MODULAR INVARIANT THEORY SUMMER SCHOOL ON ALGEBRAIC TOPOLOGY AND INVARIANT THEORY, IOANNINA, GREECE

H E A CAMPBELL

ABSTRACT. This modest work provides some insight into the subject of modular invariant theory.

CONTENTS

Date: June 30, 2000.

1991 *Mathematics Subject Classification.* 13A20.

Key words and phrases. finite groups, positive characteristic, invariant theory.

1. Introduction.

I have gathered here some of the results and problems of invariant theory that I find found particularly interesting and exciting together with some of the necessary background material. Of course, the summer school is intended for graduate students, so these lectures are aimed at them. These are the lectures that I would use to introduce a new student to the subject. My goal has been to illustrate that there are many interesting and fascinating problems that can be tackled with only a modest knowledge of the techniques of modern algebra. The books of Benson [**B**] and Smith [**Sm(a)**] are appropriate references.

In addition to my own interests, I have tried to track to some degree the lectures of the other speakers, and this led to several revisions of the original material while at the school.

The second and third sections of this note are intended to give students an idea of the elements of invariant theory: homogeneous systems of parameters, resolutions by syzygies, Poincaré series, and several examples: the symmetric and alternating groups in their usual representation, permutation groups, the general linear and upper triangular groups, as well as a few selected examples. An example of the MAGMA code needed to do a specific calculation is given here. The first lecture covered much of the second and third sections of this note.

The fourth section concentrates on the two fundamental questions, namely, given a group or a class of groups, what can be said about the structure of its ring of invariants: when is the invariant ring polynomial, a hypersurface, a complete intersection algebra, Gorenstein, or Cohen-Macaulay? Alternately, we'd like to be able to describe generators for such rings of invariants, and the relations among those generators.

Section five is a discussion of the case of the cyclic group of order p and its representations in characteristic p.

Section six consists of two distinct open problems in invariant theory. I included the second of these because it involves the Steenrod algebra and so related well to Smith's lectures.

I include here two lists of references, one from the literature at large, and a list of invariant theory papers I've been involved in over the past few years.

Acknowledgements. I would like to extend my warmest thanks to the participants in the summer school on connections between algebraic topology and invariant theory. Their enthusiasm and energy for the school made the week a fantastic and wonderful experience. I'd also like to congratulate Dr Epiminondas Kechagias, the University of Ioannina, and the City of Ioannina, whose hospitality and warmth made the conference a joy to attend, and a joy at which to speak. Thank you, Nondas.

2. Lecture On Elements of Invariant Theory

Suppose R is any non-negatively graded, finitely generated, connected commutative algebra over a field $\mathbb{F}$, so that $R = \oplus_{d \geq 0} R_d$. Here, of course, R_d denotes the elements of R of degree d, and we are assuming that $R_0 = \mathbb{F}$. Please refer to [**B**] and [**Sm(a)**] as needed.

The Krull dimension is the maximal number of algebraically independent elements in R, denoted here by n.

In our situation, we start with a (fixed representation of a) finite group $G \subset Gl(V)$ for V a vector space of dimension n over a field $\mathbb{F}$ of characteristic $p \geq 0$. We let $\mathbb{F}[V]^G = \{f \in \mathbb{F}[V] \mid \sigma(f) = f, \forall \sigma \in G\}$, denote the ring of invariants, $R = \mathbb{F}[V]^G \subset \mathbb{F}[V]$. We denote the order of G by $|G|$: in this note, we only consider finite groups. The Krull dimension of $\mathbb{F}[V]$ is n.

We denote a monomial $x_1^{i_1} \cdots x_n^{i_n}$ by x^I for the sequence $I = (i_1, \ldots, i_n)$ and we denote its degree by $|I| = i_1 + \cdots + i_n$. We note that the action of G on $\mathbb{F}[V]$ preserves degree, and therefore, in this series of lectures we always consider homogeneous polynomials, that is, $f = \sum_{|I|=d} a_I x^I$, where $a_I \in \mathbb{F}$.

Homogeneous Systems of Parameters. A homogeneous system of parameters for R is a set $\{f_1, \ldots, f_n\}$ with the property that R is finitely generated as an module over $H = \mathbb{F}[f_1, \ldots, f_n]$. Equivalently, $R/(H_+)$ is a (graded) finite dimensional algebra. Here, of course, (H_+) denotes the ideal of R generated by the positive degree elements of H.

The Noether normalization lemma (see [**S(a)**, pg 112]) guarantees that such a homogeneous system of parameters always exists.

If $\bar{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$, then $\{f_1, \ldots, f_n\}$ is a homogeneous system of parameters if and only if the only common zero of this set over $\bar{\mathbb{F}}$ is $\{0\}$, see [**S(a)**, pg 114]. This is not, in general, all that easy to check. There are, however, some handy homogeneous systems of parameters available. If $\mathbb{F}$ is finite then we may always use the Dickson invariants as a homogeneous system of parameters, see section three. If our group is a permutation group, then the elementary symmetric functions form a homogeneous system of parameters, see section three. If our group is p-group represented over a finite field, then Múi has constructed a homogeneous system of parameters, see section three.

If our group is non-modular, that is, if $|G|^{-1} \in \mathbb{F}$, then there are regular sequences of maximal length n, and any such will form a homogeneous system of parameters. Recall that a sequence $\{f_1, \ldots, f_n\}$ is regular if f_i is not a zero divisor in the quotient $R/(f_1, \ldots, f_{i-1})$, for each i, $1 \leq i \leq n$. This may be difficult to check.

I note as well that we may form the Jacobian

$$\mathcal{J} = \mathcal{J}(f_1, \ldots, f_n) = \det([\frac{\partial f_i}{\partial x_j}]).$$

If $\mathcal{J} \neq 0$ then $\{f_1, \ldots, f_n\}$ is algebraically independent. However, this is a weaker condition: if $\mathbb{F}(V)$ denotes the field of fractions of the domain $\mathbb{F}[V]$, and $\mathcal{J}(f_1, \ldots, f_n) \neq 0$, then $\mathbb{F}(V)$ is finitely generated over $\mathbb{F}(f_1, \ldots, f_n)$ but $\mathbb{F}[V]$ need not be finitely generated over $\mathbb{F}[f_1, \ldots, f_n]$. For example, the set $\{x, xy\}$ in $R = \mathbb{F}[x, y]$ has non-zero Jacobian, but R is not finite as a module over $\mathbb{F}[x, xy]$. However, it is easy to check whether or not the Jacobian is non-zero, and so its computation may be used to rule out certain sequences. See Benson, [**B**, pg 64] for more details.

Finally, we note that there is a construction due to Dade which provides a homogeneous system of parameters all of degrees less than $|G|$ provided the field is infinite. If the field is finite, we may extend the coefficients to $\bar{\mathbb{F}}$, use Dade's argument and then restrict to a finite extension of the original field. The construction can be found in Stanley's paper [**S**].

The Poincaré series. We define the Poincaré series of R as

$$P(R, t) = \sum_{i \geq 0} \dim_{\mathbb{F}}(R_i) t^i.$$

This series is sometimes called the Hilbert series of R as well.

Suppose $R = \mathbb{F}[h_1, \ldots, h_n]$ is a polynomial algebra on generators of degrees d_i. Then

$$P(R,t) = \prod_{i=1}^{n} \frac{1}{(1-t^{d_i})}.$$

This is apparent when we consider that

$$\frac{1}{1-t^d} = 1 + t^d + t^{2d} + \cdots + t^{md} + \cdots.$$

Suppose R is a free module over $H = \mathbb{F}[h_1, \ldots, h_n]$ on generators f_i, of degrees m_i, $i = 1, \ldots, r$. Then

$$P(R,t) = \frac{t^{m_1} + \cdots + t^{m_r}}{\prod_{i=1}^{n}(1-t^{d_i})}.$$

Structures. If R is free over one homogeneous system of parameters, then it is free over all such, and we say that R is *Cohen-Macaulay.*

Because we can average polynomials over the group, it can be shown that all non-modular groups have Cohen-Macaulay rings of invariants. In more detail, we can form the *trace* or *transfer* map

$$\mathrm{Tr} : \mathbb{F}[V] \to \mathbb{F}[V]^G$$

by the rule $\mathrm{Tr}(f) = \sum_{\sigma \in G} \sigma(f)$. The transfer is a map of $\mathbb{F}[V]^G$-modules, and if G is a non-modular group, then the transfer is onto. This is false for modular groups, but there is still a lot of information imbedded in the image of the transfer, and the map is the subject of a fair amount of current research.

