REVIEW OF CALCULATING INVARIANT RINGS OF SYMMETRIC GROUPS BY USING MAXIMA

Mufida M. Hmaida
Department of Mathematics, Misurata University, Misurata, Libya
mu.hmaida@sci.misuratau.edu.ly

Abstract— In this article, we survey some elementary techniques for understanding the invariant theory of finite groups with emphasis on symmetric groups, and give an overview of a package for WxMaxima, called sym which contains tools for writing invariants in terms of many bases.

Keywords: ***Invariant ring, Symmetric groups, Maxima.***

I. INTRODUCTION

In commutative algebra, the invariant theory of finite groups is a very classical subject. The origins of invariant theory go back to Lagrange (1773-1775) and Gauss (1801). Today, it is an important branch of mathematics which related to a variety of other fields such as algebraic geometry and representation theory.

The book [7] caused a broad interest in this area. Over the last three decades, computational invariant theory has made important progress. One of the important goals to find an algorithm for computing generators of the invariant ring, which was extremely difficult in some cases. Several important special cases have been investigated and all questions about them have been answered.

There are software implementations of many algorithms (of finding generators of an invariant ring) in computer algebra systems (as Maxima, Magma, Macaulay2 and Maple). The description of the functions that are related to the invariant theory in Maxima is not obvious, so we decide to study some of them in this paper.

We include some basics of invariant theory in this section as well as it will be required later. We refer to[1,2,5,6,7], from which we gather the statements provided in this section, for further insight into this fascinating subject.

Let G be a matrix group, a subgroup of the general linear group $GL(\mathbb{F}^n)$ of all invertible $n \times n$ matrices. Fix a field $\mathbb{F}$ of characteristic zero, $X = \{x_1, \dots, x_n\}$ and the set $\mathbb{F}[X] \coloneqq \mathbb{F}[x_1, \dots, x_n]$ is the ring of multivariate polynomials in variables $x_1, \dots, x_n$ with coefficients in the field $\mathbb{F}$.

Given $f_1, \dots, f_m \in \mathbb{F}[X]$, the subset of $\mathbb{F}[X]$ that is consisting of all polynomial expressions in $f_1, \dots, f_m$ with coefficients in $\mathbb{F}$ is denoted by $\mathbb{F}[f_1, \dots, f_m]$.

We illustrate some fundamental concepts and results in the non-modular invariant theory of finite groups with examples.

The group G acts naturally on the space $\mathbb{F}^n$ of column matrices by left multiplication, and this action extends to the ring $\mathbb{F}[X]$ as follows: Let $A = (a_{ij}) \in G$, this matrix transforms polynomials in $\mathbb{F}[X]$ via

$$x_i \mapsto a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n, \quad i = 1, \dots, n.$$

Let the symmetric group of degree n be $\mathfrak{S}_n$. Note that the group $\mathfrak{S}_n$ can be identified as subgroup of the group $GL(\mathbb{F}^n)$. Then, the previous action induces an action of $\mathfrak{S}_n$ on $\mathbb{F}[X]$ as follows: If $\sigma \in \mathfrak{S}_n$ and $f \in \mathbb{F}[X]$, then

$$\sigma f(x_1, \dots, x_n) := f(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

Manuscript received November 18, 2020; revised December 23, 2020; accepted December 28, 2020, published online January 3, 2021

A polynomial $f \in \mathbb{F}[X]$ is a G-invariant(or a symmetric polynomial in the case $G \subseteq \mathfrak{S}_n$) if $gf = f$ for all $g \in G$. Also, the set

$$\mathbb{F}[X]^G := \{f \in \mathbb{F}[X] | gf = f \ \forall \ g \in G\}$$

is the set of G-invarinats. This set is a subring of $\mathbb{F}[X]$, as the sum of two invariants is again an invariant, and same for the product.

Example 1: For $n = 3$, the polynomial $p(x, y, z) = x^2 + y^2 + z^2$ is invariant under $\mathfrak{S}_3$ but not under $GL(\mathbb{R}^3)$ as

$$\begin{bmatrix} 1 & 0 & 1 \\ 2 & 2 & 0 \\ 1 & -1 & 1 \end{bmatrix} p = (x + z)^2 + (2x + 2y)^2 + (x - y + z)^2 \neq p.$$

Example 2: Consider the subgroup H of $GL(\mathbb{C}^2)$ that generated by

$$h = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} ; \quad i^2 = -1.$$

A polynomial $f(x, y) = \sum_{j,k} a_{jk} x^j y^k \in \mathbb{C}[x, y]$ is a H-invariant if and only if it is invariant under the action of h, which means $f(x, y) = f(ix, -iy)$, and that is equivalent to $(i)^{j+k}(-1)^k = 1$. The last equation is satisfied when; k even and 4 is a factor of $j + k$, k odd and $j + k = 2r$ where r is odd. Thus we can write $f(x, y)$ as a polynomial in x^4, xy and y^4. This proves that $\mathbb{C}[x, y]^H = \mathbb{C}[x^4, xy, y^4]$.

