

POLYNOMIAL INVARIANTS OF FINITE GROUPS

K. IWANCIO THOMPSON

ABSTRACT. We would like to describe all polynomials in the ring $k[x_1, \dots, x_n]$ that do not change under a change of the variables. For example, what polynomials f have the property that $f(x_1, \dots, x_n) = f(x_{i_1}, \dots, x_{i_n})$ for some permutation of the variables? This is an example of the permutation group S_n acting on the variables. In general, we will look at finite matrix groups acting on polynomials.

1. INTRODUCTION

The goal of this paper is to summarize the first three sections of Chapter Seven of the book Ideals, Varieties, and Algorithms by David Cox, John Little, and Donal O’Shea. The chapter, entitled “Invariant Theory of Finite Groups”, is broken up into several sections. First we look at symmetric polynomials, develop some tools for determining whether or not a polynomial is symmetric, and observe different ways of writing polynomials which are symmetric. Following the preliminary discussion of symmetric polynomials, we review finite matrix groups and rings of invariants, and define what it means for a polynomial to be invariant under a finite matrix group. The invariant polynomials under a finite matrix group form a finitely generated ring. Ultimately, we want to describe the ring by finding the set of generators.

2. POLYNOMIALS INVARIANT UNDER S_n ACTIONS

Consider the ring of polynomials in n variables, $k[x_1, \dots, x_n]$. Recall that a linear change of variables is given by a non-degenerate $n \times n$ matrix. The group of invertible $n \times n$ matrices is denoted $GL(n, k) = GL(n)$, where the entries of the matrices are in the field k . We will consider finite subgroups, G of $GL(n)$, and we want to systematically describe all polynomials that remain unchanged under linear changes from G . For $G = S_n$, the group of permutations on n variables.

Definition 2.1. *A symmetric polynomial is a polynomial $f \in k[x_1, \dots, x_n]$ with the special property that $f(x_1, \dots, x_n) = f(x_{i_1}, \dots, x_{i_n})$ for all permutations of the variables x_1, \dots, x_n .*

In other words, we let the permutation group S_n act on the variables. A symmetric polynomial f will not change when the variables are permuted by some element of S_n . Some examples of symmetric polynomials are:

- $f = x^3 + y^3 + z^3$,
- $g = xyz + x^2 + y^2 + z^2$, and
- $h = xy + yz + xz$.

We define the elementary symmetric functions to be the polynomials $\sigma_i \in k[x_1, \dots, x_n]$ given by:

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + \dots + x_n \\ \sigma_2 &= \sum_{i_1 < i_2} x_{i_1} x_{i_2}, \\ &\vdots \\ \sigma_r &= \sum_{i_1 < i_2 < \dots < i_r} x_{i_1} x_{i_2} \dots x_{i_r}, \\ &\vdots \\ \sigma_n &= x_1 x_2 \dots x_n. \end{aligned}$$

Theorem 2.2. *Any symmetric polynomial can be expressed in terms of these elementary symmetric functions.*

This is the Fundamental Theorem of Symmetric Groups, and a proof is given in Chapter 7 of Cox, Little, and O'Shea. The next step is to determine whether or not a given polynomial is symmetric and to write it in terms of the elementary symmetric functions.

Proposition 2.3. *Let f be some polynomial in $k[x_1, \dots, x_n]$. In order to determine whether or not the polynomial is symmetric, introduce a new set of variables y_1, \dots, y_n and form the ideal $I = \langle \sigma_1 - y_1, \dots, \sigma_n - y_n \rangle$. Find a Groebner basis G for the ideal I and find the remainder g that results from dividing f by G . If the remainder term depends only on the variables y_1, \dots, y_n , then f is symmetric and can be written as $g(\sigma_1, \dots, \sigma_n)$.*

For a proof of this theorem see Cox, Little, and O'Shea.

Calculating a Groebner basis for I may prove challenging. The following result allows us to bypass Groebner basis computations.

