GENERATING FUNCTIONS ASSOCIATED TO POLYNOMIAL INVARIANTS

Matthew Evat

Supervisor: Associate Professor Daniel Chan

School of Mathematics and Statistics
UNSW Sydney

October 2017

Submitted in partial fulfillment of the requirements of the degree of
Bachelor of Science (Advanced Mathematics) with Honours

Plagiarism statement

I declare that this thesis is my own work, except where acknowledged, and has not been submitted for academic credit elsewhere.

I acknowledge that the assessor of this thesis may, for the purpose of assessing it:

- Reproduce it and provide a copy to another member of the University; and/or,
- Communicate a copy of it to a plagiarism checking service (which may then retain a copy of it on its database for the purpose of future plagiarism checking).

I certify that I have read and understood the University Rules in respect of Student Academic Misconduct, and am aware of any potential plagiarism penalties which may apply.

By signing this declaration I am agreeing to the statements and conditions above.

Signed: _____ Date: _____

Acknowledgements

First and foremost, I would like to thank my supervisor Daniel Chan. Without his guidance I would never have known where to start. Daniel's enthusiasm and love for maths made all the hours spent with him throughly enjoyable.
I would also like to thank my family and my girlfriend Eva Turco for their continued support over the year. Also, thanks to this Honours cohort for the consistent banter and support which has made this year special. Finally thanks be to God.

Abstract

The theory of invariants of finite groups is an interesting and relatively self-contained field in commutative algebra. Moreover there are close connection between this field and combinatorics, which stem from the use of the Hilbert series and Molien series, which are related to the combinatorial tool of the generating function, in invariant theory. We explore this link throughout the thesis. Also we explore the idea of Cohen-Macaulay ring and display why it is useful for invariant theory. Later we present a method of computing the sum $S_2(g)$ using the algebraic tool of invariant theory.

Contents

Chapter 1

Introduction

1.1 Preface

We begin with the concept of invariant of a finite group, which is when an element, p, of a ring R is fixed by a well defined group action Mp. These are important because any questions in combinatorial theory and other fields can be reduced to the problem of finding all polynomials $p \in \mathbb{C}[x_1, \ldots x_n]$ satisfying $Mp = p$, for all M in some finite subgroup of $G \subset \mathrm{GL}_n$.

1.2 Aim

The goal of this thesis is to provide the reader with an introduction into the theory of invariants of finite groups. We are solely interested in polynomial invariants as they have nice properties. An important object that we use is the Hilbert series, which is defined $F(R, \lambda) = \sum \dim(R_n)\lambda^n$. The Hilbert series is useful in two ways, (a) it relates the theory of invariants of finite groups to combinatorics and (b) it allows to form a nice decomposition of the algebra of invariants with the use of Cohen Macaulay structure. Another interesting concept is the different methods of computing Hilbert series, via (a) Molien's Theorem or (b) direct computation. The surprise is that $F_G(\lambda)$ is a rational function, which is impressive in the fact that it is a finite expression which contains infinite information. The importance of these two approaches is that it allows combinatorial methods to study invariant theory and visa versa.

Moreover there are close connections between this subject and combinatorics, for two reasons: firstly there is the highly combinatorial tool of a generating function, which pervades the study of the invariants of finite groups, and there are direct applications to combinatorics.

1.3 History

Invariant theory has already been pronounced dead several times, and it has risen like a phoenix from the ashes. The first big period for invariant theory was in the late 19th century and the early 20th century, with the discovery of the 'symbolic

method' which in theory allowed the computation of all invariants by a quasi-mechanical process. As these were hard to compute, the next problem in the theory was the search for 'fundamental systems' of invariants, i.e. finite sets such that any invariant would be a polynomial in the fundamental invariants. These systems were proved by Hilbert in 1890s, in a decade where Hilbert made great advances for invariant theory ([3] and [4]) which made him famous. This leads us into the theory of invariants of finite groups.
The fundamental problem of the theory of invariants of finite groups is to 'determine' the algebra R^G of invariants.

Theorem 1.3.1. *Let G have order g and degree m. Then R^G is generated as an algebra over $\mathbb{C}$ by no more than $\binom{g+m}{m}$ homogenous invariants, of degree not exceeding g.*

Proof. See [9, pp. 275-276]. □

For many purposes Noether's result, gives a satisfactory answer to the problem of determining R^G. However we can ask for more precise information, namely a description of all the invariants. This can be done in two ways, either finding a relationship between the generators of R^G or by finding a canonical form for the elements of R^G.

1.4 Structure of Thesis

Chapter 2 introduces the background theory, relevant for this thesis. The main concepts in this chapter are modules and representation theory. The first half of Chapter 3 sets up the theory of Hilbert functions and Hilbert series. However the second half uses one of the main tools at our disposal to calculate the algebra of invariants, namely Molien's Theorem. We present a proof of Molien's Theorem and then show how one can use Molien's Theorem to compute the algebra of invariants. Chapter 4 relates the Invariant Theory to the Theory of Cohen Macaulay rings. The two main ideas of this chapter are firstly that R^G is Cohen Macaulay and the decomposition of the Molien series. This decomposition of the Molien series allows us to write $F_G(\lambda)$ in the form of a rational polynomial, which is interesting as there is infinite information stored in a finite function. In chapter 5 we see one of the combinatorial applications of invariant theory in calculating $S(g) = \sum_\omega |1-\omega|^{-2}$, where ω ranges over the g-th complex roots of unity without $\omega = 1$. Later in the chapter we present an algorithm to calculate a related sum, namely $S_2(g) = \sum_\omega |1-\omega|^{-4}$. Chapter 6 gives a summary of the thesis and mentions areas of future research.

1.5 Assumed knowledge

It is assumed that the reader is sufficient in group and ring theory to an undergraduate level.

Chapter 2

Background on Invariant Theory and Generating Functions

In this chapter we shall cover some of the basic concepts and definitions of invariant theory. We shall also introduce generating functions.

2.1 Invariant theory

Over the course of this thesis, we denote $R = \mathbb{C}[x_1, \ldots, x_m]$ to be the complex polynomial ring with m variables. Also we shall denote $\mathrm{GL}(V)$ as the group of all invertible linear transformations $M \in \mathrm{GL}_m$.

Definition 2.1.1. *Take $M \in GL_m$ and $p \in R$. Then the action $Mp(x) = p(Mx)$.*

Example 2.1.2. *If we take*

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix},$$

and $f(x_1, x_2) = x_1^2 + x_2^2$, then

$$\begin{aligned} Mf(x_1, x_2) &= f\left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) \\ &= f\left(\frac{1}{\sqrt{2}}(x_1 + x_2), \frac{1}{\sqrt{2}}(-x_1 + x_2)\right) \\ &= \frac{1}{2}(x_1 + x_2)^2 + \frac{1}{2}(-x_1 + x_2)^2 \\ &= x_1^2 + x_2^2. \end{aligned}$$

So a polynomial $p \in R$ satisfying $Mp = p$ for all M in some finite subgroup $G \subset \mathrm{GL}(V)$ is called an invariant. If we collect all the invariants of R, they clearly form a subalgebra, and are denoted by R^G. Thus we define the algebra of invariants by

$$R^G = \{p \in R : Mp = p \text{ for all } M \in G\}.$$

Note that Mp is a well defined group action

Proof. Let's take $\phi : G \times X \to X$, where G is a finite group and X is the set of complex polynomials. Firstly, let e be the identity matrix and let $p \in X$. Then, it follows that

$$\phi(e, p) = ep(x) = p(e(x)) = p(x) = p.$$

Next, we let $g, h \in G$ and are required to show $\phi(g, \phi(h, p)) = \phi(gh, p)$.

$$\begin{aligned}\phi(g, \phi(h, p)) &= ghp(x) \\ &= p(gh(x)) \\ &= \phi(gh, p).\end{aligned}$$

Thus, ϕ is a well defined group action. □

Theorem 2.1.3. *If G has degree m, then there exist m, but not $m+1$ algebraically independent invariants.*

Proof. See [1, Section 262]. □

Example 2.1.4. *To get a feel for what is happening, we shall start simple. We take G to be the group generated by*

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Also let $R = \mathbb{C}[x, y]$. Then the natural question is to determine R^G. If we take $p_1(x, y) = x + y$ and $p_2(x, y) = xy$ then it follows that

$$p_1(M\boldsymbol{x}) = p_1(y, x) = y + x = x + y = p_1(\boldsymbol{x}),$$

and

$$p_2(M\boldsymbol{x}) = p_2(y, x) = yx = xy = p_2(\boldsymbol{x}),$$

which implies that p_1 and p_2 are invariants. Thus it follows that $\mathbb{C}[xy] \subset \mathbb{C}[x, y]^G$ and $\mathbb{C}[x+y] \subset \mathbb{C}[x, y]^G$. For other inclusion we use the above theorem, as $\dim V = 2$ then we have found all the invariants and xy and $x+y$ are algebraically independent. Thus we can conclude that $\mathbb{C}[x, y]^G = \mathbb{C}[x + y, xy]$. However actually know a more general statement $\mathbb{C}[x_1, \ldots, x_n]^{S_n} = \mathbb{C}[e_1, \ldots, e_n]$ where e_i is the i-th symmetric polynomial.

2.2 Generating functions

We introduce the concept of a generating function, as they are interlinked with the Hilbert function and Molien series, which we shall define later. They are a helpful

tool as they store an infinite amount of data, such as the data of differentiating an infinite sum.

Suppose a_r is the number of ways to select r objects in a certain procedure.

Definition 2.2.1. *Then $g(\lambda)$ is a generating function for a_r if $g(x)$ has the polynomial expansion:*

$$g(\lambda) = a_0 + a_1\lambda + \dots a_r\lambda^r + \dots.$$

Also note that if the polynomial has an infinite number of terms, it is called a power series. Next we shall go over some of the basic rules of generating functions.

1. **Scaling**

   Multiplying a generating function by a constant scales every term in the associated sequence by the same constant. For example we know

   $$1 + \lambda^2 + \lambda^4 + \cdots = \frac{1}{1-\lambda^2}.$$

   But multiplying this generating function by 2 gives,

   $$\frac{2}{1-\lambda^2} = 2 + 2\lambda^2 + 2\lambda^4 + \dots.$$

2. **Addition**

   Adding generating functions corresponds to adding the two sequences term by term. For example we know that

   $$1 + \lambda + \lambda^2 + \cdots = \frac{1}{1-\lambda},$$

   and that

   $$1 - \lambda + \lambda^2 - \lambda^3 + \cdots = \frac{1}{1+\lambda}.$$

   Then

   $$\frac{1}{1-\lambda} + \frac{1}{1+\lambda} = 2 + 2\lambda^2 + \cdots = \frac{2}{1-\lambda^2}.$$

3. **Differentiation**

   In general, differentiating a generating function has two effects on it. One is that each term is multiplied by it's index, and also that each term is shifted one to the left. The derivative rule is if

   $$f(x) = \sum_{k=0}^{\infty} c_k\lambda^k$$

   then

   $$f'(x) = \sum_{k=0}^{\infty} kc_k\lambda^{k-1}.$$

2.3 Module Theory

We shall define some of the basic concepts of modules.

Definition 2.3.1. *A (left)* R-module *is an additive group* M *equipped with a scalar multiplication map* $R \times M \to M : (r, m) \to rm$ *such that the following axioms hold (for all* $m, m' \in M, r, r' \in R$*)*

1. $1m = m$
2. *(associativity)* $r(r'm) = (rr')m$
3. *(distributivity)* $(m + m') = rm + rm'$ *and* $(r + r')m = rm + r'm$.

