RINGS OF INVARIANTS OF FINITE GROUPS

J. K. VERMA

1. Introduction

In these notes we discuss a few fundamental results in invariant theory of finite groups. We begin by proving the fundamental theorem on symmetric functions. We introduce the Schur polynomials and derive the Jacobi-Trudi identity which expresses the Schur polynomials as determinants of matrices whose entries are complete homogeneous symmetric polynomials.

We shall prove the fundamental results of Hilbert and Noether for invariant subrings of finite subgroups of the general linear groups in the non-modular case, i.e. when the field has characteristic zero or coprime with the order of the group. We will not discuss the modular case. We will derive the Molien's formula for the Hilbert series of the ring of invariants. We will show, through examples, that the Molien's formula helps us to see when to stop computing the invariants. We will calculate, quite explicitly, the ring of invariants of the dihedral and icosahedron groups. Finally we will present a rapid treatment of Cohen-Macaulay graded rings. The Cohen-Macaulay property is one of the crucial properties of the rings of invariants. We will show how this property helps us in presenting the ring of invariants in an economical manner via the so called Hironaka decomposition.

2. Symmetric Polynomials

The ring of polynomials in n variables $x_1, x_2, \ldots, x_n$ with coefficients in a field k will be denoted by $k[x_1, x_2, \ldots, x_n] := k[x]$. We shall assume throughout this section that the characteristic of k is zero. The symmetric group on the set $[n] = \{1, 2, 3, \ldots, n\}$ will be denoted by S_n.

Definition 2.1. *A polynomial $f(x_1, x_2, \ldots, x_n) \in k[x]$ is called symmetric if for all $\sigma \in S_n$,*

$$f(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

Symmetric polynomials form a subring of $k[x]$. This will be denoted by $k[x]^{S_n}$. Let t be a new variable. Consider the polynomial

$$g(t) = (t - x_1)(t - x_2) \ldots (t - x_n) = t^n - e_1 t^{n-1} + e_2 t^{n-2} - \ldots + (-1)^n e_n.$$

The coefficients $e_1, e_2, \ldots, e_n$ are clearly symmetric. They are given by the equations

$$\begin{aligned} e_1 &= x_1 + x_2 + \ldots + x_n \\ e_2 &= \textstyle\sum_{1 \le i < j \le n} x_i x_j, \ldots, \\ e_n &= x_1 x_2 \ldots x_n. \end{aligned}$$

Definition 2.2. *The polynomials $e_1, e_2, \ldots, e_n$ are called the elementary symmetric polynomials in $x_1, x_2, \ldots, x_n$.*

Theorem 2.3 (Fundamental theorem on symmetric polynomials)**.** *Every symmetric polynomial is uniquely written as a polynomial in $e_1, e_2, \ldots, e_n$.*

Proof: The monomials in $k[x]$ can be totally ordered by using the degree lexicographic order. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in I\!N^n$ where $I\!N = \{0, 1, 2, \ldots\}$. Put $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n} = x^\alpha$ and $|\alpha| = \alpha_1 + \alpha_2 + \ldots + \alpha_n$. Under the degree lexicographic order: $x^\alpha < x^\beta$ iff either $|\alpha| < |\beta|$ or $|\alpha| = |\beta|$ and there an r such that $\alpha_1 = \beta_1, \ldots, \alpha_{r-1} = \beta_{r-1}$ and $\alpha_r < \beta_r$.

We now describe an algorithm which enables us to write any symmetric polynomial as a polynomial in $e_1, e_2, \ldots, e_n$. Write f as a unique linear combination of monomials. The largest monomial in f with respect to the degree lexicographic order is denoted by $in(f)$. If x^α occurs in f then $\sigma(x^\alpha)$ also occurs in f. Hence $in(f) = c x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ where $c \in k$ and $\alpha_1 \ge \alpha_2 \ge \ldots \ge \alpha_n$.

Consider $\overline{f} = f - c e_1^{\alpha_1 - \alpha_2} e_2^{\alpha_2 - \alpha_3} \ldots e_{n-1}^{\alpha_{n-1} - \alpha_n} e_n^{\alpha_n}$. For any $(\beta_1, \ldots, \beta_n) \in I\!N^n$,

$$in\left(e_1^{\beta_1} e_2^{\beta_2} \ldots e_n^{\beta_n}\right) = \prod_{i=1}^{n} x_i^{\beta_i + \beta_{i+1} + \cdots + \beta_n}.$$

Hence $in(\overline{f}) < in(f)$. As there are only finitely many monomials less than a given monomial, this algorithm terminates.

For uniqueness we need to show that $e_1, e_2, \ldots, e_n$ are algebraically independent. Suppose $g(y_1, y_2, \ldots, y_n) \in k[y_1, y_2, \ldots, y_n]$ such that $g(e_1, e_2, \ldots, e_n) = 0$. Let $y_1^{\alpha_1} y_2^{\alpha_2} \ldots y_n^{\alpha_n}$ be a term in g. Then

$$in(e_1^{\alpha_1} e_2^{\alpha_2} \ldots e_n^{\alpha_n}) = \prod_{i=1}^{n} x_i^{\alpha_i + \alpha_{i+1} + \ldots + \alpha_n}.$$

As the map $\phi : I\!N^n \to I\!N^n$ where

$$\phi(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\alpha_1 + \ldots + \alpha_n, \alpha_2 + \alpha_3 + \ldots + \alpha_n, \ldots, \alpha_{n-1} + \alpha_n, \alpha_n)$$

is injective, the initial form $in(e_1^{\alpha_1} e_2^{\alpha_2} \ldots e_n^{\alpha_n})$, where $y_1^{\alpha_1} \ldots y_n^{\alpha_n}$ is the largest monomial in g, will not be cancelled by any other term in $g(e_1, e_2, \ldots, e_n)$. This is a contradiction. Hence $e_1, e_2, \ldots, e_n$ are algebraically independent.

Power sum symmetric polynomials

Definition 2.4. *The polynomials* $p_k = x_1^k + x_2^k + \ldots + x_n^k$ *for* $k = 1, 2, 3, \ldots$ *are called the power sum symmetric polynomials.*

Theorem 2.5 (Newton's identities)**.**

$$p_k = \begin{cases} e_1 p_{k-1} - e_2 p_{k-2} + e_3 p_{k-3} - \cdots + (-1)^{k-2} p_1 e_{k-1} + (-1)^{k-1} k e_k & \text{if } k \le n \\ e_1 p_{k-1} - e_2 p_{k-2} + \cdots + (-1)^{n-1} e_n p_{k-n} & \text{if } k > n \end{cases}$$

Proof: Put

$$\begin{aligned} E(t) &= (1 - tx_1)(1 - tx_2) \ldots (1 - tx_n) \\ &= 1 - e_1 t + e_2 t^2 - \ldots + (-1)^n e_n t^n \end{aligned}$$

Then $\log E(t) = \sum_{i=1}^{n} \log(1 - tx_i)$. Hence

$$-\frac{E'(t)}{E(t)} = \sum_{i=1}^{n} \frac{x_i}{(1 - tx_i)} = \sum_{i=1}^{n} x_i \sum_{k=0}^{\infty} (tx_i)^k = \sum_{k=0}^{\infty} \sum_{i=1}^{n} x_i^{k+1} t^k = \sum_{k=1}^{\infty} p_k t^{k-1}$$

Hence $E'(t) = -E(t) \sum_{k=1}^{\infty} p_k t^{k-1}$. Equate the coefficients to get the identities.