Proposition 2.4. *The g_i 's in the Groebner basis are given in terms of polynomials h_j , $h_j(u_1, \dots, u_n) = \sum_{|\alpha|=j} u^\alpha$. The expression $\sum_{|\alpha|=j} u^\alpha$ is the sum of all monomials of total degree j . For example, $h_2(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 + x_1 x_2 + x_1 x_3 + x_2 x_3$. Fix lexicographic order with $x_1 > \dots > x_n > y_1 > \dots > y_n$. Then each g_k in the Groebner basis for $\langle \sigma_1 - y_1, \dots, \sigma_n - y_n \rangle$ is given by*

$$g_k = h_k(x_k, \dots, x_n) + \sum_{i=1}^k (-1)^i h_{k-i}(x_k, \dots, x_n) y_i, \text{ for } k = 1, \dots, n.$$

(Again, see Chapter 7, Section 1 in the text for a proof of this proposition.) Let us apply this result to an example in three variables. We will then compare the result to a Groebner basis calculation using Maple.

Example 2.5. *Suppose $f \in k[x_1, x_2, x_3]$, and we want to see if f is a symmetric polynomial. We start by finding a Groebner basis for the ideal $I = \langle \sigma_1 - y_1, \sigma_2 - y_2, \sigma_3 - y_3 \rangle \subseteq k[x_1, x_2, x_3, y_1, y_2, y_3]$ using lexicographic order with*

$x_1 > x_2 > x_3 > y_1 > y_2 > y_3$. To do this we need to use:

$$\begin{aligned}\sigma_1 &= x_1 + x_2 + x_3, \\ \sigma_2 &= x_1x_2 + x_1x_3 + x_2x_3, \text{ and} \\ \sigma_3 &= x_1x_2x_3.\end{aligned}$$

Then $g_1 = h_1(x_1, x_2, x_3) - h_0(x_1, x_2, x_3)y_1$. Notice that we always have $h_0 = 1$. The polynomial $h_1(x_1, x_2, x_3) = x_1 + x_2 + x_3$. Therefore $g_1 = x_1 + x_2 + x_3 - y_1$. The second polynomial in the Groebner basis is given by $g_2 = h_2(x_2, x_3) - h_1(x_2, x_3)y_1 + h_0(x_2, x_3)y_2$, and the third is given by $g_3 = h_3(x_3) - h_2(x_3)y_1 + h_1(x_3)y_2 - h_0(x_3)y_3$. The computations give us a Groebner basis $G = \{g_1, g_2, g_3\}$, where

$$\begin{aligned}g_1 &= x_1 + x_2 + x_3 - y_1, \\ g_2 &= x_2^2 + x_2x_3 + x_3^2 - x_2y_1 - x_3y_1 + y_2, \text{ and} \\ g_3 &= x_3^3 - x_3^2y_1 + x_3y_2 - y_3.\end{aligned}$$

Then we can use this G to check if a polynomial $f \in k[x_1, x_2, x_3]$ is symmetric by calculating $g = \bar{f}^G$. If $g = \bar{f}^G$ depends only on y_1, y_2, y_3 , then f is symmetric and can be written as $f = g(\sigma_1, \sigma_2, \sigma_3)$.

Check the Groebner basis computation using Maple. The code is as follows:

```
> with(Groebner):
> sigma1:=x1+x2+x3:
> sigma2:=x1*x2+x1*x3+x2*x3:
> sigma3:=x1*x2*x3:
> WL:=[sigma1-y1,sigma2-y2,sigma3-y3]:
> gbasis(WL,plex(x1,x2,x3,y1,y2,y3));
```

$[x^3 y^2 - y^3 + x^3^2 - x^3^2 y_1, x^2^2 - x^2 y_1 + y_2 + x^2 x^3 + x^3^2 - x^3 y_1, x_1 + x_2 + x_3 - y_1]$.

Now let's choose a polynomial $f \in k[x_1, x_2, x_3]$ and use division by G to see if it is symmetric and, if possible, to write it in terms of the elementary symmetric functions.

