On Invariant Theory Of Finite Groups

Peter Fleischmann
Institut of Mathematics and Statistics
University of Kent at Canterbury
U.K.

January 27, 2003

Contents

Chapter 1

Construction of Invariant Rings

1.1 Introduction

In each basic course on algebra one will come across the following example of a **ring of invariants**:

Let R be a commutative ring, $A := R[X_1, \ldots, X_n]$ the ring of polynomials in n variables $X_1, \ldots, X_n$ and Σ_n the symmetric group on n - letters. Then Σ_n acts 'naturally' on A by 'permuting the variables' following the rule

$$\sigma(f(X_1, \ldots, X_n)) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}), \forall \sigma \in \Sigma_n,\ f \in A.$$

As one can see immediately, $\sigma(fg) = \sigma(f)\sigma(g)$ for $f, g \in A$ and the action of Σ_n on A respects homogeneity of polynomials and their degree. This means that Σ_n acts on A by automorphisms of the graded R - algebra A. Those polynomials which remain unchanged by the operation of Σ_n are called **symmetric polynomials**. They form a graded subring A^{Σ_n} of A, the **ring of symmetric polynomials** in A, being our first example of a **ring of invariants**.

A central objective of constructive invariant theory is, to give a uniform and efficient description of all invariant polynomials. Again we consider the example of symmetric functions:

Let us order the power products $\underline{X}^\alpha := X_1^{\alpha_1} X_2^{\alpha_1} \cdots X_n^{\alpha_n}$ by the 'degree - lexicographical' order saying that $\underline{X}^\alpha < \underline{X}^\beta$ if and only if deg $\underline{X}^\alpha <$ deg $\underline{X}^\beta$ or the degrees coincide and

$$\alpha_i < \beta_i \text{ for } i = \min \{j \leq n \mid \alpha_j \neq \beta_j\}.$$

Then each orbit $\{\sigma(\underline{X}^\alpha) \mid \sigma \in \Sigma_n\}$ contains a unique maximal element which we call $\underline{X}^\alpha_{\max}$ and which satisfies $\alpha_1 \geq \alpha_2 \geq \cdots$. Obviously Σ_n permutes the power products, hence each symmetric polynomial will be a unique R - linear combination of **orbit - sums**

$$\mathrm{orb}_{\Sigma_n}(\underline{X}^\alpha) := \sum_{\{\underline{X}^\beta = \sigma(\underline{X}^\alpha) \ | \ \sigma \in \Sigma_n\}} \underline{X}^\beta .$$

Let $f \in A^{\Sigma_n}$ be an arbitrary (non - constant) symmetric polynomial, and let

$$\underline{X}^\alpha_{\max}(f) = X_1^{\alpha_1} X_2^{\alpha_1} \cdots X_n^{\alpha_n}$$

be the largest power product appearing in f with a non - zero coefficient r, say. Then $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$. For $k \in \mathbb{N}$ let

$$e_k := \mathrm{orb}_{\Sigma_n}(X_1 X_2 \cdots X_k) = \sum_{1 \leq j_1 < j_2 < \ldots < j_k \leq n} X_{j_1} X_{j_2} \ldots X_{j_k}$$

be the k - th **elementary symmetric polynomial**. Then $\underline{X}^\alpha_{\max}(f)$ is also the unique maximal power product appearing in the product $e := e_1^{\alpha_1 - \alpha_2} e_2^{\alpha_2 - \alpha_3} \cdots e_n^{\alpha_n}$. Now it is easy to see that all power products appearing in $f - re$ are strictly smaller than $\underline{X}^\alpha(f)$ in the lexicographical order. Of course we can iterate the argument replacing f by the symmetric polynomial $f - re$. In each iteration the 'new' $\underline{X}^\alpha_{\max}$ will strictly decrease and the whole process must end with a constant function, because there are no infinite sequences

$$\cdots < \underline{X}^\gamma < \underline{X}^\rho < \underline{X}^\alpha .$$

In the summary this argument can be made into an algorithm to produce a polynomial $\Psi(Y_1, \cdots, Y_n)$ with $f = \Psi(e_1, \cdots, e_n)$. To show that Ψ is unique, it suffices to observe that the power products of the form $\underline{e}^\beta := e_1^{\beta_1} \cdots e_n^{\beta_n}$ are linearly independent, which in turn follows from the fact that these power products have pairwise different leading monomials of the form $\underline{X}^\alpha_{\max}(\underline{e}^\beta) = X_1^{\beta_1 + \cdots + \beta_n} X_2^{\beta_2 + \cdots + \beta_n} \cdots X_n^{\beta_n}$.

This proves the **main theorem of symmetric polynomials**, stating that every $f \in A^{\Sigma_n}$ can be rewritten in a unique way as a polynomial in the elementary symmetric polynomials e_i, which themselves are algebraically independent.

This result is remarkable in the following sense:

- it gives an overview over all symmetric polynomials and how to construct them, using the finite set of homogeneous generators $e_1, \cdots, e_n$ of degrees bounded by n;
- it describes explicitly the ring theoretic structure of $A^{\Sigma_n} = R[e_1, \ldots, e_n]$ as being isomorphic to a polynomial ring $R[Y_1, \ldots, Y_n]$.

These two *constructive* and *structural* aspects guide the investigation of more general invariant rings. Firstly we replace Σ_n by a general finite group G, secondly we skip the requirement that G acts on A by permuting variables. In most cases we will only assume that G acts via graded R - algebra automorphisms. [1] The following are natural questions in this context:

- How can we explicitly find a finite set of (homogeneous) invariants that generate A^G as an R - algebra? Is there an a priori bound for their degrees?
- If A is a polynomial ring over a field $R = \mathbb{F}$, say. How 'far away' is A^G from being a polynomial ring?

The second question is deliberately vague at this stage and the answer certainly depends on how to define the structure of a ring to be 'close to' a polynomial ring. This will be made more precise later on.

Further reading: Quite recently there have appeared or are about to appear several very good monographs on the subject ([1], [31], [23], [4]). They differ in style and focus and supplement each other in providing a full encyclopedia about all theoretical and constructive aspects of invariant theory of finite groups. Therefore I strongly recommended to read these for any deeper study in this area.

1.2 Degree Bounds

Let R be a commutative ring, $A := R[a_1, a_2, \cdots, a_n]$ a finitely generated R - algebra with set of generators $\mathbf{a} := \{a_1, \cdots, a_n\}$ and G a finite group acting on A by R - algebra automorphisms, stabilizing the R - module $\sum_{i=1}^n Ra_i$. We define the ring of G - invariants $A^G := \{a \in A \mid g(a) = a, \ \forall g \in G\}$.
Following the example of symmetric functions we are interested in finding a set of **fundamental invariants** $\{f_1, f_2, \cdots, f_s\} \subseteq A^G$ such that $A^G = R[f_1, f_2, \cdots, f_s]$.

[1]sometimes even this is not needed and A can be replaced by some ungraded finitely generated R - algebra, on which G acts by R - algebra automorphisms.

Historic Remarks:
The question, whether there is always a *finite* set of fundamental invariants for arbitrary groups was considered to be one of the most important problems in 19'th century algebra. It was proved to be true, using explicit calculations, by P Gordan for $R = \mathbb{C}$ and $G = SL_2(\mathbb{C})$ in the 1860/70's. In 1890 David Hilbert (1862-1943) introduced new methods into invariant theory, which still today are basic tools of modern algebra (Hilbert's basis theorem). Applying these he was able to prove finite generation for the invariants of the general linear groups $\mathrm{GL}_n(\mathbb{C})$.
In the year 1900, on the occasion of the international congress of mathematics in Paris, Hilbert posed the general question of finite generation of invariant rings for arbitrary groups as the 14'th of the now famous 'Hilbert problems'. [2] In general the answer to this question is negative:
In 1958 Nagata gave a counterexample of $G \cong \mathbb{C}^+ \times \ldots \times \mathbb{C}^+$ (finite product) acting on a polynomial ring A in finitely many variables such that A^G is *not* finitely generated.
For *finite groups* Hilbert's 14^{th} problem has been solved affirmatively: In 1926 Emmy Noether proved ([25]) that the invariant ring A^G is finitely generated, if G is a finite group and $R = \mathbb{F}$ is an arbitrary field. This proof, which will be outlined shortly, was one of the first major applications of her newly developed theory of rings and modules with ascending chain condition. Therefore it can be generalized in a straightforward way to the case where, in modern language, the ring R is Noetherian. The price one has to pay for this generality is, that the proof is not constructive and does not provide an immediate algorithm how to compute a finite set of fundamental invariants. Ten years earlier, in [24] Emmy Noether had considered the problem specifically for $R = \mathbb{C}$, where she was able to find constructive procedures to compute fundamental systems explicitly. We will now follow up her ideas and at the same time try to generalize them as far as possible.

Assume that $\{f_1, f_2, \cdots, f_s\}$ is a finite set of fundamental invariants; then each f_i is an R - linear combination of power products $\underline{a}^\alpha = a_1^{\alpha_1} \cdots a_n^{\alpha_n}$ and we can look at the maximal degree of an exponent function α needed to write down all the f_i's. Let us define the **Noether number** $\beta(A^G)$ to be the *minimum* of all these numbers, taken over all possible finite fundamental systems. Notice that the Noether number depends on the chosen set of generators for A; therefore we will write $\beta(A^G, \mathbf{a})$ whenever we need to express this dependence. So the statement $\beta(A^G) \leq m$ says that every element in A^G can be written as linear combination

[2] In his original lecture this problem had been posed a little bit differently, since finiteness was thought of being solved; later an error in the proof was found.

of products of invariants lying in in the R - module

$$\mathcal{M}_m(\mathbf{a}) := \sum_{\alpha\in\mathbb{N}_0^n,\ |\alpha|\le m} R\cdot \underline{a}^\alpha,$$

or in other words, $A^G = R[A^G \cap \mathcal{M}_m(\mathbf{a})]$. For example if $R = R[X_1, \cdots, X_n]$ is a polynomial ring with $\beta(A^G) \le m$, then all invariants can be generated in degree less or equal to m; in particular we have seen that $\beta(R[X_1, \cdots, X_n]^{\Sigma_n}) \le n$.