Corollary 2.6. *For* $k \le n$,

$$p_k = \begin{vmatrix} e_1 & 1 & 0 & & \cdots & 0 \\ 2e_2 & e_1 & 1 & 0 & \cdots & 0 \\ 3e_3 & e_2 & e_1 & 1 & \cdots & 0 \\ ke_k & e_{k-1} & e_{k-2} & & \cdots & e_1 \end{vmatrix} \quad \text{and} \quad k! e_k = \begin{vmatrix} p_1 & 1 & & & \\ p_2 & p_1 & 2 & & \vdots \\ p_3 & p_2 & p_1 & 3 & 0 \\ \vdots & \vdots & & & k-1 \\ p_k & p_{k-1} & \cdots & \cdots & p_1 \end{vmatrix}.$$

Proof: By Newton's identities

$$\begin{aligned} p_1 &= e_1 \\ p_2 &= e_1 p_1 - 2e_2 \\ p_3 &= e_1 p_2 - e_2 p_1 + 3e_3 \\ p_4 &= e_1 p_3 - e_2 p_2 + e_3 p_1 - 4e_4 \\ p_k &= e_1 p_{k-1} - e_2 p_{k-2} + \ldots + (-1)^{k-1} k e_k. \end{aligned}$$

$$\begin{bmatrix} 1 & & & & \\ p_1 & -2 & & & \\ p_2 & -p_1 & 3 & & \\ p_3 & -p_2 & p_1 & -4 & \\ \vdots & & & & \\ p_{k-1} & p_{k-2} & \cdots & p_1 & (-1)^k k \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_k \end{bmatrix} = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_k \end{bmatrix}.$$

By Cramer's rule and column exchanges we obtain the formula for $k!e_k$. For the other formula we use the system:

$$\begin{aligned} e_1 &= p_1 \\ 2e_2 &= p_1e_1 - p_2 \\ 3e_3 &= p_1e_2 - p_2e_1 + p_3 \\ &\vdots \\ ke_k &= p_1e_{k-1} - p_2e_{k-2} + \ldots + p_k(-1)^{k-1}. \end{aligned}$$

Hence

$$\begin{bmatrix} 1 & & & & \\ e_1 & -1 & & & \\ e_2 & -e_1 & 1 & & \\ e_3 & -e_2 & e_1 & -1 & \\ e_{k-1} & -e_{k-2} & \cdots & \cdots & (-1)^{k-1} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_k \end{bmatrix} = \begin{bmatrix} e_2 \\ 2e_2 \\ 3e_3 \\ \vdots \\ ke_k \end{bmatrix}.$$

Solve for p_k to get the formula.

Complete homogeneous polynomials

Definition 2.7. *The complete homogeneous polynomials $h_r, r = 1, 2, 3, \ldots$ are defined as $h_r = \sum x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$. where the sum is over all $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ such that $|\alpha| = r$. By convention we set $h_0 = 1, h_r = 0$ for $r < 0$.*

Proposition 2.8. *For $r = 1, 2, \ldots, n$ we have*

$$e_r = \begin{vmatrix} h_1 & 1 & 0 & \cdots & 0 \\ h_2 & h_1 & 1 & \cdots 0 & \\ \vdots & \vdots & \vdots & \vdots & \\ h_r & h_{r-1} & h_{r-2} & h_1 & \end{vmatrix}, \quad h_r = \begin{vmatrix} e_1 & 1 & 0 & \cdots & 0 \\ e_2 & e_1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ e_r & e_{r-1} & e_{r-2} & \cdots e_1 & \end{vmatrix}.$$

Proof: Consider the generating function

$$H(t) = \sum_{r=0}^{\infty} h_r t^r = \prod_{i=1}^{n} (1 + x_i t + x_i^2 t^2 + \cdots) = \prod_{i=1}^{n} (1 - x_i t)^{-1} = \frac{1}{E(t)}.$$

Thus $H(t)E(t) = 1$. Compare the coefficients of t^i for $i = 1, 2, \ldots, r$ to get

$$\begin{aligned}
-h_1 &= -e_1 \\
-h_2 &= -e_1 h_1 + e_2 \\
-h_3 &= -e_1 h_2 + e_2 h_1 - e_3 \\
-h_r &= -e_1 h_{r-1} + e_2 h_{r-2} - \ldots + (-1)^r e_r.
\end{aligned}$$

Solve for e_r and h_r by Cramer's rule to get the desired formulas.

Proposition 2.9. *For $r = 1, 2, \ldots, n$.*

$$r!h_r = \begin{vmatrix}
p_1 & -1 & 0 & 0 & \cdots & 0 \\
p_2 & p_2 & -2 & & \cdots & 0 \\
p_3 & p_2 & p_1 & -3 & \cdots & 0 \\
\vdots & & & & & \vdots \\
p_{r-1} & p_{r-2} & \cdots & & & -(r-1) \\
p_r & p_{r-1} & \cdots & & & p_r
\end{vmatrix}$$

Proof: By logarithmic differentiation of

$$H(t) = \sum_{r=D}^{\infty} h_r t^r = \Pi_{i=1}^{n} (1 - x_i t)^{-1}$$

we get $H'(t) = H(t) \sum_{r=1}^{\infty} p_r t^{r-1}$. Hence

$$(h_1 + 2h_2 t + 3h_3 t^2 + \ldots) = (1 + h_1 t + h_2 t^2 + \ldots)(p_1 + p_2 t + p_3 t^2 + \ldots).$$

This leads to the system of equations

$$\begin{aligned}
p_1 &= h_1 \\
p_2 &= -p_1 h_1 + 2h_2 \\
p_3 &= -p_2 h_1 - p_1 h_2 + 3h_3 \\
p_4 &= -p_3 h_1 - p_2 h_2 - p_1 h_3 + 4h_4 \\
&\vdots \\
p_r &= -p_{r-1} h_1 - p_{r-2} h_2 - \ldots + r h_r.
\end{aligned}$$

Hence

$$\begin{bmatrix}
-1 & 0 & 0 & \cdots & 0 & 0 \\
p_1 & -2 & 0 & \cdots & 0 & 0 \\
p_2 & p_1 & -3 & \cdots & 0 & 0 \\
\vdots & & & & & \\
p_{r-1} & p_{r-2} & p_{r-3} & \cdots & p_1 & -r
\end{bmatrix}
\begin{bmatrix} h_1 \\ h_2 \\ \vdots \\ h_r \end{bmatrix}
=
\begin{bmatrix} -p_1 \\ -p_2 \\ \vdots \\ -p_r \end{bmatrix}.$$

We get the desired formula by Cramer's rule.

Schur Polynomials

A partition is any finite sequence $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$ of nonnegative integers in decreasing order; $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_r$. Two partitions which differ only in the terminal zeros are regarded same. The nonzero λ_i are called parts of λ and their number is called the length of λ, denoted by $l(\lambda)$. Finally the sum of the parts is called the weight of λ and it is denoted by $|\lambda|$. If $|\lambda| = n$ we say λ is a partition of n. Partitions are often represented by a diagram. For example the partition (54311) is represented by the diagram.

○ ○ ○ ○ ○
○ ○ ○ ○
○ ○ ○
○
○

The conjugate λ' of a partition λ is a partition whose diagram is the transpose of λ. In the above case it will be (53321).

○ ○ ○ ○ ○
○ ○ ○
○ ○ ○
○ ○
○

Let $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{N}^n$ and $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$. Put $\sigma(x^\alpha) = x_{\sigma(1)}^{\alpha_1} x_{\sigma(2)}^{\alpha_2} \dots x_{\sigma(n)}^{\alpha_n}$. Consider the polynomial

$$a_\alpha(x_1, x_2, \dots, x_n) = a_\alpha = \sum_{\sigma \in S_n} sign(\sigma)\sigma(x^\alpha)$$

If $\tau \in S_n$ then $\tau(a_\alpha) = sign(\tau) a_\alpha$. Thus a_α is skew-symmetric. Hence $a_\alpha = 0$ unless all $\alpha_1, \alpha_2, \dots, \alpha_n$ are distinct. Hence we may assume that $\alpha_1 > \alpha_2 > \dots > \alpha_n \geq 0$. Write

$$\alpha = (\lambda_1, \lambda_2, \dots, \lambda_n) + (n-1, n-2, \dots 2, 1, 0)$$

where $(\lambda_1, \lambda_2, \dots, \lambda_n) = \lambda$ is a partition. Put $\delta = (n-1, n-2, \dots, 2, 1, 0)$. Then

$$a_\alpha = \det(x_i^{\alpha_j}) \text{ and } a_\delta = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Since $a_\delta | a_{\lambda+\delta}, S_\lambda = a_{\lambda+\delta}/a_\delta$ is a symmetric polynomial.

Definition 2.10. *The symmetric polynomial $S_\lambda(x_1, x_2, \dots, x_n)$ is called the Schur polynomial corresponding to the partition λ.*

Remark 2.11. *It is easy to see that* $\deg S_\lambda = |\lambda|$.

