+1040x_1^4x_3^5x_4^3+1340x_1^4x_3^4x_4^4+1040x_1^4x_3^3x_4^5+1732x_1^4x_3^2x_4^6+832x_1^4x_3x_4^7+$$
$$1282x_1^4x_4^8-679x_1^3x_2^9-2907x_1^3x_2^8x_3-887x_1^3x_2^8x_4-6924x_1^3x_2^7x_3^2-4456x_1^3x_2^7x_3x_4-$$
$$2148x_1^3x_2^7x_4^2-8244x_1^3x_2^6x_3^3-12432x_1^3x_2^6x_3^2x_4-10552x_1^3x_2^6x_3x_4^2-820x_1^3x_2^6x_4^3-$$
$$9726x_1^3x_2^5x_3^4-15464x_1^3x_2^5x_3^3x_4-23472x_1^3x_2^5x_3^2x_4^2-4184x_1^3x_2^5x_3x_4^3-826x_1^3x_2^5x_4^4-$$
$$9726x_1^3x_2^4x_3^5-17210x_1^3x_2^4x_3^4x_4-29220x_1^3x_2^4x_3^3x_4^2-9820x_1^3x_2^4x_3^2x_4^3-3470x_1^3x_2^4x_3x_4^4-$$
$$826x_1^3x_2^4x_4^5-8244x_1^3x_2^3x_3^6-10088x_1^3x_2^3x_3^5x_4-24740x_1^3x_2^3x_3^4x_4^2-11760x_1^3x_2^3x_3^3x_4^3-$$
$$6660x_1^3x_2^3x_3^2x_4^4-392x_1^3x_2^3x_3x_4^5-820x_1^3x_2^3x_4^6-6924x_1^3x_2^2x_3^7-6272x_1^3x_2^2x_3^6x_4-$$
$$13728x_1^3x_2^2x_3^5x_4^2-8140x_1^3x_2^2x_3^4x_4^3-6100x_1^3x_2^2x_3^3x_4^4-2016x_1^3x_2^2x_3^2x_4^5-1040x_1^3x_2^2x_3x_4^6-$$
$$2148x_1^3x_2^2x_4^7-2907x_1^3x_2x_3^8-1768x_1^3x_2x_3^7x_4-5064x_1^3x_2x_3^6x_4^2-2840x_1^3x_2x_3^5x_4^3-$$