Example 2.6. Let $f = (x_1^2 + x_2^2)(x_1^2 + x_3^2)(x_2^2 + x_3^2) \in k[x_1, x_2, x_3]$. This polynomial f was chosen from problem 5, page 318. We check to see if f is symmetric by using the method described above. Because $f \in k[x_1, x_2, x_3]$, we use the Groebner basis $G = \{g_1, g_2, g_3\}$ that was calculated for $\langle \sigma_1 - y_1, \sigma_2 - y_2, \sigma_3 - y_3 \rangle$. Use the reduce function in Maple to find the remainder of f when divided by G . The Maple code is given below.

```
> W:=expand((x1^2+x2^2)*(x1^2+x3^2)*(x2^2+x3^2));
W := x1^4 x2^2 + x1^4 x3^2 + 2 x1^2 x3^2 x2^2 + x1^2 x3^4 + x2^4 x1^2 + x2^4 x3^2 + x2^2 x3^4
> g:=reduce(W,WL,plex(x1,x2,x3,y1,y2,y3));
```

$$g := 4 y_2 y_3 y_1 - 2 y_1^3 y_3 + y_1^2 y_2^2 - 2 y_2^3 - y_3^2$$

Notice that in the above code, $\bar{f}^G = g$. We know f is symmetric if g is only in terms of y_1, y_2, y_3 . In the example, f is symmetric and can be written in terms of the elementary symmetric functions as $f = g(\sigma_1, \sigma_2, \sigma_3)$. In other words f is a symmetric function given by

$$f = 4\sigma_1\sigma_2\sigma_3 - 2\sigma_1^3\sigma_3 + \sigma_1^2\sigma_2^2 - 2\sigma_2^3 - \sigma_3^2.$$

Now we will move from looking at polynomials invariant under S_n to looking at finite matrix groups in general.

3. FINITE SUBGROUPS OF $GL(n, k)$

Henceforth, we will assume that the field k contains the rational numbers. For ease of notation, we will write $GL(n, k) = GL(n)$. The field k will be the same for the ring $k[x_1, \dots, x_n]$ and $GL(n)$.

Recall that the group $GL(n)$ is the set of all invertible $n \times n$ matrices with entries in the field k . We will be interested only in finite subgroups of $GL(n)$. A finite subgroup $G \subseteq GL(n)$ is nonempty and closed under matrix multiplication. Recall that a subgroup is a group in its own right, and the number of elements in the group is called the order of G , denoted $|G|$.

A familiar example of a finite subgroup G is the cyclic group of order m . The cyclic group of order m is generated by a matrix $A \in G$ such that $A^m = I_n$. Then the cyclic group is given by $C_m = \{I_n, A, A^2, \dots, A^{m-1}\}$.

A more specific example of a cyclic group then is $C_4 \subseteq GL(2)$. The cyclic group of order 4 then is equal to $\{I_2, A, A^2, A^3\}$, where $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

The symmetric group S_n can also be realized as a finite subgroup of $GL(n)$. The elements of S_n can be written as permutation matrices. A permutation matrix is a matrix obtained by permuting the rows or columns of the identity matrix. For example, let $A \in S_3$ be given by

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

This matrix is the permutation on (x, y, z) that sends x to y , y to z , and z to x .

With finite subgroups, G , of $GL(n)$, we have the properties:

- (1) $I_n \in G$,
- (2) $A \in G \implies A^m = I_n \exists m \in \mathbb{Z}_{>0}$, and
- (3) $A \in G \implies A^{-1} \in G$.

These are just basic properties of finite subgroups that we use implicitly throughout the discussion.

We have a good understanding of finite subgroups of $GL(n)$, but we need to gain an understanding of how these subgroups act on polynomials in the ring $k[x_1, \dots, x_n]$.

4. RING OF INVARIANTS OF A FINITE MATRIX GROUP

Recall that in linear algebra, a linear change of coordinates is given by invertible matrices. Matrices will act on polynomials by changing the variables. Let f be a

polynomial in $k[x_1, \dots, x_n]$. Denote $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$. Suppose $A = (a_{ij}) \in G \subseteq GL(n)$.

Then a change of variables is given by $A \cdot \mathbf{x}$. For any $A \in G$ and $f \in k[x_1, \dots, x_n]$, $f(A \cdot \mathbf{x})$ is again a polynomial in $k[x_1, \dots, x_n]$. This defines the action of G on polynomials in the ring $k[x_1, \dots, x_n]$. We can think of $g = f(A \cdot \mathbf{x})$ as f viewed in new coordinates where the coordinate change is given by the matrix A . Let's look at an example.