We also can similarly define right R-modules in a similar way. In our case as R is a commutative ring, it is both a left and right R-module.

Example 2.3.2. *For a field* k*, a right* k*-module is just a vector space over* k *with scalars on the right. Here module axioms are equivalent to vector space axioms.*

Example 2.3.3. R *itself is a left and right* R*-module, with module addition and scalar multiplication the same as the ring addition and scalar multiplication respectively.*

Definition 2.3.4. *Let* M *be an* R*-module. An* R-submodule *is an additive subgroup* N *of* M *which is closed under scalar multiplication. In this case,* N *is an* R*-module, and we write* $N \leq M$.
For $N \leq M$*, the quotient abelian group* M/N *has an induced* R*-module structure:* $r(m + N) := rm + N$¿ *This is called the quotient module of* M *by* N.

Definition 2.3.5. *Let* M, N *be* R*-modules. A function* $\phi : M \to N$ *is an* R-module homomorphism *if it satisfies*

$$\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2) \quad \textit{for all } m_1, m_2 \in M,$$

and

$$\phi(rm) = r\phi(m) \quad \textit{for all } r \in R, m \in M.$$

As is the case with groups and rings, a bijective R-module homomorphism is called an isomorphism.

Notation: We denote the set of R-module homomorphisms by $\mathrm{Hom}_R(M, N)$, and if $N = M$, then this is denoted by $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$. The group of all unit elements in $\mathrm{End}_R(M)$ is the automorphism group, denoted by $\mathrm{Aut}_R(M)$.

Definition 2.3.6. *We say that an R-module is a direct sum of submodules M_i, $i \in I$ and write $\bigoplus_{i\in I} M_i$, if*

$$(1) M = \sum_{i\in I} M_i$$
$$(2) M_i \cap \sum_{j\in I-\{i\}} M_j \qquad \text{for all } i \in I.$$

Note that if $M = \sum_{i\in I}^{\oplus} M_i$, then $M \cong \bigoplus_{i\in I} M_i$.

Definition 2.3.7. *Let R be a ring. A* free module *is one which is isomorphic to a direct sum of copies of R. That is, M is a free module if*

$$M \cong \bigoplus_{i\in I} R.$$

If I is finite, then we write $R^n = \bigoplus_{i\in I} R = R \times R \times \cdots \times R$.

Definition 2.3.8. *A set of elements $\{f_i | i \in I\}$ of an R-module F is called a* basis *if*

$$F = \sum_{i\in I} Rf,$$

and whenever $r_1 f_1 + \cdots + r_n f_n = 0$, all $r_j = 0$.

Definition 2.3.9. *Let M be a (left) R-module, and L be a subset of M. The* submodule generated *by L is the set of all r-linear combinations of elements of L. It is a submodule of M, and is denoted $\sum_{l\in L} Rl$.*

Definition 2.3.10. *If $\sum_{l\in L} Rl = M$ then L is a* generating set *for M.*

If L is finite, then M is called a finitely generated module.

Definition 2.3.11. *If A is a ring that is also an R-module such that the underlying abelian groups are the same and the ring multiplication and scalar multiplication satisfies the following compatibility condition:*

$$r(ab) = (ra)b = a(rb), \quad \text{for all } r \in R \text{ and } a, b \in A,$$

*then A is called an R-*algebra*.*

Example 2.3.12. *Every ring is a $\mathbb{Z}$-algebra.*

Definition 2.3.13. *Let R be a ring. Let $e \in R$, then e is* idempotent *if $e^2 = e$.*

Definition 2.3.14. *Let G be a group. Define the free R-module*

$$RG := \bigoplus_{\sigma\in G} R\sigma,$$

of all formal linear combinations of elements of G. Then RG is a R-algebra called the group algebra *of G.*

Note that RG has ring multiplication induced by group multiplication in the following sense

$$(\sum \alpha_{g_i} g_i)(\sum \beta_{g_j} g_j) = \sum_{g \in G} (\sum_{g_i g_j = g} \alpha_{g_i} \beta_{g_j} g).$$

Theorem 2.3.15 (Maschke)**.** *Let G be a finite group, k a field such that char $k \nmid |G|$. Then kG is semisimple.*

Theorem 2.3.16 (Wedderburn)**.** *if R is a right semisimple ring, then*

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r),$$

for some division ring $D_i$and positive integers $r, n_i \in \mathbb{Z}$.

2.4 Representation Theory

Next we shall introduce the notion of representations of finite groups. We start with the definition of a representation

Definition 2.4.1. *A group homomorphism $\rho : G \to \mathrm{Aut}_R(M)$ is called a* representation *of G on the R-module M.*

Before we define a k-character we shall recall the properties of the trace function. Fix a field k, then $\mathrm{tr} : M_n(k) \to k$ defined by $(a_{i,j}) \to \sum_{i=1}^{n} a_{i,j}$.

Definition 2.4.2. *Let $\rho : G \to GL(V)$ be a representation of G over a finite dimensional space k-space V. The* k-character *of ρ is the function*

$$\chi_V : G \to k, \quad g \to tr(\rho(g)).$$

Definition 2.4.3. *The* trivial character *that takes the value of one for all group elements.*

Now we introduce and define the Reynold's operator.

Definition 2.4.4. *Fix k to be a field, and denote the characteristic of k by* $\mathrm{char}\, k$*. We shall assume that G is finite and that $k \nmid G$. We let*

$$e = \frac{1}{|G|} \sum_{g \in G} g \in kG.$$

Thus the map $(\cdot)^\natural : kG \to kG, x \to xe$ is a module homomorphism and is a projection onto the component $(kG)e$.

More generally, let G be a finite group of order n, and R be a commutative ring such that $n \in R^*$. Then it follows that

$$e = \frac{1}{|G|} \sum_{g \in G} g \in RG.$$

Next, let M be a left RG-module. The left multiplication by e defines an RG-module homomorphism

$$(\cdot)^\natural : M \to M, m \to em.$$

This is called the Reynold's operator.

2.5 Grading

Definition 2.5.1. *A* homogenous polynomial *is one in which all its terms have the same degree.*

Example 2.5.2. *In $\mathbb{C}[x, y], 3x^2y + 3y^3 + x^2$ isn't homogenous, as $\deg(3x^2y) = \deg(3y^3) = 3 \neq \deg(x^2) = 2$. However, $3x^2y + 3y^3 + x^3$ would be homogenous, as all the terms have degree 3.*

We define grading of a ring as

Definition 2.5.3. *A ring R is called $\mathbb{N}$-graded if there exists a family of subgroups $\{R_n\}_{n \in \mathbb{N}}$ of R such that*

- $R = \bigoplus_n R_n$
- $R_n R_m \subseteq R_{n+m} \quad \forall n, m \in \mathbb{N}.$

Note that these are not subgroups as there is no additive inverse, so we say that $0 \in R_n$. The intuitive example is the polynomial ring, where one can grade the polynomials by their degrees. Note that the grading of an algebra and a module is defined similarly. Next we take B to be an $\mathbb{N}$-graded k-algebra which is defined to be a finitely generated k-algebra B together with a vector space direct sum decomposition

$$B. = B_0 \bigoplus B_1 \oplus B_2 \oplus \ldots,$$

such that $B_0 = k$ and $B_i B_j \subset B_{i+j}$. We call B_n the n-th homogenous part of B, and an element, $f \in B_n$, is said to be homogenous of degree n, denoted deg $f = n$. Then we define a $\mathbb{Z}$-graded B-module to be a finitely-generated B-module Λ, together with the vector space decomposition:

$$\Lambda = \oplus_{i \in \mathbb{Z}} \Lambda_i.$$

A linear map between two $\mathbb{N}$-graded vector spaces $f : V \to W$ is a graded linear map if it preserves the grading of homogenous elements. A graded linear map is

also defined to be a homomorphism of graded vector spaces if $f(V_i) \subseteq W_i$ for all $i \in \mathbb{N}$.

2.6 Symmetric Polynomials

Invariant theory is interlinked with the theory of symmetric functions as in many cases these polynomials are invariants. So we shall introduce some concepts of symmetric polynomials.

The main idea of a symmetric polynomial is that if the variables are permuted then the polynomial remains unchanged. We shall define the basic symmetric polynomials.

Definition 2.6.1. *Take $n \in \mathbb{Z}^+$. Elementary symmetric polynomials in n variables, namely $x_1, x_2, \ldots, x_n$ written $e_k(x_1, x_2, \ldots, x_n)$ (where $0 \leq k \leq n$) are defined by*

$$\begin{aligned} e_0(x_1, x_2, \ldots, x_n) &= 1 \\ e_1(x_1, x_2, \ldots, x_n) &= \sum_{1 \leq j \leq n} x_j \\ e_2(x_1, x_2, \ldots, x_n) &= \sum_{1 \leq j < k \leq n} x_j x_k \\ &\vdots \\ e_n(x_1, x_2, \ldots, x_n) &= x_1 x_2 \ldots x_n. \end{aligned}$$

Next we shall clarify the notion of monomial in this thesis

Definition 2.6.2. *A **monomial** is a product of powers of variables with positive integer exponents. The constant to this polynomial is 1, which is equal to the x_i^0 for any variable x_i.*

Example 2.6.3. *If we take $R = \mathbb{C}[x_1, x_2, x_3]$, then $x_1^3 x_2^4 x_3^5$ is a monomial in R.*

Also note that if only a single variable, x_j, is considered then a monomial is the same as x_j^n.

Chapter 3

Molien's Theorem

We now focus on one of the tools at our disposal of calculating the algebra of invariants. We can use Molien's Theorem to compute the algebra of invariants because it enumerates all of the invariants and we will have enough information to know if our set of invariants is complete. Another thing to note is that Molien's theorem changes the problem of finding the algebra of invariants from an algebraic problem to a combinatorial problem.

In this chapter, we shall explore some of the background associated with Hilbert functions and then delve into Molien's Theorem, by first stating the theorem, then offering a proof of it. After we shall go through some examples to illustrate the usefulness of Molien's Theorem.

3.1 Hilbert function

Let B to be an $\mathbb{N}$-graded k-algebra, then we define a $\mathbb{Z}$-graded B-module to be a finitely-generated B-module Λ, together with the vector space decomposition

$$\Lambda = \bigoplus_{i \in \mathbb{Z}} \Lambda_i,$$

such that $B_i \Lambda_j = \Lambda_{i+j}$.

Definition 3.1.1. *The* Hilbert function $H(\Lambda, \cdot) : \mathbb{Z} \to \mathbb{N}$ *of* Λ *is defined by* $H(\Lambda, n) = \dim_k \Lambda_n$.

Note that the Hilbert function is well defined. This is because Λ is finitely generated B-module, so $\dim_k \Lambda_n$ will not be infinite. We can next move onto the Hilbert series.