$$2630x_1^3x_2x_3^4x_4^4-392x_1^3x_2x_3^3x_4^5-1040x_1^3x_2x_3^2x_4^6-280x_1^3x_2x_3x_4^7-887x_1^3x_2x_4^8-679x_1^3x_3^9-$$
$$351x_1^3x_3^8x_4-900x_1^3x_3^7x_4^2-484x_1^3x_3^6x_4^3-546x_1^3x_3^5x_4^4-546x_1^3x_3^4x_4^5-484x_1^3x_3^3x_4^6-900x_1^3x_3^2x_4^7-$$
$$351x_1^3x_3x_4^8-679x_1^3x_4^9+268x_1^2x_2^{10}+1038x_1^2x_2^9x_3+258x_1^2x_2^9x_4+3288x_1^2x_2^8x_3^2+$$
$$1098x_1^2x_2^8x_3x_4+924x_1^2x_2^8x_4^2+2984x_1^2x_2^7x_3^3+4488x_1^2x_2^7x_3^2x_4+4488x_1^2x_2^7x_3x_4^2+232x_1^2x_2^7x_4^3+$$
$$4988x_1^2x_2^6x_3^4+5208x_1^2x_2^6x_3^3x_4+13044x_1^2x_2^6x_3^2x_4^2+1448x_1^2x_2^6x_3x_4^3+416x_1^2x_2^6x_4^4+$$
$$3156x_1^2x_2^5x_3^5+7668x_1^2x_2^5x_3^4x_4+15432x_1^2x_2^5x_3^3x_4^2+4152x_1^2x_2^5x_3^2x_4^3+2028x_1^2x_2^5x_3x_4^4+$$
$$60x_1^2x_2^5x_4^5+4988x_1^2x_2^4x_3^6+4980x_1^2x_2^4x_3^5x_4+18840x_1^2x_2^4x_3^4x_4^2+5880x_1^2x_2^4x_3^3x_4^3+$$
$$5100x_1^2x_2^4x_3^2x_4^4+132x_1^2x_2^4x_3x_4^5+416x_1^2x_2^4x_4^6+2984x_1^2x_2^3x_3^7+3416x_1^2x_2^3x_3^6x_4+$$
$$10056x_1^2x_2^3x_3^5x_4^2+5880x_1^2x_2^3x_3^4x_4^3+5880x_1^2x_2^3x_3^3x_4^4+360x_1^2x_2^3x_3^2x_4^5+184x_1^2x_2^3x_3x_4^6+$$
$$232x_1^2x_2^3x_4^7+3288x_1^2x_2^2x_3^8+1800x_1^2x_2^2x_3^7x_4+6660x_1^2x_2^2x_3^6x_4^2+2808x_1^2x_2^2x_3^5x_4^3+$$
$$4260x_1^2x_2^2x_3^4x_4^4+360x_1^2x_2^2x_3^3x_4^5+1020x_1^2x_2^2x_3^2x_4^6+312x_1^2x_2^2x_3x_4^7+924x_1^2x_2^2x_4^8+1038x_1^2x_2x_3^9+$$
$$426x_1^2x_2x_3^8x_4+1800x_1^2x_2x_3^7x_4^2+1000x_1^2x_2x_3^6x_4^3+1356x_1^2x_2x_3^5x_4^4+132x_1^2x_2x_3^4x_4^5+$$
$$184x_1^2x_2x_3^3x_4^6+312x_1^2x_2x_3^2x_4^7+54x_1^2x_2x_3x_4^8+258x_1^2x_2x_4^9+268x_1^2x_3^10+98x_1^2x_3^9x_4+$$
$$372x_1^2x_3^8x_4^2+104x_1^2x_3^7x_4^3+248x_1^2x_3^6x_4^4+60x_1^2x_3^5x_4^5+248x_1^2x_3^4x_4^6+104x_1^2x_3^3x_4^7+372x_1^2x_3^2x_4^8+$$
$$98x_1^2x_3x_4^9+268x_1^2x_4^{10}-72x_1x_2^{11}-208x_1x_2^{10}x_3-52x_1x_2^{10}x_4-1040x_1x_2^9x_3^2+4x_1x_2^9x_3x_4-$$
$$260x_1x_2^9x_4^2-744x_1x_2^8x_3^3-1116x_1x_2^8x_3^2x_4-1116x_1x_2^8x_3x_4^2-56x_1x_2^8x_4^3-1488x_1x_2^7x_3^4-$$
$$16x_1x_2^7x_3^3x_4-4464x_1x_2^7x_3^2x_4^2-16x_1x_2^7x_3x_4^3-112x_1x_2^7x_4^4-1056x_1x_2^6x_3^5-2576x_1x_2^6x_3^4x_4-$$
$$5152x_1x_2^6x_3^3x_4^2-1392x_1x_2^6x_3^2x_4^3-696x_1x_2^6x_3x_4^4-24x_1x_2^6x_4^5-1056x_1x_2^5x_3^6+24x_1x_2^5x_3^5x_4-$$
$$7728x_1x_2^5x_3^4x_4^2+16x_1x_2^5x_3^3x_4^3-2088x_1x_2^5x_3^2x_4^4+24x_1x_2^5x_3x_4^5-24x_1x_2^5x_4^6-1488x_1x_2^4x_3^7-$$
$$1680x_1x_2^4x_3^6x_4-5040x_1x_2^4x_3^5x_4^2-2960x_1x_2^4x_3^4x_4^3-2960x_1x_2^4x_3^3x_4^4-192x_1x_2^4x_3^2x_4^5-$$
$$64x_1x_2^4x_3x_4^6-112x_1x_2^4x_4^7-744x_1x_2^3x_3^8-16x_1x_2^3x_3^7x_4-3360x_1x_2^3x_3^6x_4^2+16x_1x_2^3x_3^5x_4^3-$$
$$2960x_1x_2^3x_3^4x_4^4+16x_1x_2^3x_3^3x_4^5-128x_1x_2^3x_3^2x_4^6-16x_1x_2^3x_3x_4^7-56x_1x_2^3x_4^8-1040x_1x_2^2x_3^9-$$
$$444x_1x_2^2x_3^8x_4-1776x_1x_2^2x_3^7x_4^2-944x_1x_2^2x_3^6x_4^3-1416x_1x_2^2x_3^5x_4^4-192x_1x_2^2x_3^4x_4^5-$$
$$128x_1x_2^2x_3^3x_4^6-288x_1x_2^2x_3^2x_4^7-72x_1x_2^2x_3x_4^8-260x_1x_2^2x_4^9-208x_1x_2x_3^{10}+4x_1x_2x_3^9x_4-$$
$$444x_1x_2x_3^8x_4^2-16x_1x_2x_3^7x_4^3-472x_1x_2x_3^6x_4^4+24x_1x_2x_3^5x_4^5-64x_1x_2x_3^4x_4^6-16x_1x_2x_3^3x_4^7-$$