The example of symmetric functions also gives us an idea how to construct invariants: Let $H \le G$ be a subgroup of index m and let $\{1 = g_1, g_2, \cdots, g_m\}$ denote a set of representatives for the cosets gH. Take a new variable Y and consider for any $a \in A^H$ the polynomial $f_a(Y)$ defined by:

$$f_a(Y) = \prod_{i=1}^m (Y - g_i(a)) = Y^m + f_{a,1}Y^{m-1} + \cdots + f_{a,m-1}Y + f_{a,m}.$$

It is easy to check that $f_a(Y)$ is independent of the particular choice of the system $\{g_1, g_2, \cdots, g_m\}$ and that $f_a(Y) \in A^G[Y]$. In fact, up to sign the coefficient $f_{a,i}$ is equal to the i'th elementary symmetric function $e_i(g_1(a), g_2(a), \cdots, g_m(a))$. Note that $f_a(a) = 0$, so

$$a^m = -f_{a,1}a^{m-1} + \cdots - f_{a,m-1}a - f_{a,m}.(*)$$

In particular we can take $H = 1$ and define a subring of A^G by

$$B := R[f_{a_i,j} \mid i = 1, \cdots, n,\ j = 1, \cdots, |G|].$$

Using equation (*) we see that A can be viewed as the *module* over B generated by the finite set of power products $\{\underline{a}^\alpha \mid \alpha_i < |G|,\ \forall\ i = 1, \cdots, n\}$. If R is a Noetherian ring, then by Hilbert's basis theorem, so is B and hence submodules of finitely generated B - modules are again finitely generated. In particular A^G, being a B - submodule of A, is a finitely generated B - module, hence a finitely generated R - algebra. This is precisely Emmy Noether's argument for finite generation of A^G in case of finite groups and Noetherian coefficient rings. Note that the argument tells us that $A^G = R[B, b_1, b_2, \cdots, b_\ell]$ with the b_i's being B - module generators, but it does not tell us how to construct these.

To attack that problem, consider the (absolute) transfer map

$$t_1^G:\ A \to A^G,\ a \mapsto \sum_{g\in G} g(a),$$

which is a homomorphism of A^G - modules and therefore of B - modules as well. It is also surjective, whenever $|G|$ is invertible in R. In that case, using equation (*) and the fact that t_1^G is A^G - linear, we see that

$$A^G = R[B,\ t_1^G(\underline{a}^\alpha) \mid \text{all } \alpha_i \leq |G|]$$

from which we can conclude $\beta(A^G) \leq \max\{|G|, n \cdot (|G|-1)\}$.

In ([24]) Emmy Noether used a similar approach to give two different proofs for the fact that $\beta(A^G) \leq |G|$ if R is a polynomial ring over the complex numbers. This is usually referred to as the **Noether bound** in invariant theory. To get from the bound above to the Noether bound, one needs some combinatorics to reduce exponents in transfer elements $t_1^G(\underline{a}^\alpha)$. The original arguments used in [24] only work if the *factorial* of $|G|$ is invertible. Recently different techniques have been found, which also work in the more general case that $|G|$ is invertible in R (see [9], [14]; for earlier work on that problem see [26], [28], [32], [12],[13]).

I will present a 'combined version' of these methods, incorporating an essential observation by D Benson which makes the required combinatorics very transparent.

First let us convince ourselves that the requirement $|G|$ to be invertible in R is really needed: Consider the simple example $A := A(k,2) := \mathbb{F}_2[X_1, \cdots, X_k, Y_1, \cdots, Y_k]$ with $G = \Sigma_2 = \langle g \rangle$ acting by swapping the 'variable types' $X_i \leftrightarrow Y_i$.

Lemma 1.2.1 *The invariant* $\mathfrak{X} := (X_1 \cdots X_k)^+ := X_1 \cdots X_k + Y_1 \cdots Y_k \in A^G$ *is indecomposable, i.e. cannot be written as a sum of products of invariants of smaller degree. Therefore*

$$\beta(A^G) \geq k \to \infty \text{ if } k \to \infty.$$

Proof: We will use the fact that A and A^G are graded not just by $\mathbb{N}_0$, but by $\mathbb{N}_0^k$: For each $M = (m_{ij}) \in \mathbb{N}_0^{k\times 2}$ and power product $\mathfrak{F}_M := X_1^{m_{11}} X_2^{m_{21}} \cdots X_k^{m_{k1}} \cdot Y_1^{m_{12}} Y_2^{m_{22}} \cdots Y_k^{m_{k2}}$ we define a multi-degree

$$\mathrm{md}(\mathfrak{F}_M) := (m_{11}+m_{12}, m_{21}+m_{22}, \cdots, m_{k1}+m_{k2}) \in \mathbb{N}_0^k.$$

Then $A = \oplus_{v\in\mathbb{N}_0^k} A_v$, with $A_v := \langle \mathfrak{F}_M \in A \mid \mathrm{md}(\mathfrak{F}_M) := v\rangle$ and $A_v \cdot A_w \subseteq A_{v+w}$. Since the G - action on A respects the multi-degree, we have as well $A^G = \oplus_{v\in\mathbb{N}_0^k} (A_v)^G$ and $\mathfrak{X}$ is 'multi-homogeneous' of multi - degree $\mathbf{1} := (1,1,\cdots,1)$. Obviously G permutes power products in A and therefore every invariant in A^G is a linear combination either of G - stable power products or of 'orbit - sums' of the form $\mathfrak{F}_M^+ := \mathfrak{F}_M + g(\mathfrak{F}_M)$. Note that the power product $\mathfrak{F}_M$ is G - stable if and only if the two columns of M coincide.

Now we consider the algebra homomorphism $\pi : A(k,2) \to A(1,2) = \mathbb{F}_2[X_1, Y_1]$ induced by the specialization $X_i \mapsto 1, Y_i \mapsto 1$ for $i > 1$. Clearly π is G -equivariant and if M has two different columns, then $\pi(\mathfrak{F}_M^+) = X_1^{m_{11}} Y_1^{m_{12}} + X_1^{m_{12}} Y_1^{m_{11}}$, which is zero if and only if $m_{11} = m_{12}$. Now assume that $\mathfrak{X}$ is decomposable; then it is a sum of products of the form $\mathfrak{F}_{M_1}^+ \cdot \mathfrak{F}_{M_2}^+ \cdots \mathfrak{F}_{M_s}^+$ with $s > 1$, $\mathbf{0} \neq \mathrm{md}(\mathfrak{F}_{M_j}^+)$ for all j and $\mathrm{md}(\mathfrak{F}_{M_1}^+) + \cdots + \mathrm{md}(\mathfrak{F}_{M_s}^+) = \mathbf{1}$. In particular all occurring M_j's have different columns and in each product there must be at least one $\mathfrak{F}_{M_{j_0}}$ with multi-degree $(0, d_2, \cdots, d_k)$ and $d_i \in \{0,1\}$. Hence $\pi(\mathfrak{F}_{M_{j_0}}^+) = X_1^0 Y_1^0 + X_1^0 Y_1^0 = 1 + 1 = 0$ and since π is linear and multiplicative, we get the contradiction $X_1 + Y_1 = \pi(\mathfrak{X}) = 0$. $\diamond$

It is interesting, though, to observe that for $k \geq 3$:

$$\mathfrak{X} = (X_2 \cdots X_k)^+ X_1 + (X_1 X_3 \cdots X_k)^+ Y_2 - (X_3 \cdots X_k)^+ X_1 Y_2,$$

i.e. $\mathfrak{X}$ decomposes in the **Hilbert - ideal** $A^{G,+}A$, generated *in* A by all invariants of positive degree. Extending the definition of the Noether number in an obvious way to cover ideal generators, one can easily see that $\beta(A^{G,+}A) = 2$ for all $k \geq 2$. In fact a generalization of this observation led to the proof of Noether's bound in [9].

Let $H \leq G$ be a subgroup of index m and $G := \cup_{i=1}^m g_i H$ the coset decomposition. Assume that A^H is known and consider the **relative transfer map** with respect to H:

$$t_H^G : A^H \to A^G, \ a \mapsto \sum_{i=1}^m g_i(a)$$

Again this is an A^G - module homomorphism and the image $t_H^G(A^G)$ is an ideal in A^G, called the **relative transfer ideal** (w.r.t. H). The following describes a decomposition, **in the ambient ring** A, of high degree relative transfer elements:

Lemma 1.2.2 *For* $b, b_1, b_2, \cdots, b_m \in A^H$ *we have*

$$t_H^G(bb_1 \cdots b_m) = \sum_{I \subset \underline{m},\ I \neq \underline{m}} (-1)^{m-|I|+1}\ t_H^G(b \prod_{j \in I} b_j) \prod_{j \notin I} g_j(b_j).$$

Proof: We consider the obvious equality:

$$\prod_{j=1}^m (\ g_i(b_j) - g_j(b_j)\ ) = 0.$$

Expansion and multiplication with $g_i(b)$ for fixed i gives:

$$0 = \sum_{I \subseteq \underline{m}} (-1)^{|I|} \prod_{j \notin I} g_j(b_j) \cdot (\prod_{j \in I} g_i(b_j)) \cdot g_i(b).$$

Now summation over $i \in \underline{m}$ yields the claimed identity. $\diamond$

The following result contains the statement of the Noether bound for $H = 1$ and $|G|$ invertible:

Theorem 1.2.3 *Let $A := R[a_1, \cdots, a_n]$ as above and let H be a subgroup of G such that either $|G|$ is invertible in R or $H \lhd G$ a normal subgroup with index $[G : H]$ invertible in R. Then*

$$\beta(A^G, \mathbf{a}) \leq \beta(A^H, \mathbf{a}) \cdot [G : H].$$

Proof: Under both assumptions on H, the relative transfer map t_H^G is surjective. Now suppose that $\beta := \beta(A^H) = \beta(A^H, \mathbf{a})$ and $A^H = R[b_1, \cdots, b_k]$ with $b_i \in A^H \cap \mathcal{M}_\beta(\mathbf{a})$. If $H \leq G$ and $|G|$ is invertible, we have $t_H^G(b_\ell b_{i_1} \cdots b_{i_m}) = \frac{1}{|G|} t_1^G(t_H^G(b_\ell b_{i_1} \cdots b_{i_m})) =$

$$\sum_{I \subset \underline{m},\ I \neq \underline{m}} (-1)^{m-|I|+1}\ t_H^G(b_\ell \prod_{j \in I} b_{i_j}) \frac{1}{|G|}\ t_1^G(\prod_{j \notin I} g_j(b_{i_j})) \in R[A^G \cap \mathcal{M}_{m\beta}(\mathbf{a})].$$

If $H \lhd G$, then A^H is G - invariant and the elements $g_j(b_{i_j})$ lie in A^H. If in addition $|G/H|$ is invertible, replacing $|G|$ by $|G/H|$ and t_1^G by t_H^G we conclude in a similar way that $t_H^G(b_\ell b_{i_1} \cdots b_{i_m}) \in R[A^G \cap \mathcal{M}_{m \cdot \beta}(\mathbf{a})]$. Now an iterative application of this result finishes the proof. $\diamond$

1.3 Further Results and Conjectures

Firstly one might hope to remove the requirement $H \lhd G$ for subgroups of invertible index:

Conjecture 1.3.1 *: If $H \leq G$ with index $[G : H]$ invertible in R, then*

$$\beta(A^G) \leq \beta(A^H) \cdot [G : H].$$

An argument similar to the original one in [24] can be used to show that $\beta(A^G) \leq \beta(A^H) \cdot [G : H]$ whenever $[G : H]!$ is invertible (see 2.3.5).

For the rest of this section let $A = \mathbb{F}[X_1, \cdots, X_n]$, a polynomial ring over a field of characteristic $p > 0$. In this case, the formula in Lemma 1.2.2 can be used to describe a decomposition of relative transfer elements in the Hilbert - ideal $A^{G,+}A$.[3] Sample calculations done by Harm Derksen and Gregor Kemper led them to the following far reaching conjecture:

[3]If A is $\mathbb{N}_0$ - graded, A^+ denotes the ideal generated by homogeneous elements of positive degree.

Conjecture 1.3.2 *[Noether bound for Hilbert ideals] (H. Derksen / G. Kemper): Let G be a finite group, $\mathbb{F}$ a field and $A := \mathbb{F}[X_1, \cdots, X_n]$ a polynomial ring, such that G acts by graded algebra automorphisms. Then*

$$\beta(A^{G,+}A) \leq |G|.$$

Let P be a fixed Sylow p - group of G with normalizer $N_G(P)$ and $N := N_G(P)/P$. For subgroups $U \leq H \leq G$ we define the (homogeneous) **relative transfer ideal**

$$\mathcal{I}^H_{<U} := \sum_{Y<U} t^H_Y(A^Y) \lhd A^H.$$

Lemma 1.3.3

$$\beta(A^{G,+} \cdot A) \leq \max\{\beta(A^Q/\mathcal{I}^Q_{<Q}) \cdot [G:Q] \mid Q \leq P\}.$$

Proof: Let $f \in A^{G,+}$ be indecomposable in $A^{G,+}A$. Since $n := [G:P]$ is invertible, f is of the form $t^G_P(h)$ for some $h \in A^{P,+}$, which itself can be written as

$$h = \sum_{Q \leq P} t^P_Q(b_{Q,1}b_{Q,2} \cdots b_{Q,\ell_Q})$$

with ℓ_Q factors of the form $b_{Q,j} + \mathcal{I}^Q_{<Q} \in A^Q/\mathcal{I}^Q_{<Q}$, $b_{Q,j}$ homogeneous of positive degree $\leq \beta_Q := \beta(A^Q/\mathcal{I}^Q_{<Q})$. Moreover we can assume that every nonzero transfer element

$$t^G_P(t^P_Q(b_{Q,1}b_{Q,2} \cdots b_{Q,\ell_Q})) = t^G_Q(b_{Q,1}b_{Q,2} \cdots b_{Q,\ell_Q})$$

is indecomposable in $A^{G,+}A$ as well. But from Lemma 1.2.2 we see that this requires $\ell_Q \leq [G:Q]$, hence

$$f \in A^{G,+} \cap \mathcal{M}_{\beta_Q[G:Q]}(\mathbf{X}).$$

$\diamond$

Hence Noether's bound for relative transfer quotients of p - groups would imply Conjecture 1.3.2:

Corollary 1.3.4 *If $\beta(A^Q/\mathcal{I}^Q_{<Q}) \leq |Q|$ for all $Q \leq P \in \mathrm{Syl}_p(G)$, then Conjecture 1.3.2 holds, i.e. $\beta(A^{G,+}A) \leq |G|$.*

To obtain degree bounds for A^G rather than $A^{G,+}A$ one can make use of the **Brauer homomorphism** from representation theory, i.e. is the canonical homomorphism $A^G \to \overline{A^G} := A^G/\mathcal{I}^G_{<P}$. Now Mackey's formula [21] for the relative transfer states

$$t^G_P(b) = \sum_{g\in P:G:P} t^P_{P\cap\, {}^gP}({}^gb),$$

where $P:G:P$ denotes a chosen system of double cosets of P in G. For $g \in G\backslash N_G(P)$ the summand $t^P_{P\cap\, {}^gP}({}^gb)$ lies in $\mathcal{I}^P_{<P}$, hence we get

$$t^G_P(b) \equiv \sum_{g\in N/P} {}^gb \equiv t^N_1(b) \bmod \mathcal{I}^P_{<P}.$$

It is easy to see that $\mathcal{I}^P_{<P} \cap A^G = \mathcal{I}^G_{<P}$, hence we get

$$\overline{A^G} = (A^G + \mathcal{I}^P_{<P})/\mathcal{I}^P_{<P} = t^N_1(A^P/\mathcal{I}^P_{<P}) \cong (A^P/\mathcal{I}^P_{<P})^N.$$

Since p does not divide $|N|$, Theorem 1.2.3 gives

Lemma 1.3.5

$$\beta(\overline{A^G}) \leq \beta(\overline{A^P}) \cdot |N|.$$
$$\beta(A^G) \leq \max\{\beta(\mathcal{I}^G_{<P}),\ \beta(\overline{A^P}) \cdot |N|\}.$$

It has been conjectured that the bound in the previous section

$$\beta(A^G) \leq \max\{|G|, n(|G|-1)\}$$

might be a 'natural degree bound' for modular invariant rings in polynomial rings. Using the above technique this certainly would follow from the next two slightly sharper conjectures:

Conjecture 1.3.6 *Let P be a Sylow p - group of G. Then*

1. $\beta(A^G/\mathcal{I}^G_{<P}) \leq |N_G(P)|$.
2. *If $A = \mathbb{F}[X_1, \cdots, X_n]$, then*

$$\beta(\mathcal{I}^G_{<P}) \leq \max\{|G|, n(|G|-1)\}.$$

All these conjectures have been verified for p - permutation modules, as we will see in the next section. We have seen that the Noether bound is not valid for modular invariant rings. In fact it has been shown that no 'global degree bound' exists, that depends only on the group G and the ring or field of scalars. In fact the following has been shown:

Theorem 1.3.7 *[Richman [27]] Let V be a finite - dimensional vector space over $\mathbb{F}$ and G a finite subgroup of $\mathrm{GL}(V)$ with $p = \mathrm{char}\ \mathbb{F} \mid |G|$. For $m \in \mathbb{N}$ let V^m denote the direct sum of m copies of V and $\mathrm{Sym}(V^m)$ the corresponding symmetric algebra with natural G - action. Then there is a positive number α depending only on $|G|$ and p, such that every set of $\mathbb{F}$ - algebra generators of $\mathrm{Sym}(V^m)^G$ contains a generator of degree $\geq \alpha m$.*

Chapter 2

Permutation Invariants

2.1 Basic Constructions

In this section we investigate the special class of permutation invariants, constructed from a group action on a polynomial ring which permutes the independent variables. For the sake of notational flexibility the variables are indexed by a finite set Ω on which G acts. Thus we consider a polynomial ring $A = A(\Omega) := R[X_\omega \mid \omega \in \Omega]$ and without loss of generality we can assume that G is a subgroup of the symmetric group Σ_Ω acting by $\sigma(X_\omega) := X_{\sigma(\omega)}$. We will use the standard symbol Ω/G to denote the set of all G - orbits on Ω.