Example 2.12. Let $\lambda = (1,1,1)$. Then $\delta = (2,1,0)$ and

$$\frac{a_{\lambda+\delta}}{a_\delta} = \begin{vmatrix} x_1^3 & x_1^2 & x_1 \\ x_2^3 & x_2^2 & x_2 \\ x_3^3 & x_3^2 & x_3 \end{vmatrix} \div (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = x_1x_2x_3$$

Example 2.13. Let $\lambda = (3,0,0)$. Then

$$a_{\lambda+\delta} = \begin{vmatrix} x_1^5 & x_1 & 1 \\ x_2^5 & x_2 & 1 \\ x_3^5 & x_3 & 1 \end{vmatrix} = a_\delta h_3$$

Hence $S_\lambda = h_3$.

Proposition 2.14. *The set $\{S_\lambda | \lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n), |\lambda| = d\}$ is a basis of the vector space of all symmetric polynomials of degree d.*

Proof: Let A be the vector space of all antisymmetric polynomials. Put $a_\delta = D$. If f is antisymmetric then $f = gD$, where g is symmetric. Define the vector space isomorphism

$$\mu : k[x]^{S_n} \to A, \quad \mu(g) = gD.$$

Under this isomorphism the Schur polynomials are mapped to all antisymmetrized monomials. Since antisymmetrized monomials constitute a basis of A, the Schur polynomials form a basis of $k[x]^{S_n}$.

Invariants of the alternating group

Proposition 2.15. *Every element of $f \in k[x]^{A_n}$ is uniquely written as $f = g + hD$ where g and h are symmetric polynomials.*

Proof: For $\sigma \in S_n$ write $\sigma(f) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$. Put $\tau = (12)$. Set

$$g = \frac{1}{2}(f + \tau(f)) \text{ and } l = \frac{1}{2}(f - \tau(f)).$$

Then g is symmetric and l is antisymmetric. Thus $D|l$. Write $l = Dh$ for some symmetric polynomial h. Then $f = g + hD$. Suppose g_1 and h_1 are symmetric and $f = g_1 + h_1D$. Then $(g - g_1) = (h_1 - h)D$. Since 0 is the only polynomial which is both symmetric and antisymmetric, we get $g = g_1$ and $h = h_1$.

Jacobi-Trudi Identity

Theorem 2.16. *Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ be a partition with atmost n parts. Let λ' be the conjugate partition corresponding to λ. Suppose that $l(\lambda')$ is the number of nonzero parts of $\lambda' \leq m$. Then*

$$S_\lambda = \det(h_{\lambda_i - i + j})_{1 \leq i,j \leq n} = \det(e_{\lambda'_i - i + j})_{1 \leq i,j \leq m}.$$

Proof: We work in $k[x_1, x_2, \ldots, x_n]$. Let $e_1^{(k)}, e_2^{(k)}, \ldots, e_{n-1}^{(k)}$ denote the elementary symmetric functions of the variables $\{x_1, x_2, \ldots, \overset{\wedge}{x_k}, \ldots, x_n\}$. These are obtained from $e_1, e_2, \ldots, e_n$ by putting $x_k = 0$. Consider the generating function

$$\begin{aligned} E^{(k)}(t) &= 1 + e_1^{(k)} t + e_2^{(k)} t^2 + \ldots + e_{n-1}^{(k)} t^{n-1} \\ &= \Pi_{i \neq k}(1 + x_i t) \end{aligned}$$

Recall that $H(t) = \sum\limits_{r=0}^{\infty} h_r t^r = \Pi_{i=1}^n (1 - x_i t)^{-1}$.
Hence

$$H(t) E^{(k)}(-t) = (1 - x_k t)^{-1}. \tag{1}$$

Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in I\!N^n$. Put

$$A_\alpha = (x_j^{\alpha_i}) = \begin{bmatrix} x_1^{\alpha_1} & x_2^{\alpha_1} & \ldots & x_n^{\alpha_1} \\ x_1^{\alpha_2} & x_2^{\alpha_2} & \ldots & x_n^{\alpha_2} \\ \vdots & & & \\ x_1^{\alpha_n} & x_2^{\alpha_n} & \ldots & x_n^{\alpha_n} \end{bmatrix}.$$

Equate the coefficient of t^{α_i} on either side of (1):

$$x_k^{\alpha_i} = \sum_{j=1}^{n} h_{\alpha_i - (n-j)} (-1)^{n-j} e_{n-j}^{(k)}.$$

Define

$$H_\alpha = (h_{\alpha_i - (n-j)})_{1 \leq i,j \leq n} \text{ and } M = ((-1)^{n-i} e_{n-i}^{(k)})_{1 \leq i,k \leq n}.$$

Then $A_\alpha = H_\alpha M$. Put $\alpha = \delta = (n-1, n-2, \ldots, 2, 1, 0)$. As $\det H_\delta = 1, \det M = \det A_\delta = a_\delta.$ Hence $a_\alpha = a_\delta \det(H_\alpha)$. Put $\alpha = \lambda + \delta$ to get

$$S_\lambda = a_{\lambda+\delta}/a_\delta = \det(H_{\lambda+\delta}) = \det(h_{\lambda_i - i + j}).$$

3. **Theorems of Hilbert and Noether**

Let $k[x]$ denote the polynomial ring in the indeterminates $x_1, x_2, \ldots, x_n$. Let $G < GL(n,k)$ be a finite subgroup. The ring of invariants of G is the ring

$$k[x]^G = \{f \in k[x] \mid M(f) = f \quad \text{for all } M \in G\}.$$

Any $M \in GL(n,k)$ acts on the indeterminates linearly by the rule

$$(x_1, x_2, \dots, x_n)^t \longmapsto M(x_1, x_2, \dots, x_n)^t.$$

This action extends to all $f \in k[x]$ so that $f \longmapsto M(f)$ is an automorphism of $k[x]$. The fundamental problems of invariant theory are the following:
(1) Find a set of generators of $k[x]^G$. These are called the fundamental invariants.
(2) Describe the relations among the fundamental invariants. These are called the syzygies.
(3) Write an arbitrary invariant as a polynomial in the fundamental invariants.
(4) Relate geometric properties with invariants and vice-versa.

We have seen that $k[x]^{S_n}$ is generated by n elementary symmetric polynomials. They are also algebraically independent. Hence $k[x]^{S_n}$ has transcendence degree n over k. We now show that this property is shared by $k[x]^G$ for all finite subgroups G of $GL(n,k)$.

Proposition 3.1. *The ring $k[x]^G$ has transcendence degree n over k.*

Proof: Let trdeg denote the transcendence degree. Then $\text{trdeg}_k k[x] = n$. Thus it is enough to show that $x_1, x_2, \dots, x_n$ are algebraic over $k[x]^G$. Define for $i = 1, 2, \dots, n$;

$$P_i(t) = \prod_{g \in G} (t - g(x_i)).$$

The coefficients of $P_i(t)$ are in $k[x]^G$. As $P_i(x_i) = 0$, x_i is integral over $k[x]^G$ for $i = 1, 2, \dots, n$. Hence $k[x]$ and $k[x]^G$ have same transcendence degree over k.

Let R be any ring, G a finite group of automorphisms of R such that $|G|$ is invertible in R. Put $S = R^G$, the ring of invariants of G acting on R. Consider the map $\rho : R \longrightarrow S$ defined as:

$$\rho(r) = \frac{1}{|G|} \sum_{g \in G} g(r).$$

Then (i) ρ is S-linear (ii) $\rho|_S = id_S$. Such a map $\rho : R \longrightarrow S$ is called the **Reynolds operator** of the pair $S \subset R$.

Proposition 3.2. *Let S be a subring of a ring R and $\rho : R \to S$ be a Reynolds operator. Then (i) $IR \cap S = I$ for all ideals I of S. (ii) If R is Noetherian then so is S.*

Proof: (i) Let $\sum_{i=1}^{n} a_i r_i = a \in S$ where $a_1, \dots, a_n \in I$ and $r_1, r_2, \dots, r_n \in R$. Then $a = \rho(a) = \sum_i \rho(r_i) a_i \in I$.

(ii) Let $I_1 \subset I_2 \subset \dots$ be an ascending chain of ideals in S. Then $I_n R = I_{n+1} R = \dots$ for some n as R is Noetherian. Hence

$$I_n = I_n R \cap S = I_{n+1} R \cap S = I_{n+1} = \dots .$$

Thus S is Noetherian.