$$72x_1x_2x_3^2x_4^8+4x_1x_2x_3x_4^9-52x_1x_2x_4^{10}-72x_1x_3^{11}-20x_1x_3^{10}x_4-100x_1x_3^9x_4^2-24x_1x_3^8x_4^3-48x_1x_3^7x_4^4-24x_1x_3^6x_4^5-24x_1x_3^5x_4^6-48x_1x_3^4x_4^7-24x_1x_3^3x_4^8-100x_1x_3^2x_4^9-20x_1x_3x_4^{10}-72x_1x_4^{11}+12x_2^{12}+208x_2^{10}x_3^2+52x_2^{10}x_4^2+372x_2^8x_3^4+1116x_2^8x_3^2x_4^2+28x_2^8x_4^4+352x_2^6x_3^6+2576x_2^6x_3^4x_4^2+696x_2^6x_3^2x_4^4+8x_2^6x_4^6+372x_2^4x_3^8+1680x_2^4x_3^6x_4^2+1480x_2^4x_3^4x_4^4+64x_2^4x_3^2x_4^6+28x_2^4x_4^8+208x_2^2x_3^{10}+444x_2^2x_3^8x_4^2+472x_2^2x_3^6x_4^4+64x_2^2x_3^4x_4^6+72x_2^2x_3^2x_4^8+52x_2^2x_4^{10}+12x_3^{12}+20x_3^{10}x_4^2+12x_3^8x_4^4+8x_3^6x_4^6+12x_3^4x_4^8+20x_3^2x_4^{10}+12x_4^{12}$$

APPENDIX A: gengroup

```
# gengroup #
# a GAP program #
# generates group of matrices given generators #
# CHANGE generators #

a:=[[-1,1,0,0],[0,1,0,0],[0,0,1,0],[0,0,0,1]];
b:=[[1,0,0,0],[1,-1,1,0],[0,0,1,0],[0,0,0,1]];

g:=Group(a,b);
Size(g);
G:=Elements(g);
PrintTo("group","group:=",G,":\n");


quit;
```

APPENDIX B: molien

```
# molien #
# a Maple program #
# computes the Molien series for a given group #
# CHANGE dim - the dimension #

with(linalg):

# CHANGE n #
dim:=4:

# GET group #
read group:

og:=nops(M);

for i from 1 to og do
   a[i]:=array(M[i])
   od:

f:=0:
g:=0:

for i from 1 to og do
    g:=(-1)^dim*det(a[i])/charpoly(a[i],t):
    f:=f+g
  od:

f:=f/og:

f:=simplify(f);

taylor(f,t=0,50);

quit;
```