Example 4.1. Let $f(\mathbf{x}) = f(x, y) = x^2 + xy + y^2 \in k[x, y]$ and $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in GL(2)$. Then let $g(\mathbf{x}) = f(A \cdot \mathbf{x})$. Clearly $A \cdot \mathbf{x} = \begin{pmatrix} -y \\ x \end{pmatrix}$. Therefore $g(\mathbf{x}) = f(-y, x) = y^2 - yx + x^2 = x^2 - xy + y^2$. Notice that if we write the coordinates of f as $(1, 1, 1)$ using $\{x^2, xy, y^2\}$ as a basis, then the new coordinates of f under the transformation A are $(1, -1, 1)$. In this example, $f(\mathbf{x}) \neq f(A \cdot \mathbf{x})$.

Sometimes it will be the case that $f(\mathbf{x}) = f(A \cdot \mathbf{x})$. If this is true for all $A \in G \subseteq GL(n)$, then we say the polynomial $f \in k[x_1, \dots, x_n]$ is invariant under G . The set of all invariant polynomials is denoted by $k[x_1, \dots, x_n]^G$. We have already seen an example of $k[x_1, \dots, x_n]^G$. When $G = S_n$, then $k[x_1, \dots, x_n]^{S_n} = \{\text{all symmetric polynomials in } k[x_1, \dots, x_n]\}$. Then we write $k[x_1, \dots, x_n]^{S_n} = k[\sigma_1, \dots, \sigma_n]$ to indicate that any symmetric polynomial can be expressed as a polynomial in $\{\sigma_1, \dots, \sigma_n\}$ with coefficients in k .

One can check that $k[x_1, \dots, x_n]^G$ satisfies the definition of a ring. We call $k[x_1, \dots, x_n]^G$ the ring of invariants of a finite matrix group.

We want to take a given finite group $G \subseteq GL(n)$ and find the ring of invariants of G .

Lemma 4.2. Suppose that the finite group G is generated by the set $\{A_1, \dots, A_m\}$. Then a polynomial $f \in k[x_1, \dots, x_n]$ is in the ring of invariants of G if and only if $f(x) = f(A_1 \cdot \mathbf{x}) = f(A_2 \cdot \mathbf{x}) = \dots = f(A_m \cdot \mathbf{x})$.

This result is proved on page 235. We will now try some examples.

Example 4.3. Let $G = V_4 = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\} \in GL(2)$ and $f \in k[x, y]$. The group G is known as the Klein four group and is generated by the matrices $A_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ and $A_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. A polynomial $f \in k[x, y]$ is in $k[x, y]^{V_4}$ if and only if $f(\mathbf{x}) = f(A_1 \cdot \mathbf{x}) = f(A_2 \cdot \mathbf{x})$. This gives the conditions that $f \in k[x, y]^{V_4}$ if and only if $f(x, y) = f(-x, y) = f(x, -y)$. Let $f = \sum a_{ij} x^i y^j$. Then the condition

$f(x, y) = f(x, -y)$ gives us:

$$\begin{aligned} \sum a_{ij}x^i y^j &= \sum a_{ij}x^i (-y)^j, \\ \sum a_{ij}x^i y^j &= \sum (-1)^j a_{ij}x^i y^j, \\ (-1)^j a_{ij} &= a_{ij}, \\ a_{ij} &= 0 \text{ for } j \text{ odd.} \end{aligned}$$

We conclude that $f \in k[x, y]^{V_4}$ only has even powers of y . In a similar manner, we can conclude that only even powers of x appear. Therefore any $f \in k[x, y]^{V_4}$ can be written uniquely in terms of x^2 and y^2 , and $k[x, y]^{V_4} = k[x^2, y^2]$.