Theorem 3.3 (Hilbert's finiteness theorem). *Let G be a subgroup of $GL(n,k)$ acting linearly on $k[x]=R$. Put $S=k[x]^G$. Suppose that there is a Reynolds operator $\rho : R \to S$. Then S is a finitely generated k-algebra.*

Proof: Let M be the maximal ideal of S generated by homogeneous elements of positive degree. Since R is Noetherian MR is finitely generated. Put $M=(f_1,f_2,\dots,f_s)$ where $f_1,f_2,\dots,f_n$ are homogeneous. We claim that $R=k[x]^G=k[f_1,f_2,\dots,f_s]$. Let $f\in R$ be homogeneous of degree d. Apply induction on d. If $d=0, f\in k$. Suppose that $d>0$. Then $f\in M$. Hence there exist $g_1,\dots,g_s\in R$ such that $f=g_1f_1+\cdots+g_sf_s$. Hence $\rho(f)=f=\rho(g_1)f_1+\cdots+\rho(g_s)f_s$. We may assume that g_i are homogeneous. Then $deg\,\rho(g_i)=deg\,g_i=deg\,f-deg\,f_i<deg\,f$. Since $\rho(g_i)$ are of smaller degree than $deg\,f$, by induction $\rho(g_1),\dots,\rho(g_s)\in k[f_1,f_2,\dots f_s]$. Hence $f\in k[f_1,f_2,\dots,f_s]$.

Corollary 3.4. *Let G be a finite subgroup of $GL(n,k)$ acting linearly on $k[x]$. Suppose that $(|G|, char\,k)=1$. Then $k[x]^G$ is a finitely generated k-algebra.*

Theorem 3.5 (Noether's bound). *Let $G\subset GL(n,k)$ be a finite subgroup of order g such that $(g, char\,k)=1$. Then $k[x]^G$ is generated by atmost $\binom{n+g}{g}$ invariants of degree atmost g.*

Proof: For an integral vector $(\alpha_1,\alpha_2,\dots,\alpha_n)\in I\!N^n$ we have $\rho(x^\alpha)=\dfrac{1}{g}\sum_{M\in G} M(x^\alpha)$. The action of M on $k[x]$ gives rise to an automorphism of $k[x]$. Note that $M(x_i)$ is the ith entry of the column vector $M(x_1,x_2,\dots,x_n)^t$. Let $f(x)=\sum_\alpha f_\alpha x^\alpha$, $f_\alpha\in k$ be an invariant and put $M(x^\alpha)=M(x_1^{\alpha_1})\dots M(x_n^{\alpha_n})$. Then

$$f=\rho(f(x_1,x_2,\dots,x_n))=\frac{1}{g}\sum_{\alpha,M} f_\alpha M(x_1)^{\alpha_1}\dots M(x_n)^{\alpha_n}.$$

Thus each invariant is a k-linear combination of the invariants $\sum_M M(x^\alpha) := J_\alpha$. Let $u_1,u_2,\dots,u_n$ be another set of variables. In the polynomial

$$S_d(u)=\sum_M (u_1M(x_1)+\cdots+u_nM(x_n))^d,\quad d=|\alpha|.$$

J_α appears upto a constant factor as the coefficient of $u_1^{\alpha_1}u_2^{\alpha_2}\dots u_n^{\alpha_n}$. The polynomial $S_d(u)$ is the dth power sum in the g polynomials $u_1M(x_1)+\cdots+u_nM(x_n)$. By Newton's identities we know that $S_d(u)$ are polynomials in the first g power sums $S_1(u),S_2(u),\dots,S_g(u)$. Hence all invariants J_α where $|\alpha|>g$ are in the subring $k[J_\alpha|\ |\alpha|\le g]$. Hence

$$k[x]^G=k[J_\alpha \mid |\alpha|\le g],$$

which shows that $k[x]^G$ can be generated by $\binom{n+g}{g}$ invariants $\rho(x^\alpha)$ where $|\alpha|\le g$.

The next example indicates that Noether's bound is the best possible under the given assumptions.

Theorem 3.6. *Let p be a prime number and $n \geq 2$. Consider the cyclic group*

$$G = \{\, \mathrm{diag}(w^k, w^k, \dots, w^k) : k = 0, 1, \dots, p-1\}$$

where $w = e^{2\pi i/p}$. Then $\mathbb{C}[x]^G = \mathbb{C}[\{x^\alpha \mid |\alpha| = p\}]$.

Proof: Let $\rho : \mathbb{C}[x] \to \mathbb{C}[x]^G$ be the Reynolds operator. Then

$$\rho(x^\alpha) = \frac{1}{p}\sum_{k=0}^{p-1}(w^k x_1)^{\alpha_1}\cdots(w^k x_n)^{\alpha_n} = \frac{1}{p}\sum_{k=0}^{p-1} w^{k|\alpha|}x^\alpha = \frac{x^\alpha}{p}\sum_{k=0}^{p-1} w^{k|\alpha|}.$$

If $(p, |\alpha|) = 1$ then $w^{|\alpha|}$ is a primitive pth complex root of 1. Hence $\sum_{k=0}^{p-1} w^{k|\alpha|} = 0$. If p divides $|\alpha|$, then $\rho(x^\alpha) = x^\alpha$. Hence $\mathbb{C}[x]^G$ is generated as a $\mathbb{C}$-algebra by all monomials of total degree p.

4. **Molien's Theorem**

Theorem 4.1. *Let G be a finite subgroup of $GL(n, \mathbb{C})$ acting linearly on $R = \mathbb{C}[x]$. Let $\mathbb{C}[x]^G_i$ denote the vector space generated by all homogeneous invariants of degrees i. Put $H(\mathbb{C}[x]^G, \lambda) = \sum_{i=0}^{\infty} \dim \mathbb{C}[x]^G_i \lambda^i$. Then*

$$H(\mathbb{C}[x]^G, \lambda) = \frac{1}{|G|}\sum_{M\in G}\frac{1}{\det(I - \lambda M)}.$$

Proof: Put $g := |G|$. The Reynolds operator $\rho : R \to R^G$ is a $\mathbb{C}$-linear map. Hence ρ induces a linear map $\rho|_{R_i} = \rho_i : R_i \to (R^G)_i$ where $(\ )_i$ denotes elements of degree i. Clearly $\rho_i^2 = \rho_i$. Hence 0 and 1 are the only eigenvalues of ρ_i. Thus $\mathrm{rank}(\rho_i) = tr(\rho_i) = \dim(R^G)_i$. Therefore

$$H(R^G, \lambda) = \sum_{i=0}^{\infty}\dim(R^G)_i\lambda^i = \sum_{i=0}^{\infty} tr(\rho_i)\lambda^i = \frac{1}{g}\sum_{M\in G}\sum_{i=0}^{\infty} trM|_{R_i}\lambda^i = \frac{1}{g}\sum_{M\in G}\left(\sum_{i=0}^{\infty} trM|_{R_i}\lambda^i\right).$$

We now prove that

$$\sum_{i=0}^{\infty} trM|_{R_i}\lambda^i = \frac{1}{\det(I - \lambda M)}.$$

Since $\mathbb{C}$ is algebraically closed and each M has finite order, M can be diagonalised. Let $x_1, x_2, \dots, x_n$ be a basis of eigenvectors in $\mathbb{C}[x]_1$ whose eigenvalues are $\lambda_1, \lambda_2, \dots, \lambda_n$. A basis of $\mathbb{C}[x]_i$ consists of all monomials of degree i in $\mathbb{C}[x]$. Hence eigenvalues of $M|_{R_i}$ are $\lambda_1^{\alpha_1}\dots\lambda_n^{\alpha_n}$ where $\alpha=(\alpha_1,\alpha_2,\dots,\alpha_n)\in I\!N^n$ and $|\alpha|=i$. Thus

$$trM|_{R_i}=\sum_{\alpha_1+\cdots+\alpha_n=i}\lambda_1^{\alpha_1}\lambda_2^{\alpha_1}\dots\lambda_n^{\alpha_n}.$$

Hence

$$\sum_{i=0}^{\infty}trM|_{R_i}\lambda^i=\prod_{j=1}^{n}\frac{1}{(1-\lambda_j\lambda)}=\prod_{j=1}^{n}\frac{\lambda_j^{-1}}{(\lambda_j^{-1}-\lambda)}=\frac{\det M^{-1}}{\det(M^{-1}-\lambda I)}=\frac{1}{\det(I-\lambda M)}.$$

Therefore $H(R^G,\lambda)=\dfrac{1}{|G|}\sum_{M\in G}\dfrac{1}{\det(I-\lambda M)}$.