Due to the fact that G acts on $\mathbb{F}[X]$ by linear transformations, a polynomial is invariant if and only if its homogeneous components are invariant. Hence, the action of G on $\mathbb{F}[X]$ is graded (Recall that an algebra $A = \bigoplus_i A_i$ is graded if the multiplication satisfies $A_i A_j \subset A_{i+j}$). Therefore

$$\mathbb{F}[X]^G = \bigoplus_{d=1}^{\infty} \mathbb{F}[X]_d^G$$

where $\mathbb{F}[X]_d^G$ is the vector space of homogeneous invariants of degree d.

Invariant theory has two basic questions to answer about the ring $\mathbb{F}[X]^G$: Can we find finitely many homogeneous invariants that are generating the algebra $\mathbb{F}[X]^G$, and in how many ways can an invariant be written in terms of these generators. For finite groups acting on a ring of polynomials with coefficient in an algebraically closed field of characteristic zero, both questions have been answered completely. See [1,2,5,7] for more information

Many algorithms can be found for the computation of invariant rings of finite groups, see [7,5]. Some of these methods do not work for an arbitrary ground field. Today, there exist performance implementations of some of them within the computer system Maxima. This paper includes both the source code as well as explanation of an algorithm for writing a symmetric polynomial in terms of the elementary functions.

II. THE INVARIANT THEORY OF THE SYMMETRIC GROUPS

In this section, we review two bases for the ring $\mathbb{F}[X]^{\mathfrak{S}_n}$ and explain an algorithm for writing any symmetric polynomial in terms of these generators by examples.

Define the kth elementary symmetric polynomial as

$$e_k := e_k(x_1, \ldots, x_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k},$$

$1 \le k \le n$. For example, $e_1 = x_1 + \cdots + x_n$ and $e_n = x_1 x_2 \cdots x_n$. Alternatively, the polynomial e_k can be defined as the coefficient of t^{n-k} in the function $\prod_{1 \le i \le n}(t + x_i)$. As $e_k \in \mathbb{F}[X]^{\mathfrak{S}_n}$ for each k, hence every polynomial expression in the elementary symmetric polynomials is symmetric.

Theorem 1 [7, theorem 1.1.1](Main theorem on symmetric polynomials):

$$\mathbb{F}[X]^{\mathfrak{S}_n} = \mathbb{F}[e_1, \ldots, e_n].$$

The proof just given is due to Gauss, who needed the properties of symmetric polynomials for his second proof (dated 1816) of the fundamental theorem of algebra. Note that the proof of theorem 1 gives an algorithm for writing a symmetric polynomial in terms of $e_1, \ldots, e_n$. The following examples of how this algorithm works.

Example 3: Consider the function $f(x, y) = x^6 + y^6$. The leading term of f is $x^6 = \left(e_1(x, 0)\right)^6$, then following the procedure of the proof of the theorem:

$$x^6 + y^6 - \big(e_1(x,y)\big)^6 = x^6 + y^6 - (x+y)^6$$
$$= -(6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5).$$

Dividing by $-e_2(x,y) = -xy$ we obtain

$$6x^4 + 15x^3y + 20x^2y^2 + 15xy^3 + 6y^4.$$

Now the leading term is $6x^4 = 6\big(e_1(x,0)\big)^4$, and thus

$$6x^4 + 15x^3y + 20x^2y^2 + 15xy^3 + 6y^4 - 6e_1^4$$
$$= -(9x^3y + 16x^2y^2 + 9xy^3)$$
$$= -e_2(9x^2 + 16xy + 9y^2).$$

Then one easily sees that

$$9x^2 + 16xy + 9y^2 = 9(x+y)^2 - 2xy = 9e_1^2 - 2e_2.$$

Going backward, we have

$$x^6 + y^6 = e_1^6 - e_2\big(6e_1^4 - e_2(9e_1^2 - 2e_2)\big)$$
$$= e_1^6 - 6e_1^4e_2 + 9e_1^2e_2^2 - 2e_2^3.$$

Remark: The proof also shows that if the total degree(the maximum of the total degrees of its monomial summands) of a symmetric polynomial $f(x_1,\dots,x_n)$ is less than or equal n , then the expression for $f(x_1,\dots,x_{n-1},0)$ in terms of $e_i(x_1,\dots,x_{n-1})$ gives the correct expression for $f(x_1,\dots,x_n)$ in terms of $e_i(x_1,\dots,x_n)$.