APPENDIX C: CMbasis

```
#################################################################
# CMbasis                                October 30, 1992       #
# a Maple program to compute a Cohen-Macaulay basis for         #
# a finite group  --- computes f's (free invariants) and        #
# then g's (transient invariants)                               #
# CHANGE dim  - the dimension                                   #
# CHANGE degrees - the degrees of basic invariants              #
# generate the group with the GAP script - gengroup             #
# written by Janet M. McShane                                   #
# e-mail   mcshane@odin.math.nau.edu                            #
#################################################################

print('Finding a Cohen-Macaulay basis for a'):
print(' 4-dimensional representation of c2xc4.'):

tt:=time():

with(linalg):
with(grobner):
with(combinat):

### get group elements ###
read group:

### determine order of the group ###
og:=nops(group):

### CHANGE dim ###
dim:=4:

### CHANGE degrees ###
degrees:=[$1..og];   ### optional -- if degrees aren't known ###
# degrees:=[2,4];


### procedure to average monomials  -  actually not the average ###
### since we do not divide by the order of the group            ###
Average:=proc(mon)
   local avg, h, i:
   avg:=0:
   for i from 1 to og do
      h:=subs(S[i],mon):
      avg:=avg+h:
   od:
   avg:=expand(avg):
   RETURN(avg):
```

```
end:

### procedure to test whether we have full radical ###
FullRadical:=proc(F)
   local b, gbfx, h, i, m, L, T, Xset:
   print('Checking whether we have full radical --'):
   gbfx:=gbasis(F,X):
   L:={}:
   for h in gbfx do L:=L union {leadmon(h,X)[2]} od:
   m:=1:
   for h in L do m:=max(m,degree(h,X)) od:
   T:={}:
   for b in X do
      for i from 1 to m do
         if member(b^i,L) then  T:=T union {b}  fi:
      od:
   od:
   Xset:=convert(X,set):
   if T=Xset then
     print('We do!'):
     lastj:=j:
     j:=nops(M)+1:
        else
          print('Not yet!')
     fi:
   RETURN(j):
end:

### procedure to test whether we have full ###
### radical if we normalize ###
FullRadicalNorm:=proc(F)
   local b, gbfx, h, i, m, L, T, Xset:
   gbfx:=gbasis(F,X):
   L:={}:
   for h in gbfx do L:=L union {leadmon(h,X)[2]} od:
   m:=1:
   for h in L do m:=max(m,degree(h,X)) od:
   T:={}:
   for b in X do
      for i from 1 to m do
         if member(b^i,L) then  T:=T union {b}  fi:
      od:
   od:
   Xset:=convert(X,set):
   if T=Xset then
      nt:=1:
   fi:
   RETURN(nt):
end:
```

```
### procedure to generate monomials ###
GenerateMonomial:=proc(exponents)
   local i, mon:
   mon:=1:
   for i from 1 to dim do
      mon:=mon*X[i]^exponents[i]:
   od:
   RETURN(mon):
end:

### procedure to generate polynomial ###
GenPoly:=proc(exponents,begin)
   local i, poly:
   poly:=begin:
   for i from 1 to dim do
      poly:=poly*F[i]^exponents[i]
   od:
   poly:=expand(poly):
   RETURN(poly):
end:

### procedure to check module membership ###
InMod:=proc(possibleg)
   local c,degpg,h,i,j,k,pieces,pieceswcoef,poly,sol,summ,
         summinpg,A,C,MM,Smon:
   degpg:=degree(possibleg,X):
   for i from 1 to nops(G) do
      Smon[i]:=[]:
      if iquo(degpg-ei[i],di[1])=0 then Smon[i]:=[[0 $ c=1..dim]]:
         else
            for j from 1 to iquo(degpg-ei[i],di[1]) do
               MM:=MonomialPowers(j,dim,[],1):
               for k from 1 to nops(MM) do
                  if dotprod(di,MM[k])=degpg-ei[i] then
                     Smon[i]:=[op(Smon[i]),MM[k]]:
                  fi:
               od:
            od:
      fi:
   od:
   pieces:=[]:
   for i from 1 to nops(G) do
      for j from 1 to nops(Smon[i]) do
         poly:=GenPoly(Smon[i][j],G[i]):
         pieces:=[op(pieces),poly]:
      od:
   od:
   pieceswcoef:=[]:
   A:=[]:
   for i from 1 to nops(pieces) do
```

```
      A:=[op(A),a[i]]:
      pieceswcoef:=[op(pieceswcoef),expand(a[i]*pieces[i])]:
   od:
   summ:=convert(pieceswcoef,'+'):
   summinpg:=summ-possibleg:
   summinpg:=collect(summinpg,X,distributed):
   C:={coeffs(summinpg,X)}:
   sol:=solve(C,convert(A,set)):
   if sol=NULL then print(' and we keep it!'):
      G:=[op(G),possibleg]:
      ei:=[op(ei),degree(possibleg,X)]:
      ca:=ca-1:
      if ca=0 then gcounter:=gcounter+1:
        if gcounter <= nops(degg) then ca:=numg[gcounter] fi:
      fi:
         else
           print(' but it is rejected.'):
   fi:
   if nops(G)=numofgs then
      print('A Cohen-Macaulay basis is ',[op(F),op(G)]):
      lprint([op(F),op(G)]):