Example 4.2. Consider the quaternion group Q_8 acting on $\mathbb{C}[x,y]$. The Molien series is calculated as follows

M	$\det(I-\lambda M)$	M	$\det(I-\lambda M)$
$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$(1-\lambda)^2$	$\begin{bmatrix}-1&0\\0&-1\end{bmatrix}$	$(1+\lambda)^2$
$\begin{bmatrix}i&0\\0&-i\end{bmatrix}$	$1+\lambda^2$	$\begin{bmatrix}-i&0\\0&i\end{bmatrix}$	$1+\lambda^2$
$\begin{bmatrix}0&1\\-1&0\end{bmatrix}$	$1+\lambda^2$	$\begin{bmatrix}0&-1\\1&0\end{bmatrix}$	$1+\lambda^2$
$\begin{bmatrix}0&i\\i&0\end{bmatrix}$	$1+\lambda^2$	$\begin{bmatrix}0&-i\\-i&0\end{bmatrix}$	$1+\lambda^2$

Hence,

$$H(\mathbb{C}[x,y]^{Q_8},\,\lambda)=\frac{1}{8}\left[\frac{1}{(1-\lambda)^2}+\frac{1}{(1+\lambda)^2}+\frac{6}{1+\lambda^2}\right]=\frac{1+\lambda^6}{(1-\lambda^4)^2}=1+2\lambda^4+\lambda^6+\cdots.$$

Hence there are 2 invariants of degree 4 and one of degree 6. The orbit of x and y is $\{\pm x, \pm y, \pm ix, \pm iy\}$. Hence

$$\begin{aligned}\rho(x^4) &= \frac{1}{8}\left\{x^4+x^4+y^4+y^4+x^4+x^4+y^4+y^4\right\} = \frac{1}{2}(x^4+y^4),\\ \rho(x^2y^2) &= x^2y^2.\end{aligned}$$

Let J denote the Jacobian. If $f_1, f_2, \ldots, f_n \in \mathbb{C}[x_1, x_2, \ldots, x_n]$ and $M \in GL(n, \mathbb{C})$ then by chain rule:

$$J(M(f_1), M(f_2), \ldots M(f_n)) = \det M J(f_1, \ldots, f_n).$$

In the present situation, $J(x^4+y^4, x^2y^2) = 8(x^5y - xy^5)$. Hence $\alpha = x^4+y^4, \beta = x^2y^2, \gamma = x^5y - xy^5 \in \mathbb{C}[x,y]^{Q_8}$. Hence $\mathbb{C}[\alpha,\beta,\gamma] \in \mathbb{C}[x,y]^{Q_8}$. It can be verified that $\gamma^2 = \alpha^2\beta - 4\beta^3$. Hence

$$\mathbb{C}[\alpha,\beta,\gamma] \simeq \frac{\mathbb{C}[u,v,w]}{(w^2 - u^2v + 4v^3)}.$$

where $\deg u = \deg v = 4$ and $\deg w = 6$. Therefore the Hilbert series is

$$H(\mathbb{C}[\alpha,\beta,\gamma],\lambda) = \frac{1-\lambda^{12}}{(1-\lambda^4)^2(1-\lambda^6)} = \frac{1+\lambda^6}{(1-\lambda^4)^2}.$$

Therefore $\mathbb{C}[\alpha,\beta,\gamma] = \mathbb{C}[x,y]^{Q_8}$.

Example 4.3. The dihedral group $G = D_{12}$ has a representation in $GL(3,\mathbb{C})$, namely

$$G = \{\sigma^i\delta^j \mid i = 0,1,\ j = 0,1,\ldots,5\}$$

where

$$\sigma = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \text{ and } \delta = \begin{bmatrix} 1/2 & -\sqrt{3}/2 & 0 \\ \sqrt{3}/2 & 1/2 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Thus the Molien series of $\mathbb{C}[x]^G$ is

$$M_G(t) = \frac{1}{12}\left[\frac{1}{(1-t)^3} + \frac{2}{(1-t)(t^2-t-1)} + \frac{2}{(1-t)(t^2+t+1)} + \frac{7}{(1-t)(1+t)^2}\right].$$

Hence

$$M_G(t) = \frac{1+t^7}{(1-t^2)^2(1-t^6)} = 1 + 2t^2 + 3t^4 + 5t^6 + t^7 + 7t^8 + \cdots$$

Thus there are two invariants of degree 2. Since

$$\sigma\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x \\ -y \\ -z \end{bmatrix}, \qquad \delta\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} \frac{1}{2}x - \frac{\sqrt{3}}{2}y \\ \frac{\sqrt{3}}{2}x + \frac{1}{2}y \\ z \end{bmatrix},$$

the polynomials $f = x^2 + y^2$ and $g = z^2$ are two algebraically independent invariants. As f^2, fg, g^2 are linearly independent, we have the desired number of degree 4 invariants. There is an invariant of degree 6 which does not lie in $\mathbb{C}[f,g]$. Using Reynolds operator applied to degree 6 monomials in x, y, z, we find that $h = x^6 - 6x^4y^2 + 9x^2y^4$ is an invariant. Since $J(f, g, h)$ is

$$\begin{vmatrix} 2x & 0 & 6x^5 - 24x^3y^2 + 18xy^4 \\ 2y & 0 & -12x^4y + 36x^2y^3 \\ 0 & 2z & 0 \end{vmatrix} = -2z(-24x^5y + 72x^3y^3 - 12x^5y + 48x^3y^3 - 36xy^5)$$

is nonzero, f, g, h are algebraically independent. Let $S = \mathbb{C}[f, g, h]$. Then

$$H(S, t) = \frac{1}{(1-t^2)^2(1-t^6)}.$$

Thus

$$M_G(t) - H(S, t) = t^7 + \cdots.$$

Hence we need an invariant of degree 7. The polynomial $p = 3x^5yz - 10x^3y^3z + 3xy^5z$ is a degree 7 invariant. Let F, G, H, P be indeterminates. Consider the ideal

$$I = (f - F, g - G, h - H, p - P) \subset \mathbb{C}[x, y, z, F, G, H, P].$$

Let $\mathcal{G}$ be a Gröbner basis of I. Then

$$\mathcal{G} \cap \mathbb{C}[F, G, H, P] = \{P^2 - F^3GH + GH^2\}.$$

Hence there is a degree 14 syzygy among the invariants constructed above. Therefore

$$T := \mathbb{C}[f, g, h, p] \simeq \mathbb{C}[F, G, H, P]/(P^2 - F^3GH + GH^2),$$

$$H(T, t) = \frac{1 - t^{14}}{(1-t^2)^2(1-t^6)(1-t^7)} = \frac{1 + t^7}{(1-t^2)^2(1-t^6)}.$$

Therefore $H(T, t) = H(\mathbb{C}[x]^G, t)$. This shows that the ring of invariants is $\mathbb{C}[f, g, h, p]$.