It seems to be rare that modular groups have Cohen-Macaulay rings of invariants, you'll read more about this later on.

You know what is meant if R is a polynomial algebra. If R is generated by $n+1$ elements then we say R is a *hypersurface.* If R/H_+ is a Poincaré duality algebra, then R is said to be *Gorenstein.* If R is a quotient of a polynomial algebra by the ideal generated by a regular sequence, then we say R is a *complete intersection algebra.*

All of these definitions deserve much fuller exploration, but we won't have space for much.

Resolutions by means of syzygies. We let $Q(R)$ denote the vector space of indecomposables R/R_+^2. Any lift of any basis for R determines a minimal generating set for R as an algebra.

Let $\{f_1, \ldots, f_s\}$ denote a minimal algebra generating set for R. Let $A = \mathbb{F}[z_1, \ldots, z_s]$ denote the polynomial algebra on generators z_i of degree $|f_i|$ and ρ the obvious map from A to R. The map ρ provides R with the structure of an A-module. A resolution of R as an A-module is called a resolution of R by means of syzygies. The resolution has length at most s. If R is Cohen-Macaulay then the resolution has length exactly $s-n$.

$$0 \to M_s \to \cdots \to M_1 \to A \to R \to 0.$$

We note that

$$P(R,t) = \sum_{i=0}^{s-n} (-1)^i P(M_i, t).$$

Since A is a polynomial algebra, we have that $P(A) = \prod_{i=1}^{s} \frac{1}{(1-t^{|f_i|})}$. And, as a free A-module, $M_i = \oplus_{j=1}^{k} A\phi_j$ for some $\{\phi_j \in M_i\}$ of degrees m_j. Therefore, $P(M_i,t) = t^{m_1} + \cdots + t^{m_r} / \prod_{i=1}^{s}(1-t^{|f_i|})$.

Molien's Theorem. Suppose $|G|^{-1} \in \mathbb{F}$, that is, G is a non-modular group. Elements of representation theory give us a complex representation of G which shares the same Poincaré series as $\mathbb{F}[V]^G$, see [**Si**, pg 504]. Over the complex numbers, the elements of character theory give us the following.

Theorem. **(Molien)**

$$P(\mathbb{F}[V]^G, t) = \frac{1}{|G|}(\sum_{g\in G} \frac{1}{\det(1-tg)})$$

As an example, we note that any permutation g of n variables is a product of cycles $g_{i_1} \cdots g_{i_k}$. Here I mean that g_{i_j} is a cycle of length i_j. It can be shown that $\det(1-tg) = \prod_{j=1}^{k}(1-t^{i_j})$.

As a further example, if g has eigenvalues $\lambda_1, \ldots, \lambda_n$ then

$$det(1-tg) = \prod_{i=1}^{n}(1-\lambda_i t).$$

Construction of invariants. Given $G \subset Gl(V)$ and an element $f \in \mathbb{F}[V]$ we define the *G-orbit* of f, to be $\{g(f) \mid g \in G\}$ denoted $\mathcal{O}_G(f)$. A slightly different way to define the orbit of f is to define $Stab_G(f) = \{g \in G \mid g(f) = f\}$. Then $\mathcal{O}_G(f) = \{g(f) \mid g \in G/Stab_G(f)\}$. Here $G/Stab_G(f)$ denotes a set of coset representatives.

Suppose, then, that $|\mathcal{O}_G(f)| = m$. From here, we can form the polynomial

$$\mathcal{P}_f(t) = \prod_{h\in\mathcal{O}_G(f)} (t-h) = \sum_{i=0}^{m} (-1)^i s_i t^{m-i},$$

where $s_i \in \mathbb{F}[V]^G$. The coefficients are elementary symmetric functions in the elements of $\mathcal{O}_G(f)$. That is, if we write $\mathcal{O}_G(F) = \{f_1, \ldots, f_m\}$, then

$$\begin{aligned} s_1 &= f_1 + \cdots f_m,\ s_2 = f_1 f_2 + \cdots f_{m-1} f_m, \ldots, \\ s_m &= f_1 \cdots f_m. \end{aligned}$$

Smith [**S(a)**] refers to the invariants so constructed as orbit Chern classes.

3. Examples.

Suppose $G = C_2$ acts on $V^* = \langle x, y \rangle$ by

$$\{I_2 = [\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}],\ g = [\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}]\}.$$

We observe that we have $g(x^i y^j) = x^j y^i$. In particular, $(xy)^i$ is invariant. If $i \neq j$ then $x^i y^j + x^j y^i$ is invariant. This suggests that if $i = j + k$ then we write

$$\begin{aligned} x^i y^j + x^j y^i &= (xy)^j (x^k + y^k) \\ &= (xy)^j (x+y)^k + \text{ other terms.} \end{aligned}$$

It isn't difficult to show from here that

$$\mathbb{F}[V]^G = \mathbb{F}[x+y, xy].$$

This is the best possible situation in invariant theory, in which the ring of invariant polynomials is again polynomial algebra. We see from this calculation, or from Molien's theorem, that

$$P(\mathbb{F}[V]^G, t) = \frac{1}{(1-t)(1-t^2)}.$$

Hand Calculations. Suppose G acts on $V^* = \langle x, y \rangle$ by the matrices $\{[\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}],\ g = [\begin{matrix} -1 & 0 \\ 0 & -1 \end{matrix}]\}$. We note that $g(x^i) = (-1)^i x^i$ so that x^i is invariant if and only if $i = 2j$. Similarly, y^i is invariant if and only if $i = 2j$. We have $x^{2j} = (x^2)^j$. Moreover, we observe that $g(x^i y^i) = x^i y^i$ is invariant.

It isn't hard to prove from here that $\mathbb{F}[V]^G = \mathbb{F}[x^2, y^2, xy]$. There are a variety of ways we can parse this, One view is that

$$\mathbb{F}[V]^G \cong \mathbb{F}[a, b, c]/(c^2 - ab)$$

where $|a| = |b| = |c| = 2$. In another, we observe that $\{x^2, y^2\}$ forms homogeneous system of parameters for $\mathbb{F}[V]^G$, and that $\mathbb{F}[V]^G$ is a free module over $H = \mathbb{F}[x^2, y^2]$ on the basis $\{1, xy\}$.

Q What is the Poincaré series of this ring of invariants?

Example: Calculations in Magma. Magma is a computer program that is, at the moment, the language of choice of the Invariant Theory Group at Queen's. It incorporates algorithms due to Gregor Kemper and others. Here is an excerpt from a Magma session that computes the example of Bertin. The example itself is important in the history of commutative algebra as the first example of a unique factorization domain which was not Cohen-Macaulay, answering a question of Kaplansky.