Example 4.4. Now let $G = C_2 = \{\pm I_2\}$. Then $f \in k[x, y]^{C_2}$ if and only if $f(\mathbf{x}) = f(A \cdot \mathbf{x})$, where $A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. The polynomial $f \in k[x, y]$ is in the ring of invariants of C_2 if and only if $f(x, y) = f(-x, -y)$. Let $f = \sum a_{ij}x^i y^j$. We have:

$$\begin{aligned} \sum a_{ij}x^i y^j &= \sum a_{ij}(-x)^i (-y)^j, \\ \sum a_{ij}x^i y^j &= \sum (-1)^i (-1)^j a_{ij}x^i y^j, \\ \sum a_{ij}x^i y^j &= \sum (-1)^{i+j} a_{ij}x^i y^j, \\ a_{ij} &= (-1)^{i+j} a_{ij}, \\ a_{ij} &= 0 \text{ for } i + j \text{ odd.} \end{aligned}$$

Each of the above statements are if and only if. Therefore the factors of x and y in $f \in k[x, y]^{C_2}$ either both have even power or both have odd power. We conclude then that $k[x, y]^{C_2} = k[x^2, xy, y^2]$. Notice that in this example, we cannot write f uniquely in terms of x^2 , xy , and y^2 . For example, if $f = x^6 y^4$, we can write $f = (x^2)^3 (y^2)^2 = x^2 (xy)^4$. Uniqueness breaks down here because there is a relationship between x^2 , xy , and y^2 , namely $x^2 y^2 = (xy)^2$.

The questions that remain are:

- Can we always finitely generate the ring of invariants for a given finite matrix group?
- Can an invariant polynomial be written uniquely in terms of the generators?

The rest of this paper will focus on answering the first question.

5. GENERATING THE RING OF INVARIANTS

In Examples 4.3 and 4.5 we found the generators for the ring of invariants of a given group by using the generators of the group. Now we want to develop a more algorithmic approach. Let $f_1, \dots, f_m \in k[x_1, \dots, x_n]$, and let $k[f_1, \dots, f_m] \subseteq k[x_1, \dots, x_n]$ be the subset that consists of polynomials in f_1, \dots, f_m with coefficients in k . In terms of this notation, we want to find f_1, \dots, f_m such that $k[x_1, \dots, x_n]^G = k[f_1, \dots, f_m]$.

Consider the example with $G = V_4$ in the above notation. We have $f_1 = x^2$, and $f_2 = y^2$. Then $k[x, y]^{V_4} = k[f_1, f_2]$.

To find the ring of invariants algorithmically, we will use the Reynolds operator. We let $G \subseteq GL(n)$ be a finite group. The Reynolds operator is then a map $R_G : k[x_1, \dots, x_n] \rightarrow k[x_1, \dots, x_n]$ that is defined as

$$R_G(f)(\mathbf{x}) = \frac{1}{|G|} \sum_{A \in G} f(A \cdot \mathbf{x}),$$

where $f \in k[x_1, \dots, x_n]$.

This map has the following important properties:

- (1) R_G is linear in f over the field k ,
- (2) If $f \in k[x_1, \dots, x_n]$, then $R_G(f) \in k[x_1, \dots, x_n]^G$, and
- (3) If $f \in k[x_1, \dots, x_n]^G$, then $R_G(f) = f$.

In other words, we can use the Reynolds operator to check if something is an invariant and/or to create invariants.

Example 5.1. Let $G = C_2 = \{\pm I_2\}$. Recall $k[x, y]^{C_2} = \{f \in k[x, y] \mid f(x, y) = f(-x, -y)\}$. The Reynolds operator for any $f \in k[x, y]$ is given by $R_{C_2} = \frac{1}{2}(f(x, y) + f(-x, -y))$. Let $f(\mathbf{x}) = xy$. Then $R_{C_2}(f)(\mathbf{x}) = \frac{1}{2}(xy + xy) = xy$. This tells us that xy is in $k[x, y]^{C_2}$, which we saw earlier. Now let $g = x + y^2$. The Reynolds operator is $R_{C_2} = \frac{1}{2}(x + y^2 - x + y^2) = y^2$. Notice that y^2 is an invariant that we observed before. The polynomial g was not an invariant, but we created one from g using the Reynolds operator.

If we find the Reynolds operator for a monomial x^α , then the result will be either zero or a homogeneous invariant with total degree $|\alpha|$.

Theorem 5.2. In order to find the ring of invariants of a group G , it is sufficient to calculate the Reynolds operator for every monomial x^β such that $|\beta| \leq |G|$. These calculations will result in finitely many homogeneous invariants that generate the ring of invariants.