In this situation G stabilizes the set of power products

$$\mathcal{P} := \{\underline{X}^\alpha := \prod_{\omega\in\Omega} X_\omega^{\alpha_\omega} \mid \alpha \in \mathbb{N}_0^\Omega\}$$

and the map $\mathcal{P} \ni \underline{X}^\alpha \to \alpha \in \mathbb{N}_0^\Omega$ is an isomorphism of G - semigroups and defines a G - equivariant isomorphism between $A(\Omega)$ and the R - semigroup - ring $R[\mathbb{N}_0^\Omega]$. Note that G acts naturally on $\mathbb{N}_0^\Omega$ by the rule $g\alpha := \alpha\circ g^{-1}$. For the ease of notation, we will occasionally abuse language and identify the multiplicative semigroup of power products $\mathcal{P}$ with the additive semigroup $\mathbb{N}_0^\Omega$. Since G permutes $\mathcal{P}$ it follows that every $f \in A^G$ is an R - linear combination of power products with constant coefficients along G - orbits on $\mathcal{P}$. This shows that A^G is a free R - module of infinite rank, with basis given by the G - **orbit - sums**

$$\mathrm{orb}_G(\underline{X}^\alpha) := \sum_{\beta\in\alpha^G} \underline{X}^\beta = t^G_{G_\alpha}(\underline{X}^\alpha).$$

Here G_α denotes the stabilizer subgroup $\{g \in G \mid \alpha \circ g = \alpha\}$ of $\alpha \in \mathbb{N}_0^\Omega$. In particular, if $G_\alpha < G$, the orbit - sum $t^G_{G_\alpha}(\underline{X}^\alpha)$ lies in the ideal $\mathcal{I}^G_{<G}$. On the

other hand, if $G_\alpha = G$, then α is constant on G - orbits in Ω and therefore $\underline{X}^\alpha$ is a power product of orbit - products of 'norms' $\mathfrak{n}_i := \prod_{\omega\in\mathcal{O}_i} X_\omega$, where the $\mathcal{O}_i$, $i = 1,\cdots,k$ run through the set of G - orbits on Ω. As different G - orbits are disjoint, the norms $\mathfrak{n}_i$ are algebraically independent and generate a polynomial subring $S \cong R[Y_1,\ldots,Y_k] \le A^G$, where k is the number of G - orbits on Ω. For each $\alpha \in \mathbb{N}_0^\Omega$ consider the greatest common divisor $g_\alpha := \gcd(\frac{|G_\alpha|}{|H_\alpha|} \mid H < G)\cdot 1_R$. Then for each $H < G$ and $a = \sum_\alpha c_\alpha t^H_{H_\alpha}(X^\alpha) \in A^H$ we have

$$t^G_H(a) = \sum_\alpha c_\alpha t^G_{H_\alpha}(X^\alpha) = \sum_\alpha c_\alpha t^G_{G_\alpha}(t^{G_\alpha}_{H_\alpha}(X^\alpha)) = \sum_\alpha c_\alpha \frac{|G_\alpha|}{|H_\alpha|} t^G_{G_\alpha}(X^\alpha) \in \sum_\alpha g_\alpha A^G.$$

On the other hand, if g_α is expressed as a linear combination $\sum_{H<G} \frac{|G_\alpha|}{|H_\alpha|} c_H$ with $c_H \in \mathbb{Z}$, then $g_\alpha \cdot \mathrm{orb}_G(\underline{X}^\alpha) =$

$$\sum_{H<G} \frac{|G_\alpha|}{|H_\alpha|} c_H t^G_{G_\alpha}(\underline{X}^\alpha) = \sum_{H<G} c_H t^G_{G_\alpha} t^{G_\alpha}_{H_\alpha}(\underline{X}^\alpha) = \sum_{H<G} c_H t^G_H t^H_{H_\alpha}(\underline{X}^\alpha) \in \mathcal{I}^G_{<G}.$$

So $\mathcal{I}^G_{<G} = \oplus_{\alpha\in\mathbb{N}_0^\Omega/G} R g_\alpha \cdot \mathrm{orb}_G(\underline{X}^\alpha)$ and $A^G = \mathcal{I}^G_{<G} + S$ with $\mathcal{I}^G_{<G} \cap S = g\cdot S$ with $g := \gcd(\ \frac{|G|}{|H|} \mid H < G)\cdot 1_R$. Hence

$$A^G/\mathcal{I}^G_{<G} \cong S/gS \cong R/gR\ [Y_1,\cdots Y_k],$$

where $Y_i = \mathfrak{n}_i$ is homogeneous of degree $|\mathcal{O}_i| \le |G|$. In the case of 'p - groups in characteristic p' we get:

Lemma 2.1.1 *If R has prime characteristic p and P is a p - group acting on Ω, then*

$$A(\Omega)^P = \mathcal{I}^P_{<P} \oplus S \text{ with } A^P/\mathcal{I}^P_{<P} \cong S \cong R[Y_1,\ldots,Y_k],$$

where k is the number of P - orbits on Ω and each Y_i is homogeneous of degree $\le |P|$. In particular

$$\beta(A(\Omega)^P/\mathcal{I}^P_{<P}) \le |P|.$$

We can use this result to prove some of the conjectures in the previous section, at least for the special type of 'p - permutation invariants'. Let $R := \mathbb{F}$ be a field of characteristic p dividing $|G|$ and V a finitely generated $\mathbb{F}G$ - module. Then V is called a p **- permutation module** or **trivial source module** if its restriction to any Sylow p - subgroup of G is an ordinary permutation module, or in other words, if a basis $\mathfrak{b}$ of V can be found, which is permuted by some Sylow p - group. As any two Sylow p - groups are conjugate in G, the property of being a p - permutation module does not depend on the choice of the Sylow group. Note also that V is a p - permutation module if and only if so is the dual V^*. It is a known fact in modular representation theory that V is a p - permutation module if and only if it is a direct summand of a permutation module for G (see for example [34], Proposition 27.3). Now Lemma 2.1.1 together with Lemma 1.3.3 gives:

Proposition 2.1.1 *Let $R := \mathbb{F}$ be a field of characteristic $p \mid |G|$, V a finitely generated $\mathbb{F}G$ - module and $A := \mathrm{Sym}(V^*)$ the symmetric algebra of the dual module V^*. If V is a p - permutation module and P is a Sylow p - group of G, then $\beta(A^Q/\mathcal{I}^Q_{<Q}) \le |Q|$ for each subgroup $Q \le P$. In particular Conjecture 1.3.2 holds for $A = \mathrm{Sym}(V^*)$.*

To show that the second degree bound of Conjecture 1.3.6 holds in this case, we can argue in a similar way as in the proof of Lemma 1.3.3:
Let $f \in \mathcal{I}^{G,+}_{<P}$ be indecomposable. By the transitivity of relative transfers [1] we can assume that f is of the form $t^G_Q(h)$ with $Q < P$ and $h \in A^Q$ is a power product in norms $\mathfrak{n}_i$ corresponding to the Q - orbits on a chosen P - permutation basis of V. Each polynomial $F[T] := \prod_{g \in G:Q} (T - g(\mathfrak{n}_i)) \in A^G[T]$ has $\mathfrak{n}_i$ as a zero. Expansion of $F[T]$ shows that the power $\mathfrak{n}_i^{[G:Q]}$ lies in the A^G - span of the $\mathfrak{n}_i^j$ with $j < [G:Q]$. This allows for reductions of exponents in h and since the operator t^G_Q is A^G - linear, we can assume that these exponents do not exceed $|G:Q| - 1$. Hence the total degree of f can be assumed to be less or equal to $s \cdot (|G:Q| - 1)$, where s is the number of Q - orbits. Since $s \le d = \dim(V)$ and deg $\mathfrak{n}_i \le |Q|$ we conclude that $\beta(\mathcal{I}^G_{<P}) \le \max\{|G|, d \cdot (|G| - 1)\}$. Since V is a p - permutation module (or a trivial source module) if and only if V is a direct summand of a permutation module, we get

Proposition 2.1.2 *If the $\mathbb{F}G$ - module V is a trivial source module, then*

$$\beta(\mathrm{Sym}(V^*)^G) \le \max\{|G|, \dim(V) \cdot (|G| - 1)\}.$$

In 1994 M Goebel developed a general reduction technique for permutation invariants, which produces generators for $A(\Omega)^G$ of degree less or equal to $\frac{1}{2}|\Omega|(|\Omega| - 1)$ (see [15]). A very good description including all details of Goebel's algorithm and theorem can be found in [4] 3.10.2. Therefore I will only briefly sketch Goebel's result here.

Definition 2.1.2 *A function $\alpha \in \mathbb{N}_0^\Omega$ will be called* **special**, *if its image is an interval in $\mathbb{N}_0$ which includes 0, i.e. if $\alpha(\Omega) = [0, m_\alpha] = \{0, 1, 2, \cdots, m_\alpha\}$.*
Note that if α is special, then

$$|\alpha| = \sum_\omega \alpha(\omega) \le 0 + 1 + 2 + \cdots + (|\Omega| - 1) = \frac{1}{2}|\Omega|(|\Omega| - 1).$$

[1] $t^H_{U\,|A^U} = (t^H_Y \circ t^Y_U)_{|A^U}$ for $U \le Y \le H$

Let $e_i := \sum_{T \subseteq \Omega,\ |T|=i} \prod_{\omega \in T} X_\omega$ be the i'th elementary symmetric polynomial in $A(\Omega)$.

Theorem 2.1.3 *(M Goebel) Let $\mathcal{S} \subset \mathbb{N}_0^\Omega$ be the subset of special functions. Then $A(\Omega)^G$ is a finitely generated $A(\Omega)^{\Sigma_\Omega}$ - module with generating set*

$$\mathcal{S}^+ := \{\mathrm{orb}_G(\underline{X}^\alpha) \mid \alpha \in \mathcal{S}\}.$$

In particular

$$A(\Omega)^G = R[e_i,\ \mathcal{S}^+ \mid 1 \leq i \leq |\Omega|], \text{ and}$$

$$\beta(A(\Omega)^G) \leq \binom{|\Omega|}{2}.$$

Goebel also proved a refinement of his theorem for intransitive G - actions, which leads to the bound

$$\beta(A(\Omega)^G) \leq \sum_{j \in \underline{m}} \max\ \{|\Omega_j|, \binom{|\Omega_j|}{2}\},$$

if Ω is the disjoint union of G - sets $\Omega_1,\ \Omega_2,\ \cdots \Omega_k$.

2.2 The Noether Homomorphism

Special types of permutation invariants can be used to construct generators of arbitrary invariant rings, using ideas from Emmy Noether's paper [24]. Of particular interest are the *vector invariants* of symmetric groups, which we will now introduce.