In what you read below, you will find the user input next to the

```
>
```

prompt, and the replies from Magma without such a prompt. Most of the Magma commands are self-explanatory. However, the reader should know that the command *PrimaryInvariants* computes a homogeneous system of parameters, while *SecondaryInvariants* computes a set of module generators for the ring of invariants over the polynomial algebra generated by the homogeneous system. The command *TotalDegree* reports on the degrees of the polynomials in the set given as its argument, while *FundamentalInvariants* computes a minimal generating set for the ring of invariants as an algebra.

```
[eddy@noether]$magmaV2.5

Magma V2.5-1      Mon Nov  1 1999 08:09:07

[Seed = 1416756397] Type ? for help.
Type <Ctrl>-D to quit.
> G := MatrixGroup<4,GF(2) |
[0,1,0,0, 0,0,1,0, 0,0,0,1, 1,0,0,0] >;
> #G;
4
> R := InvariantRing(G);
> time prim := PrimaryInvariants(R);
Time: 0.019
> [TotalDegree(f): f in prim];
[ 1, 2, 2, 4 ]
> S<x,y,z,w> := PolynomialRing(R);
> prim;
[
    x + y + z + w,
    x*y + x*w + y*z + z*w,
    x*z + y*w,
    x*y*z*w
]
> time sec := SecondaryInvariants(R);
Time: 0.029
> [TotalDegree(f): f in sec];
[ 0, 3, 3, 4, 5 ]
> IsCohenMacaulay(R);
false
> time fun := FundamentalInvariants(R);
Time: 0.000
> [TotalDegree(f): f in fun];

[ 1, 2, 2, 3, 3, 4, 4, 5 ]
```

Symmetric Functions. Consider $G = \Sigma_n \subset Gl(V)$ acting as all permutations of a basis $\{x_1, \dots, x_n\}$ for V^*. We note that $\mathcal{O}_G(x_1) = \{x_1, \dots, x_n\}$ and that $\mathcal{P}_{x_1}(t) = \prod_{i=1}^{n}(t - x_i) = \sum_{j=0}^{n}(-1)^j s_j t^{n-j}$. Here, the s_j is the j-th elementary symmetric function

$$s_j = x_1 x_2 \cdots x_j + \cdots + x_{n-j+1} x_{n-j+2} \cdots x_n.$$

Of course, the elementary symmetric functions enjoy many beautiful properties, and symmetric functions occur in many different situations in mathematics.

Exercise Prove that $\{s_1, \dots s_n\}$ are algebraically independent, and hence that $\mathbb{F}(s_1, \dots, s_n)$ has transcendence degree n.

Now we note that $\mathbb{F}(V)^G \subset \mathbb{F}(V)$ is a Galois extension, with Galois group G, hence of transcendence degree $|G| = n!$. Further,

$$\mathbb{F}(s_1, \dots, s_n) \subset \mathbb{F}(V)$$

has transcendence degree $\prod_{i=1}^{n} |s_i|$. Therefore, $\mathbb{F}(s_1, \dots, s_n) = \mathbb{F}(V)^G$. However, a polynomial algebra is integrally closed and hence

$$\mathbb{F}[s_1, \dots, s_n] = \mathbb{F}[V]^G.$$

The paragraph just above provides a general template for proving that rings of invariant are polynomial algebras, if, in fact, they are.

Of course, this is far from the end of the story. For example, given a symmetric function, how can it be written in terms of the elementary symmetric functions? As well, there are other generating sets for the symmetric functions, for example, the power sums

$$h_i = x_1^i + \dots x_n^i,$$

for $1 \leq i \leq n$. The sum of all monomials of a given degree d is called the complete symmetric function of degree d. There is great fun to be had in trying to understand how to rewrite symmetric functions expressed in one way or another in a different way.

The Alternating groups. We study A_n the sub-group of Σ_n consisting of all even permutations. We know that an alternating function is the sum of a symmetric function together with a symmetric function times the discriminant. Here the discriminant may be described as

$$\Delta_n = \prod_{1 \leq i < j \leq n} (x_j - x_i),$$

if $p = 0$ or if $p > 2$. Otherwise take the orbit sum of $x_1^{n-1} x_2^{n-2} \cdots x_{n-1}$.

In modern language, we have

$$\mathbb{F}[V]^{A_n} = \mathbb{F}[V]^{\Sigma_n} \oplus \mathbb{F}[V]^{\Sigma_n} \Delta.$$

Hence, $\mathbb{F}[V]^{A_n}$ is generated by $n+1$ elements as an algebra, and so $\mathbb{F}[V]^{A_n}$ is a hypersurface. It is easy to see that Δ^2 is invariant under Σ_n when $p = 0$ or $p > 2$.

All of this is nicely described in [**S(a)**, pg 10].

For now we note that we have two Galois extensions

$$\mathbb{F}(v)^{\Sigma_n} \subset \mathbb{F}(V)^{A_n} \subset \mathbb{F}(V).$$

The one on the right has Galois group A_n, hence has transcendence degree $|A_n|$. The Galois group from one end to the other is $|\Sigma_n| = n!$. Further, the index $[\Sigma_n : A_n] = 2$, and we have $\mathbb{F}(V)^{\Sigma_n}[\Delta^{\pm 1}]$ has degree two as an extension of the field of fractions of the ring $\mathbb{F}[V]^{\Sigma_n}$. Therefore $\mathbb{F}(V)^{\Sigma_n}[\Delta^{\pm 1}] = \mathbb{F}(V)^{A_n}$.

Exercise. Prove $\mathbb{F}(V)^{\Sigma_n}[\Delta^{\pm 1}] = \mathbb{F}(V)^{A_n}$ implies $\mathbb{F}[V]^{A_n} = \mathbb{F}[V]^{\Sigma_n} \oplus \mathbb{F}[V]^{\Sigma_n} \Delta$.

This kind of argument will work more generally for Cohen-Macaulay rings.

Invariants of Permutation Groups. Suppose $G \subset \Sigma_n \subset Gl(V)$. That is, G is a permutation group. A key observation is that every element of G takes monomials to monomials. Therefore, given a monomial x^I, we form the orbit sum $s(I) = \sum_{g \in G/Stab_G(x^I)} g(x^I)$.

Lemma. *The orbit sums $s(I)$ of degree d form a basis for $\mathbb{F}[V]_d^G$.*

Proof. Any $f \in \mathbb{F}[V]$ may be written as sum of monomials $f = \sum_{|I|=d} a_i x^I$. But for any $g \in G$ we have $g(f) = \sum a_I g(x^J)$. It follows that, if f is G-invariant and $x^J \in \mathcal{O}_G(x^I)$, then $a_J = a_I$. The result is immediate. ♠

Corollary. *The Poincaré series of $\mathbb{F}[V]^G$ depends only on $G \subset \Sigma_n$ and not on the field $\mathbb{F}$.*

Theorem. *(Göbel) If G is a permutation group then $\mathbb{F}[V]^G$ is generated in degrees less than or equal to $\binom{n}{2}$.*

Key idea. We say that a sequence I has no 2-gaps if the entries of I, *viewed as a set*, are consecutive, and include 0. We can show that any invariant of the form $s(I)$ where the entries of I are not consecutive, or are all positive, can be decomposed — shown to be a sum of product of elements of smaller degree — by subtracting 1's from every entry above the largest gap. Here are some of the details.

Proof. We are going to induct on the following order. Given an exponent sequence, I, of degree d, we think of I as a partition of d and write $\lambda(I) = (\lambda_0(I), \lambda_1(I), \ldots, \lambda_d(I))$ where λ_i is the number of entries of I equal to i. We compare exponent sequences I and J of the same degree by the lexicographic order on $\lambda(I)$ and $\lambda(J)$ from right to left, that is, by comparing the number of largest entries, and if they are equal, the number of next largest entries, and so on. Note that any two sequences of the same size in this order are permutations of each other.

In this notation, a sequence I has no 2-gaps if $\lambda_0(I) \neq 0$ and if $\lambda_{\ell+1}(I) \neq 0$ implies $\lambda_\ell(I) \neq 0$.

A stronger version of the theorem is that the sequences $s(I)$ with no 2-gaps, together with $s(1, \ldots, 1)$, generates $\mathbb{F}[V]^G$. The version given here follows when we note that a sequence of largest degree with no 2-gaps is

$$(n-1, n-2, \ldots, 2, 1, 0).$$

Let $A \subset \mathbb{F}[V]^G$ denote the subalgebra generated by all elements $s(I)$ with no 2-gaps, together with $s(1, \ldots, 1)$. We wish to show that, if I is a sequence with a 2-gap, then $s(I) \in A$. The argument given below can be used to start the induction, but the details are omitted.