      print('Time',time()-tt):
      quit
   fi:
   RETURN:
end:

### procedure to test whether a polynomial (avg) is in the ###
### radical of the previous f's   ---   returns a gbasis   ###
InRadical:=proc(avg)
   local g, u, GB, H, Y:
   g:=1-u*avg:
   Y:=[op(X),u]:
   H:=[op(F),g]:
   GB:=gbasis(H,Y):
   RETURN(GB):
end:

###   procedure to obtain Molien series    ###
### returns rational form of Molien series ###
Molien:=proc()
   local i, mf, mg:
   mf:=0:
   for i from 1 to og do
      mg:=(-1)^dim*det(array(group[i]))/charpoly(array(group[i]),t):
      mf:=mf+mg
   od:
   mf:=simplify(mf/og):
   RETURN(mf):
end:
```

```
### procedure to generate exponents ###
MonomialPowers:=proc(deg,dim,mpow,i)
   local j, m, mpows, H, N, TG:
   if dim =1 then
      pow:=copy(mpow):
      pow[i]:=deg:
      mpows:=[op(pow)]:
      pow:=copy(pow):
   else
      mpows:=[]:
      for m from 0 to deg do
         pow[i]:=m:
         mpows:=[op(mpows),op(MonomialPowers(deg-m,dim-1,pow,i+1))]:
      od:
   fi:
   H:=[]:
   for j from 1 to nops(mpows) do
      TG[j]:=convert(mpows[j],list):
      H:=[op(H),TG[j]]:
   od:
   N:=sort(H,Sorter):
   RETURN(N):
end:

### procedure to normalize ###
Normalize:=proc(H)
   local d, hm, k, m, p, D, HM:
   D:=[]:
   for i from 1 to nops(H) do
      d[i]:=degree(H[i],X):
      D:=[op(D),d[i]]:
   od:
   m:=ilcm(op(D)):
   HM:=[]:
   for i from 1 to nops(H) do
      hm[i]:=expand(H[i]^(m/degree(H[i],X))):
      HM:=[op(HM),hm[i]]:
   od:
   T:=[]:
   for i from 1 to dim do
      k:=randcomb(HM,2):
      p:=k[1]+(-1 )^(rand())*k[2]:
      T:=[op(T),p]:
   od;
   RETURN(T):
end:

### procedure to sort exponents ###
Sorter:=proc(a,b)
```

```
   local i:
   for i from 1 to dim
      while a[i]=b[i] do next
   od:
   RETURN(evalb(a[i]>b[i])):
end:

#################################################################
#                          MAIN PROGRAM                         #
#################################################################

### generate the variable list ###
X:=['x.i' $ i=1..dim]:

### turn variable list into a matrix ###
v:=transpose(array([X])):

for i from 1 to og do
   p[i]:=multiply(array(group[i]),v):
         # element action on indeterminates #
   S[i]:={}:
   for j from 1 to dim do          # forms substitution sets #
      S[i]:=S[i] union {X[j]=p[i][j,1]}:
   od:
od:

F:=[]:

nonzeroavg:=[]:

### find the free invariants that give us full radical ###
for k from 1 to nops(degrees) do         # generates exponents of #
   M:=MonomialPowers(degrees[k],dim,[],1):  # a particular degree #
   for j from 1 to nops(M) do
      monomial:=GenerateMonomial(M[j]):     # finds monomial #
      avg:=Average(monomial):               # averages monomial #
      if avg=0 then next                    # next j #
         else
            avg:=avg/leadmon(avg,X,plex)[1]:
            if member(avg,nonzeroavg) then next fi:    # next j #
            nonzeroavg:=[op(nonzeroavg),avg]:
            print(`A possible f `,avg):
            print(`Now check whether it's in the radical.`):
            GB:=InRadical(avg):
            if GB=[1] then print(`It is ----`): next   # next j #
               else
                  print(`It is not!  We have a new f!`):
                  avg:=sort(expand(avg)):
                  F:=[op(F),avg]:
                  print(`The set F so far `,F):
```

```
                if nops(F)<dim then next              # next j #
                   else
                      j:=FullRadical(F):
                      if j=nops(M)+1 then lastk:=k:
                         k:=nops(degrees)+1:
                      fi:
                fi:
             fi:
       fi:
   od:
od:

numfs:=nops(F):

if numfs=dim then
   print('The set F of primary invariants is ', F):
   print(' and we have the correct number.')
fi:

### throw out unneeded f's ###
if numfs > dim then
   print('The number of f's is more than the dimension.'):
   print('We will try to obtain the correct number.'):
   ctr:=0:
   for i from numfs-1 by -1 to 1 do
         TF:=[]:
         g:=1-u*F[i]:
         Y:=[op(X),u]:
         Fset:=convert(F,set):
         H:=Fset minus {F[i]} union {g}:
         GB:=gbasis(H,Y):
         if GB=[1] then
            ctr:=ctr+1:
            for j from 1 to i-1 do
               TF:=[op(TF),F[j]]:
            od:
            for j from i+1 to numfs-ctr+1 do
               TF:=[op(TF),F[j]]
            od:
            F:=TF:
         fi:
         if numfs-ctr=dim then i:=0 fi:
   od:
   if nops(F)=dim then
      print('The set F of primary invariants is ', F):