Let $A(k,n)$ be the polynomial ring $R[X_{11},...,X_{k1},...,X_{1n},...,X_{kn}]$ in $k \times n$ variables and define the action of Σ_n on $A(k,n)$ by extending the permutation action $\sigma(X_{ij}) := X_{i\sigma(j)}$. The corresponding ring of invariants $A(k,n)^{\Sigma_n}$ is usually called the ring of (k - fold) **vector invariants**.
Let $\underline{Y} := (Y_1, \ldots, Y_k)$ be a 'vector of variables'; then the multivariate polynomial

$$G(\underline{X}_1, \ldots, \underline{X}_n; \underline{Y}) := \prod_{j=1}^{n}(1 + \sum_{i=1}^{k} X_{i,j} Y_i) \in A(k,n)^{\Sigma_n}[Y_1, \ldots, Y_k]$$

is called the **Galois - resolvent**. In Hermann Weyl's celebrated book 'Classical groups' [35] one can find a proof of the following

Theorem 2.2.1 *(Weyl) If $\mathbb{Q} \subseteq R$ then $A(k,n)^{\Sigma_n}$ is generated by the coefficients of the Galois - resolvent $G(\underline{X}_1, \ldots, \underline{X}_n; \underline{Y})$. They all have total degree $\leq n$, so $\beta(A(k,n)^{\Sigma_n}) \leq n$.*

The analogue of Weyl's theorem is false if $R = \mathbb{Z}$ or a field of characteristic $p \leq n$. This can be seen from the Σ_2 - invariant $\mathfrak{X} := (X_1 \cdots X_k)^+ := X_1 \cdots X_k + Y_1 \cdots Y_k$ of section 1.2.1, because $\mathfrak{X}$ is indecomposable over $\mathbb{Z}$ or $\mathbb{F}_2$ for all $k \in \mathbb{N}$. In [26] it was proved by D. Richman, that the analogue of Weyl's theorem holds if $n!$ is invertible in R (for a different proof, see 2.3). For arbitrary coefficients the following has been shown in [7]

Theorem 2.2.2 *$\beta(A(k,n)^{\Sigma_n}) \leq max\{n, k \cdot (n-1)\}$ with equality if $n = p^s$ and* char *$R = p$ or $R = \mathbb{Z}$.*

To make use of these results in the context of arbitrary invariant rings, consider a subgroup $H \leq G$ with index n and with set of left - cosets $G/H := \{H := g_1H, g_2G, \ldots, g_nH\}$. The left multiplication action of G on the set G/H gives rise to the the **Cayley - homomorphism**

$$c: \ G \to \Sigma_{G/H} \cong \Sigma_n, g \mapsto (g_iH \mapsto g_jH := gg_iH).$$

Suppose that $A := R[a_1, \ldots, a_d]$ and $A^H = R[b_1, \ldots, b_k]$ with $b_i \in \mathcal{M}_\beta(\mathbf{a})$ and $\beta := \beta(A^H, \mathbf{a})$. Then the map $X_{si} \mapsto g_i(b_s)$ defines a unique G - equivariant homomorphism $\nu : A(k,n) \to A$ of R - algebras. In fact, ν does not depend on the choice of the g_i and

$$\nu(g(X_{si})) = \nu(X_{sj}) = g_j(b_s) = gg_ih(b_s) = gg_i(b_s) = g\nu(X_{si}),$$

because $gg_i = g_jh^{-1}$ for a suitable $h \in H$. The map ν for $H = 1$ had been used in Emmy Noether's 1916 - paper to prove her degree bound in characteristic zero. It is therefore called the **Noether homomorphism**. We can use her original argument to show that the restriction $\nu_| : A(k,n)^{\Sigma_n} \to A^G$ is surjective, whenever n is invertible in R:
In that case for each $f = f(b_1, \ldots, b_k) \in A^G \leq A^H$ there is a polynomial

$$F := \frac{1}{n}(f(X_{11}, X_{21}, \ldots, X_{k1}) + \ldots + f(X_{1n}, X_{2n}, \ldots, X_{kn})) \in A(k,n)^{\Sigma_n}$$

which satisfies

$$\nu(F) = \frac{1}{n}(f(g_1(b_1), g_1(b_2), \ldots, g_1(b_k)) + \ldots + f(g_n(b_1), g_n(b_2), \ldots, g_n(b_k))$$

$= \frac{1}{n}(g_1f(b_1, b_2, \ldots, b_k) + \ldots + g_nf(b_1, b_2, \ldots, b_k)) = f.$

Let $\beta(k,n) := \beta(A(k,n)^{\Sigma_n})$ and $A(k,n)^{\Sigma_n} = R[F_1,\dots,F_s]$ with $F_i \in \mathcal{M}_{\beta(k,n)}(\mathbf{X})$, then $A^G = R[\nu(F_1),\dots,\nu(F_s)]$ with $\nu(F_i) \in \mathcal{M}_{\beta(k,n)\beta}(\mathbf{a}) \cap A^G$. In particular if the index $n = [G:H]$ is invertible in R, then

$$\beta(A^G,\mathbf{a}) \leq \beta(k,n)\beta(A^H,\mathbf{a}).$$

Together with 2.2.1 (or [26]) and 2.2.2 we get:

Theorem 2.2.3 *Let A be an R - algebra as above and $H \leq G$ with $[G:H]$ invertible in R and $A^H = R[b_1,\dots,b_k]$ with $b_i \in A^H \cap \mathcal{M}_b(\mathbf{a})$ and $b := \beta(A^H,\mathbf{a})$. Then*

$$\beta(A^G,\mathbf{a}) \leq \max\{[G:H], k\cdot([G:H]-1)\}\beta(A^H,\mathbf{a}).$$

In particular, if A^H is finitely generated then so is A^G. If moreover $[G:H]!$ is invertible in R, then

$$\beta(A^G,\mathbf{a}) \leq |G:H|\beta(A^H,\mathbf{a}).$$

If p is a prime and R is of characteristic p, then we can take $H = P$, a Sylow - p group of G. Since the index $[G:P]$ is invertible, we can apply 2.2.3 and construct A^G from A^P via vector invariants. So in modular invariant theory the most serious problem is to construct invariant rings of p - groups in characteristic $p > 0$. Gregor Kemper developed general construction algorithms, which work for arbitrary finite groups (see [17]). Current research is investigating enhanced methods for p - groups ([30], [29]). But note that a bound for the degrees *and the numbers of generators* for A^P is needed to obtain a degree bound for A^G via 2.2.3.

2.3 Weyl's Theorem on Vector Invariants

In this section we will give a proof of Hermann Weyl's **Main Theorem on vector invariants** of the symmetric group, which is a generalized version of the theorem on symmetric polynomials. The result is beautiful and interesting in its own right, and can be used to derive 'conceptually simple' fundamental systems for A^G, provided that all natural numbers $m \leq |G|$ are invertible in R. Again this approach dates back to Emmy Noether's 1916 paper ([24]), where she used it in the situation $R = \mathbb{C}$.

The following combinatorial lemma is a straightforward generalization of the identity

$$XY = \frac{1}{2}[(X+Y)^2 - X^2 - Y^2].$$

Lemma 2.3.1 *For $a_1, \ldots, a_n \in A$ one has:*

$$(-1)^n n! \cdot a_1 \ldots a_n = \sum_{I \subseteq \underline{n}} (-1)^{|I|} (\sum_{i \in I} a_i)^n.$$

Proof:

$$\sum_{I \subseteq \underline{n}} (-1)^{|I|} (\sum_{i \in I} a_i)^n = \sum_{I \subseteq \underline{n}} (-1)^{|I|} \sum_{\alpha \in \mathbb{N}_0^I, |\alpha| = n} \binom{n}{\alpha_{i_1}, \ldots, \alpha_{i_{|I|}}} \underline{a}^\alpha =$$

$$\sum_{\beta \in \mathbb{N}_0^n,\ |\beta| = n} \binom{n}{\beta_1, \cdots, \beta_n} \underline{a}^\beta \sum_{I \subseteq \underline{n},\ \mathrm{supp}(\beta) \subseteq I} (-1)^{|I|} =$$

$$(-1)^n \binom{n}{1, \ldots, 1} \underline{a}^{\mathbf{1}} = (-1)^n n! \cdot a_1 \ldots a_n.$$

The latter equation holds because $\sum_{I \subseteq \underline{n},\ \mathrm{supp}(\beta) \subseteq I} (-1)^{|I|} = (-1)^n$, if $\mathrm{supp}(\beta) = \underline{n}$ and $= 0$ otherwise. $\diamond$

Definition 2.3.2 *(Polarization) For $f \in R[X_1, \ldots, X_n]$ and $\mu \in \mathbb{N}_0^k$ we define*

$$\mathrm{Pol}(f) := f(X_{11} + \ldots + X_{k1},\ X_{12} + \ldots + X_{k2},\ \ldots,\ X_{1n} + \ldots + X_{kn}) \in A(k, n)$$

and $\mathrm{Pol}(f)_\mu$ to be the homogeneous component of multi degree μ.

Obviously $f \in R[X_1, X_2, \ldots, X_n]^{\Sigma_n}$ implies $\mathrm{Pol}(f)_\mu \in A(k, n)^{\Sigma_n}$. If f is homogeneous of degree m, then $\mathrm{Pol}(f)_\mu$ is homogeneous of total degree m and $\mathrm{Pol}(f)_\mu = 0$ if $|\mu| \neq m$. It is straightforward to see that the polarized elementary symmetric polynomials $\mathrm{Pol}(e_t)_\mu$ are precisely the coefficients of the Galois resolvent

$$G(\underline{X}_1, \cdots, \underline{X}_n; \underline{Y}) = \prod_{i=1}^n (1 + \sum_{s=1}^k X_{si} Y_s).$$

For $t \in \mathbb{N}$ let $e_t^{(n)}$ denote the t - th elementary symmetric polynomial in n - variables, i.e.

$$e_t^{(n)} := \sum_{\substack{I \subseteq \underline{n} \\ |I| = t}} \prod_{i \in I} X_i.$$

Then we have the recursion formula $e_t^{(n)} = e_t^{(n-1)} + e_{t-1}^{(n-1)} X_n$.