Let r denote the largest 2-gap in I, that is, there is no entry of I equal to r, but there is at least one entry of I equal to $r+1$, and r is the largest integer with this property. That is, we assume that r is the largest integer with $\lambda_r(I) = 0$ and $\lambda_{r+1} \neq 0$.

Let K denote the sequence which has a 1 wherever I has an entry bigger than r and 0's elsewhere. Let $J = I - K$. We observe that $Stab_G(J) \subset Stab_G(K)$, although, to my amazement, we don't need this observation.

Consider the product $s(J)s(K)$. We observe that the exponent sequences which arise in this product are of the form $\sigma(J) + \tau(K)$. We show that $s(I)$ occurs with coefficient 1 in the product and, simultaneously, that $\sigma(J) + \tau(K)$ is smaller than I in our order, provided

$\sigma(J) + \tau(K) \notin \mathcal{O}_G(I)$. Suppose then, that $I = \sigma(J) + \tau(K)$, for some σ, and $\tau \in G \subset \Sigma_n$.

Now I has largest entries k in certain places, and therefore $\sigma(J)$ must have entries $k-1$ in those same places, and $\tau(K)$ must have 1's in those same places, or $\sigma(J) + \tau(K)$ will be smaller than I in our order. The same argument also applies in turn to those places where I has entries $k-1, \ldots, r+1$. But our argument shows that $\sigma(J) = J$ and $\tau(K) = K$, but this cannot happen for non-trivial σ and τ. ♠

The Dickson Invariants. Suppose $\mathbb{F}$ is a finite field of order $q = p^s$. Then consider $G = \mathrm{Gl}(V)$. Then any vector $v \in V^* \setminus \{0\}$ has $\mathcal{O}_G(v) = V^* \setminus \{0\}$. Now we obtain

$$\mathcal{P}_v(t) = \prod_{w \in \mathcal{O}_G(v)} (t - w) = \sum_{i=0}^{n} (-1)^{n-i} d_{i,n} t^{q^{n-i}}.$$

The $d_{i,n}$ are known as the Dickson invariants, and they enjoy many beautiful properties.

For example, when $p = 2$ and $n = 2$ we have

$$\mathcal{P}_v(t) = t(t+x)(t+y)(t+x+y)$$

so that $d_{1,2} = x^2 + xy + y^2$ and $d_{2,2} = xy(x+y) = x^2y + xy^2$.
Exercise Develop recursive formulae for the Dickson invariants. That is write $d_{i,n}$ in terms of $d_{i,n-1}$ and x_n.

For now we note that $|d_{i,n}| = q^n - q^{n-i}$. Therefore, we have $\prod_{i=1}^{n} |d_{i,n}| = |\mathrm{Gl}(V)|$.

This latter calculation is very pretty. There are q^n vectors in V, and any one of them may be identified with the first row of a matrix in $\mathrm{Gl}(V)$ excepting the zero vector. Hence there are $q^n - 1$ choices for the first row. Similarly, the second row corresponds to vectors in V that are linearly independent of the first, and there are $q^n - q$ choices for these. And so on.
Exercise Prove that $\{d_{1,n}, \ldots, d_{n,n}\}$ are algebraically independent. Carry on with an argument similar to the one given for the symmetric groups to show that $\mathbb{F}[d_{1,n}, \ldots, d_{n,n}] = \mathbb{F}[V]^G$.

Upper Triangular Invariants. Suppose $\mathbb{F}_q$ is a finite field of order $q = p^s$. Consider $G = U_n(\mathbb{F}_q)$, the group of upper triangular matrices with 1's along the diagonal acting on V^* with respect to the basis $\{x_1, \ldots, x_n\}$. Note that $\mathcal{O}_G(x_i) = x_i + V_{i-1}$ where V_{i-1} denotes the subspace of V^* with basis $\{x_1, \ldots, x_{i-1}\}$. Therefore, we define

$$h_i = \prod_{v \in V_{i-1}} (x_i + v).$$

Note that the degree of h_i is q^{i-1}. Therefore, $\prod_{i=1}^{n} |h_i| = |U_n(\mathbb{F})|$.

When $p = 2$, we get $h_1 = x$, $h_2 = y(y+x) = y^2 + xy$. For arbitrary p, we have $h_2 = \prod_{\alpha \in \mathbb{F}_p}(y + \alpha x) = y^p - x^{p-1}y$.

Exercise Carry on with an argument similar to the one just given to show that $\mathbb{F}_q[h_1, \dots, h_n] = \mathbb{F}_q[V]^G$.

Exercise Prove that $U_n(\mathbb{F}_q)$ is a q-Sylow subgroup of $\mathrm{Gl}_n(\mathbb{F}_q)$.

A 2-dimensional representation of C_3, $p = 2$, [B, pg 103.] Suppose G acts on $V^* = \langle x, y \rangle$ by

$$\{I_2,\ g = [\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}]\},$$

over the field $\mathbb{F}_2$. Note that $|G| = 3$, and, in our conventions, σ acting on $\mathbb{F}_2[V] = \mathbb{F}_2[x, y]$ sends x to y and sends y to $x + y$.

It is straightforward to calculate the ring of invariants for G. First we observe that the Dickson invariants $r = x^2 + xy + y^2, s = x^2y + xy^2$ form, as always, a homogeneous system for $\mathbb{F}_2[V]^G$. Second we observe that G has index 2 in $\mathrm{Gl}_2(\mathbb{F}_2)$, and that $t = x^3 + x^2y + y^3$ is invariant. It isn't hard to see using Galois theory that

$$\mathbb{F}_2[x, y]^G = \mathbb{F}_2[x^2 + xy + y^2, x^2y + xy^2, x^3 + x^2y + y^3],$$

and, therefore, this ring is a hypersurface. As part of this calculation, we note $t^2 = r^3 + s^2 + rs$.

Therefore, we obtain a resolution over the ring $A = \mathbb{F}_2[a, b, c]$ with $|a| = 2$, $|b| = |c| = 3$, and $\rho(a) = x^2 + xy + y^2$, $\rho(b) = x^2y + xy^2$, $\rho(c) = x^3 + x^2y + y^3$. We obtain

$$0 \to A(c^2 + a^3 + b^2 + bc) \to A \to \mathbb{F}_2[x, y]^G \to 0.$$

It follows that

$$\mathcal{P}(\mathbb{F}_2[V]^G, t) = \frac{1 + t^2 + t^4}{(1 - t^3)^2}.$$

4. Lecture on Structures and Fundamental Questions.

There are two sorts of problems to be considered

(1) Find generators for $\mathbb{F}[V]^G$. Failing that, find a bound for the degrees of a generating set.
(2) Determine the structure of $\mathbb{F}[V]^G$. For example, determine for which groups G is $\mathbb{F}[V]^G$ a polynomial algebra, a hypersurface, Gorenstein or Cohen-Macaulay?

Both questions are interesting for either specific groups, or for classes of groups. In general, much more is known when $p = 0$ and in the non-modular case than in the modular case. These differences are the focus of this lecture.

Bounds for Generating Sets. Noether showed that generators of degree at most $|G|$ are required when $p = 0$. For non-modular groups with $p > |G|$, this theorem is still true. Richman, Smith and others have shown Noether's original bound, $|G|$, applies if G is solvable. Smith [**S(a)**, pg 175], Fleischmann [**Fl**], and others have shown that for non-modular groups $\mathbb{F}[V]^G$ is generated in degrees at most $\dim_{\mathbb{F}}(V)(|G|-1)$, see also [**FL**]. Here I need $\dim_{\mathbb{F}}(V) > 1$ and $|G| > 1$.

Up until last fall, it was a conjecture that non-modular groups have rings of invariants that are generated in degrees less than or equal $|G|$. The difference between the known bound and this conjectural bound was known as the problem of Noether's Gap: is there a non-modular group in the gap or not? In the fall of 1999, Peter Fleischmann gave a beautiful and clever variation of Noether's original argument that showed the conjecture was true (see below). Independently, Fogarty proved the same result.