Definition 3.1.2. *The* Hilbert series *(which is sometimes called the Poincare series) of* Λ *is defined as the formal Laurent series*

$$F(\Lambda, \lambda) = \sum_{n \in \mathbb{Z}} H(\Lambda, n) \lambda^n.$$

Example 3.1.3. *Let $\Lambda_2 = k[x_1, x_2]$, and now we shall calculate the Hilbert function in degree n. So we consider all the possible monomials of degree n:*

$$x_1^n, x_1^{n-1}x_2, \ldots, x_2^n.$$

So we can see that $H(\Lambda_2, n) = n + 1$. Further we shall calculate the Hilbert series of Λ_2:

$$\begin{aligned} F(\Lambda_2, t) =& \sum_{n\geq 0}(n+1)t^n \\ =& \frac{d}{dt}(1 + t + t^2 + \ldots) \\ =& \frac{d}{dt}\left(\frac{1}{1-t}\right) \\ =& \frac{1}{(1-t)^2}. \end{aligned}$$

In this example we can clearly see the relationship between the Hilbert series and a generating function.
Next we shall prove the general case, for a polynomial ring, $R' = \mathbb{C}[y_1, y_2, \ldots, y_n]$, where y_i have degree d_i, has Hilbert function of form

$$\prod_i \frac{1}{(1-\lambda^{d_i})}.$$

We claim that there is a bijective correspondence, in terms of monomials in their sums, between $F(R', t)$ and $\left(\sum_{i=0}^{\infty} t^{d_1 i}\right)\left(\sum_{i=0}^{\infty} t^{d_2 i}\right)\cdots\left(\sum_{i=0}^{\infty} t^{d_n i}\right)$.

Proof. First we shall consider monomials in

$$\left(\sum_{i_1=0}^{\infty} t^{d_1 i_1}\right)\left(\sum_{i_2=0}^{\infty} t^{d_2 i_2}\right)\cdots\left(\sum_{i_n=0}^{\infty} t^{d_n i_n}\right),$$

which are of the form $t^{d_1 i_1 + d_2 i_2 + \cdots + d_n i_n}$. Now this corresponds to $x_1^{d_1 i_1} x_2^{d_2 i_2} \ldots x_n^{d_n i_n} \in R'$. Next we consider an arbitrary monomial in R', which has the form $x_1^{d_1 i_1} x_2^{d_2 i_2} \ldots x_n^{d_n i_n}$, which is contained in $(\sum_{i_1=0}^{\infty} t^{d_1 i_1})(\sum_{i_2=0}^{\infty} t^{d_2 i_2}) \ldots (\sum_{i_n=0}^{\infty} t^{d_n i_n})$. □

Next as $\sum_{i_1=0}^{\infty} t^{d_1 i_1} = \frac{1}{(1-\lambda^{d_1})}$, we have a formula for the general case of R. The importance of this formula is that we can now read off the generators of the algebra of invariants.
We now prove two natural results about Molien series

Lemma 3.1.4. $F(\Lambda_1 \oplus \Lambda_2, \lambda) = F(\Lambda_1, \lambda) + F(\Lambda_2, \lambda)$.

Proof. If we consider the Hilbert series then it follows that

$$\begin{aligned} F(\Lambda_1 \oplus \Lambda_2, \lambda) &= \sum_{n\in\mathbb{Z}^+} H(\Lambda_1 \oplus \Lambda_2, n)\lambda^n \\ &= \sum_{n\in\mathbb{Z}^+} H(\Lambda_1, n)\lambda^n + \sum_{n\in\mathbb{Z}^+} H(\Lambda_2, n)\lambda^n \\ &= F(\Lambda_1, \lambda) + F(\Lambda_2, \lambda). \end{aligned}$$

□

Lemma 3.1.5. *If we let θ be a polynomial of degree d, then*

$$F(\theta\Lambda, \lambda) = \lambda^d F(\Lambda, \lambda).$$

Proof. If we recall the Hilbert series

$$F(\Lambda, \lambda) = \sum_{n\in\mathbb{Z}^+} H(\Lambda, n)\lambda^n.$$

Then it follows that $h(\theta\Lambda, n) = \dim(\theta\Lambda)_n$, where $\theta : \Lambda \to \theta\Lambda$ is a vector space isomorphism. Which is defined by $\Lambda_i \cong \theta\Lambda_i = (\theta\Lambda)_{i+d}$. Next from this isomorphism it follows that

$$\begin{aligned} \dim\ (\theta\Lambda)_n &= \dim\ \Lambda_{n-d} \\ &= H(\Lambda, n-d). \end{aligned}$$

Thus if we set $m = n - d$, then we can conclude

$$\begin{aligned} F(\theta\Lambda, n) &= \sum_{n\in\mathbb{Z}^+} H(\theta\Lambda, n)\lambda^n \\ &= \sum_{n\in\mathbb{Z}^+} H(\Lambda, n-d)\lambda^n \\ &= \sum_{m\in\mathbb{Z}^+} H(\Lambda, m)\lambda^{m+d} \\ &= \lambda^d F(\Lambda, n). \end{aligned}$$

□

Now when $\Lambda = R^G_\chi$ we call $\chi(1)^{-1}F(R^G_\chi, \lambda)$ the Molien series of the pair (G, χ) and we write $F_{G,\chi}(\lambda) = \chi(1)^{-1}F(R^G_\chi, \lambda)$. However for the majority of this thesis we shall only consider cases when χ is trivial, so we shall denote $F(R^G, \lambda)$ as the Molien series of G and write $F_G(\lambda) = F(R^G, \lambda)$.

3.2 Molien's Theorem

Lemma 3.2.1. *Let $p : W \to W^G$ be a projection of W onto W^G, defined by $w \to \frac{1}{|G|}\sum_{N\in G} Nw$. Then $\dim W^G = \operatorname{tr} p$.*

Proof. We claim that $W = W^G \oplus \ker p$. We take $w \in W$, and since p is idempotent, we must have $pw = p^2w$ and so $p(w - pw) = 0$. Hence $w - pw = x$ for some $x \in \ker p$. Thus $w = pw + x$, and this shows that $W = \operatorname{Im} p + \ker p$. Now take $y \in W^G \oplus \ker p$. Since $y \in \operatorname{Im} p$ we have $y = pz$ for some $z \in W$. Applying p to both sides we get $py = p^2z$, but as $y \in \ker p$ it follows that $0 = py = p^2z = pz = y$. Thus $W^G \cap \ker p = 0$ and we conclude $W = W^G \oplus \ker p$. This implies that we can write p with respect to a basis for W^G and with a basis for $\ker p$. If we were to represent this in a matrix, the lemma clearly follows. □

Theorem 3.2.2. *Let G be a finite subgroup of $GL(V)$ of order g, and let $\chi \in X(G)$. Then the Molien series $F_{G,\chi}(\lambda)$ is given by*

$$F_{G,\chi}(\lambda) = \frac{1}{g}\sum_{M\in G} \frac{\chi(M)}{det(I - \lambda M)}.$$

Proof. We shall assume that $G = \{1, M, M^2, \ldots, M^{g-1}\} \cong \mathbb{Z}/g\mathbb{Z}$, and χ is trivial. As $F_G(\lambda) = \sum \dim R_n^G \lambda^n$, we have to compute $\dim R_n^G$.
Suppose G acts on a vector space W linearly.

$$w + Mw + M^2w + \cdots + M^{g-1}w = \sum_{N\in G} Nw.$$

We have the fact that $p : W \to W$ defined by $w \to \frac{1}{|G|}\sum_{N\in G} Nw$ is a projection of W onto W^G. Since this is a projection, it follows that $\dim W^G = \operatorname{tr} p$. Next we consider $\operatorname{tr} p = \frac{1}{|G|}\sum_{N\in G} \operatorname{tr}(N \text{ acting on } W)$. So we look at $W = R_n$, where R_n is the span of monomials of the form $x_1^{a_1}x_2^{a_2}\cdots x_m^{a_m}$ where $a_1 + a_2 + \cdots + a_m = n$.
Now N acting on W is diagonalisable because $N^{|G|} = 1$ and $X^{|G|} - 1 = 0$ have distinct roots. We now change basis and assume $x_1, \ldots, x_m$ is an eigenbasis with eigenvales $v_1, \ldots, v_m$. This implies that an eigenbasis for R_n is

$$\{x_1^{a_1}x_2^{a_2}\cdots x_m^{a_m} | \sum_{i=1}^{m} a_i = n\}$$

and the corresponding eigenvalues is $v_1^{a_1}\cdots v_m^{a_m}$. Hence from this action of N we have

$$\operatorname{tr}(N|_{R_n}) = \sum v_1^{a_1}\cdots v_m^{a_m}.$$

As we can write $\det(I - \lambda M) = (1 - \lambda v_1) \cdots (1 - \lambda v_m)$, it follows that

$$\begin{aligned}\frac{1}{\det(I - \lambda M)} &= \frac{1}{(1 - \lambda v_1)(1 - \lambda v_2) \cdots (1 - \lambda v_m)} \\ &= (1 + \lambda v_1 + \cdots)(1 + \lambda v_2 + \lambda^2 v_2^2 + \cdots) \cdots (1 + \lambda v_m + \cdots \lambda^2 v_m^2 + \cdots).\end{aligned}$$

Now if we compare coefficients of λ^n in $\operatorname{tr}(N|_{R_n})$ and $\frac{1}{\det(I-\lambda M)}$ we can conclude that $\sum \dim R_n^G \lambda = \frac{1}{g} \sum_{M \in G} \frac{1}{\det(1-\lambda M)}$. □

As $\det(I - \lambda M) = \det(M) \det(\lambda - M^{-1})$, the roots are the eigenvalues of M^{-1}. As $(M^{-1})^{|G|} = I$, it follows that the minimum polynomial of $\det(I - \lambda M)$ divides $\lambda^{|G|} - 1$. This implies that Molien's Theorem does not have any poles, as λ is the Maclaurin series around 0, so λ. Now the benefit of Molien's Theorem is that this gives a method to compute the algebra of invariants and then we are able to check whether the tentative list of invariants we have is complete. Compared to Noether's result this gives more precise information on the algebra of invariants. Another thing to note about Molien's Theorem, is that it relates invariant theory to combinatorics, with the combinatorial tool of generating functions.
Now in this example we shall display how one would use Molien's Theorem to compute the algebra of invariants, or more correctly, to show that we have found a complete list of invariants. However before we present an example of how to compute the algebra of invariants with the use of Molien's Theorem, we first prove a useful result about homogenous polynomials.

Lemma 3.2.3. *Suppose we have a homogenous polynomial in $\mathbb{C}[x, y]$ of degree n. Then this can rewritten as*

$$a_n(x - \alpha_1 y)(x - \alpha_2 y) \dots (x - \alpha_n y),$$

where $a_n, \alpha_i \in \mathbb{C}$.