(e.g. for $n = 4$:)
$e_1^{(4)} = X_1 + \ldots + X_4 = e_1^{(3)} + X_4$

$e_2^{(4)} = X_1X_2 + \ldots + X_3X_4 = e_2^{(3)} + X_4e_1^{(3)}$
$e_3^{(4)} = X_1X_2X_3 + \ldots + X_2X_3X_4 = e_3^{(3)} + X_4e_2^{(3)}$
$e_4^{(4)} = X_1X_2X_3X_4 = X_4e_3^{(3)}$.

Now polarization yields:

$$\mathrm{Pol}(e_t^{(n)})_\mu = \mathrm{Pol}(e_t^{(n-1)})_\mu + [\mathrm{Pol}(e_{t-1}^{(n-1)})(X_{1n} + X_{2n} + \cdots + X_{kn})]_\mu =$$

$$\mathrm{Pol}(e_t^{(n-1)})_\mu + \sum_{s=1}^{k} X_{sn} \cdot \mathrm{Pol}(e_{t-1}^{(n-1)})_{\mu-\delta_s},$$ [2]

with $\mathrm{Pol}(e_t^{(n-1)})_\mu = 0$ if $|\mu| > t$. Using an obvious induction argument, we observe

Lemma 2.3.3

$$\mathrm{Pol}(e_t^{(n-1)})_\mu \in R[\mathrm{Pol}(e_s^{(n)})_\nu, X_{in} \mid s \in \underline{n}, i \in \underline{k},\ \nu \in \mathbb{N}_0^k\ ].$$

Now we can formulate Weyl's theorem on vector invariants of Σ_n. Our proof is a generalization of the one in Weyl's book 'Classical groups' [35]. A different one can be found in [26], but theorem 1.2.3 facilitates the proof substantially.

Theorem 2.3.4 *Let $n!$ be invertible in R. Then the invariant ring*

$$R[X_{ij} \mid i \in \underline{k},\ j \in \underline{n}]^{\Sigma_n}$$

is generated by the polarized elementary symmetric polynomials $\mathrm{Pol}(e_m)_\mu$. In particular $\beta(R[X_{ij} \mid i \in \underline{n},\ j \in \underline{k}]^{\Sigma_n}) = n$.

Proof: The proof is by induction on n. The induction hypothesis, applied to Σ_{n-1} yields $A(k,n)^{\Sigma_{n-1}} = R[\mathrm{Pol}(e_m^{(n-1)})_\mu, X_{jn} \mid m \in \underline{n-1},\ \mu \in \mathbb{N}_0^k,\ j \in \underline{k}]$. Using 2.3.3 we see $A(k,n)^{\Sigma_{n-1}} = R[\mathrm{Pol}(e_m^{(n)})_\mu,\ X_{jn} \mid m \in \underline{n},\ j \in \underline{k},\ \mu \in \mathbb{N}_0^k]$. Since $n! = |\Sigma_n|$ is invertible in R, we can apply theorem 1.2.3. Its proof shows that $A(k,n)^{\Sigma_n} =$

$$R[t_{\Sigma_{n-1}}^{\Sigma_n}(\underline{b}^\alpha) \mid 0 \neq \alpha \in \mathbb{N}_0^{\mathbb{N}_0},\ |\alpha| \leq n],$$

where $b_i \in \{\mathrm{Pol}(e_m^{(n)})_\mu,\ X_{jn}, \ldots\}$. Since the $\mathrm{Pol}(e_m^{(n)})_\mu$'s are Σ_n - invariant, we have $A(k,n)^{\Sigma_n} =$

$$R[\mathrm{Pol}(e_m^{(n)})_\mu,\ t_{\Sigma_{n-1}}^{\Sigma_n}(\underline{X}_{*,n}^\alpha) \mid 0 \neq \alpha \in \mathbb{N}_0^k,\ |\alpha| \leq n],$$

[2] $\delta_s := (0, \cdots, 0, 1, 0, \cdots .0) \in \mathbb{N}_0^k$ with 1 in position s.

and it remains to show that the elements $t^{\Sigma_n}_{\Sigma_{n-1}}(\underline{X}^\alpha_{*,n})$ with $|\alpha| \leq n$ lie in $\mathcal{P} := R[\mathrm{Pol}(e^{(n)}_m)_\mu \mid m, \mu \ldots]$.

For that purpose we consider the power sums

$$p_m := X_1^m + X_2^m + \ldots + X_n^m \in R[X_1, \ldots, X_n]^{\Sigma_n}.$$

We have $\mathrm{Pol}(p_{|\alpha|})_\alpha =$

$$(\sum_{i=1}^n (X_{1i} + \ldots + X_{ki})^{|\alpha|})_\alpha = \sum_{i=1}^n (\sum_{\beta \in \mathbb{N}_0^k, |\beta| = |\alpha|} \begin{pmatrix} |\alpha| \\ \beta_1, \ldots, \beta_k \end{pmatrix} \underline{X}^\beta_{*,i})_\alpha =$$

$$\begin{pmatrix} |\alpha| \\ \alpha_1, \ldots, \alpha_k \end{pmatrix} t^{\Sigma_n}_{\Sigma_{n-1}}(\underline{X}^\alpha_{*,n}).$$

Since $|\alpha| \leq n$ and $n! \in R^*$, the multinomial coefficient

$$\begin{pmatrix} |\alpha| \\ \alpha_1, \ldots, \alpha_k \end{pmatrix} = \frac{|\alpha|!}{\alpha_1! \ldots \alpha_k!}$$

is invertible in R. By the main theorem on symmetric functions, the power sums p_m can be expressed over $\mathbb{Z}$ by elementary symmetric functions. Polarization of the corresponding formulae gives polynomial expressions for $\mathrm{Pol}(p_{|\alpha|})_\alpha$ in terms of the $\mathrm{Pol}(e_m)_\mu$'s. Finally we see that $t^{\Sigma_n}_{\Sigma_{n-1}}(\underline{X}^\alpha_{*,n}) \in \mathcal{P}$ and the proof is finished. $\diamond$

Now 2.3.4, together with the Noether homomorphism from 2.2 gives the following

Corollary 2.3.5 (Richman [26]) *Let $H \leq G$ such that $n := [G : H]$ with $n!$ invertible in R. Let $g_1, \cdots, g_n$ be a set of representatives for the left H - cosets in G and assume that $A^H = R[b_1, b_2, \cdots, b_k]$. Then A^G is generated as an R - algebra by the coefficients of the specialized Galois resolvent*

$$\phi(A^G)(\underline{Y}) := \prod_{i=1}^n (1 + \sum_{\ell=1}^k g_i(b_\ell) Y_\ell).$$

In particular for $A := R[a_1, \cdots, a_d]$ one has

$$\beta(A^G, \mathbf{a}) \leq [G : H] \beta(A^H, \mathbf{a}).$$

Chapter 3

On the Structure of Invariant Rings

In this chapter we want to take up the question from 1.1.

- Let A be a polynomial ring over a field $R = \mathbb{F}$, say, and G a finite group acting on A via graded $\mathbb{F}$ - algebra automorphisms. How 'far away' is A^G from being a polynomial ring?

The fact that not all invariant rings are polynomial rings can be seen from the example $G = \langle g \rangle \cong C_2$ acting on $A := \mathbb{F}[X, Y]$ by $g(X) = -X$ and $g(Y) = -Y$ (with $\mathbb{F}$ of characteristic $\neq 2$). It is easy to see that $A^G = \mathbb{F}[X^2, Y^2, XY]$, which is not isomorphic to a polynomial ring, because it is not factorial. Indeed X^2, Y^2 and XY are different irreducibles in $\mathbb{F}[X, Y]^G$ giving a non - unique factorization $X^2Y^2 = (XY)^2$. However, A^G contains a polynomial subalgebra $\mathfrak{P} = \mathbb{F}[X^2, Y^2]$ such that $A^G = \mathfrak{P} \cdot 1 \oplus \mathfrak{P} \cdot XY$ is free of rank 2 as $\mathfrak{P}$ - module. On the other hand the map $X_1 \mapsto X^2, X_2 \mapsto Y^2, X_3 \mapsto XY$ extends to a surjective homomorphism of algebras $\mathbb{F}[X_1, X_2, X_3] \to A^G$ which shows that

$$A^G \cong \mathbb{F}[X_1, X_2, X_3]/(X_1X_2 - X_3^2).$$

Let us start with some special geometric features that are due to the fact that G is a **finite group**.

3.1 Geometric Aspects

Historically a major motivation for invariant theory comes from the analysis of symmetries on affine algebraic varieties. One way to set up the scene goes as follows: Let A be an **affine algebra**, i.e. a finitely generated commutative $\mathbb{F}$ - algebra without nonzero nilpotent elements. Let $\bar{\mathbb{F}}$ be the algebraic closure and $\hat{A} := A \otimes_{\mathbb{F}} \bar{\mathbb{F}}$; then using Hilbert's Nullstellensatz, the set $\hat{Y}$ of maximal ideals in $\hat{A}$ can be viewed as an affine algebraic variety in the usual sense of algebraic geometry, with $\hat{A} := \mathcal{O}(\hat{Y})$ as corresponding algebra of regular functions. In a similar way one can view the set Y of maximal ideals of A as an $\mathbb{F}$ - variety and, even more generally, consider the "affine scheme" $X := \text{spec}(A)$ consisting of all prime ideals $\mathrm{p} \triangleleft A$, $\mathrm{p} \neq A$. Every $\mathbb{F}$ - algebra automorphism of A induces a (dual) automorphism of X and for a group G of automorphisms of A one can define a **categorical quotient** $X//G$. Then a natural question is, whether $X//G$ is again an affine algebraic variety. A necessary condition for this is, that the invariant ring

$$A^G := \{a \in A \mid g(a) = a \ \forall \ g \in G\}$$

is a finitely generated $\mathbb{F}$ - algebra. In this case the prime ideal spectrum spec A^G is a natural candidate for $X//G$ and one might hope that $X//G$ coincides with the set - theoretic quotient, namely the orbit space X/G. For an arbitrary group neither does A^G have to be finitely generated, nor does the categorical quotient $X//G$ have to coincide with the 'geometric quotient' X/G, but if G is a finite group, then the situation is much better (see e.g. [1] 1.4.4):