It is proved in [**2**] that if $\mathbb{F}_p[V]^G$ is a hypersurface, then this ring is generated in degrees less than $|G|$ while if $\mathbb{F}_p[V]^G$ is Gorenstein, then the bound $\dim_{\mathbb{F}_p}(V)(|G|-1)$ applies. More generally, Broer [**Br**] has shown that this latter bound applies if $\mathbb{F}_p[V]^G$ is Cohen-Macaulay.

Kemper conjectures that Noether's bound, $|G|$, applies whenever $\mathbb{F}[V]^G$ is Cohen-Macaulay.

Dade has shown that there exists a homogeneous system of parameters all of whose generators may be taken to be either from V^G or of degree $|G|$. This may involve a finite extension of the original field. Then $\dim_{\mathbb{F}}(V/V^G)(|G|-1)$ is the degree of a top *module* generator of $\mathbb{F}[V]^G$ over this homogeneous system of parameters. In general, one would expect to find algebra generators in degrees somewhat less than this. However, there are examples where the bound $\dim_{\mathbb{F}}(V/V^G)(|G|-1)$ is sharp (see below).

There is no explicit bound for modular groups known. It is easy to see that there is a bound that depends on $\dim_{\mathbb{F}}(V)$ and q, for $\mathrm{Gl}_n(\mathbb{F}_q)$ is a finite group, hence has finitely many subgroups, hence there are finitely many rings of invariants to be calculated, for any given n and q.

Fleischmann on non-modular groups. Suppose $G = \{g_1, \ldots, g_k\}$ is a non-modular group. Consider the vector space Z with basis

$$\{z_{ij} \mid 1 \leq i \leq n,\ 1 \leq j \leq k\},$$

together with the map $\rho : Z \to V$ defined by $\rho(z_{ij}) = g_j x_i$. We extend to a map

$$\mathbb{F}[Z] \to \mathbb{F}[V].$$

Note that G acts on Z by permuting the columns of the matrix z_{ij} in the obvious way, via the regular representation of G. This is the original construction of Emmy Noether.

We obtain $\rho : \mathbb{F}[Z]^{\Sigma_k} \to \mathbb{F}[V]^G$. For $f \in \mathbb{F}[V]$ we may define $a_j(z_{1j}, \ldots, z_{nj}) = f(z_{1j}, \ldots, z_{nj})$, with $\rho(a_j) = g_j f(x_1, \ldots, x_n)$. Therefore, if $f \in \mathbb{F}[V]^G$ we have $\frac{1}{k}\rho(\sum a_j) = f$. Further, $\sum a_j$ is the orbit sum of a_j over Σ_k.

Fleischmann's proof works as follows.

First, note that a_j is concentrated in a single "row" of the matrix z_{ij}.

He shows that the orbit sums of such row polynomials may be written as sums of products of the form ab where a is in $\mathbb{F}[Z]^{\Sigma_k}$, has positive degree, and is a product of invariants of degree less than or equal to k, and b is in $\mathbb{F}[Z]$.

Therefore, $f \in \mathbb{F}[V]^G$ may be written as a sum of terms of the form ab where $a \in \mathbb{F}[V]^G$ has positive degree, is a product of invariants of degree less than or equal to k, and $b \in \mathbb{F}[V]$.

But $\frac{1}{k}\operatorname{Tr}_G(f) = \frac{1}{k}\sum_{i=0}^{k} g_i(f) = f$, for $f \in \mathbb{F}[V]^G$. Applying the trace to each of the terms ab gives the result.

Vector Invariants. Consider the coordinate ring of $mV = V^{\oplus m}$ with the diagonal action of G. The ring $\mathbb{F}[mV]^G$ is called the ring of vector invariants of G, a terminology used by Weyl. Rings of vector invariants provide an important class of examples and counterexamples.

Hughes and I in [**6**] give generators, as conjectured by Richman [**R**], for $\mathbb{F}_p[mV]^{C_p}$ where C_p denotes the cyclic group of order p, and V denotes its 2-dimensional indecomposable representation. An easy corollary is the fact, first observed by Richman, that this invariant ring requires a generator of degree $m(p-1)$. Therefore, Noether's bound does not hold for p-groups, and the bound $\dim_{\mathbb{F}_p}(V/V^G)(|G|-1)$ is sharp in this example.

If G is a p-group and $m \geq 3$ then $\mathbb{F}_p[mV]^G$ cannot be Cohen-Macaulay, see [**2**]. Kemper has proved that, if G is any modular group, then $\mathbb{F}_p[mV]^G$ is not Cohen-Macaulay for all sufficiently large m. We know of no examples where "sufficiently large" is bigger than 3.

As an example of the kind of argument used here, consider $\mathbb{F}_p[3V_2] = \mathbb{F}_p[x_1, y_1, x_2, y_2, x_3, y_3]$ with an action of $\sigma(x_i) = x_i$ and $(y_i) = y_i + x_i$. We note that $u_{ij} = \left|\begin{smallmatrix} x_i & x_j \\ y_i & y_j \end{smallmatrix}\right| = x_i y_j - x_j y_i$ is invariant. Further, we have that the matrix

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{pmatrix}$$

has zero determinant, since two rows are equal, and, on the other hand, is equal to $x_1 u_{23} - x_2 u_{13} + x_3 u_{12}$. At Queen's, we call this the equation of the three amigos, and with a little work, it can be used to show that the ring in question is not Cohen-Macaulay. Generalizations of it are used in the papers listed above.

If we consider now $\mathbb{F}_p[mV_2] = \mathbb{F}_p[x_i, y_i \mid 1 \leq i \leq m]$ with the action of C_p described above, then we find, after a great deal of hard work (see [**6**]), that $\mathbb{F}_p[mV_2] = \mathbb{F}_p[x_i, N(y_i), u_{ij}, \mathrm{Tr}(m) \mid m|(y_1 \cdots y_m)^{p-1}]$. Of course, this ring is far from Cohen-Macaulay, but at least this collection of invariants appears to be understandable.

Kemper has also proved that, if G is a p-group and $\mathbb{F}_p[V]^G$ is Cohen-Macaulay, then G is generated by elements that fix a subspace of codimension at most 2 (such elements are known as *bi-reflections*). This theorem shows us how rarely we may expect to encounter Cohen-Macaulay rings as the invariants of p-groups.

On the Structure of $\mathbb{F}[V]^G$: classical results. The invariant theory of finite groups is much better understood in the non-modular case.

For example, in this situation, it is a famous and beautiful theorem that $\mathbb{F}[V]^G$ is a polynomial algebra if and only if G is generated by pseudo-reflections (Shephard-Todd, Chevalley, Serre, Clark-Ewing, Steinberg, Kane).

There are other beautiful and wonderful theorems concerning characterizations of hyper-surfaces (Nakajima), Gorenstein (Watanabe), or Cohen-Macaulay (Hochster and Eagon) in the non-modular case.

Structure of $\mathbb{F}[V]^G$: modular case. It is known (Serre) that groups with polynomial rings of invariants must be pseudo-reflection groups, and many groups are known to have polynomial rings of invariants — the symmetric groups, and the parabolic groups.

Nakajima has characterized those p-groups with polynomial rings of invariants when $\mathbb{F} = \mathbb{F}_p$. Roughly speaking, he shows that such groups resemble the ring of invariants of the Upper Triangular group, the last example of section 3. He gave examples of elementary Abelian reflection p-groups with non-Cohen-Macaulay invariant rings, a somewhat simpler example is given below. Nakajima's characterization fails over larger fields, as shown by an example due to Stong, see below.

Roughly speaking, Nakajima's characterization is as follows. Let G be a p-group represented over the finite field $\mathbb{F}_p$ on a vector space, V, of dimension n. Since $U_n(\mathbb{F}_p)$ is a p-Sylow subgroup of $\mathrm{Gl}_n(\mathbb{F}_p)$, we may find a basis for V with respect to which G is a subgroup of $U_n(\mathbb{F}_p)$. The theorem asserts that $\mathbb{F}_p[V]^G$ is a polynomial algebra if and only if there is a (upper triangular) basis $\{x_1, \ldots, x_n\}$ of V with respect to which G "stands up straight", that is, for each generating pseudo-reflection of G, there is a basis element of V, say x_i, such that σ fixes the hyperplane spanned by $x_1, \ldots, \hat{x}_i, \ldots, x_n$, where $\hat{x}_i$ indicates x_i has been deleted. Then we have that $\sigma(x_i) = x_i + v$ where v is a vector in the span of $x_1, \ldots, x_{i-1}$. The implication $\Leftarrow$ is easy, but the other direction is much harder.