Example 4: Express the function

$$f(x_1,\dots,x_n) = x_1^3 + \cdots + x_n^3 + 2\sum_{i\neq j} x_i x_j^2$$

in terms of the elementary symmetric polynomials.

The induction of n and the previous remark indicate that the general formula will be found by finding the formula for n = 3, since the total degree is 3. Following the procedure of the proof of the theorem, we have

$$x_1^3 + x_2^3 + 2x_1x_2^2 + 2x_2x_1^2 - (x_1+x_2)^3$$
$$= -(x_1^2x_2 + x_1x_2^2) = -e_2e_1.$$

So we obtain

$$x_1^3 + x_2^3 + 2x_1x_2^2 + 2x_2x_1^2$$
$$= (e_1(x_1,x_2))^3 - e_2(x_1,x_2)e_1(x_1,x_2)$$

Passing to three variables and consider

$$x_1^3 + x_2^3 + x_3^3 + 2\sum_{i\neq j} x_i x_j^2 - \big(e_1(x_1,x_2,x_3)\big)^3$$
$$+ e_2(x_1,x_2,x_3)e_1(x_1,x_2,x_3)$$
$$= -x_1x_2x_3.$$

Thus with three variables,

$$x_1^3 + x_2^3 + x_3^3 + 2\sum_{i\neq j} x_i x_j^2 = (e_1)^3 - e_2e_1 - e_3.$$

By the remark above, this shows that for arbitrary $n \geq 3$ we have

$$x_1^3 + \cdots + x_n^3 + 2\sum_{i\neq j} x_i x_j^2 = (e_1)^3 - e_2e_1 - e_3.$$

There are other common homogeneous bases for $\mathbb{F}[X]^{\mathfrak{S}_n}$, the set $\{p_k\}_{k=1}^n$ is one of them, defined as follows:

$p_k := p_k(x_1,\dots,x_n) = \sum_{1\leq i\leq n} x_i^k$ (the k-th power sum polynomial).

Theorem 2: If $\mathbb{F}$ is a field containing the rational numbers $\mathbb{Q}$, then

$$\mathbb{F}[X]^{\mathfrak{S}_n} = \mathbb{F}[p_1,\dots,p_n]$$

Proof: By using theorem 1, it suffices to prove that the elementary polynomials are polynomials in $p_1,\dots,p_n$. From the Newton identities, which state that:

$$ke_k = \sum_{i=1}^{k}(-1)^{i-1}e_{k-i}p_i, \quad n \geq k \geq 1.$$

Since $\mathbb{Q}$ is contained in $\mathbb{F}$, we can divide by the integer k. Then the elementary may be expresses recursively in terms of the power sums as:

$$e_k = \frac{1}{k}\sum_{i=1}^{k}(-1)^{i-1}e_{k-i}p_i, \qquad n \geq k \geq 1.$$

Note that $e_1 = p_1$. □

Example 5: From the previous theorems, we have

$$\mathbb{R}[x,y,z]^{\mathfrak{S}_3} = \mathbb{R}[x+y+z, xy+xz+yz, xyz]$$
$$= \mathbb{R}[x+y+z, x^2+y^2+z^2, x^3+y^3+z^3].$$

III. THE MAXIMA PACKAGE SYM

Maxima is a free computer algebra system whose development started in 1968. WxMaxima (graphical user interface for the Maxima) allows one to use all of Maxima's functions. For more details, see [2].

We will show how to use sym package in WxMaxima. Sym is a package for working with symmetric polynomials. It was written by Annick Valibouze for

Macsyma-Symbolics, she used algorithms that are described in [8,9,10,11].

Maxima has several functions which can be used for studying a symmetric polynomial. These are described in the Maxima manual, Section 32. We will present some examples of the use of some of these functions. Some of them can be used for writing a symmetric polynomial as a polynomial expression in terms of $e_1, \dots, e_n$ or in terms of $p_1, \dots, p_n$, and for changing bases.

Let $f(x_1, \dots, x_n)$ be a symmetric polynomial which is a homogeneous of degree $d \neq 0$. This section gives examples of the following Maxima functions:

i). **elem**($[n], \frac{1}{n} f(x_1, \dots, x_n), [x_1, \dots, x_n]$): decomposes the polynomial f in terms of the elementary symmetric functions $e_1, \dots, e_n$.

ii). **pui**($[n], \frac{1}{n} f(x_1, \dots, x_n), [x_1, \dots, x_n]$): decomposes the polynomial f in terms of the polynomials $p_1, \dots, p_n$.

iii). **ele2pui**($n, [e_n]$): implements passing from the elementary symmetric functions $e_1, \dots, e_n$ to the power sums from 0 to n.

iv). **ele2pui**($n, [m, e_1]$): restricting the answer of elem2pui($n, [e_n]$) from n to m.