From now on let G be a finite group. Note that A is integral and finite over A^G and A as well as A^G are integrally closed in their quotient fields Quot(A) and Quot$(A)^G$ respectively. In particular A^G and A have the same Krull - dimension [1], which is equal to the dimension of the algebraic variety $\hat{Y}$. Moreover Quot(A) $\geq$ Quot$(A)^G$ is a Galois extension with Galois group G. The dual i^* of the inclusion map $i : A^G \hookrightarrow A$ is the map spec $A \to$ spec A^G, $p \mapsto p \cap A^G$. In this situation the classical 'lying over', 'going up', 'going down' and transitivity theorems of commutative algebra apply (see [1] Theorem 1.4.4. on pg. 7). We have $A^G \otimes_{\mathbb{F}} \bar{\mathbb{F}} = \hat{A}^G$ and the above statements also hold for $\hat{A}$ instead of A. Hence $\max - \text{spec } \hat{A}^G$ can be identified with the set $\hat{Y}/G$ of G - orbits on $\hat{Y}$ and $\hat{i}^*$, the dual of the inclusion $\hat{A}^G \hookrightarrow \hat{A}$ can be identified with the orbit map $y \mapsto y^G$. Thus a strict geometric quotient $\hat{Y}/G$ exists and the invariant ring $\hat{A}^G$ can be interpreted as the ring of regular functions $\mathcal{O}(\hat{Y}/G)$ of the quotient variety (e.g. see [14] Theorem 5.52 pg. 187 or [1] pg.8). Notice that all G - orbits are closed in the Zariski topology since G is finite. The orbit map $\hat{i}^*$, being the comorphism of a finite embedding, is surjective and closed, i.e. sends closed irreducible subvarieties of $\hat{Y}$ to closed irreducible subvarieties of $\hat{Y}/G$.

[1] recall that the Krull - dimension Dim(A) is the maximal length of a properly ascending chain of prime ideals of A.

Now let us return to our usual (linear) setup. To avoid trivialities, we assume that $G \leq \mathrm{GL}(V)$ with V a finite - dimensional $\mathbb{F}$ - vector space with dual module $V^* = \oplus_{i=1}^n \mathbb{F}X_i$ and $A = \mathbb{F}[V] = \mathrm{Sym}(V^*) = \mathbb{F}[X_1, \cdots, X_n]$. Since G is finite, we know that A^G is a finitely generated $\mathbb{N}_0$ - graded $\mathbb{F}$ - algebra with degree zero component isomorphic to $\mathbb{F}$. Such an algebra is called **graded connected over** $\mathbb{F}$. Many arguments in invariant theory work in this wider context of graded connected algebras. In the following we will, unless explicitly stated otherwise, use A to denote $\mathrm{Sym}(V^*)$ and B to denote a general finitely generated graded connected sub algebra B such that the B - module A is finitely generated. Typically we have in mind $B = A^G$.

3.2 Hilbert - Series

Let M be a finitely generated $\mathbb{N}_0$ - graded B - module. Recall that the **Hilbert - series** (or Poincaré - series) of M is defined to be the power series

$$H(M,t) := \sum_{i \geq 0} \dim_{\mathbb{F}}(M_i)\ t^i,$$

where M_i denotes the i'th homogeneous component of M. From the geometric series $1 + t + t^2 + \cdots = \frac{1}{1-t}$ and the rule $H(M \otimes_{\mathbb{F}} N, t) = H(M,t) \cdot H(N,t)$ one can easily see that $H({}_AA, t) = \frac{1}{(1-t)^n}$. In general for $B = \mathbb{F}[b_1, \cdots, b_m]$ one has $H({}_BB, t) = \frac{f}{\prod_{i=1}^m (1-t^{s_i})^n}$, with $f \in \mathbb{Z}[t]$ and s_i being the degrees of the homogeneous generators b_i.

There is a beautiful theorem about the Hilbert - series of non - modular invariant rings and modular permutation invariants. Assume that $\mathrm{char}(\mathbb{F})$ does not divide $|G|$ and let V be a finitely generated $\mathbb{F}G$ - module. It is known from representation theory of finite groups, that there is a 'Brauer lift' $\hat{V}$ to zero characteristic: in brief terms, this is an $\mathcal{O}G$ - module which is free as an $\mathcal{O}$ - module, where $\mathcal{O}$ is a suitable discrete valuation ring with quotient field K of characteristic zero and maximal ideal $\mathfrak{P} \lhd \mathcal{O}$ such that $\mathcal{O}/\mathfrak{P} \cong \mathbb{F}$ and $\hat{V} \otimes_{\mathcal{O}} \mathbb{F} \cong V$. In particular for each $g \in G$ there is a 'lift' of $\det g_{|V} \in \mathbb{F}$ to $\det g_{|\hat{V}} \in \mathcal{O}$.

Theorem 3.2.1 *(Molien) If* $\mathrm{char}(\mathbb{F})$ *does not divide* $|G|$, *then for* $A = \mathbb{F}[V]$ *one has*

$$H(A^G, t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(1 - g_{|\hat{V}^*} t)}.$$

If $\mathbb{F}$ *is arbitrary and* $G \leq \Sigma_\Omega$, *then*

$$H(\mathbb{F}[\mathbb{F}^\Omega]^G, t) = H(\mathbb{C}[\mathbb{C}^\Omega]^G, t).$$

Proof: Assume first that $\mathrm{char}(\mathbb{F}) = 0$. The dimensions of homogeneous fixed point spaces do not change with extension of scalars, so we can assume that $\mathbb{F}$ is algebraically closed and therefore we can use character theory: the dimension of A_m^G is equal to the multiplicity of the trivial G - module in the $\mathbb{F}G$ - module A_m, so it is the inner product $\langle \chi_{A_m}, 1_G \rangle$. Our assumptions on $\mathbb{F}$ imply that all elements $g \in G$ are diagonalisable on V and hence as well on A_m. If $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of g on V (with multiplicities), then the products $\underline{\lambda}^\alpha$ with $\alpha \in \mathbb{N}_0^n$ and $|\alpha| = m$ are exactly the eigenvalues of g. We conclude

$$H(A^G, t) = \sum_{m=0}^{\infty} \langle \chi_{A_m}, 1_G \rangle t^m = \frac{1}{|G|} \sum_{m=0}^{\infty} \sum_{g \in G} \sum_{\alpha \in \mathbb{N}_0^n,\ |\alpha| = m} \underline{\lambda}^\alpha(g) t^m =$$

$$\frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{n} (1 + \lambda_i t + \lambda_i^2 t^2 + \ldots) = \frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{n} \frac{1}{1 - \lambda_i t}.$$

If $\mathbb{F}$ has positive characteristic not dividing $|G|$, we replace V^* by a Brauer lift $\hat{V}^*$. Then $\hat{A} := \mathrm{Sym}(\hat{V}^*)$ is a Brauer lift of A. Moreover the group order $|G|$ is invertible in $\mathcal{O}$, hence we get

$$A_m^G = t_1^G(A_m) = t_1^G\left(\hat{A}_m \otimes_{\mathcal{O}} \mathbb{F}\right) = t_1^G(\hat{A}_m) \otimes_{\mathcal{O}} \mathbb{F} \cong (\hat{A}_m)^G \otimes_{\mathcal{O}} \mathbb{F}.$$

Similarly we see for $A_K := \hat{A} \otimes_{\mathcal{O}} K$: $(A_K)_m^G \cong (\hat{A}_m)^G \otimes_{\mathcal{O}} K$. Hence $\dim_{\mathbb{F}}(A_m^G) = \dim_K\left((A_K)_m^G\right)$, which shows that the Hilbert series of A^G and $(A_K)^G$ coincide and are given by Molien's formula.

Now let $\mathbb{F}$ be arbitrary but $V = \mathbb{F}^\Omega$ a G - permutation module. Then each A_m is a permutation module as well and the dimension of A_m^G is equal to the number of G - orbits on the set $\{\alpha \in \mathbb{N}_0^\Omega \mid |\alpha| = m\}$. This number is obviously independent of the characteristic of $\mathbb{F}$. $\diamond$

It has been shown by Gregor Kemper that for p - permutation modules one also has $H(\mathbb{F}[V]^G, t) = H(\mathbb{F}[\hat{V}]^G, t)$ with Brauer lift $\hat{V}$([20]). Hence the Hilbert series of direct summands of permutation modules can be determined using Molien's formula.

3.3 Homogeneous Systems of Parameters

There are various ways to measure how close B comes to be a polynomial algebra. A very intuitive way of comparison is to exhibit a maximal polynomial subalgebra $\mathfrak{P} \leq B$ such that the module ${}_{\mathfrak{P}}B$ is finitely generated. This is always possible by Noether's normalization lemma and it can be shown that the transcendence degree of $\mathfrak{P}$ is equal to the Krull - dimension of B, i.e. $\mathfrak{P} = \mathbb{F}[h_1, \cdots, h_n]$ with algebraically independent elements $h_1, \cdots, h_n$ that can be chosen to be homogeneous. They form a **homogeneous system of parameters** (hsop). In fact a set $\{h_1, \cdots, h_n\}$ of homogeneous elements of positive degree forms an hsop, if and only if $B/(h_1, \cdots, h_n)B$ is a finite - dimensional $\mathbb{F}$ - vector space. Let $\{h_1, \cdots, h_n\}$ be an hsop with $d_i := \deg\, h_i$ and let $s_{n+1}, \cdots, s_k$ be generators for the $\mathfrak{P}$ - module B. Then the h_i are also called **primary generators** of B with corresponding **secondary generators** s_j.