5. Invariants of the dihedral group D_{2k}

The dihedral group D_{2k} is the group of symmetries of a regular k-gon centerd at the origin. As a subgroup of $GL(2, \mathbb{C})$, it is generated by

$$\rho = \begin{bmatrix} \cos 2\pi/k & -\sin 2\pi/k \\ \sin 2\pi/k & \cos 2\pi/k \end{bmatrix}, r = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Thus $D_{2k} = \{r^i\rho^j \mid i = 0, 1;\ j = 1, 2, \ldots, k-1\}$. The matrix ρ is diagonalizable with eigenvalues $\lambda = e^{2\pi i/k}$ and $\lambda^{-1} = \overline{\lambda}$. Hence $\det(1 - \rho^i t) = (1 - \lambda^i t)(1 - \lambda^{-i} t)$. The reflections $r\rho^i$ are all diagonalizable with eigenvalues 1 and -1. Hence $\det(1 - r\rho^i t) = (1-t)(1+t) = (1-t^2)$. By Molien's theorem

$$H\left(\mathbb{C}[x, y]^{D_{2k}}, t\right) = \frac{1}{2k}\left\{\frac{k}{1-t^2} + \sum_{i=0}^{k-1} \frac{1}{(1-\lambda^i t)(1-\lambda^{-i} t)}\right\}.$$

We now calculate the sum

$$\sum_{i=0}^{k-1} \frac{1}{(1-\lambda^i t)(1-\lambda^{-i}t)}$$

by invariant theory. Consider the cyclic groups C_k generated by ρ. The matrix of ρ can be diagonalized and its diagonal form is $\operatorname{diag}(\lambda, \lambda^{-1})$. We have

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

Hence monomials $x^a y^b$ are mapped to monomials $(\lambda x)^a (\lambda^{-1} y)^b = \lambda^{a-b} x^a y^b$. Hence $\rho(x^a y^b) = \frac{1}{k}\sum_{i=0}^{k-1} \lambda^{i(a-b)} x^a y^b$. Therefore the monomial $x^a y^b$ is an invariant if and only if $(\lambda^i x)^a (\lambda^{-1} y)^b = \lambda^{i(a-b)} x^a y^b = x^a y^b$ for all i if and only if $k | a-b$. Write $a = ka_1 + r_1$, $b = kb_1 + s_1$ where $0 \leq r, s \leq k-1$. As $a - b = k(a_1 - b_1) + (r_1 - s_1)$, $r_1 = s_1$. Therefore invariant monomials are $x^{ka} y^{kb} (xy)^c$ where $0 \leq c \leq k-1$ and $a, b \in I\!N$. Thus

$$\mathbb{C}[x,y]^{C_k} = \bigoplus_{i=0}^{k-1} \mathbb{C}[x^k, y^k](xy)^i.$$

Hence

$$H(\mathbb{C}[x,y]^{C_k}, t) = \sum_{i=0}^{k-1} \frac{t^{2i}}{(1-t^k)^2}.$$

Therefore

$$\frac{1}{k}\sum_{i=0}^{k-1} \frac{1}{(1-\lambda^i t)(1-\lambda^{-i}t)} = \frac{1+t^2+t^4+\cdots+t^{2k-2}}{(1-t^k)^2}.$$

We substitute the above expression into the Molien series of D_{2k} to get

$$\begin{aligned} H(\mathbb{C}[x,y]^{D_{2k}}, t) &= \frac{1}{2k}\left\{ \frac{k(1+t^2+\cdots+t^{2k-2})}{(1-t^k)^2} + \frac{k}{1-t^2} \right\} \\ &= \frac{1}{(1-t^k)(1-t^2)}. \end{aligned}$$

Hence the Molien series is the Hilbert series of a polynomial algebra with generators of degree 2 and degree k. The matrices in D_{2k} are orthogonal. Hence they preserve $f = x^2 + y^2$. Now we look for a degree k invariant. The vertices $(\cos\theta p, \sin\theta p)$ are permuted by the action of the matrices in D_{2k}. Here $\theta = \frac{2\pi}{k}$. Hence for $p = 0, 1, \ldots, k-1$,

$$\begin{aligned} \rho(x\cos p\theta + y\sin p\theta) &= (x\cos\theta - y\sin\theta)\cos p\theta + (x\sin\theta + y\cos\theta)\sin p\theta \\ &= x\cos(p-1)\theta + y\sin(p-1)\theta \\ r(x\cos p\theta + y\sin p\theta) &= x\cos(-p\theta) + y\sin(-p\theta). \end{aligned}$$

Hence $h = \prod_{p=0}^{k-1} x\cos p\theta + y\sin p\theta$ is an invariant of degree k. The invariants f and h are algebraically independent by the fact that

$$\det \begin{bmatrix} f_x & f_y \\ h_x & h_y \end{bmatrix} = \begin{vmatrix} 2x & 2y \\ h_x & h_y \end{vmatrix} = 2(xh_y - yh_x) \neq 0.$$

6. **Invariants of the icosahedron group**

The group I of symmetries of an icosahedron in $\mathbb{R}^3$ centerd at origin is isomorphic to the alternating group of order 60. The icosahedron has 20 faces each of which is an equilateral triangle. The group $I \subset SO(3) \subset GL(3, \mathbb{C})$. Each matrix in I represents a rotation about an axis. There are 12 vertices and hence 6 lines joining pairs of opposite vertices. There are 15 axes joining mid points of opposite edges and 10 axes joining the centers of opposite faces. There are 4 rotations of angle $2\pi k/5$, $k = 1, 2, 3, 4$ about the axes joining opposite vertices. There are 15 rotations through π about the axes joining mid points of the edges. There are 2 rotations of angles $2\pi/3$ and $4\pi/3$ about the axes joining pairs of faces. These add upto $1 + 10.2 + 6.4 + 15.1 = 60$ rotations. There are 4 conjugacy classes of rotations. Hence there are 4 types of characteristic polynomials of the matrices in I. Put $w = \exp(2\pi i/5)$ and $\zeta = \exp(2\pi i/3)$.

diagonal form	$\det(I - Mt)$	No. of matrices	order
$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$(1-t)^3$	1	1
$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$(1-t)(1-t^2)$	15	2
$\begin{bmatrix} \zeta & 0 & 0 \\ 0 & \zeta^{-1} & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$1-t^3$	20	3
$\begin{bmatrix} w^i & 0 & 0 \\ 0 & w^{-i} & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$(1-t)[1-t(w^i+w^{-i})+t^2]$ $i = 1, 2, 3, 4$	24	5

Hence the Molien series is given by

$$H(\mathbb{C}[x,y,z]^I,t) = \frac{1}{60}\left[\frac{1}{(1-t)^3} + \frac{15}{(1-t)(1-t^2)} + \frac{20}{1-t^3}\right] + \sum_{i=1}^{4} \frac{6}{(1-t)(1-t(w^i+w^{-i})+t^2)}.$$

Consider the sum

$$\begin{aligned}\sum_{i=1}^{4} \frac{1}{(1-t(w^i+w^{-i})+t^2)} &= \sum_{i=0}^{4} \frac{1}{(1-w^it)(1-w^{-i}t)} - \frac{1}{(1-t)^2} \\ &= \frac{5(1+t^2+t^4+t^6+t^7)}{(1-t^5)^2} - \frac{1}{(1-t)^2}.\end{aligned}$$

Hence

$$H(\mathbb{C}[x,y,z]^I,t) = \frac{1+t^{15}}{(1-t^2)(1-t^6)(1-t^{10})}.$$

This indicates that the ring of invariants has algebraically independent elements of degree 2,6 and 10 and an invariant of degree 15. The polynomial $f = x^2+y^2+z^2$ is an invariant as I consists of orthogonal matrices. The polar axes are permuted among themselves under the action of I. They form 3 orbits A, B, C consisting of 6, 10, and 15 axes consisting of rotations of order 5, 3 and 2. Take the equations of 6 planes perpendicular to the axes in A and multiply them to get a degree 6 invariant. Similarly we obtain invariants of degree 10 and 15.

7. **Cohen-Macaulay graded rings**

In this section we present a rapid treatment of Cohen-Mecaulay graded rings. Among various classes of rings studied in commutative Algebra, these rings are most useful in applications.

Let k be an infinite field and $R = \oplus_{n=0}^{\infty} R_n$ be a Noetherian graded $R_0 = k$-algebra. Elements of R_n are called homogeneous of degree n. Let R_+ denote the ideal generated by homogeneous elements of positive degree. The Krull dimension of R is defined to be the maximum number of algebraically independent elements of R over k. A system of homogeneous elements $\theta_1, \theta_2, \ldots, \theta_d$ in R where $d = \dim R$ is called a homogeneous system of parameters of R if the ideal $\operatorname{rad}(\theta_1, \theta_2, \ldots, \theta_d) = R_+ =$ the unique maximal homogeneous ideal of R. It is easy to see that $\theta_1, \theta_2, \ldots, \theta_d$ is a homogeneous system of parameters (hsop) if and only if $R/(\theta_1, \ldots, \theta_d)R$ is a finite dimensional k-vector space if and only if R is a finite module over $k[\theta_1, \theta_2, \ldots, \theta_d]$.