This theorem was proved by Emmy Noether, and is given on page 332 of Cox, Little, and O'Shea. We will demonstrate the use of the theorem with an example.

Example 5.3. Let $G = V_4 = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\} \in GL(2)$. We saw in an earlier example that $k[x, y]^{V_4} = k[x^2, y^2]$. To use the above theorem, we will need $R_G(f)(x, y) = \frac{1}{4}(f(x, y) + f(-x, y) + f(x, -y) + f(-x, -y))$. We will calculate this for every monomial with total degree less than or equal to four. The results are given in the table at the top of the next page.

Then according to Noether's result, $k[x, y]^{V_4} = k[x^2, y^2, x^4, y^4, x^2y^2]$. We do not need x^4, y^4 , or x^2y^2 . These three monomials can be generated by x^2 and y^2 .

In the above example, it was quite clear that we only needed x^2 and y^2 to generate the ring of invariants. In some cases it may not be so clear that some generators are redundant. We need some way to be able to check if a polynomial is in the ring of invariants. We can use this to check generators. For example, one could start with a single invariant, f_1 and check to see if f_2 is already in $k[f_1]$. We can do this with each subsequent invariant, and the end result will be a set of independent generators for the ring of invariants.

$x^i y^j$	$R_{V_4}(x^i y^j)$
x	0
y	0
x^2	x^2
y^2	y^2
xy	0
x^3	0
y^3	0
$x^2 y$	0
xy^2	0
x^4	x^4
y^4	y^4
$x^3 y$	0
xy^3	0
$x^2 y^2$	$x^2 y^2$

TABLE 1. Reynolds Operator for V_4

In order to check if a polynomial is in the ring $k[f_1, \dots, f_m]$, we will need to introduce some new variables.

Proposition 5.4. *Assume that $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ are given polynomials. Then we introduce the variables y_1, \dots, y_m . Calculate a Groebner basis for $\langle f_1 - y_1, \dots, f_m - y_m \rangle$ with a monomial ordering such that any monomial in x_1, \dots, x_n is greater than all monomials in $k[y_1, \dots, y_m]$. Let g be the remainder of f under division by the Groebner basis. If g depends only on the variables y_1, \dots, y_m , then f is in the ring $k[f_1, \dots, f_m]$. Furthermore, f can be written as $g(f_1, \dots, f_m)$.*

This proposition is proved on p. 334 in the text.

Example 5.5. *Recall that when we looked at the Klein four group, we found the generators $x^2, y^2, x^2 y^2, x^4$ and y^4 . It is clear that the last three generators are redundant. Let's verify the redundancy by using the above result. Let our ring be $k[x^2, y^2]$ and check to see that $x^2 y^2, x^4, y^4 \in k[x^2, y^2]$. To do this we use a Groebner basis for $\langle x^2 - u, y^2 - v \rangle$ with lexicographic ordering on $x > y > u > v$. Then find the remainders of $x^2 y^2, x^4, y^4$ under division by the Groebner basis. We will use Maple for these calculations. See the code below:*

```

> with(Groebner):
> f1:=x^2:
> f2:=y^2:
> f3:=x^4:
> f4:=y^4:
> f5:=x^2*y^2:
> WL:=gbasis([f1-u,f2-v],plex(x,y,u,v)):
> p:=plex(x,y,u,v):
> reduce(f3,WL,p);

```

u^2

> `reduce(f4,wL,p);`

$$v^2$$

> `reduce(f5,wL,p);`

$$uv$$

The remainder of x^4 is u^2 . This tells us that $x^2 \in k[x^2, y^2]$ and that $f = (x^2)^2$. This is exactly what we would expect, and the other two generators work similarly. We can conclude then that $k[x, y]^{V_4} = k[x^2, y^2]$. Now let $f = x^4 + 2y^4 - 3x^2y^2$ and $g = x^3 - y$. We will check to see if $f, g \in k[x^2, y^2]$, and write them in terms of x^2, y^2 if possible. The Maple code is as follows:

> `f:=x^4+2*y^4-3*x^2*y^2;`

> `reduce(f,wL,p);`

$$u^2 - 3uv^3 + 2v^2$$

> `g:=x^3-y;`

> `reduce(g,wL,p);`

$$-y + xu$$

These computations tell us that f can be written in terms of $f_1 = x^2$ and $f_2 = y^2$. Therefore $f = f_1^2 - 3f_1f_2 + 2f_2^2 \in k[x, y]^{V_4}$. On the other hand, $g \notin k[x, y]^{V_4}$.