      print(' and we have the correct number.')
   fi:
fi:

### normalization ###
```

```
if nops(F) > dim then
   print(‘The number of f’s is still more than the dimension.‘):
   print(‘We need to normalize.‘):
   nt:=0:
   while  nt < 1 do
      F:=Normalization(F):
      nt:=FullRadicalNorm(F):
   od:
fi:

di:=[]:
for i from 1 to dim do
   di:=[op(di),degree(F[i],X)]:
od:
lprint(‘The degrees of the f’s are‘,di):
print():
degbound:=convert(di,‘+‘)-dim:
lprint(‘The bound on the degree of a g is‘,degbound):
print():
numofgs:=(convert(di,‘*‘))/og:
lprint(‘The number of g’s is‘, numofgs):
print():

bot:=1:
for i from 1 to nops(di) do
   bot:=bot*(1-t^(di[i]))
od:

mol:=Molien();
polyg:=expand(simplify(bot*mol));
degg:=[]:
numg:=[]:
for i from 1 to nops([coeffs(polyg)])-1  do
   aa:=degree(polyg):
   degg:=[aa,op(degg)]:
   numg:=[lcoeff(polyg),op(numg)]:
   polyg:=polyg-lcoeff(polyg)*t^aa:
od:
print(’degg’,degg):
print(’numg’,numg):

if numofgs=1 then
   print(‘A Cohen-Macaulay basis is ‘,[op(F),1]):
   lprint([op(F),1]):
   print(‘Time‘, time()-tt):
   quit
fi:

G:=[1];
ei:=[0]:
```

```
gcounter:=1:
ca:=numg[gcounter]:

newnon:=[]:
for i from 1 to nops(nonzeroavg) do
   if member(nonzeroavg[i],F) then next
      else newnon:=[op(newnon),nonzeroavg[i]]
   fi:
od:

for i from 1 to nops(newnon)  do
   if member(degree(newnon[i]),degg) then
      if degree(newnon[i])=degg[gcounter] and ca>0 then
      print(`A possible g `, newnon[i]):
      InMod(newnon[i]):
      fi:
   fi:
od:

GbasF:=gbasis(F,X):

for j from lastj+1 to nops(M) do
   if member(convert(M[j],`+`),degg) then
      monomial:=GenerateMonomial(M[j]):
      if degree(monomial)=degg[gcounter] and ca>0 then
         for i from 1 to nops(GbasF) do
            if divide(monomial,leadmon(GbasF[i],X)[2])
               then i:=nops(GbasF)+1:
            fi:
         od:
         if i=nops(GbasF)+2 then      # +2 due to Maple #
            next                      #  idiosyncracies #
         fi:
         avg:=Average(monomial):
         if avg=0 then next
            else
               avg:=avg/leadmon(avg,X,plex)[1]:
               if member(avg,nonzeroavg) then next fi:
               avg:=sort(expand(avg)):
               nonzeroavg:=[op(nonzeroavg),avg]:
         fi:
         print(`A possible g `,avg):
         InMod(avg):
      fi:
   fi:
od:

for k from lastk+1 to nops(degrees) do
   if degrees[k] > degbound then
      print(`A partial Cohen-Macaulay basis(bound)`,[op(F),op(G)]):
```

```
      print('Time',time()-tt): quit
   fi:
   M:=MonomialPowers(degrees[k],dim,[],1);
   for j from 1 to nops(M) do
      if member(convert(M[j],'+'),degg) then
         monomial:=GenerateMonomial(M[j]):
         if degree(monomial)=degg[gcounter] and ca>0 then
            for i from 1 to nops(GbasF) do
               if divide(monomial,leadmon(GbasF[i],X)[2])
                  then i:=nops(GbasF)+1:
               fi:
            od:
            if i=nops(GbasF)+2 then next fi:
            avg:=Average(monomial):
            if avg=0 then next
               else
                  avg:=avg/leadmon(avg,X,plex)[1]:
                  if member(avg,nonzeroavg) then next fi:
                  avg:=sort(expand(avg)):
                  nonzeroavg:=[op(nonzeroavg),avg]:
            fi:
            print('A possible g ',avg):
            InMod(avg):
         fi:
      fi:
   od:
od:

newdeg:=[]:
for i from 1 to nops(degg) do
   if member(degg[i],degrees) then next
      else newdeg:=[op(newdeg),degg[i]]
   fi:
od:

for i from 1 to nops(newdeg) do
   if newdeg[i] > degbound then
      print('A partial Cohen-Macaulay basis(bound)',[op(F),op(G)]):
      print('Time',time()-tt):
      quit
   fi:
   M:=MonomialPowers(newdeg[i],dim,[],1):
   for j from 1 to nops(M) do
      monomial:=GenerateMonomial(M[j]):
      if degree(monomial)=degg[gcounter] and ca>0 then
         for k from 1 to nops(GbasF) do
            if divide(monomial,leadmon(GbasF[k],X)[2])
               then k:=nops(GbasF)+1:
            fi:
         od:
```

```
         if k=nops(GbasF)+2 then next fi:
         avg:=Average(monomial):
         if avg=0 then next
            else
               avg:=avg/leadmon(avg,X,plex)[1]:
               if member(avg,nonzeroavg) then next fi:
               avg:=sort(expand(avg)):
               nonzeroavg:=[op(nonzeroavg),avg]:
         fi:
         print('A possible g ',avg):
         InMod(avg):
      fi:
   od:
od:

print('A partial Cohen-Macaulay basis',[op(F),op(G)]);

print('Time',time()-tt):

quit;
```