Proof. First let's consider an arbitrary homogenous polynomial $a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_0 y^n = 0$. If we take out a 'common factor' of y we can conclude that

$$y^n \left(a_n \left(\frac{x}{y} \right)^n + a_{n-1} \left(\frac{x}{y} \right)^{n-1} + \cdots + a_0 \right) = 0.$$

Next, as we are working over the field of complex numbers we are guaranteed by the fundamental Theorem of Algebra that there exist α_i such that

$$a_n y^n \left(\frac{x}{y} - \alpha_1\right)\left(\frac{x}{y} - \alpha_2\right)\cdots\left(\frac{x}{y} - \alpha_n\right) = 0.$$

So if we distribute one y to each term it we conclude that

$$a_n(x - y\alpha_1)\cdots(x - y\alpha_n).$$

□

Example 3.2.4. *First we let $R = \mathbb{C}[x, y]$. Then let $G = \{I, M, M^2, M^3\}$ where $M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Now the Molien series of G is given by*

$$\begin{aligned} F_G(\lambda) &= \frac{1}{4}\left[\frac{1}{(1-\lambda)^2} + \frac{2}{1+\lambda^2} + \frac{1}{1+\lambda)^2}\right] \\ &= \frac{1}{4}\left(\frac{(1+\lambda^2)(1+\lambda)^2 + 2(1-\lambda)^2(1+\lambda)^2 + (1-\lambda)^2(1+\lambda^2)}{(1-\lambda)^2(1+\lambda^2)(1+\lambda)^2}\right) \\ &= \frac{1+\lambda^4}{(1-\lambda^2)(1-\lambda^4)}. \end{aligned}$$

Now we may rewrite $F_G(\lambda)$ as

$$F_G(\lambda) = (1+\lambda^2+\lambda^4+\dots)(1+\lambda^4+\lambda^8+\dots)+\lambda^4(1+\lambda^2+\lambda^4+\dots)(1+\lambda^4+\lambda^8+\dots).$$

From the definition of the Hilbert function, it follows that dim R_2^G = the coefficient of λ^2 in the Molien series. So we conclude that there exists a $\theta_1 \in R_2^G$ and this implies that $\mathbb{C}[\theta_1] \subseteq R^G$.
As dim $R_4^G = 3$, one of these invariants we can construct from θ_1^2, as $\theta_1 \in R_4^G$. Nevertheless we suspect that there might be another invariant θ_2, such that $\theta_2 \in R_4^G - \mathbb{C}[\theta_1]$. Now another way to rephrase this question would be to ask if $\mathbb{C}[\theta_1, \theta_2]$ is a polynomial ring.
We know that $\mathbb{C}[\theta_1, \theta_2]$ is a polynomial ring if

$$p_n(\theta_1)\theta_2^n + p_{n-1}(\theta_1)\theta_2^{n-1} + \cdots + p_0(\theta_1) = 0.$$

As we can choose p_i such that the polynomial is homogenous, from lemma 3.0.11 we can conclude that the equation only holds if θ_1 and θ_2 are dependent. Thus we can conclude that $\mathbb{C}[\theta_1, \theta_2] \subseteq R^G$. However we are still missing one part of the dimension. So we shall pick $\eta \in R^G - \mathbb{C}[\theta_1, \theta_2]$. Next we know that $\mathbb{C}[\theta_1, \theta_2, \eta]$ is not a polynomial ring, as $R = \mathbb{C}[x, y]$ guarantees that there is only two algebraic independent invariants. So this implies that R^G is of the form $\mathbb{C}[\theta_1, \theta_2] \oplus \eta\mathbb{C}[\theta_1, \theta_2]$.

In this example we saw the usefulness of the Hilbert function and why it used to compute the algebra of invariants. Although in this example we also saw one of the setbacks of using the Hilbert function, namely that in the coefficient of λ^n we can't differentiate whether it came from the numerator and the denominator. This is a setback, as the denominators of the Molien series can relate to the generator of the algebra of invariants.

Example 3.2.5. *For a better understanding of this theorem, we shall calculate the invariants of the dihedral group of order k. Note that in this example, we shall take* $R = \mathbb{C}[x, y]$. *The dihedral group* ($G = D_{2k}$) *is generated by*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix},$$

where ω *is a complex k-th root of unity. Next as*

$$\det \left[I - \lambda \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \omega^i & 0 \\ 0 & \omega^{-i} \end{pmatrix} \right] = 1 - \lambda^2,$$

and

$$det \left[1 - \lambda \begin{pmatrix} \omega^i & 0 \\ 0 & \omega^{-i} \end{pmatrix} \right] = (1 - \lambda\omega^i)(1 - \lambda\omega^{-i}),$$

we now have an expression for the Molien series:

$$F_G(\lambda) = \frac{1}{2g} \sum_{i=0}^{g-1} \frac{g}{1 - \lambda^2} + \frac{1}{(1 - \lambda\omega^i)(1 - \lambda\omega^{-i})}.$$

If we simplify this expression, it turns out that $F_G(\lambda) = \frac{1}{(1-\lambda^2)(1-\lambda^g)}$. *From this we can guess that the algebra of invariants might be generated by a degree 2 polynomial and a degree g polynomial.*
If we let $C_k = \langle \left(\begin{smallmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{smallmatrix} \right) \rangle$, *then we claim that*

$$R^{C_k} = \mathbb{C}[xy, x^k, y^k].$$

Now C_k *is generated by a matrix* ρ *which can be written as diag* (λ, λ^{-1}). *We have*

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \lambda x \\ \lambda^{-1} y \end{pmatrix}.$$

Hence monomials $x^{a_1}y^{a_2}$ *are mapped to monomials* $(\lambda x)^{a_1}(\lambda^{-1}y)^{a_2} = \lambda^{a_1-a_2}x^{a_1}y^{a_2}$. *Hence* $x^{a_1}y^{a_2}$ *is only invariant if and only if* $k \mid a_1 - a_2$. *Next we write* $a_1 = ka + r_1, a_2 = kb + r_2$ *,where* $0 \leq r_1, r_2 \leq k-1$. *As* $a_1 - a_2 = k(a-b) + (r_1 - r_2), r_1 = r_2$.

Therefore the invariant monomials are of the form $x^{ga_1}y^{ga_2}(xy)^c$ *where* $0 \leq c \leq k-1$. *Thus our claim is true.*
Next, we first have to see if any of the generators of R^{C_k} *are fixed under the action of* $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. *As this action is the same as swapping* x *and* y *around, it follows that* xy *is an invariant under the dihedral group, and thus we can conclude that it is still a generator of the algebra of invariants. Next both* x^g *and* y^g *aren't invariants under the group action of* $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, *because*

$$p_1\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right) = p_1\left(\begin{pmatrix} y \\ x \end{pmatrix}\right) = y^g.$$

Using a similar argument, it follows that y^g *is not an invariant. However, we are still looking for an invariant of degree* g, *and by inspection we can see that* $x^g + y^g$ *is an invariant of the dihedral group and thus we can conclude that*

$$R^G = \mathbb{C}[xy, x^g + y^g].$$

Note that another way of proving that x^k and y^k are not invariants is to use what have showed earlier, namely that the algebra of invariants when $G = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is $\mathbb{C}[xy, x+y]$. As we can not construct $p_1(xy) + p_2(x+y) = x^k$, we can conclude that x^k is not an invariant under the action of $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and also not an invariant of the dihedral group. In this example we saw one useful aspect of the Molien series, the fact that we can work backwards, to compute the algebra of invariants.

Chapter 4

Cohen Macaulay Rings

In this chapter we shall explore the relationship between the algebra of invariants and Cohen Macaulay rings. First we shall set up some of the theory about Cohen Macaulay rings and then we shall prove some interesting results relating to these and explain why they are useful.
The reason why we are interested in Cohen Macaulay rings is that they have nice properties, namely having a direct sum decomposition.

4.1 Cohen Macaulay Rings

Definition 4.1.1. *Let B be an $\mathbb{N}$-graded k-algebra, as defined in the previous chapter. We denote by dim B, as the* Krull dimension *of B, i.e. the maximum number of elements of B which are algebraically independent over k.*

Next we shall define a Cohen Macaulay ring as one in which Krull dimension is equal to the depth. Over the course of this chapter h.s.o.p. shall denote homogenous system of parameters.

Proposition 4.1.2. *Let B be as above, and let $\theta_1, \ldots, \theta_m$ be a h.s.o.p. for B. Then the following are equivalent:*

1. *B is a free module over $k[\Psi_1, \ldots, \Psi_m]$-module. In other words, there exists $\eta_1, \ldots, \eta_t \in B$ (which may be chosen to be homogenous) such that:*

$$B = \oplus_{i=1}^{t} \eta_i k[\theta_1, \ldots, \theta_m].$$

2. *For every h.s,o.p. $\psi_1, \ldots, \psi_m$ of B, B is a free $k[\psi_1, \ldots, \psi_m]$-module.*

The proof that these are equivalent can be found in [7, Theorem 2, p. iv-20]. Next we move on to one of the important and more interesting results of invariant theory/commutative algebra, namely that for finite G, that R^G is a Cohen Macaulay algebra. The first explicit answer to this question appeared in [5, Proposition 13]. But it was already apparently part of the folklore of commutative algebra before [5] appeared.
Before we prove this theorem, we must first state a useful result, Noether's normalisation Lemma.

Lemma 4.1.3. *Let D be an integral domain and let R be any finitely generated D-algebra extension of D. Then there is a non-zero element $c \in D$ and elements $z_1, \ldots, z_d$ in R_c algebraically independent over D_c such that R_c is a finitely generated module over its subring $D_c[z_1, \ldots, z_d]$, which is isomorphic to a polynomial ring over D_c.*

Proof. Originally proved in [6, pp. 28-35] but another proof is in [2, pp. 284-285]. □

Theorem 4.1.4. *For any finite $G \subset GL(V)$, R^G is a Cohen-Macaulay algebra.*

Proof. We claim that we can write $R = R^G \oplus U$, where U is an R^G-module. If $f \in R$, let $\phi(f) = \left(\frac{1}{g}\right) \sum_{M \in G} Mf$, which we recall from before is the Reynolds operator.
Next it follows that $\phi^2 = \phi$, (as the Reynolds operator is idempotent), we can take

$$U = \{f \in R : \phi f = 0\} = \{f - \phi f : f \in R\}.$$

Next we claim that R is finitely generated R^G-module. This is the same as integrability.
Let $f \in R$ and consider

$$P_f(t) = \prod_{M \in G} (t - M(f)).$$

The coefficients of $P_f(t)$ are symmetric functions of the $M(t)$'s, so by the action they will just get permuted, thus they are elements of R^G. Also $P_f(t)$ is clearly monic, and $P_f(t) = 0$ as there is an identity element, which implies $t - f$ is a factor of $P_f(t)$. Hence f is integral over R^G, which implies that R is a finitely generated R^G-module.
Now let $\theta_1, \ldots, \theta_m$ be a h.s.o.p. for R^G,note the existence of this is given by Noether's Lemma [8][p. 482]. Since R^G is finite over $\mathbb{C}[\theta_1, \ldots, \theta_m]$ and R is finite over R^G, it follows that R is finitely generated over $\mathbb{C}[\theta_1, \ldots, \theta_m]$, so $\theta_1, \ldots, \theta_m$ is a h.s.o.p. for R.
Since $x_1, \ldots, x_m$ is also a h.s.o.p. for R, and R is clearly a free $\mathbb{C}[x_1, \ldots, x_m]$-module, it follows from 5.0.3. that R is a free $\mathbb{C}[\theta_1, \ldots, \theta_m]$-module.
It follows from the decomposition $R = R^G \oplus U$ that

$$R/(\theta_1, \ldots, \theta_m) = R^G/(\theta_1, \ldots, \theta_m) \oplus U/(\theta_1, \ldots, \theta_m),$$

Next we choose a homogenous basis $\mathbb{C}$-basis $\bar{\eta}_1, \ldots, \bar{\eta}_s$ for $R/(\theta_1, \ldots, \theta_m)$ such that $\bar{\eta}_1, \ldots, \bar{\eta}_t$ is a $\mathbb{C}$-basis for $R^G/(\theta_1, \ldots, \theta_m)$ and $\bar{\eta}_{t+1}, \ldots, \bar{\eta}_s$ is a $\mathbb{C}$-basis for $U/(\theta_1 U + \cdots + \theta_m U)$. Now we lift $\bar{\eta}_i$ to a homogenous element η_i of R^G if $1 \leq i \leq t$ and

similarly to a homogenous element $\eta_i \in U$ if $t+1 \leq i \leq s$. By the previous proposition (as R^G, R are free over $\mathbb{C}[\theta_1, \ldots, \theta_m]$), we have $R = \oplus_1^s \eta_i \mathbb{C}[\theta_1, \ldots, \theta_m]$ and also $R^G = \oplus_1^t \eta_i \mathbb{C}[\theta_1, \ldots, \theta_m]$. Hence R^G is a free $\mathbb{C}[\theta_1, \ldots, \theta_m]$-module, so R^G is Cohen-Macaulay. □