Definition 7.1. *A sequence $a_1, a_2, \ldots, a_n$ in a commutative ring R is called an R-regular sequence if $(a_1, a_2, \ldots, a_n)R \neq R$ and a_i is a nonzerodivisor on $R/(a_1, a_2, \ldots, a_{i-1})R$ for $i = 1, 2, \ldots, n$.*

Lemma 7.2. *Let $b_1, b_2, \dots, b_n$ be a regular sequence in R and $b_1r_1 + b_2r_2 + \dots + b_nr_n = 0$ for some $r_1, r_2, \dots, r_n \in R$. Then $r_i \in (b_1, b_2, \dots, b_n)$ for $i = 1, 2, \dots, n$.*

Proof: Induct on n. The $n = 1$ case is clear. Suppose that $b_1r_1 + \dots + b_nr_n = 0$. Then $r_n \in (b_1, b_2, \dots, b_{n-1}) : b_n = (b_1, \dots, b_{n-1})$. Hence $r_n = b_1s_1 + b_2s_2 + \dots + b_{n-1}s_{n-1}$ for some $s_1, \dots, s_{n-1} \in R$. Therefore $b_1r_1 + b_2r_2 + \dots + b_n(b_1s_1 + \dots + b_{n-1}s_{n-1}) = 0$ Hence $b_1(r_1 + b_ns_1) + b_2(r_2 + b_ns_2) + \dots + b_{n-1}(r_{n-1} + b_ns_{n-1}) = 0$ By induction hypothesis $r_i + b_ns_i \in (b_1, b_2, \dots, b_{n-1})$ for $i = 1, 2, \dots, n-1$. Thus $(r_1, r_2, \dots, r_n) \subseteq (b_1, b_2, \dots, b_n)$.

Proposition 7.3. *Let $r_1, r_2, \dots, r_n \in R$. Then $r_1, r_2, \dots, r_g$ is a regular sequence if and only if $r_1^{n_1}, r_2^{n_2}, \dots, r_g^{n_g}$ is a regular sequence for any positive integers $n_1, n_2, \dots, n_g$.*

Proof: Apply induction on g. Suppose r is a nonzerodivisor in R and n is an integer. If $br^n = 0$ then $(br^{n-1})r = 0$. Hence $br^{n-1} = 0$. Hence induction on n shows that r^n is regular for all $n \geq 1$. Conversely let r^n be regular for some $n \geq 1$. If $br = 0$ then $br^n = 0$. Hence $b = 0$. Thus r is regular.

It is enough to prove the proposition for $n_1 = n, n_2 = n_3 = \dots = n_g = 1$. Suppose that $s \in (r_1^n, r_2, \dots, r_{i-1}) : r_i$ for some $i \geq 2$. Then $sr_i = t_1r_1^n + t_2r_2 + \dots + t_{i-1}r_{i-1}$ for some $t_1, t_2, \dots, t_{i-1} \in R$. Since $r_1^{n-1}, r_2, \dots, r_{i-1}$ is a regular sequence, $s \in (r_1^{n-1}, r_2, \dots, r_{i-1})$. Write $s = r_1^{n-1}u_1 + \dots + r_{i-1}u_{i-1}$ for some $u_1, u_2, \dots, u_{i-1} \in R$. Hence

$$r_i(r_1^{n-1}u_1 + r_2u_2 + \dots + r_{i-1}u_{i-1}) = t_1r_1^n + t_2r_2 + \dots + t_{i-1}r_{i-1}.$$

Therefore

$$r_1^{n-1}(u_1r_i - t_1r_1) + r_2(u_2r_i - t_2) + \dots + r_{i-1}(r_iu_{i-1} - t_{i-1}) = 0.$$

Thus $u_1r_i - t_1r_1 \in (r_1^{n-1}, r_2, \dots, r_{i-1})$. Hence $u_1 \in (r_1, \dots, r_{i-1})$ which proves that $r_1^n, r_2, \dots, r_i$ is regular sequence for all i and all n.

Lemma 7.4. *Let R be a one dimensional Noetherian graded k-algebra. Let $a_1, a_2, \dots, a_n$ be homogeneous elements of equal positive degree in R such that $R_+ = rad\,(a_1, \dots, a_n)$. Then there is a k-linear combination $\lambda_1a_1 + \lambda_2a_2 + \dots + \lambda_na_n = a$ such that $rad\,(aR) = R_+$.*

Proof: Put $S = k[a_1, a_2, \dots, a_n]$. Then R is a finite S-module. Thus $\dim S = \dim R = 1$. As S is a standard graded k-algebra, there exist $\lambda_1, \lambda_2, \dots, \lambda_n \in k$ such that $a = \lambda_1a_1 + \dots + \lambda_na_n$ is a homogeneous parameter for S. Thus $\text{rad}(aR) = R_+$.

Lemma 7.5. *Let $\underline{b} = (b_1, b_2, \dots, b_d)$ and $\underline{a} = (a_1, a_2, \dots, a_d)$ be hsops for a graded Noetherian k-algebra R. Suppose $a_1, a_2, \dots, a_d$ have equal degree. Then there is a k-linear combination $a = \lambda_1a_1 + \lambda_2 + \dots + \lambda_da_d$ such that $b_1, b_2, \dots, b_{d-1}, a$ is an hsop for R.*

Proof: Apply induction on d. The case $d = 1$ is clear. Let m be the maximal homogeneous ideal of R. Put $S = R/(b_1, b_2, \dots, b_{d-1})R$. Then $mS = \operatorname{rad}(\overline{a_1}, \overline{a}_2, \dots, \overline{a}_d)S$ where " $-$ " denotes images in S. As $\dim S = 1$, there is a k-linear combination $\lambda_1\overline{a}_1 + \ldots + \lambda_d\overline{a}_d = \overline{a}$ such that $\overline{a}$ is an hsop for S. Hence $(a_1, a_2, \dots, a_{d-1}, a)$ is an hsop for R.

Theorem 7.6. *Let R be a graded Noetherian k-algebra of dimension d. Let $\underline{a} = (a_1, a_2, \dots, a_d)$ and $\underline{b} = (b_1, b_2, \dots, b_d)$ be two hsops of R. If $\underline{a}$ is a regular sequence then so is $\underline{b}$.*

Proof: Induction on d. Let $d = 1$. Then $\operatorname{rad}(a_1) = \operatorname{rad}(b_1)$. Hence there is an $r \geq 1$ such that $a_1^r = b_1 c$ for some $c \in R$. As a_1 is regular, a_1^r is regular. Hence b_1 is regular.

We may assume that $a_1, a_2, \dots, a_d$ have equal degree. Then there is a k-linear combination $a = \lambda_1 a_1 + \cdots + \lambda_d a_d$ such that $a_1, a_2, \dots, a_{d-1}, a$ and $b_1, b_2, \dots, b_{d-1}, a$ are hsops. Let $S = R/aR$. Then $(\overline{a}_1, \overline{a}_2, \dots, \overline{a}_{d-1})$ and $(\overline{b}_1, \overline{b}_2, \dots, \overline{b}_{d-1})$ are hsops in S. As $\overline{a}_1, \overline{a}_2, \dots, \overline{a}_{d-1}$ is regular in $S, \overline{b}_1, \dots, \overline{b}_{d-1}$ is regular in S. Hence a is regular in R. As a is regular on $T = R/(b_1, b_2, \dots, b_{d-1})R, b_d$ is regular on T. Hence $b_1, b_2, \dots, b_d$ is a regular sequence.

Definition 7.7. *A Noetherian graded k-algebra R is called Cohen-Macaulay, abbreviated as CM, if there is an hsop in R which is a regular sequence.*

Theorem 7.8. *R is CM if and only if for any hsop $a_1, a_2, \dots, a_d$ in R, R is a finitely generated free $S = k[a_1, a_2, \dots, a_d]-$module.*

Proof: Let R be a free S-module. As $a_1, a_2, \dots, a_d$ are algebraically independent, they constitute an S-sequence. Freeness of R over S yields $(I : a)R = IR : aR$ for any ideal I of S and $a \in S$. Hence $a_1, a_2, \dots, a_d$ is an $R-$regular sequence.