APPENDIX D: Sample of Output From CMbasis

```
                Finding a Cohen-Macaulay basis for a

                4-dimensional representation of c2xc4.

Warning: new definition for   norm
Warning: new definition for   trace
Warning: new definition for   combine
Warning: new definition for   fibonacci
                   degrees := [1, 2, 3, 4, 5, 6, 7, 8]

                                        2
                          A possible f , x1

                Now check whether it's in the radical.

                     It is not!  We have a new f!

                                          2
                       The set F so far , [x1 ]

                         A possible f , x1 x2

                Now check whether it's in the radical.

                              It is ----

                                        2
                          A possible f , x2

                Now check whether it's in the radical.

                     It is not!  We have a new f!

                                     2    2
                    The set F so far , [x1 , x2 ]

                                     2     2
                       A possible f , x3  + x4

                Now check whether it's in the radical.

                     It is not!  We have a new f!

                                  2    2    2     2
                The set F so far , [x1 , x2 , x3  + x4 ]

                                        4
```

A possible f , x1

Now check whether it's in the radical.

It is ----

$$\text{A possible f , } x1^{3}\ x2$$

Now check whether it's in the radical.

It is ----

$$\text{A possible f , } x1^{2}\ x2^{2}$$

Now check whether it's in the radical.

It is ----

$$\text{A possible f , } x1^{2}\ x3^{2} + x1^{2}\ x4^{2}$$

Now check whether it's in the radical.

It is ----

$$\text{A possible f , } x1\ x2^{3}$$

Now check whether it's in the radical.

It is ----

$$\text{A possible f , } x1\ x2\ x3^{2} + x1\ x2\ x4^{2}$$

Now check whether it's in the radical.

It is ----

$$\text{A possible f , } x2^{4}$$

Now check whether it's in the radical.

It is ----

$$\text{A possible f , } x2^2\ x3^2 + x2^2\ x4^2$$

Now check whether it's in the radical.

It is ----

$$\text{A possible f , } x3^4 + x4^4$$

Now check whether it's in the radical.

It is not! We have a new f!

$$\text{The set F so far , } [x1^2 , x2^2 , x3^2 + x4^2 , x3^4 + x4^4]$$

Checking whether we have full radical --

We do!

The set F of primary invariants is,

$$[x1^2 , x2^2 , x3^2 + x4^2 , x3^4 + x4^4]$$

and we have the correct number.

The degrees of the f's are [2, 2, 2, 4]

The bound on the degree of a g is 6

The number of g's is 4

$$\text{mol} := \frac{t^4 + 1}{(t - 1)^4\ (t + 1)^4}$$

$$\text{polyg} := 1 + t^2 + t^4 + t^6$$

degg, [2, 4, 6]

numg, [1, 1, 1]

G := [1]

A possible g , x1 x2

and we keep it!

A possible g , $x1^4$

but it is rejected.

A possible g , $x1^3$ x2

but it is rejected.

A possible g , $x1^2$ $x2^2$

but it is rejected.

A possible g , $x1^2$ $x3^2$ + $x1^2$ $x4^2$

but it is rejected.

A possible g , $x1^3$ x2

but it is rejected.

A possible g , x1 x2 $x3^2$ + x1 x2 $x4^2$

but it is rejected.

A possible g , $x2^4$

but it is rejected.

A possible g , $x2^2$ $x3^2$ + $x2^2$ $x4^2$

but it is rejected.

A possible g , $x3^3$ $x4^3$ - x3 x4

and we keep it!

```
                                  3                   3
A possible g , x1 x2 x3  x4 - x1 x2 x3 x4

and we keep it!

A Cohen-Macaulay basis is ,

    2    2    2     2    4     4
[x1 , x2 , x3  + x4 , x3  + x4 , 1, x1 x2,

    3          3         3                  3
 x3  x4 - x3 x4 ,x1 x2 x3  x4 - x1 x2 x3 x4 ]

[x1**2, x2**2, x3**2+x4**2, x3**4+x4**4, 1, x1*x2,
 x3**3*x4-x3*x4**3, x1*x2*x3**3*x4-x1*x2*x3*x4**3]
                        Time, 17.084
```

REFERENCES

[1] L. Bachmair and B. Buchberger, *A Simplified Proof of the Characterization Theorem for Gröbner Bases,* ACM SIGSAM Bull. **14**, No. 4 (1980), 29-34.