Kemper and Malle have examined the class of irreducible representations of modular pseudo-reflection groups and determined which have polynomial rings of invariant. Unfortunately, irreducible representations are few and far between.

Much work remains to be done on characterizing groups with polynomial rings of invariants.

A cautionary tale concerning p-groups. Consider the group

$$G = \{ \begin{pmatrix} 1 & 0 & \alpha+\gamma & \gamma \\ 0 & 1 & \gamma & \beta+\gamma \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid \alpha,\ \beta,\ \gamma \in \mathbb{F}_p\}.$$

Our convention is that G acts on V^* with basis $\{x_1, x_2, y_1, y_2\}$ with x_1 and x_2 as fixed points. Then G has order p^3. Let H be the subgroup of G of order p^2 determined by the elements with $\gamma = 0$. Both G and H, of course, are elementary Abelian groups generated by pseudo-reflections (elements that fix a hyperplane). However, only H is a Nakajima group.

Let $N_i(y_i) = y_i - x_i^{p-1}y_i$ for $1 \leq i \leq 2$. It isn't hard to see that

$$\mathbb{F}_p[V]^H = \mathbb{F}_p[x_1, x_2, N(y_1), N(y_2)].$$

Further, since H is normal in G, we have an action of $G/H = C_p$ on $\mathbb{F}_p[V]^H$.

We let

$$\sigma = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

and we calculate $\sigma(N_1(y_1)) = N_1(y_1) - N_1(x_2)$, and $\sigma(N_2(y_2) = N_2(y_2) - N_2(x_1)$. From here we can construct three new invariants:

$$\begin{aligned} &N_1(y_1)^p - N_1(x_2)^{p-1}N_1(y_1), \\ &N_2(y_2)^p - N_2(x_1)^{p-1}N_2(y_2) \\ &\text{ and} \\ &N_1(x_2)N_2(y_2) - N_2(x_1)N_1(y_1). \end{aligned}$$

It can be shown without a great deal of difficulty that $\mathbb{F}_p[V]^G$ is the hypersurface generated by these three invariants together with x_1 and x_2.

Stong's example. We work over the field $\mathbb{F}_q$ with $q = p^3$. We may suppose the field has basis over $\mathbb{F}_p$ consisting of $\{1, \omega, \mu\}$. Let H be the group generated by the matrices

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and let G be the group generated by H and the matrix

$$\sigma = \begin{pmatrix} 1 & \omega & \mu \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

with respect to the basis $\{x, y, z\}$ of V^*. We note that both groups are generated by psuedo-reflections, but that G is not a "Nakajima" group, since we cannot choose a basis with respect to which each generating pseudo-reflection is concentrated in a single column.

It is not hard to see that $\mathbb{F}_q[V]^H = \mathbb{F}_q[x, N(y), N(z)]$, where $N(t) = t^p - x^{p-1}t$. We calculate $\sigma(N(y)) = N(y) - (\omega^p - \omega)x^p$, and $\sigma(N(z)) = N(z) - (\mu^p - \mu)p$. From here we can construct two G invariants $f_1 = (\mu^p - \mu)N(y) - (\omega^p - \omega)N(z)$ and $f_2 = N(y)^p - (\omega^p - \omega)^{(p-1)}n(y)x^{p(p-1)}$. It isn't hard to see that these form a homogeneous system of parameters, and that $\mathbb{F}_q[V] = \mathbb{F}_q[x, f_1, f_2]$.

5. Lecture on the cyclic group of order p over $\mathbb{F}_p$

There are p indecomposable representations of C_p over $\mathbb{F}_p$, one of dimension n for each n less than or equal p. We have a tower $V_1 \subset V_2 \subset \cdots \subset V_p$, and the matrix of the generator for V_n^* may be taken to be the $n \times n$ matrix

$$\sigma = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

It isn't hard to compute the rings of invariants associated to the three lowest dimensional representations. The first two are polynomial on "top" Chern classes of the basis elements (use the basis assumed above) and the third is a hypersurface. Shank [**Sh**] has given algebra generators for the rings of invariants associated to the four and five dimensional representations. Also, using techniques and results of Almqvist and Fossum, it can be shown that *any* representation V of C_p has its invariant ring generated in degrees less than or equal $\dim_{\mathbb{F}_p}(V)(p-1)$. Kemper and Hughes have a very nice paper about this.

We conjecture that the rings of invariants of all representations of C_p are generated by elements we call norms, traces and rational invariants. This latter class of invariants is obtained from certain classical invariants of binary forms studied by Hilbert and others working in the last century. We must show that the invariants of degree less than p are either traces or rational invariants. While this result seems to be in reach, we haven't yet proved it.

Conjectures about Modular Groups. Do norms, traces and rational invariants form a generating set for the invariant rings of all p-groups? Well, there are cohomology classes as well. I hope to say something about this at the end of the lecture.

I (and many others!) conjecture that modular groups are generated in degrees less than or equal to

$$\dim_{\mathbb{F}_p}(V/V^G)(|G|-1).$$

Of course, this bound is known to hold in all known examples, provided, of course, that $\dim_{\mathbb{F}_p}(V) > 1$ and $|G| > 1$.

Generators for p-Groups? Take N to be a normal subgroup of a p-group G with quotient group $G/N \simeq C_p$. Then $\mathbb{F}_p[V]^G = (\mathbb{F}_p[V]^N)^{C_p}$.

Suppose that we know $\mathbb{F}_p[V]^N = \mathbb{F}_p[f_1, \ldots, f_r]$, perhaps by induction. Let $A = \mathbb{F}_p[z_1, \ldots, z_r]$ mapping onto $\mathbb{F}_p[V]^N$ by the rule $z_i \longrightarrow f_i$, with kernel the ideal I. Suppose that C_p acts on A. This need not happen, and there may be a paper subsequent to this one in which this issue is explored.

Write $\Delta = 1 - \sigma$ and $\mathrm{Tr} = \sum_{i=0}^{p-1} \sigma^i$ where σ a generator of C_p. Because $\mathrm{Tr} = \Delta^{p-1}$, we obtain a resolution of $\mathbb{F}_p$ as the trivial module over the group ring $\mathbb{F}_pC_p$ as follows:

$$\ldots \rightarrow \mathbb{F}_pC_p \xrightarrow{\Delta} \mathbb{F}_pC_p \xrightarrow{\mathrm{Tr}} \mathbb{F}_pC_p \rightarrow \cdots \rightarrow \mathbb{F}_pC_p \xrightarrow{\Delta} \mathbb{F}_pC_p \xrightarrow{\epsilon} \mathbb{F}_p,$$

where $\epsilon : \mathbb{F}_pC_p \rightarrow \mathbb{F}_p$ is defined by $\epsilon(\sum_{i=0}^{p-1} \alpha_i\sigma^i) = \sum_{i=0}^{p-1} \alpha_i$.