Applying Cohen Macaulay rings to combinatorics is Stanley's claim to fame. Now if we combine these Lemma 3.1.4 and 3.1.5 we can prove the surprising result that the Molien series of the algebra of invariants is always a rational function:

Proposition 4.1.5. *As we can write $R^G = \bigoplus_{i=1}^s \eta_i \mathbb{C}[\theta_1, \ldots, \theta_r]$, where θ_i is degree d_i and η_i is degree e_i. Then*

$$F_G(\lambda) = \frac{\lambda^{e_1} + \lambda^{e_2} + \cdots + \lambda^{e_s}}{(1-\lambda^{d_1}) \ldots (1-\lambda^{d_r})}.$$

Proof. We know

$$\begin{aligned} F_G(\lambda) &= F(R^G, \lambda) \\ &= F(\oplus_{i=1}^s \eta_i \mathbb{C}[\theta_1, \ldots, \theta_r], \lambda) \\ &= \sum_{i=1}^{s} \lambda^{e_i} F(\mathbb{C}[\theta_1, \ldots, \theta_r], \lambda) \\ &= \frac{\lambda^{e_1} + \lambda^{e_2} + \cdots + \lambda^{e_s}}{(1-\lambda^{d_1}) \ldots (1-\lambda^{d_r})}, \end{aligned}$$

where we move from line 2 to line 3 by Lemma 3.1.4 and 3.1.5 and proof follows from the Hilbert series of the general polynomial ring. □

This proposition tells us that if we know the structure of the algebra of invariants, namely the generators (θ_i), then we can work backwards to construct an expression for the Molien series of R^G. It would be convenient if from the Molien series we could work read off the generators of the algebra of invariants, however the best we can do is suggest what the degrees of the generators are from the Molien series.

This next example explores this idea:

Example 4.1.6. *Let $G = \{1, M, M^2\}$, where $M = \left(\begin{smallmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{smallmatrix}\right)$, where $\omega = exp\ (\frac{2\pi i}{3})$. Also we shall let $R = \mathbb{C}[x, y]$. Then x^3, y^3 is an homogenous system of parameters (h.s.o.p.) for R^G, corresponding to the decomposition $R^G = (1 \oplus xy \oplus x^2y^2)\mathbb{C}[x^3, y^3]$, which is the standard decomposition of the algebra of invariants of the cyclic group.*

Also, xy, x^3+y^3 is an h.s.o.p., corresponding to $R^G = (1 \oplus x^3)\mathbb{C}[xy, x^3+y^3]$. Hence if we use the proposition 3.0.7, it follows that we can write

$$F_G(\lambda) = \frac{1+\lambda^2+\lambda^4}{(1-\lambda^3)^2} = \frac{1+\lambda^3}{(1-\lambda^2)(1-\lambda^3)}.$$

However we can simplify the expression for the Molien series, by factorising through by $(1+\lambda)$. From this, we conclude that

$$F_G(\lambda) = \frac{1-\lambda+\lambda^2}{(1-\lambda)(1-\lambda^3)}.$$

From this example we see that the coefficients of the numerator of the Molien series and the factors of the denominator of the Molien series contain no information with which we can compute the algebra of invariants.
We now wish to give an explicit description of a certain h.s.o.p. $\psi_1, \ldots, \psi_m$ for R^G. We will show directly that R is a free $\mathbb{C}[\psi_1, \ldots, \psi_m]$ module. However before we can do this, we require the following result (Lemma 4.1.14), although this requires set up. Next we let $D = k[\theta_1, \ldots, \theta_{l-1}]$ and $I = (\theta_1, \ldots, \theta_{l-1}) \triangleleft D$, so $D/I \cong k$. Assume $\theta_1, \ldots, \theta_{l-1}$ positive degrees. Let $B =$ free D-module which is $\mathbb{N}$-graded and dim $B_d < \infty$.

Theorem 4.1.7. *Let $b_\alpha \in B$ be homogenous elements such that $B/IB = \oplus k(b_\alpha + IB)$ i.e. $W = \sum kb_\alpha \subset B$ is a graded vector space complement to IB in B. Then $B \cong \oplus Db_\alpha$.*

Proof.

Lemma 4.1.8. *I^nB is 0 in degrees less than n so $(I^nB)_d = 0$ for $n \gg 0$.*

Proof. The basic idea is that $\theta_1, \ldots, \theta_{l-1}$ have positive degrees, so $ib \in I^nB$ at least degree n. So if we take $n > d$, than this implies that $(I^nB)_d = 0$, so we conclude for all d, there exist some $n \gg 0$ such that $(I^nB)_d = 0$. □

Lemma 4.1.9. *Given any nilpotent $m \times m$ matrix N, $I_m + N$ is invertible.*

Proof. $I_m + N$ is invertible as we can take $I_m - N + N^2 - N^3 + \cdots + (-1)^d N^d$ to be its inverse. Note that as N is nilpotent, we are guaranteed that there exists $N^{d+1} = 0$. □

Now we suppose that x_β is a graded D-basis for B so $B \cong \oplus Dx_\beta$ and $V = \sum kx_\beta$ is a vector space complement to IB in B. Therefore we get the graded vector space isomorphism: $T \cong B/IB \cong W$. Since x_β is a basis, we may extend D-linearly to $T : B \to B$.

Lemma 4.1.10. *T is an isomorphism.*

Proof. It suffices to show that $T|_{B_\alpha}$ is invertible. If we take $N = T - \mathrm{id} : B \to IB$ as the vector space isomorphism implies that $Tv = w$, where $v + IB = w + IB$, so we can conclude that $(T - \mathrm{id})(v) = Tv - v \in IB$. Now by lemma 4.1.8, it follows that N is nilpotent. Next by Lemma 4.1.9, $T|_{B_d}$ is invertible. □

The previous lemma implies that the k-basis $\{Tx_\beta\}$ for W is also a D-basis for B. Using change of basis, we see $\{b_\alpha\}$ is also a D-basis for B. □

Corollary 4.1.11. *Suppose furthermore, B is a graded $C = k[\theta_1, \ldots, \theta_l]$-module such that $B/IB \cong \oplus k[\theta_l](b_\alpha + IB)$. Then $B \cong \oplus C b_\alpha$.*

Proof. As $\{\theta_l^i b_\alpha\}_{i \geq 0}$ is a k-basis for B/IB so by the previous theorem, we can conclude that

$$B \cong D\theta_l^i b_\alpha \cong C b_\alpha.$$

□

Lemma 4.1.12. *B is a free $k[\theta_1, \ldots, \theta_l]$-module if and only if B is a free $k[\theta_1, \ldots \theta_{l-1}]$-module and $B/(\theta_1, \ldots, \theta_{l-1})$ is a free $k[\theta_l]$-module.*

Proof. ($\Rightarrow$) We have

$$\begin{aligned} B &= \oplus_{i=1}^n k[\theta_1, \ldots, \theta_l]\eta_i \\ &= \oplus_{j=0}^\infty \oplus_{i=1}^n k[\theta_1, \ldots, \theta_{l-1}]\theta_l^j \eta_i. \end{aligned}$$

This shows that B is a free $k[\theta_1, \ldots, \theta_{l-1}]$-module.
Next, by the homomorphism $\phi : k[\theta_1, \ldots, \theta_l]/(\theta_1, \ldots, \theta_{l-1}) \to k[\theta_1, \ldots, \theta_l]$, defined by $p \to p(0, 0, \ldots, 0, \theta_l)$ and by the first isomorphism theorem it follows that

$$\frac{k[\theta_1, \ldots, \theta_l]}{(\theta_1, \ldots, \theta_{l-1})} \cong k[\theta_l].$$

Next from this it follows that

$$B/(\theta_1, \ldots, \theta_{l-1}) \cong \oplus_{i=1}^n k[\theta_l].$$

($\Rightarrow$) We pick a $b_\alpha \in B$ such that

$$B/IB \cong \oplus k[\theta_l](b_\alpha + IB).$$

Next we claim that $B \cong C b_\alpha$, where $C = k[\theta_1, \ldots, \theta_j]$. This is true by the above corollary.

□

Let $\bar{B} = B/(\theta_1, \ldots, \theta_m)$ is a finitely generated algebra over k.

Lemma 4.1.13. *Suppose $\bar{B}$ is a commutative k-algebra generated by positive degree elements $f_1, \ldots, f_r$ such that all f_i are nilpotent. Then $\dim_k \bar{B} < \infty$.*

Proof. Suppose $f_i^{n_i} = 0$. Then $\bar{B}$ is spanned by $\{f_1^{d_1} f_2^{d_2} \ldots f_r^{d_r}\}$, where $0 \leq d_i < n_i$. Thus $\dim_k \bar{B} < \infty$. □

Lemma 4.1.14. *Let B be an N-graded k-algebra of Krull dimension m, and let $\theta_1, \ldots, \theta_j$ be algebraically independent homogenous elements of B of positive degree. Set $C = k[\theta_1, \ldots, \theta_m]$. Then B is a free C-module if and only if θ_{i+1} is not a zero-divisor in $B/(\theta_1, \ldots, \theta_i)$ for $0 \leq i \leq j-1$. Moreover, given that B is free C-module, then B is finitely generated as a C-module if $j = m$.*

Proof. We use induction on j. First assume that $j = 1$, and let $\theta = \theta_1$.
Let W be a vector space compliment in B of the ideal θB. The statement that θ is not a zero-divisor in B is equivalent to saying $B = W + \theta W + \theta^2 W + \ldots$, i.e. B is a free module.
Now assume that the lemma is true for $j = e - 1$. We know that B is a free $k[\theta_1, \ldots, \theta_l]$-module if and only if B is a free $k[\theta_1, \ldots, \theta_{l-1}]$-module and $B/(\theta_1, \ldots, \theta_{l-1})$ is a free $k[\theta_l]$-module (as we proved it Lemma 4.1.12).
By the induction hypothesis we have that B is a free C-module if and only if θ_{i+1} is not a zero-divisor in $B/(\theta_1, \ldots, \theta_i)$.

Next suppose that $j = m$ and let Y be a graded vector space complement in B to the ideal $(\theta_1, \ldots, \theta_m)$. Hence $B = \oplus Yu$, where u ranges over all monomials in $\theta_1, \ldots, \theta_m$. To show that B is finitely generated we want to show $\dim_k Y < \infty$. If we take the contrapositive of the previous lemma, we can conclude that $\bar{B}$ contains a homogenous element f of positive degree that isn't nilpotent.
Next we assume that f is algebraically independent to $\theta_1, \ldots, \theta_m$. As they are independent, it follows that

$$0 = p_0(\theta_1, \ldots, \theta_m) + p_1(\theta_1, \ldots, \theta_m) f + \cdots + p_n(\theta_1, \ldots, \theta_m) f^m,$$

where we assume $p_0(\theta_1, \ldots, \theta_m) \neq 0$. Next as we know that we can write $f^d = \sum r_\alpha y_\alpha$, where $r_\alpha \in k[\theta_1, \ldots, \theta_m]$. Next we can write $\sum q_\alpha(\theta_1, \ldots, \theta_m) y_\alpha$, where

$q_\alpha(\theta_1, \ldots, \theta_m) \in J^{i+j}$. Next as B is a free module over $k[\theta_1, \ldots, \theta_m]$ we are guaranteed that $p_n(\theta_1, \ldots, \theta_m)$ divides $q_\alpha(\theta_1, \ldots, \theta_m)$. From this we can conclude that

$$f^d = \sum \frac{q_\alpha(\theta_1, \ldots, \theta_m)}{p_n(\theta_1, \ldots, \theta_m)} y_\alpha,$$

which implies that $f^d = 0$ modulo $(\theta_1, \ldots, \theta_m)$. This tells that $\dim_k Y < \infty$, and thus that B is a finitely generated $k[\theta_1, \ldots, \theta_m]$-module. □

Definition 4.1.15. *Choose* linear forms $f_1, \ldots, f_m \in V$ *as follows: pick* $f_1 \neq 0$. *Once* $f_1, \ldots, f_i$ *have been chosen, pick* f_{i+1} *not to be any of the* i*-dimensional subspaces* $\langle M_1 f_1, \ldots, M_i f_i \rangle$ *of* V*, where* $M_1, \ldots, M_i \in G$.