[2] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes Nach einem Nulldimensionalen Polynomideal,* Ph.D. Thesis, Univ. of Innsbruck (Austria), Math. Inst., 1965.

[3] B. Buchberger, *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory* – in *Multidimensional Systems Theory,* (N.K. Bose, *ed.*), Reidel Publ. Co., Dordrecht (1985), 184-232.

[4] W. Burnside, *Theory of Groups of Finite Order (2nd Edn.),* Cambridge University Press, 1911.

[5] B. Char, K. Geddes, G. Gonnet, M. Monagan, and S. Watt, *Maple Reference Manual (5th Edn.),* Waterloo Maple Publishing, Waterloo, Ontario, 1990.

[6] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms (prepublication manuscript),* Amherst, Mass., 1990.

[7] W. Gröbner, *Moderne Algebraische Geometrie,* Springer-Verlag, Wien–Innsbruck, 1949.

[8] L. Grove, *Algebra,* Academic Press, New York, 1983.

[9] L. Grove and C. Benson, *Finite Reflection Groups (2nd Edn.),* Springer-Verlag, New York, 1985.

[10] R. Hartshorne, *A Property of A-Sequences,* Bull. Soc. Math. France **94** (1966), 61-64.

[11] D. Hilbert, *Über die Theorie der Algebraischen Formen,* Math. Ann. **36** (1890), 471-534.

[12] D. Hilbert, *Über die Vollen Invariantensysteme,* Math. Ann. **42** (1893), 313-373.

[13] H. Hironaka, *Resolution of Singularities of an Algebraic Variety over a Field of Characteristic Zero,* Ann. Math. **79** (1964), 109-326.

[14] M. Hochster and J. Eagon, *Cohen-Macaulay Rings, Invariant Theory, and the Generic Perfection of Determinantal Loci,* Amer. J. of Math. **93** (1971), 1020-1058.

[15] W. Huffman and N. Sloane, *Most Groups Have Messy Invariants,* Advances in Math. **32**, No. 2 (1979), 118-127.

[16] I. Kaplansky, *Commutative Rings (Revised Edn.),* Univ. of Chicago Press, Chicago, 1974.

[17] G. Kempf, *Computing Invariants* – in *Invariant Theory,* (S. S. Koh, *ed.*), Springer Lecture Notes in Math. No. 1278, Springer-Verlag, Heidelberg, 1987.

[18] G. Kempf, *The Hochster-Roberts Theorem of Invariant Theory,* Michigan Math. J. **26** (1979), 19-32.

[19] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry,* Birkhäuser, Boston, 1985.

[20] H. Matsumura, *Commutative Ring Theory,* Cambridge Univ. Press, 1986.

[21] S. McAdam, *Primes and Annihilators,* Bull. Amer. Math. Soc. **76** (1970), 92.

[22] T. Molien, *Über die Invarianten der Linearen Substitutionsgruppe,* Sitzungsber. König. Preuss. Akad. Wiss. (1897), 1152-1156.

[23] E. Noether, *Der Endlichkeitssatz der Invarianten Endlicher Gruppen,* Math. Ann. **77** (1916), 89-92.

[24] D. Northcott, *Lessons on Rings, Modules and Multiplicities,* Cambridge at the University Press, 1968.

[25] M. Schönert et al. *GAP – Groups, Algorithms, and Programming.* Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, first edition, 1992.

[26] N. Sloane, *Error-correcting Codes and Invariant Theory,* Amer. Math. Monthly **84** (1977), 82-107.

[27] W. Smoke, *Dimension and Multiplicity for Graded Algebras,* J. of Algebra **21** (1972), 149-173.

[28] T. Springer, *Invariant Theory,* Springer Lecture Notes in Math. No. 585, Springer–Verlag, Berlin, 1977.

[29] R. Stanley, *Invariants of Finite Groups and Their Applications to Combinatorics,* Bull. Amer. Math. Soc **1**, no. 3 (1979), 475-511.

[30] B. Sturmfels and N. White, *Computing Combinatorial Decompositions of Rings,* Combinatorica, **11** (1991), 275-293.

[31] H. Weyl, *The Classical Groups,* Princeton Univ. Press, Princeton, 1946.