Then we have exact sequences of C_p-modules

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r] & A \arrow[r] & \mathbb{F}_p[V]^N \arrow[r] & 0 & & \\
0 \arrow[r] & I^{C_p} \arrow[r] \arrow[u, phantom, "\cup"] & A^{C_p} \arrow[r] \arrow[u, phantom, "\cup"] & \mathbb{F}_p[V]^G \arrow[r] \arrow[u, phantom, "\cup"] & H^1(C_p, I) \arrow[r] & H^1(C_p, A) \arrow[r] & \ldots
\end{tikzcd}$$

Hence the problem of determining elements of $\mathbb{F}_p[V]^G$ not determined by A^{C_p} amounts to understanding the right-hand side of the long exact sequence above. Of course, because of the periodic nature of the resolution of $\mathbb{F}_p$, we have

$$H^0(C_p, M) = \mathrm{Kernel}(M \xrightarrow{\Delta} M) = M^{C_p}$$

$$\begin{aligned} H^1(C_p, M) &= \frac{\mathrm{Kernel}(M \xrightarrow{Tr} M)}{\mathrm{Im}(M \xrightarrow{\Delta} M)} \\ &= H^{\mathrm{odd}}(C_p, M) \end{aligned}$$

$$\begin{aligned} H^2(C_p, M) &= \frac{\mathrm{Kernel}(M \xrightarrow{\Delta} M)}{\mathrm{Im}(M \xrightarrow{Tr} M)} \\ &= H^{\mathrm{even}}(C_p, M) \end{aligned}$$

Now the cohomology of C_p-modules is well understood. In particular, let's try and understand $H^*(C_p, V_n)$ for V_n an indecomposable representation of C_p. Let us denote a basis for V_n^* by $\{x_1, \ldots, x_n\}$ and note that $\Delta(x_i) = x_{i-1}$ for $1 < i \leq n$, $\Delta(x_1) = 0$, and, therefore, that $\mathrm{Tr}(x_i) = 0$ for $1 \leq i < p$, and $\mathrm{Tr}(x_p) = x_1$.

We have that $x_i \in \mathrm{Im}(\Delta)$ for $1 \leq i < n$. Further, we have $\mathrm{Im}(\mathrm{Tr}) = 0$ for $n < p$ and $\mathrm{Im}(\mathrm{Tr}) =< x_1 >$, for $n = p$. Finally, $H^0(C_p, V_i) = V_i^{C_p} =$

$\mathbb{F}_p$ on the cohomology class associated to x_1. Putting all of this together we obtain

$$\begin{aligned}
&H^0(C_p, V_n) = \mathbb{F}_p, \text{ on the class associated to } x_1\\
&H^1(C_p, V_p) = 0 = H^2(C_p, V_p)\\
&H^1(C_p, V_n) = \mathbb{F}_p, \ n < p, \text{ on the class associated to } x_n\\
&H^2(C_p, V_n) = \mathbb{F}_p, \ n < p, \text{ on the class associated to } x_1
\end{aligned}$$

In our situation we must first understand the decomposition of (each graded piece of) I and A into C_p-modules, study the effect of mapping from one to other, and find the kernel of the induced mapping.

Shank and Wehlau have a recent preprint [**SW(b)**] in which they make use of this technology to prove the following. Suppose U is a sub-module of the C_p-module V. Suppose $\mathbb{F}_p[V]$ is generated in degrees less than or equal η. Then $\mathbb{F}_p[U]$ is generated in degrees less than or equal η. They further obtain a lower bound for η.

6. Two Problems from Invariant Theory.

The Dixmier-Erdös-Nicholas Problem. Let C_n be the cyclic group of order n over a field with a primitive n-th root of unity ω. The generator σ of the group with respect to the natural basis given by x_i corresponding to σ^i has the form

$$\sigma = \begin{pmatrix} 0\,0\,0 \dots 0\,1 \\ 1\,0\,0 \dots 0\,0 \\ 0\,1\,0 \dots 0\,0 \\ \vdots\ \vdots\ \vdots\ \ddots\ \vdots\ \vdots \\ 0\,0\,0 \dots 1\,0 \end{pmatrix}$$

Of course, C_n can be diagonalized, that is, there is a basis

$$\{y_0, y_1, \dots, y_{n-1}\}$$

with respect to which σ is diagonal of the form

$$\sigma = \mathrm{diag}(1, \omega, \omega^2, \dots, \omega^{n-1}).$$

We note immediately that y_0^i will be an invariant polynomial for all $i \geq 0$ and so we will work with the reduced regular representation, that is, we will take the vector space V with basis $\{y_1, \dots, y_{n-1}\}$.

The computation of $\mathbb{F}[V]^{C_n}$ is connected with problems in the representation theory of Lie groups of type A_n, and with problems in graph theory. We proceed as follows.

We note that $\sigma(y^I) = \omega^{i_1+2i_2+\cdots+(n-1)i_{n-1}}y^I$, so that the group maps monomials to monomials. It follows that invariant polynomials consist of sums of invariant monomials. Writing $\theta = (1, 2, \ldots, n-1)$ we see that y^I is invariant if and only if

$$\theta \cdot I = i_1 + 2i_2 + \cdots + (n-1)i_{n-1} = m(I)n,$$

for some $m(I) \in \mathbb{N}$. We refer to $m(I)$ as the *multiplicity* of I. We let $\mathcal{M}$ denote the collection of generating monomials, or rather, by abuse of notation, their exponent sequences. We denote by Δ_i the exponent sequence which consists of 0's everywhere except for a 1 in the i-th position. It is easy to see that the sequences $n\Delta_i$ are generators, and, in fact, the associated monomials form a homogeneous system for the ring of invariants. It follows that, if $I \in \mathcal{M}$, and I is not one of the $n\Delta_i$, then each entry in I is less than n.

We are interested in the problem of characterizing elements of $\mathcal{M}$, or in counting their number, denoted here $f(n)$. We've labeled the problem in the way we do because of a theorem due to Dixmier -Erdös-Nicholas, which says,

Theorem.

$$\liminf_{n\to\infty} \frac{f(n)}{\sqrt{n}p(n)} \log n \log\log(n) > 0.$$

Here $p(n)$ denotes the number of partitions of n. This theorem points to a phenomenonal growth in the number of generators for these rings of invariants as n grows.

One view is that the equation above takes place in $\mathbb{N}^{n-1} \subset \mathbb{Z}^{n-1} \subset \mathbb{R}^{n-1}$. If you prefer, we are studying an action of C_n on these three sets. Of course, we can interpret the action on $\mathbb{Z}^{n-1}$ as associated to the ring of Laurent polynomials. To continue, in Euclidean space, the equation defines the hyperplane of multiplicity m. We can find a integral basis for the multiplicity 0 hyperplane, the hyperplane through the origin. And then any of the multiplicity planes can be obtained by identifying just one integer vector in them, and using the basis above. We haven't been able to characterize the generators of our ring in this manner, though.

Special cases related to these sorts of invariants can be found in [**3**, **4**, **11**].

Steenrod module structures on the syzygies. First, we'll restrict our attention to the case $p = 2$. I'll try to illustrate with examples an interesting situation. Let V be a vector space of dimension 2 over the field $\mathbb{F}_2$. Let $G = C_3$ be the subgroup of $\mathrm{Gl}_2(\mathbb{F}_2)$ generated by the matrix $\sigma = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. The group G has order 3, and we described the ring of invariants at the end of the section on examples.

We recall

$$\mathbb{F}_2[x,y]^G = \mathbb{F}_2[a,b,c]$$

where

$$\begin{aligned} a &= x^2 + xy + y^2, \\ b &= x^3 + x^2y + y^3, \text{ and} \\ c &= x^3 + xy^2 + y^3, \text{ with relation} \\ a^3 &= b^2 + bc + c^2, \end{aligned}$$

together with its resolution by syzygies over the ring $A = \mathbb{F}_2[a,b,c]$. Here $|a| = 2$, $|b| = |c| = 3$, and $\rho(a) = x^2 + xy + y^2$, $\rho(b) = x^2y + xy^2$, $\rho(c) = x^3 + x^2y + y^3$. We also had

$$0 \longrightarrow A(c^2 + a^3 + b^2 + bc) \longrightarrow A \longrightarrow \mathbb{F}_2[x,y]^G \longrightarrow 0.$$

We will refer to the relation by the name d.

Here is a table of Steenrod operations on A which we write down after considering the corresponding operations on $\mathbb{F}_2[V]^G$.