Let $f_{i_1}, \ldots, f_{i_a}$ (need to fix this up later) be the distinct images of f_i under G. Next we define $\psi_i = f_{i_1} f_{i_2} \ldots f_{i_a}$.

Proposition 4.1.16. R *(and hence* R^G*) is a finitely generated free* $C[\psi_1, \ldots, \psi_m]$*-module.*

Proof. By the above lemma, it suffices to prove that ψ_{i+1} is not a zero-divisor in $R/(\psi_1, \ldots, \psi_i)$. In other words, if

$$Y\psi_{i+1} = \sum_{j=1}^{i} Z_j \psi_j, \tag{4.1.1}$$

where $Y, Z_j \in R$, then $Y \in (\psi_1, \ldots, \psi_i)$. Now the right hand side of (6.1.1) belongs to the prime ideal $\mathfrak{p} = (f_{1c_1}, \ldots, f_{ic_i})$ of R for any $(c_1, \ldots, c_i)$ where c_i are chosen from the i_n which are the distinct $f_{i1}, f_{i2}, \ldots f_{ia_1}$. So as we have the equality, it follows that some factor of the left hand side belongs to this prime ideal. But by the definition, we have $f_{i+1,j} \notin \mathfrak{p}$, so $\psi_{i+1} \notin \mathfrak{p}$. This implies that $Y \in (f_{1c_1}, \ldots, f_{ic_i})$ for every $(c_1, \ldots, c_i)$, so it follows that $Y \in \cap(f_{1c_1} \ldots, f_{ic_i}) = (\psi_1, \ldots, \psi_i)$. □

The previous proposition shows that there exists an h.s.o.p. $\psi_1, \ldots, \psi_m$ for R^G such that $\deg \psi_i$ divides g for all i. Now if we raised the ψ_i's to the appropriate powers we get an h.s.o.p. for R^G whose elements all have degree g. This implies that we can always write $F_G(\lambda)$ in the form $P_G(\lambda)/(1-\lambda^g)^m$, where $P_G(\lambda)$ is a polynomial with nonnegative coefficients.

The previous proposition tells us information about the possible values of $d_i = \deg \theta_i$ in a decomposition $R^G = \oplus_1^t \eta_i \mathbb{C}[\theta_1, \ldots, \theta_m]$. However next we consider if we wanted more information about the numbers $e_i = \deg \eta_i$. So from now on we shall assume that the η_i are ordered such that $e_1 \leq e_2 \leq . \cdots \leq e_t$. We now provide a calculation of e_i.

Lemma 4.1.17. *Let σ be the linear character of G given by $\sigma(M) = (detM)^{-1}$. Then as rational functions we have*

$$F_G\left(\frac{1}{\lambda}\right) = (-1)^m \lambda^m F_{G,\sigma}(\lambda).$$

Proof. By Molien's theorem, we have

$$\begin{aligned}
F_G\left(\frac{1}{\lambda}\right) &= \frac{1}{g}\sum_{M\in G}\frac{1}{\det(1-\lambda^{-1}M)} \\
&= \frac{1}{g}\sum_{M\in G}\frac{1}{\det(\lambda^{-1}M-I)\det(-I)} \\
&= \frac{(-1)^m}{g}\sum_{M\in G}\frac{1}{\det(\lambda^{-1}M-\lambda)} \\
&= \frac{(-1)^m}{g}\sum_{M\in G}\frac{1}{\det(\lambda^{-1}M)\det(I-\lambda M^{-1})} \\
&= \frac{(-1)^m\lambda^m}{g}\sum_{M\in G}\frac{(\det(M))^{-1}}{\det(1-\lambda M^{-1})} \\
&= (-1)^m\lambda^m\left(\frac{1}{g}\sum_{M\in G}\frac{\sigma(M)}{\det(1-\lambda M)}\right).
\end{aligned}$$

Note that we can interchange M^{-1} with M as inverses exist in groups. □

Proposition 4.1.18. *Let $R^G = \oplus_{i=1}^t \eta_i \mathbb{C}[\theta_1,\ldots,\theta_m]$, where deg $\theta_i = d_i$, deg $\eta_i = e_i$ and $0 = e_1 \le e_2 \le \cdots \le e_t$.*
Let μ be the least degree of a σ-invariant, i.e. the least degree of an $p \in R$ satisfying $Mp = (M)^{-1}p$ for all $M \in G$. Then

$$e_t = \sum_{i=1}^{m}(d_i - 1) - \mu.$$

Proof. We have

$$F_G(\lambda) = \left(\sum \lambda^{e_l}\right)\prod\left(1-\lambda^{d_l}\right)^{-1},$$

which follows from our Molien Series of the general polynomial ring. Next by lemma 4.1.16

$$\begin{aligned}
F_G(\frac{1}{\lambda}) &= (-1)^m\left(\sum \lambda^{d_1+\cdots+d_m-e_i}\right)\prod(1-\lambda^{d_i})^{-1} && (4.1.2)\\
&= (-1)^m\lambda^m F_{G,\sigma}(\lambda). && (4.1.3)
\end{aligned}$$

Where σ is defined as in the previous lemma. Next if we compare the least degree of the numerator of 4.1.2 and 4.1.3 it follows that

$$d_1 + \cdots + d_m - e_t = m + \mu.$$

□

The natural question that one would ask next is if R_χ^G is Cohen Macaulay. Note that R_χ^G is called the isotypical component of the action of G on R. Interestingly enough, this also turns out to be true, because of the decomposition of $R = \oplus R_\chi^g$ and the fact that R is a finitely generated R_χ^G-module.

Theorem 4.1.19. *Let $\theta_1, \ldots, \theta_m$ be a homogenous system of parameters for R^G, and let $\chi \in X(G)$. Let $p_1, \ldots, p_\mu$ be homogenous elements of R_χ^G whose images in the quotient module*

$$S_\chi = R_\chi^G/(\theta_1 R_\chi^G + \cdots + \theta_m R_\chi^G),$$

form a $\mathbb{C}$-basis for S_χ. Then

$$R_\chi^G = \oplus_{i=1}^u p_i \mathbb{C}[\theta_1, \ldots, \theta_m].$$

Proof. In the proof of Theorem 6.1.5, we obtained the decomposition $R = R^G \oplus U$. However, we actually claim that we have a finer decomposition $R = \oplus R_\chi^G$. As the action of G on R corresponds to the action of $\mathbb{C}G$. By Maschke's theorem (Theorem 2.3.15), we are guaranteed that $\mathbb{C}G$ is semisimple. Thus from Wedderburn's Theorem (2.3.16), we can conclude that there exists such a decomposition. Also note that R is a finitely generated R_χ^G, see [8, p. 478].
Next we choose a homogenous $\mathbb{C}$-basis $\bar{\eta}_1, \ldots, \bar{\eta}_s$ for $R/(\theta_1, \ldots, \theta_m)$ such that each $\bar{\eta}_i$ lies in some S_χ. Now we can argue similarly to the proof of R^G being Cohen Macaulay, and it follows as before that $R_\chi^G = \oplus \rho_i \mathbb{C}[\theta_1, \ldots, \theta_m]$ where ρ_i are those η_i's belonging to R_χ^G. □

Chapter 5

Applications of Invariant Theory

Invariant theory is an algebraic concept which at first glance has no direct application to combinatorics. However because of the relation between Hilbert series and computing the invariants there are links to combinatorics. In this chapter we first compute the sum $S(g)$, with the surprising tool of invariant theory. Later in the chapter we present a method of computing $S_2(g)$.

5.1 Computing S(g)

The first application that we shall look at is the sum

$$S(g) = \sum_{\omega} |1-\omega|^{-2}.$$

Where we let g be a positive integer, and this is the sum over $g-1$ complex numbers satisfying $\omega^g = 1$ and $\omega \neq 1$. We shall go through methods of computing this sum with invariant theory and with Molien theorem.
First we shall consider the case when $k = 1$. Now we can see that $S(g)$ is reminiscent of the Molien series corresponding to the invariants of $R = \mathbb{C}[x, y]$ and the cyclic group G of order g generated by

$$\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix},$$

where ζ is a primitive gth root of unity. From this the method to obtain $S(g)$ is as such:

$$S(g) = \lim_{\lambda \to 1} \left[gF_G(\lambda) - \frac{1}{(1-\lambda)^2} \right].$$

So next we are required to determine the Molien series in this case, and it turns out that

$$F_G(\lambda) = \frac{f_0 + f_1\lambda + \cdots + f_{2g-2}\lambda^{2g-2}}{(1-\lambda^g)^2},$$

where f_n is the number of monomials $x^{a_1}y^{a_2} \in R$, where $a_1, a_2 \in \mathbb{Z}$ and $0 \leq a_1, a_2 \leq g-1$. Also a_1, a_2 must satisfy $a_1 \equiv a_2 (\mathrm{mod} g)$ and $a_1 + a_2 = n$. So if we run through

the degrees we can see that f_n is defined by

$$f_n = \begin{cases} 0 \text{ when } n \text{ is odd} \\ 1 \text{ when n is even.} \end{cases}$$

Note that another way of computing the Molien series is to work backwards from the algebra of invariants of the cyclic group which we have already computed in Example 3.2.5. We would do this by using the information about algebra of invariants being Cohen-Macaulay and by Proposition 4. blah we would have an expression for the Molien series.
Thus it follows that

$$F_G(\lambda) = \frac{1 + \lambda^2 + \cdots + \lambda^{2g-2}}{(1-\lambda^g)^2}.$$

Our next task is to compute $S(g)$, which we can now do through l'Hopital's rule:

$$\begin{aligned} S(g) &= \lim_{\lambda \to 1} \left[gF_G(\lambda) - \frac{1}{(1-\lambda)^2} \right] \\ &= \lim_{\lambda \to 1} \left[\frac{g(1 + \lambda^2 + \cdots + \lambda^{2g-2})}{(1-\lambda)^2(1 + \lambda + \cdots + \lambda^{g-1})^2} - \frac{1}{(1-\lambda)^2} \right] \\ &= \lim_{\lambda \to 1} \left(\frac{g(1 + \lambda^2 + \cdots + \lambda^{2g-2}) - (1 + \lambda + \cdots + \lambda^{g-1})^2}{(1-\lambda^g)^2} \right) \end{aligned}$$

Now we can rewrite the numerator in terms of two geometric sums.