v). **pui2ele**($n, [e_n]$) and pui2ele($n, [m, e_1]$): go from the power sums to the elementary symmetric functions. Similar to ele2pui.

vi). **multi_elem**($[\,[m, e_1, \dots, e_m], [m', g_1, \dots, g_{m'}]\,], f, [[x_1, \dots, x_m], [x_{m+1}, \dots, x_n]]$) : decomposes a multi-symmetric polynomial $\widehat{m}f$ in terms of the elementary symmetric functions e_i's and g_i's and $\widehat{m}$ is a constant is depended on the values of m and m', where $m' = n - m, f \in \mathbb{F}[x_1, \dots, x_m]^{\mathfrak{S}_m}$ and $f \in \mathbb{F}[x_{m+1}, \dots, x_n]^{\mathfrak{S}_{n-m}}$.

Maxima has more functions which related to other types of symmetric functions as monomial symmetric functions, complete homogeneous symmetric functions and Schur functions. Also, the function ratsimp( ) is usually used after the previous functions to obtain a simpler expression for the expression between the brackets.

We conclude this paper with examples that showing how the previous Maxima functions work. To begin, the packages sym, facexp and compile should be loaded.

The function elem:

(%i1) elem([2],x^4+y^4,[x,y]);

(%o1) $e_1(e_1(2e_1^2 - 2e_2) - 2e_1e_2) - 2(2e_1^2 - 2e_2)e_2$

(%i2) ratsimp(%/2);

(%o2) $2e_2^2 - 4e_1^2e_2 + e_1^4$

(%i3) elem([3],x^4+y^4+z^4,[x,y,z]);

(%o3) $e_1\big(3e_3 - 3e_1e_2 + e_1(3e_1^2 - 3e_2)\big) + 9e_1e_3 - 2(3e_1^2 - 3e_2)e_2$

(%i4) ratsimp(%/3);

(%o4) $4e_1e_3 + 2e_2^2 - 4e_1^2e_2 + e_1^4$

Similarly,

(%i5) pui([2],x^4+y^4,[x,y]);

(%o5) $2p_1(p_1p_2 - \frac{p_1(p_1^2-p_2)}{2}) - (p_1^2 - p_2)p_2$

(%i6) ratsimp(%/2);

(%o6) $\frac{p_2^2+2p_1^2p_2-p_1^4}{2}$

To change between bases, we can use for example:

(%i7) ele2pui(3,[e3]);

(%o7) $[4, e_1, e_1^2 - 2e_2, 3e_3 - e_1e_2 + e_1(e_1^2 - 2e_2)]$

Which means

$p_1 = e_1,\;\; p_2 = e_1^2 - 2e_2,$

$p_3 = 3e_3 - e_1e_2 + e_1(e_1^2 - 2e_2)$

Finally, the use of the function multi_elem:

(%i9)multi_elem([[2,e1,e2],[2,g1,g2]],(x^2+y^2)*(a*b), [[x,y],[a,b]]);

(%o9) $2(e_1^2 - 2e_2)g_2$

Modern computer algebra and computational methods have largely expanded in the last years. However, much progress is still needed to enlarge the spectrum of applications and make them easier to use with different types of groups

REFERENCES

[1] D.J. Benson. *Polynomial invariants of finite groups*. Cambridge university press, 1993.

[2] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate texts in mathematics. Springer, 2007.

[3] H. Derksen and G. Kemper. *Invariant Theory and Algebraic Transformation Groups*, I. Encyclopaedia of mathematical sciences, 130. Springer, 2002.

[4] M Kanagasabapathy. Introduction to WXMaxima for Scientific Computations. BPB publication, 2018.

[5] G. Kemper. Calculating invariant rings of finite groups over arbitrary fields. Journal of symbolic computation, 21(3):351-66, 1996.

[6] G. Kemper. Using extended Derksen ideals in computational invariant theory. Journal of symbolic computation, 72:161-81, 2016.

[7] B. Sturmfels. *Algorithms in Invariant Theory*. Texts and monographs in symbolic computation. Springer-Verlag, 1993.

[8] A. Valibouze. *Fonctions symétriques et changements de bases.* EUROCAL 87, 323-332, Lecture notes in Computation science 378. Springer, 1989.

[9] A. Valibouze. *Résolvantes et fonctions symétriques*. Proceedings of the ACM-SIGSAM. ACM Press, 390-399, 1989.

[10] A. Valibouze. Symbolic computation with symmetric polynomials, an extension to Macsyma. Springer-Verlag, 308-320, 1989.

[11] A. Valibouze. *Théorie de Galois Constructive*. Annick Valibouze. Mémoire d'habilitation à diriger les recherches (HDR), Université P. et M. Curie (Paris VI), 1994.