	Sq^1	Sq^2	Sq^3
a	b	a^2	0
b	0	ab	b^2
c	a^2	$ab + ac$	$\mathbf{c^2 + d}$

We won't go into the details here, but there is a proposition which states that if the Adem relations are satisfied on the generators of an algebra, and the action of the operations on products are given by the Cartan formula, then we obtain an action of the Steenrod algebra on the algebra. There are more sophisticated versions, but, for now, let's just point out that it is enough to determine $Sq^i(f)$ for $0 \leq i \leq |f|$ for each generator f of the algebra in question, and then verify $2^{|f|}$ Adem relations on f, beginning with $Sq^{2|f|-1}Sq^{|f|}(f) = 0$ and working our way down to $Sq^1Sq^1(f) = 0$.

In our example, because of the Adem relation $Sq^1Sq^2 = Sq^3$, we can calculate $Sq^3(c)$. However, we note that $Sq^3(c) \neq c^2$, so that A is not a $\mathcal{A}$-algebra, but rather a $\mathcal{A}$-module. We need to check that $Sq^3Sq^2 = 0$, $Sq^2Sq^2 = Sq^3Sq^1$. It is straightforward to observe that the $\mathcal{A}$-action preserves the ideal generated by d.

Here is another example. Let $A = \mathbb{F}_2[x,y]/(xy^2 + x^3)$ with $\mathcal{A}$ action given by $Sq^1(x) = xy$, and $Sq^1(y) = y^2$. It is trivial that $Sq^1Sq^1(y) = 0$, and we obtain $Sq^1Sq^1(x) = Sq^1(xy) = xy^2 + x^3 = 0$. These are the only Adem relations we need check, and therefore A carries the structure of a $\mathcal{A}$-module. However, it is fairly easy to see that the "natural" (from a certain point of view) algebra $B = \mathbb{F}_2[x, y]$ doesn't admit a compatible action of $\mathcal{A}$. In particular, there is no possible modification of our definition $Sq^1(x) = xy$. Therefore we obtain $Sq^1Sq^1(x) = xy^2 + x^3$ which is **not** 0 in B. Therefore, of course, B is not an $\mathcal{A}$-module, and can't be made to carry such a structure, given that the ideal (through which our choices might be modified) doesn't begin until degree 3. Of course, we might seek to modify B, but this is a story for another day.

There is much more to be said about even these two examples, and in the verification of the underlying theorems producing $\mathcal{A}$ actions, but these need await another time. We've computed a number of different examples, which we hope to analyze in more detail.

7. References

A word about the two lists that follow. In the beginning there was Stanley's paper [**S**]. Then came the books of Smith [**S(a)**] and Benson [**B**]. Smith's book, in particular, has an extensive bibliography. I urge the interested reader to consult it. I've included one limited list of references, and a list of the papers on invariant theory with which I have been involved. They were all lots of fun.

Stanley's paper appeared in the Bulletin of the AMS in the May 1979 volume. In many ways, our work since 1986 has been our attempt to understand how the theorems and techniques of this paper could be understood in positive characteristic.

Also recommended is the paper of Larry Smith, *A note on the realization of complete intersection algebras as cohomology algebras of a space*, Quart. J. Math. Ox. (2), **33** (1982), 379–384.

[**B**] D J Benson, *Polynomial invariants of finite groups*, LMS **190** Cambridge University Press (1993).

[**BZ**] D Bourguiba and S Zarati, *Depth and the Steenrod algebra*, Inventiones Math, **128** (1997) 589-602.

[**Br**] A Broer, *Remarks on invariant theory of finite groups*, preprint (1997).

[**DW**] W M Dwyer and C Wilkerson, *Kahler differentials, the T functor, and a theorem of Steinberg*, Trans AMS, **350** No 12 (1998) 4919–4930.

[**Fl**] P Fleischmann, *A new degree bound for vector invariants of symmetric groups* Trans AMS, **350** No 4 (1998) 1703–1712.

[**FL**] P Fleischmann and W Lempken, *On generators of modular invariant rings of finite groups* Bull AMS, **29** No 5 (1997) 585–591.

[**K**] R M Kane, *Poincaré duality and the ring of coinvariants*, Can Math Bull, **37** (1994) 82–88.

[**N**] H Nakajima, *Regular rings of invariants of unipotent groups*, Journal of Algebra, **85** (1983) 253–286.

[**R**] D R Richman,*On vector invariants over finite fields*, Advances in Math., **81** (1990) 30–65.

[**Sh**] R J Shank, *SAGBI bases for ring of formal modular semi-invariants*, Comment Math Helv, **73** No 4 (1998) 548-565.

[**Si**] W M Singer, *The transfer in homological algebra*, Math Z, **202** (1989) 493–523.

[**SW(a)**] R J Shank and D L Wehlau, *The transfer in modular invariant theory*, Journal of Pure and Applied Algebra, **141** No 3 (1999) 299-313.

[**SW(b)**] R J Shank and D L Wehlau, *Noether numbers for subrepresentations of cyclic groups of prime order*, preprint, August 2000.

[**S(a)**] L Smith, *Polynomial invariants of finite groups*, A. K. Peters, Wellesley MA USA (1995).

[**S(b)**] L Smith, *Polynomial invariants of finite groups. A survey of recent developments.* Bull AMS, **34** No 3 (1997) 211–250.

[**S**] R P Stanley,*Invariants of finite groups and their applications to combinatorics.*, Bull AMS , **1**, No 3 (1979) 475–511.

[**W**] C Wilkerson, *A primer on the Dickson invariants*, Proceedings of the Northwestern Homotopy Theory Conference, AMS, Cont Math, **19** (1983) 421–434.

Queen's Papers.

(1) H E A Campbell, I P Hughes, G Kemper, R J Shank, and D L Wehlau, *Depth of modular invariant rings*, Transformation Groups **5** No 1 (2000) 21–34.

(2) H E A Campbell, A V Geramita, I P Hughes, R J Shank, and D L Wehlau, *Non-Cohen-Macaulay vector invariants and a Noether bound for a Gorenstein ring of invariants*, Can Math Bull, **42 (2)**, (1999), 155–161.

(3) H E A Campbell, J Harris and D Wehlau, *On rings of invariants of non-modular Abelian groups*, Bulletin of the Australian Mathematics Society, **60** No 3 (1999) 509–520.

(4) H E A Campbell, J Harris and D Wehlau, *Internal duality for resolutions of rings*, Journal of Algebra, **215** (1999) 1–33.

(5) H E A Campbell and I P Hughes, *Rings of invariants of certain p-groups over the field $\mathbf{F}_p$*, Journal of Algebra, **211** (1999) 549–561.

(6) H E A Campbell and I P Hughes, *On the vector invariants of $U_2(\mathbf{F}_p)$: a proof of a conjecture of David Richman*, Advances in Math, **126** No 1 (1997) 1–20.

(7) H E A Campbell, I P Hughes, R J Shank, and D L Wehlau, *Bases for rings of covariants*, Transformation Groups, **1** No 4 (1996) 307–336.

(8) H E A Campbell and I P Hughes, *The ring of upper triangular invariants as a module over the Dickson invariants*, Mathematische Annalen, **306** (1996) 429–443.

(9) H E A Campbell and I P Hughes, *2-dimensional vector invariants of parabolic subgroups of $GL_2(\mathbf{F}_p)$*, Journal of Pure and Applied Algebra, **112** (1996) 1–12.

(10) R B Bell, H E A Campbell, and I P Hughes, *Properties of functions associated to invariant theory*, Comm in Alg **22** (1994), 381–396.

(11) H E A Campbell, I P Hughes, F Pappalardi, and P S Selick, *On the ring of invariants of $\mathbf{F}_{2^s}^*$*, Comment Math Helv **66** (1991) 322–331.

(12) H E A Campbell, I P Hughes, and R D Pollack, *Rings of invariants and p-Sylow subgroups*, Can Math Bull **34** No 1 (1991) 42–47.

(13) H E A Campbell, I P Hughes, and R D Pollack, *Vector invariants of symmetric groups*, Can Math Bull **33** No 4 (1990) 391–397.

Mathematics and Statistics Department, Queen's University, Kingston, Ontario, Canada, K7L 3N 6

E-mail address: eddy@mast.queensu.ca