$$\begin{aligned} S(g) &= \lim_{\lambda \to 1} \frac{g\left(\frac{1-\lambda^{2g}}{1-\lambda^2}\right) - \left(\frac{(1-\lambda^g}{1-\lambda}\right)^2}{1-\lambda^g)^2} \\ &= \lim_{\lambda \to 1} \frac{g(1-\lambda^{2g})(1-\lambda) - (1+\lambda)(1-\lambda^g)^2}{(1-\lambda^2)(1-\lambda)(1-\lambda^g)^2} \\ &= \lim_{\lambda \to 1} \frac{g(1+\lambda^g)(1-\lambda) - (1+\lambda)(1-\lambda^g)}{1-\lambda^2)(1-\lambda)(1-\lambda^g)} \\ &= \lim_{\lambda \to 1} \frac{1}{(1+\lambda)(1+\lambda^2+\cdots+\lambda^{g-1})} \frac{g(1+\lambda^g-\lambda-\lambda^{g+1}) - 1 - \lambda + \lambda^g + \lambda^{g+1}}{(1-\lambda)^3} \\ &= \lim_{\lambda \to 1} \frac{(g-1) - (g+1)\lambda + (g+1)\lambda^g + (1-g)\lambda^{g+1}}{(1-\lambda)^3} \end{aligned}$$

Next we differentiate twice, in order that the numerator and the denominator are not both 0. After differentiating $S(g)$ twice we get:

$$\begin{aligned} S(g) =& \lim_{\lambda \to 1} \frac{(g+1)g(g-1)(g-2) - (g-1)(g+1)g(g-1)}{-12g} \\ =& \frac{(g+1)(g-1)[g-2-(g-1)]}{-12} \\ =& \frac{(g+1)(g-1)}{12}. \end{aligned}$$

5.2 Computing $S_2(3)$

So we have now calculated $S(g)$, but this opens up other avenues of extension. Like one might to investigate $S_k(g)$, which is defined as such:

Definition 5.2.1. *Let g and k be positive integers, we define the sum of $S_k(g)$ to be*

$$S_k(g) = \sum_{\omega} |1-\omega|^{-2k}.$$

Also note that the sum does not include $\omega = 1$ as before.

Next we shall look at the claim that

$$S_2(g) = \frac{(g^2-1)(g^2+11)}{2^4 \times 3^2 \times 5}.$$

So we first shall consider an easier case $S_2(3)$, and then we shall prove the general $S_2(g)$ case. Note that we still have the relation:

$$S_2(g) = \lim_{\lambda \to 1} \left[gF_G(\lambda) - \frac{1}{(1-\lambda)^4} \right].$$

Also we have a similar set up as before as G is generated by

$$\begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 \\ 0 & 0 & \omega^{-1} & 0 \\ 0 & 0 & 0 & \omega^{-1} \end{pmatrix}.$$

Also similar to the previous case we are required to calculate

$$f_n = \#x_1^{a_1} x_2^{a_2} x_3^{a_3} x_4^{a_4},$$

satisfying

$$a_1 + a_2 + a_3 + a_4 = n, \text{ for } 0 \leq n \leq 4(g-1) \tag{5.2.1}$$

$$a_1 + a_2 \equiv a_3 + a_4 (\mathrm{mod} g). \tag{5.2.2}$$

If both (5.2.1) and (5.2.2) are satisfied we shall denote this by (*). To reduce the amount of computation required for f_n, we introduce this proposition.

Proposition 5.2.2. *Let $t \in \mathbb{Z}$, where $0 \leq t \leq 2k(g-1)$, it follows that*

$$f_t = f_{2k(g-1)-t}.$$

Proof. We have $a_1 + a_2 + a_3 + a_4 = t$, $a_1 + a_2 \equiv a_3 + a_4 (\mathrm{mod} g)$ and $a_i \leq g - 1$. Next if we let $b_i = g - 1 - a_i$, it follows that

$$\begin{aligned} t =& \sum_i (g - 1 - b_i) \\ =& 4g - 4 - \sum_i b_i. \end{aligned}$$

Next we have that $4g - 4 - t = \sum_i b_i$, it also follows from how we have defined b_i, that $0 \leq b_i \leq g - 1$. Finally it is clear that $b_1 + b_2 \equiv b_3 + b_4 (\mathrm{mod} g)$. □

Definition 5.2.3. *So now the* reflection *of f_t is defined to be $f_{2k(g-1)-t}$.*

Definition 5.2.4. *Let $p(\lambda) = f_0 + f_1\lambda + \lambda^2 f_2 \ldots \lambda^{2k(g-1)} f_{2k(g-1)}$. Now the* reflection *of $p(\lambda)$ is defined to be*

$$p_r(\lambda) = f_{2k(g-1)} + f_{2k(g-1)-1}\lambda + \cdots + \lambda + f_{k(g-1)}\lambda^{k(g-1)} + \cdots + f_0\lambda^{2k(g-1)}.$$

One further thing about f_n to note is that they are reflected in $f_{2(g-1)}$, which means $f_{2(g-1)+n} = f_{2(g-1)-n}$ assuming that $n \leq 2(g-1)$. So this implies that for the $S_2(3)$ case we only need to compute up to f_4.

Now f_0 is clearly 1, and similarly for f_1 is clearly 0. Next for f_2 the only way that (*) can be satisfied is for $a_1 + a_2 = a_3 + a_4$ as the degree of the monomial is less than 3. From this it follows that we can have $a_1 = a_3$ or a_4 and similarly with a_2, thus it follows that $f_2 = 4$.

Next for f_3, the only way that we can satisfy (*) is if $a_1 + a_2 = 3$ or if $a_3 + a_4 = 3$ and each of these can happen in two ways, so that implies $f_3 = 2 \times 2 = 4$. Now with f_4 there are a few ways that (*) is satisfied. We need $a_1 + a_2 = 2 = a_3 + a_4$, which can occur in 9 different ways as $a_1 + a_2 = 2$ can occur in 3 ways, namely

$(1+1, 2+0, 0+2)$.
Thus we can write an expression for $F_G(\lambda)$

$$F_G(\lambda) = \frac{1+4\lambda^2+4\lambda^3+9\lambda^4+4\lambda^5+4\lambda^6+\lambda^8}{(1-\lambda^3)^4}.$$

So now we have enough information to calculate $S_2(3)$, which will be done through in a similar manner to $S(g)$.

$$\begin{aligned} S_2(3) =& \lim_{\lambda\to 1}\left[gF_G(\lambda) - \frac{1}{(1-\lambda)^4}\right] \\ =& \frac{3(1+4\lambda^2+4\lambda^3+9\lambda^4+4\lambda^5+4\lambda^6+\lambda^8) - (1+\lambda+\lambda^2)^4}{(1-\lambda^3)^4}. \end{aligned}$$

Now after applying l'Hopital's rule 4 times in maple we get that

$$S_2(3) = \frac{2}{9} = \frac{(3^2-1)(3^2+11)}{2^4\times 3^2\times 5},$$

as claimed.

5.3 Method for computing $S_2(g)$

Now we shall move onto the general $S_2(g)$ case, however we first take g to be odd.
Step 1: Compute f_n for $0 \le n \le 4(g-1)$.

Furthermore we split this up into n-even and n-odd. For the n-even case, we claim that

$$f_n = (\frac{n}{2}+1)^2 \qquad \text{for } 0 \le n \le 2(g-1).$$

To prove this claim we must consider the different ways one could satisfy (*), one way that this could occur is if we have

$$a_1 + a_2 = \frac{n}{2} = a_3 + a_4.$$

As the number of ways $a_1 + a_2 = n$ is n+1, this implies that $f_n \ge (\frac{n}{2}+1)^2$, but we know that this is an equality because the only other way that (*) could be satisfied is if we had something of the form

$$a_1 + a_2 \equiv a_3 + a_4 \bmod (g).$$

However this is not possible as we know that n is even and g is odd we would have an $n+g$ split up onto two sides of that inequality and this won't be able to satisfy

(*), thus we the claim is correct.
We continue with the computation of f_n, but now for when n is odd. We claim that

$$f_n = \begin{cases} 0 \text{ if } 1 \leq n < g \\ (\frac{n-g}{2}+1)(3g-n-2) \text{ if } g \leq n < 2(g-1). \end{cases}$$

For the first part of the claim we take $n < g$. It is clear that there is no solution which satisfies (*) because if $a_1 + a_2$ is odd then $a_3 + a_4$ is forced to be even (this is from 5.2.1 and g being odd), thus they can not be equal. Also note that as only taking $n < g$, it is impossible for

$$a_1 + a_2 \equiv a_3 + a_4 \bmod g.$$

Thus we conclude $f_n = 0$, for $n < g$. Next we take $g \leq n < 2(g-1)$. We have that

$$a_1 + a_2 = \frac{n-g}{2}, \quad a_3 + a_4 = \frac{n+g}{2},$$

or vise versa. Now the number of ways that $a_1 + a_2 = \frac{n-g}{2}$ is $\frac{n-g}{2} + 1$, as $\frac{n-g}{2} < g$. Next we have to calculate the number of ways that $a_3 + a_4 = \frac{n+g}{2}$, so first we note that $\frac{n+g}{2} \geq g$. So all the combinations of a_3 and a_4 are

$$\left(g-1, \frac{n-g-2}{2}\right), \ldots, \left(\frac{n-g-2}{2}, g-1\right).$$

Thus we conclude that the number of combinations that $a_3 + a_4 = \frac{n+g}{2}$ is $g - 1 - \frac{n-g-2}{2} + 1 = \frac{3g-n-2}{2}$. Thus conclude that $f_n = (\frac{n-g}{2}+1)(3g-n-2)$ if $g \leq n < 2(g-1)$.

Step 2: Rewrite these polynomials with respect to generating functions.

To do this we split $F_G(\lambda)$ into parts, so first we shall consider all the even powers of $F_G(\lambda)$ which we shall denote $F_{G_e}(\lambda)$. From above we have

$$\begin{aligned} F_{G_e}(\lambda) =& f_0 + f_2\lambda^2 + \cdots + f_{2g-4}\lambda^{2g-4} + f_{2g-2}\lambda^{2g-2} + f_{2g-4}\lambda^{2g} + \ldots f_2\lambda^{4g-6} + f_0\lambda^{4g-4} \\ =& 1 + 2^2\lambda^2 + \cdots + (g-1)^2\lambda^{2g-4} + g^2\lambda^{2g-2} + (g-1)^2\lambda^{2g} + \cdots + 2^2\lambda^{4g-6} + \lambda^{4g-4}. \end{aligned}$$

Now we introduce this lemma which will be useful to compute the even powers of the Molien series

Lemma 5.3.1. $1 + 2^2x + 3^2x^2 + \cdots + (n-1)^2x^{n-2} = \frac{d}{dx}(h(x)) + x\frac{d^2}{dx^2}(h(x))$, *where*

$$h(x) = \frac{1-x^n}{1-x}.$$

Proof. The proof of this lemma follows from a rearranging of $h(x)$:

$$\begin{aligned} h(x) =& \frac{1-x^n}{1-x} \\ =& 1 + x + x^2 + \dots x^{n-1}. \end{aligned}$$

It follows that $\frac{d}{dx}h(x) = 1 + 2x + 3x^2 + \cdots + (n-1)x^{n-2}$, and $x\frac{d^2}{dx^2}h(x) = (1)(2)x + (2)(3)x^2 + \cdots + (n-1)(n-2)x^{n-2}$. After adding these the lemma follows. □

Now by substituting $x = \lambda^2$, we have the equality:

$$e(\lambda) = \frac{d}{d\lambda^2}h(\lambda^2) + \lambda^2\frac{d^2}{d\lambda^2} = 1 + 2^2\lambda^2 + \cdots + (g-1)^2\lambda^{2g-4}.$$