Conversely let R be CM. If $d = \dim R = 0$ then R is a finite dimensional $k-$vector space and $S = k$. Hence R is a free S-module. Let $d > 0$. We show that the natural map $f : S/a_1S \to R/a_1R$ is injective. As R/a_1R is integral over $f(S/a_1S), \dim f(S/a_1S) = \dim R/a_1R = d-1$. But S/a_1S is a polynomial ring of dimension $d-1$, hence f is injective. Therefore S/a_1S is a graded Noether normalization of R/a_1R. Hence R/a_1R is a free, finite S/a_1S-module by induction hypothesis. Pick a homogeneous basis $\{e_1^{'}, e_2^{'}, \dots, e_n^{'}\}$ of R/a_1R as an S/a_1S-module.

We prove that $\{e_1, \dots, e_n\}$ is a free S-basis of R. First we show that $R = Se_1 + \ldots + Se_n$ by inducting on degree. Let $b \in R$ and degree $b = d$. Then $b^{'} = s_1^{'}e_1 + \ldots + s_n^{'}e_n$ for certain homogeneous elements $s_1, \dots, s_n \in S$. Hence $b - s_1e_1 - \ldots - s_ne_n = a_1c$ for some $c \in R$. Clearly $\deg c < \deg b$. By induction $c \in \sum_{i=1}^{n} Se_i$.

Suppose that $\sum_{i=1}^{n} s_i e_i = 0$. Then $\sum_{i=1}^{n} s_i' e_i' = 0$. Hence $s_i = a_1 t_i$ for some $t_i \in S$. Hence $\sum a_1 t_i e_i = 0$. But a_1 is a nonzero divisor in R. Hence $\sum t_i e_i = 0$. Induction on $\max\{\deg s_i | i = 1, 2, \ldots, n\}$ finishes the argument.

8. Cohen-Macaulayness of rings of invariants

Theorem 8.1. *Let $G \subset GL(n, k)$ be a finite group acting linearly on $k[x]$. Suppose that char(k) and $|G|$ are coprime. Then the ring of invariants $k[x]^G$ is CM.*

Proof: Put $R = k[x]$ and $S = k[x]^G$ and let $\rho : R \to S$ be the Reynolds operator. Let I be an ideal of S. Then we claim that $IR \cap S = I$. Suppose $a_1, a_2, \ldots, a_n \in I$ and $r_1, r_2, \ldots, r_n \in R$ such that $S = a_1 r_1 + \ldots + a_n r_n \in S'$. Then $\rho(s) = s = a_1 \rho(r_1) + \ldots + a_n \rho(r_n) \in I$.

Let $k[a_1, a_2, \ldots, a_n]$ be a graded Noether normalization of S. Then $(a_1, a_2, \ldots, a_n)R$ is primary for R_+. As R is CM, $\underline{a} = a_1, a_2, \ldots, a_n$ is an R-regular sequence. We claim that $\underline{a}$ is also an S-regular sequence.

Suppose that $1 \leq i \leq n$ and $sa_i \in (a_1, a_2, \ldots, a_{i-1})S$. Then $sa_i \in (a_1, a_2, \ldots, a_{i-1})R$. Hence $s \in (a_1, a_2, \ldots, a_{i-1})R \cap S = (a_1, a_2, \ldots, a_{i-1})$. Thus $\underline{a}$ is an S-regular sequence. Therefore S is Cohen-Macaulay.

Since $k[x]^G$ is Cohen-macaulay, it is a finite free module over any graded Noether normalization $S = k[a_1, a_2, \ldots, a_n]$ of $k[x]^G$. Therefore there are invariants $b_1, b_2, \ldots, b_r$ such that

$$k[x]^G = \bigoplus_{i=1}^{r} S b_i.$$

The polynomials $a_1, a_2, \ldots, a_n$ are called primary invariants and $b_1, b_2, \ldots, b_r$ are called secondary invariants. The above decomposition of $k[x]^G$ is called a *Hironaka decomposition.*

Proposition 8.2. *Let $d_1, d_2, \ldots, d_n$ be degrees of a collection of primary invariants of a finite matrix group $G \subseteq GL(n, \mathbb{C})$. Then*
(i) the number of secondary invariants is $r = d_1 d_2 \ldots d_n / |G|$ and
(ii) the degrees (together with multiplicities) of the secondary invariants are the exponents of the generating function

$$H(\mathbb{C}[x]^G, t)\, \Pi_{i=1}^{n} (1 - t^{d_i}) = t^{e_1} + t^{e_2} + \ldots + t^{e_r}.$$

Proof: By Molien's theorem

$$H(\mathbb{C}[x]^G, t) = \frac{1}{|G|} \sum_{M \in G} \frac{1}{\det(I - Mt)} = \frac{t^{e_1} + t^{e_2} + \ldots + t^{e_r}}{\Pi_{i=1}^{n} (1 - t^{d_i})}.$$

Hence

$$\frac{1}{|G|}\sum_{M\in G}\frac{(1-t)^n}{\det(I-Mt)}=\frac{t^{e_1}+t^{e_2}+\ldots+t^{e_r}}{\Pi_{i=1}^n(1+t+t^2+\ldots+t^{d_i-1})}.$$

Put $t=1$ on both sides. On the right hand side we get $r/d_1d_2\ldots d_n$. On the left hand side the only nonzero term after putting $t=1$ is the one for $M=I$. Hence the result.

(ii) Clear.

Example 8.3. Consider the matrix group

$$G=\left\{\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix},\begin{bmatrix}0&1&0\\-1&0&0\\0&0&-1\end{bmatrix},\begin{bmatrix}-1&0&0\\0&-1&0\\0&0&1\end{bmatrix},\begin{bmatrix}0&-1&0\\1&0&0\\0&0&-1\end{bmatrix}\right\}$$

G is a cyclic group of order 4. The ring of invariants $\mathbb{C}[x_1,x_2,x_2]^G=R$ has the Hilbert series

$$\begin{aligned}H(R,t)&=\frac{1}{4}\left[\frac{1}{(1-t)^3}+\frac{2}{(1+t)(1+t^2)}+\frac{1}{(1+t)^2(1-t)}\right]\\&=\frac{1-t+t^2+t^3}{(1+t)^2(1+t^2)(1-t)^3}\\&=1+2t^2+2t^3+5t^4+4t^5+\cdots\end{aligned}$$

The polynomials $\theta_1=x_1^2+x_2^2$, $\theta_2=x_3^2$, $\theta_3=x_1^4+x_2^4$ are invariants. They are algebraically independent by Jacobian criterion. Hence these are primary invariants. The number of secondary invariants is $\deg\theta_1\deg\theta_2\deg\theta_3/4=4$. To find their degrees we find

$$\begin{aligned}H(\mathbb{C}[x]^G,t)(1-t^2)^2(1-t^4)&=\frac{1-t+t^2+t^3}{(1+t)^2(1+t^2)(1-t)^3}\cdot(1-t^2)^2(1-t^4)\\&=1+2t^3+t^4.\end{aligned}$$

Hence $e_1=1, e_2=e_3=3$ and $e_4=4$. Apply Reynolds operator to get the secondary invariants:

$$\eta_1=1,\ \eta_2=x_1x_2x_3,\ \eta_3=x_1^2x_3-x_2^2x_3,\ \eta_4=x_1^3x_2-x_1x_2^3.$$

It is easy to verify that a Hironaka decomposition of $\mathbb{C}[x]^G$ is given by

$$\mathbb{C}[x]^G=\bigoplus_{i=1}^4\mathbb{C}[\theta_1,\theta_2,\theta_3]\eta_i.$$

References

[1] W. Bruns and J. Herzog, *Cohen-Macaulay rings*, Cambridge studies in advanced mathematics 39, Revised edition, Cambridge University Press, 1998.

[2] H. Derksen and G. Kemper, *Computational Invariant Theory*, Springer-Verlag, Berlin, 2002.

[3] L. Smith, *Polynomial invariants of finite groups*, A. K. Peters, Wellesley, Mass. 1995.

[4] R. P. Stanley, *Invariant theory of finite groups and their applications to combinatorics*, Bulletin of Amer. Math. Soc, New Series, vol 1 (1979),475-511.

[5] B. Sturmfels, *Algorithms in invariant theory*, Springer-Verlag, New York, 1993.

Dept. of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400 076

E-mail address: jkv@math.iitb.ac.in