Example 5.6. Let G be the cyclic group of order 3. Then $G = \langle A \rangle$, where $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \in GL(2)$. The Reynolds operator is $R_{C_3}(f)(x, y) = \frac{1}{3}(f(x, y) + f(-y, x - y) + f(y - x, -x))$. We can write a process in Maple that will allow us to calculate the Reynolds operator for any given polynomial. The code is given below.

> `Ren:=proc(m)`

> `simplify(1/3*(m(x,y)+m(-y,x-y)+m(y-x,-x)));end;`

When we want to use this process, we define our polynomial m as a function. Then call `Ren(m)`, and Maple will calculate the Reynolds operator for the given polynomial. We use Maple to calculate the Reynolds operator for all monomials of total degree less than or equal to three and summarize the results in the table below.

$x^i y^j$	$R_{C_3}(x^i y^j)$
x	0
y	0
x^2	$\frac{2}{3}(x^2 + y^2 - xy)$
y^2	$\frac{2}{3}(x^2 + y^2 - xy)$
xy	$\frac{1}{3}(x^2 + y^2 - xy)$
x^3	$x^2y - xy^2$
y^3	$xy^2 - x^2y$
x^2y	$x^2y - \frac{1}{3}x^3 - \frac{1}{3}y^3$
xy^2	$xy^2 - \frac{1}{3}x^3 - \frac{1}{3}y^3$

TABLE 2. Reynolds Operator for C_3

Clearly the first three nonzero entries are multiples of one another. So we only need one of them, and we can drop the coefficient. We need to check to see if we need all the others. We will check this using Maple.

```

> with(Groebner):
> f1:=y^2-y*x+x^2:
> f2:=-y^2*x+y*x^2:
> f3:=y^2*x-y*x^2:
> f4:=y^2*x-1/3*y^3-1/3*x^3:
> f5:=y*x^2-1/3*y^3-1/3*x^3:
> p:=plex(x,y,u,v,w,z):
> WL1:=gbasis([f5-u],p):
> reduce(f4,WL1,p);
          y^2 x - y x^2 + u
> WL2:=gbasis([f5-u,f4-v],p):
> reduce(f3,WL2,p);
          -u + v
> reduce(f2,WL2,p);
          u - v
> reduce(f1,WL2,p);
          y^2 - y x + x^2

```

When $f_2 = x^2y - xy^2$ and $f_3 = xy^2 - x^2y$ are reduced using a Groebner basis for $\langle f_5 - u, f_4 - v \rangle$, we see that $f_2 = f_5 - f_4$ and $f_3 = f_4 - f_5$. Therefore, we do not need f_2, f_3 in our list of generators. On the other hand, we do need $f_1 = x^2 + y^2 - xy$.

Then if we renumber, the generators for $k[x, y]^{C_3}$ are $f_1 = x^2 + y^2 - xy$, $f_2 = x^2y - \frac{1}{3}x^3 - \frac{1}{3}y^3$, and $f_3 = xy^2 - \frac{1}{3}x^3 - \frac{1}{3}y^3$. Any polynomial in $k[x, y]^{C_3}$ can be written in terms of f_1, f_2, f_3 .

6. CONCLUSION

We have demonstrated an algorithm that will always find a finite number of generators for the ring of invariants of a finite matrix group. This method has the disadvantage that it may require many calculations. For the Klein four group, we had to calculate the Reynolds operator for 14 monomials, and this group only has order four. We have not discussed the issue of whether or not we can write an invariant polynomial uniquely in terms of the generators. Looking at other methods for finding the ring of invariants, and addressing the question of uniqueness are topics for further research.

REFERENCES

- [1] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. New York, New York: Springer-Verlag New York Inc., 1997.