Now, we move onto the odd powers of $F_G(\lambda)$. First we consider f_n:

$$\begin{aligned} f_n =& \left(\frac{n-g}{2} + 1\right)(3g - n - 2) \\ =& 3g - n - 2 + \frac{3gn - n^2 - 2n - 3g^2 + gn + 2g}{2} \\ =& \left(4g - \frac{3g^2}{2} - 2\right) + n(2g-2) + n^2\left(\frac{-1}{2}\right). \end{aligned}$$

We denote the odd powers of the numerator of the Molien series by $F_{G_o}(\lambda)$. By the algorithm we now break up into 6 parts, namely in their powers of n and then their reflection. So first we shall rewrite $g_1(\lambda)$

$$\begin{aligned} g_1(\lambda) =& (4g - \frac{3g^2}{2} - 2)(\lambda^g + \lambda^{g+2} + \cdots + \lambda^{2g-3}) \\ =& (4g - \frac{3g^2}{2} - 2)\left(\frac{1-\lambda^{g-1}}{1-\lambda^2}\right)\lambda^g \\ =& (4g - \frac{3g^2}{2} - 2)\left(\frac{\lambda^g - \lambda^{2g-1}}{1-\lambda^2}\right) \end{aligned}$$

From now on we shall denote

$$p(\lambda) = \frac{\lambda^g - \lambda^{2g-1}}{1-\lambda^2}.$$

Next as

$$x + 3x^3 + \cdots + 2n - 1x^{2n-1} = x\frac{d}{dx}\left(\frac{1-x^{2n}}{1-x^2}x\right),$$

it follows that

$$\begin{aligned} g_2(\lambda) =& 2(g-1)(g\lambda^g + g + 2\lambda^{g+2} + \cdots + 2g - 3\lambda^{2g-3}) \\ =& 2(g-1)\lambda\frac{d}{d\lambda}(p(\lambda)). \end{aligned}$$

We shall use a similar process, in how we calculated g_2, to calculate g_3.

$$g_3(\lambda) = \frac{-1}{2}\left(\lambda\frac{d}{d\lambda}\left[x\frac{d}{d\lambda}p(\lambda)\right]\right).$$

Next we denote $o(\lambda) = g_1(\lambda) + g_2(\lambda) + g_3(\lambda)$.

Step 3: Compute the reflection of the polynomial.

From this equality we can compute $e_r(\lambda)$, as

$$\begin{aligned} e_r(\lambda) = f_{2g-4}\lambda^{2g} + \cdots + f_2\lambda^{4g-6} + f_0\lambda^{4g-4} =& \lambda^{4g-4}(f_{2g-4}\lambda^{-2g+4} + \cdots + f_2\lambda^{-2} + f_0) \\ =& \mu^{4-4g}(f_0 + f_2\mu^2 + \cdots + f_{2g-4}\mu^{2g-4}), \quad (\text{if we let } \frac{1}{\mu} = \lambda). \end{aligned}$$

Note that this is useful because we now have $e_r(\lambda)$ in terms of $e(\lambda)$, a function which we have written in a generating function form. Now to calculate the reflection of $o(\lambda)$, we use a similar technique that we used to compute the reflection in $e(\lambda)$, namely the reflection, $g_{i+3}(\lambda)$, of $g_i(\lambda)$ is

$$g_{i+3}(\lambda) = \lambda^{4g-4}g_i\left(\frac{1}{\lambda}\right).$$

So now we have $o_r(\lambda) = g_4(\lambda) + g_5(\lambda) + g_6(\lambda)$.

Step 4: Combine polynomials to get an expression for Molien Series.

$$F_G(\lambda) = \frac{e(\lambda) + e_r(\lambda) + o(\lambda) + o_r(\lambda)}{(1-\lambda^g)^4}.$$

Now the main part of the computation of $S_2(g)$ is complete, the rest of the computation will be omitted. However it can be done by repeatedly applying L'Hospital's rule until we find an answer for $S_2(g)$.
We now consider the general case for g-even.
Step 1: Compute f_n for $0 \leq n \leq 4(g-1)$.
First we claim that $f_n = 0$, when n is odd.

Proof. We have $a_1 + a_2 + a_3 + a_4 = n$, and that they must satisfy $a_1 + a_2 = a_3 + a_4 (\mathrm{mod} g)$. It is clear that $a_1 + a_2 \neq a_3 + a_4$, and it is also clear that $a_1 + a_2 \neq a_3 + a_4 (\mathrm{mod} g)$ as g is even. □

Next we are required to calculate f_n for n-even. We claim that

$$f_n = \begin{cases} (\frac{n}{2}+1)^2 & \text{for } 0 \leq n \leq g-1 \\ (\frac{n}{2}+1)^2 + 2(\frac{n}{2} - \frac{g}{2} + 1)(\frac{3g}{2} - \frac{n}{2} - 1) & \text{for } g \leq n \leq 2g-2. \end{cases}$$

Case 1: $n < g$. Let $2m = n$. In this case, (*) (note to self - make a universal condition) is only satisfied when

$$a_1 + a_2 = m = a_3 + a_4.$$

It follows that $f_n = (m+1)^2 = (\frac{n}{2}+1)^2$, as required.
Case 2: $n \geq g$. After combining $a_3 + a_4 = n - a_1 - a_2$ and $a_1 + a_2 \equiv a_3 + a_4 (g)$, it follows that

$$a_1 + a_2 \equiv m \mod \left(\frac{g}{2}\right).$$

Now the only two valid solutions to this are

$$a_1 + a_2 = m + \frac{g}{2}, \quad a_3 + a_4 = m - \frac{g}{2}, \tag{5.3.1}$$

and

$$a_1 + a_2 = m - \frac{g}{2}, \quad a_3 + a_4 = m + \frac{g}{2}. \tag{5.3.2}$$

So the number of different combinations in which $a_1 + a_2 = m + \frac{g}{2}$ is $g - 1 - (m - \frac{g}{2} + 1) + 1 = \frac{3g}{2} - m - 1$. Similarly the number of different combination in which $a_3 + a_4 = m - \frac{g}{2}$ is $m - \frac{g}{2} + 1$.
Now we conclude that

$$f_n = \left(\frac{n}{2}+1\right)^2 + 2\left(\frac{n}{2} - \frac{g}{2} + 1)(\frac{3g}{2} - \frac{n}{2} - 1\right),$$

as claimed.

Step 2: Rewrite these polynomials with respect to generating functions.

Next we compute the Molien series for the general g-even case. We shall break

f_n up into powers of n, and then compute the Molien series. First we shall split up the Molien series to help the calculation of it, we shall first compute

$$e_1(\lambda) = f_0 + f_2\lambda^2 + \cdots + f_{g-2}\lambda^{g-2},$$

and

$$e_2(\lambda) = f_g\lambda^g + f_{g+2}\lambda^{g+2}\cdots + f_{2g-4}\lambda^{2g-4} + f_{2g-2}\lambda^{2g-2}.$$

Note that $e(\lambda) = e_1(\lambda) + e_2(\lambda)$. First we have computed a similar result (Lemma 4.0.4) to e_1, thus if we let $h(\lambda) = 1 + \lambda + \lambda^2 + \cdots + \lambda^{\frac{g+1}{2}}$, then it follows that

$$e_1(\lambda) = \frac{d}{d\lambda}(h(\lambda)) + \lambda\frac{d^2}{d\lambda^2}(h(\lambda)).$$

So we shall move onto e_2:

$$e_2(\lambda) = h_0(\lambda) + h_1(\lambda) + h_2(\lambda).$$

So

$$\begin{aligned} f_n &= \left(\frac{n}{2}+1\right)^2 + 2\left(\frac{n}{2} - \frac{g}{2} + 1\right)\left(\frac{3g}{2} - \frac{n}{2} - 1\right) \\ &= \left(\frac{3g^2}{2} + 4g - 1\right) + n\left(2g-1\right) + n^2\left(\frac{-1}{4}\right). \end{aligned}$$

Next we can write $h_0(\lambda)$ with respect to a generating function:

$$\begin{aligned} h_0(\lambda) &= \left(\frac{3g^2}{2} + 4g - 1\right)\left(1 + \lambda^2 + \cdots + \lambda^{2g-2}\right) \\ &= \left(\frac{3g^2}{2} + 4g - 1\right)\frac{1-\lambda^{2g}}{1-\lambda^2}. \end{aligned}$$

Next

$$\begin{aligned} h_1(\lambda) &= (2g-1)(g\lambda^g + (g+2)\lambda^{g+2} + \cdots + (2g-2)\lambda^{2g-2} \\ &= (2g-1)\lambda\frac{d}{d\lambda}\left(\frac{\lambda^g - \lambda^{2g}}{1-\lambda^2}\right). \end{aligned}$$

$$\begin{aligned} h_2(\lambda) &= \frac{-1}{4}(g^2\lambda^g + (g+2)^2\lambda^{g+2} + \cdots + (2g-2)^2\lambda^{2g-2}) \\ &= \frac{-1}{4}\lambda\frac{d}{d\lambda}\left(\lambda\frac{d}{d\lambda}\left(\frac{\lambda^g - \lambda^{2g}}{1-\lambda^2}\right)\right). \end{aligned}$$

Step 3: Compute the reflection of the polynomial..

The reflection for $e(\lambda)$ is

$$e_r(\lambda) = \lambda^{4g-4}\left(e_1\left(\frac{1}{\lambda}\right) + e_2\left(\frac{1}{\lambda}\right)\right).$$

Step 4: Combine polynomials to get an expression for Molien Series

Now combining these functions we have an expression for $e(\lambda)$ and $e_r(\lambda)$, which is written solely in generating functions. So it follows that

$$F_G(\lambda) = \frac{e(\lambda) + e_r(\lambda)}{(1-\lambda^g)^4}.$$

Similarly with the g-odd we have now completed the main part of the computation of $S_2(g)$ and by repeatedly L'Hospital's rule we would achieve the desired result for $S_2(g)$.

Chapter 6

Conclusion

6.1 Summary

We began this thesis with the idea of an algebra of invariants and throughout we have explored how it is intrinsically linked to combinatorics. As we have seen, this link has come from the Hilbert function and Molien's Theorem. Later we used the Cohen Macaulay nature of the algebra of invariants to prove that surprising result that $F_G(\lambda)$ is a rational function.

6.2 Future Work

While I was able to compute a method for $S_2(g)$, I would like to be able to prove the more general even case. I also would like to delve into invariants generated by psuedo-reflections.

References

[1] Burnside W., 'Theory of groups of finite order', *Cambridge Univ. Press*, **2**, (1955).

[2] Eisenbud D., 'Commutative algebra. With a view toward algebraic geometry', *Graduate Texts in Mathematics*, **150**, (1995).

[3] Hilbert D., 'Üeber die Theorie der algebraischen Formen', *Math. Ann.*, **36**, (1890), 473-534.

[4] Hilbert D., 'Über die vollen Invariantensysteme', *Math. Ann.*, **42**, (1893), 313.

[5] Hochster M. and Eagon J. A., 'Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci, *Amer. J. Math.*, **93**, (1971), 1020-1058.

[6] Noether E., 'Der Endlichkeitsatz der Invarianten endlicher linearer Gruppen der Charakteristik p', *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen*, (1926), 28-35.

[7] Serre J.-P., 'Algébre locale-multiplicitiés', *Lecture Notes in Math.*, **11**, (1965)

[8] Stanley R., 'Invariants of Finite Groups and their Applications to Combinatorics', *Bulletin of the American Mathematical Society*, **1**, (May 1979), 475-511.

[9] Weyl H., 'The classical groups, *Proc. Amer. Math. Soc.*, **2**, (1953).