Note that, since A is finite over B, an hsop for B is also an hsop for A. If $\mathfrak{P} \leq B \leq A = \mathbb{F}[V]$, then the $\mathfrak{P}$ - **module** A is free of finite rank , hence ${}_{\mathfrak{P}}A \cong \mathfrak{P} \otimes_{\mathbb{F}} W$ with a finite dimensional graded $\mathbb{F}$ - vector space W of dimension d, say, which is also the degree of the quotient field extension $[\mathrm{Quot}(A) : \mathrm{Quot}(\mathfrak{P})]$. We then get for the Hilbert - series, $H(A,t) = H(\mathfrak{P}, t) \cdot H(W,t)$ and we conclude

$$H(W,t) = \frac{\prod_{i=1}^{n} (t^{d_i} - 1)}{(t-1)^n} = \prod_{i=1}^{n} (1 + t + \cdots + t^{d_i - 1}),$$

hence $d := \dim_{\mathbb{F}}(W) = \prod_{i=1}^{n} d_i$. Let $\ell := [\mathrm{Quot}(B) : \mathrm{Quot}(\mathfrak{P})]$, then $\ell = d/m$ with $m = [\mathrm{Quot}(A) : \mathrm{Quot}(B)]$ and the module ${}_{\mathfrak{P}}B$ is finitely generated *free* if and only if it can be generated by ℓ homogeneous elements. Since $\mathrm{Quot}(A)$ is Galois over $\mathrm{Quot}(A^G)$ with Galois - group G, we get:

Lemma 3.3.1 *Let $\mathfrak{P} = \mathbb{F}[h_1, \cdots, h_n] \leq A^G \leq A$ with hsop $h_1, \cdots, h_n$ of A^G of degrees $d_1, \cdots, d_n$. Then the degree of the extension of quotient fields $\mathrm{Quot}(\mathfrak{P}) \hookrightarrow \mathrm{Quot}(A)$ is equal to the product $d := \prod_{i=1}^{n} d_i$. In particular $|G|$ divides d. Moreover A^G is a finitely generated free $\mathfrak{P}$ - module [2] if and only if ${}_{\mathfrak{P}}A^G$ is generated by $\ell = \frac{d}{|G|}$ homogeneous elements.*

Using this lemma and the fact that polynomial algebras are integrally closed, one can now prove the following criterion for invariant rings to be polynomial algebras:

Theorem 3.3.2 *Let $A := \mathbb{F}[V]$ with $\mathbb{F}G$ - module V of dimension n. Then the following are equivalent:*

1. *A^G is a polynomial ring.*

2. *There is an hsop $\{h_1, \cdots, h_n\}$ of A^G with $|G| = \prod_{i=1}^{n} \deg\, h_i$.*

[2] this is in fact equivalent to A^G being a Cohen - Macaulay algebra

In particular $A^G = \mathbb{F}[h_1, \cdots, h_n]$ *implies* $|G| = \prod_{i=1}^n \deg h_i$.

Proof: Let $\{h_1, \cdots, h_n\} \subseteq A^G$ be an hsop with $\deg h_i = d_i$ and $\mathfrak{P} := \mathbb{F}[h_1, \cdots, h_n]$. Then $[\mathrm{Quot}(A) : \mathrm{Quot}(\mathfrak{P})] = d := \prod_{i=1}^n d_i$. Now the implication '1) $\Rightarrow$ 2)' follows from 3.3.1. To prove '2) $\Rightarrow$ 1)' assume that $d = |G|$. Then

$$d = [\mathrm{Quot}(A) : \mathrm{Quot}(\mathfrak{P})] = |G| \cdot [\mathrm{Quot}(A)^G : \mathrm{Quot}(\mathfrak{P})]$$

implies $\mathrm{Quot}(\mathfrak{P}) = \mathrm{Quot}(A)^G$. The polynomial ring $\mathfrak{P}$ is factorial and therefore integrally closed, hence

$$A^G = \mathrm{Quot}(A)^G \cap A = \mathrm{Quot}(\mathfrak{P}) \cap A = \mathfrak{P}.$$

$\diamond$

Consider the elementary symmetric polynomials $e_i \in \mathbb{F}[X_1, \cdots, X_n]$. The product of their degrees is $n! = |\Sigma_n|$, hence 3.3.2 contains an algebraic proof for the fact that $\mathbb{F}[X_1, \cdots, X_n]^{\Sigma_n} = \mathbb{F}[e_1, \cdots, e_n]$. In particular the elementary symmetric functions form a 'generic hsop' for each ring of permutation invariants $\mathbb{F}[X_1, \cdots, X_n]^G$ with $G \leq \Sigma_n$.

If $\mathbb{F} = \mathbb{F}_q$ is finite of order q and $\tilde{G} := \mathrm{GL}(V)$, then

$$\mathbb{F}[V]^{\tilde{G}} = \mathbb{F}[d_{i,n} \mid i = 1, \cdots, n]$$

where the **Dickson - invariants** $d_{i,n}$ are defined by

$$F_n(T) := \prod_{v \in V^*} (T - v) = \sum_{i=0}^n d_{i,n} T^{q^{n-i}}$$

with $d_{0,n} = 1$. Of course it has to be shown that $F_n(T)$ is a sparse polynomial as described. An elementary way to see this has been suggested by C. Wilkerson [36]: consider the determinant

$$\Delta_n(T) = \begin{vmatrix} X_1 & \cdots & X_n & T \\ X_1^q & \cdots & X_n^q & T^q \\ \cdots & \cdots & \cdots & \cdots \\ X_1^{q^n} & \cdots & X_n^{q^n} & T^{q^n} \end{vmatrix}.$$

It is clear that $\Delta(v) = 0$ for each $v \in V$; comparing the coefficients at T^{q^n} we get $\Delta_n(T) = \Delta_{n-1}(X_n) \cdot F_n(T)$. The needed fact that the 'constant' $\Delta_{n-1}(X_n)$ is nonzero follows for example from the normal basis theorem for the finite field extension $V \cong \mathbb{F}_{q^n} \geq \mathbb{F}_q$. Now for $i > 0$, $\deg d_{n-i,n} = q^n - q^i$, hence $\prod_{i=0}^{n-1} \deg d_{n-i,n} =$

$|\mathrm{GL}(V)|$ and clearly $A = \mathbb{F}[V]$ is finite over $\mathbb{F}[d_{i,n} \mid i = 1, \cdots, n]$. Hence the $d_{i,n} \in \mathbb{F}[V]^{\mathrm{GL}(V)}$ form an hsop and 3.3.2 shows that

$$\mathbb{F}[V]^{\mathrm{GL}(V)} = \mathbb{F}[d_{i,n} \mid i = 1, \cdots, n].$$

For any subgroup $G \leq \mathrm{GL}(V)$, $\mathbb{F}[V]^G$ is a finite extension of $\mathbb{F}[V]^{\mathrm{GL}(V)}$, therefore the $d_{i,n}$ form 'generic hsops' for invariant rings of finite groups over finite fields.

The arguments above contain a general recipe to prove that an invariant ring is polynomial. Following C. Wilkerson we condense them into the following three steps:

- Guess a set of n homogeneous algebra generators $a_1, \cdots, a_n \in A^G$.
- Show that A is finite over $\mathbb{F}[a_1, \cdots, a_n]$.
- Show that the degree of $\mathrm{Quot}(A)$ over $\mathbb{F}(a_1, \cdots, a_n)$ equals $|G|$, e.g. by showing that $\prod_{i=1}^n \deg a_i = |G|$. [3]

Besides the cases Σ_n and $\mathrm{GL}(V)$ one can for example determine the invariant rings $\mathbb{F}[V]^{\mathrm{SL}(V)}$ and $\mathbb{F}[V]^U$ in that way, with U being the full upper triangular subgroup in $\mathrm{GL}(V)$. To find hsops in the general case, one can use a construction of E. Dade, which always gives an hsop whose elements have degrees not exceeding $|G|$. Dade's original construction works over an algebraically closed field, but can be generalized with a 'scalar extension' argument.

3.4 Cohen - Macaulay Property

One can expect to measure the 'distance' of A^G from being polynomial by the complexity of the module - structure of ${}_{\mathfrak{P}}A^G$, which of course is free of rank one in case $A^G = \mathfrak{P}$ is a polynomial ring. But the choice of hsop's is far from unique, as can be seen by expressing $\mathbb{F}[X_1, \cdots, X_n]$ as a finitely generated module over the polynomial subalgebra $\mathbb{F}[X_1^{s_1}, \cdots, X_n^{s_n}]$ for $s_i \in \mathbb{N}$. Hence we look for more 'intrinsic' ring theoretic properties to compare $\mathbb{F}$ - algebras.

For each choice of hsop the module ${}_{\mathfrak{P}}\mathbb{F}[X_1, \cdots, X_n]$ is free of finite rank over $\mathfrak{P}$. In the context of graded connected algebras, this can be used as a defining property of a **Cohen - Macaulay algebra**. More precisely, if a graded connected algebra B is free over some hsop, it is so over every hsop. A different definition of the Cohen - Macaulay property, which is equivalent in the case of connected algebras, uses

[3] It has been shown by Kemper ([17]) that it suffices to verify that the a_i are algebraically independent.

the notion of **regular sequences** and **depth**. If B is graded connected and M is a finitely generated $\mathbb{N}_0$ - graded B - module, then a sequence $\underline{b} := (b_1, b_2, \cdots, b_k)$ of homogeneous elements in B^+ is called **regular on** M, or an M - sequence for short, if multiplication with b_i on $M/(b_1, b_2, \cdots, b_{i-1})M$ is injective for each $i \leq k$. If $I \leq B^+$ is a homogeneous ideal, then all maximal M - sequences in I have the same length, which is called grade(I, M), or depth M if $I = B^+$. In general depth $M \leq \text{Dim } M := \text{Dim } (B/\text{ann } M)$ [4] and one calls M a **Cohen - Macaualay module**, if equality holds. It turns out that B is a Cohen - Macaualay algebra if and only if the regular module ${}_BB$ is a Cohen - Macaulay module. Clearly a polynomial algebra $\mathbb{F}[X_1, \cdots, X_n]$ is a Cohen - Macaulay algebra (CM - algebra) with maximal regular sequence $(X_1, X_2, \cdots, X_n)$. From 3.3.1 we know that A^G is Cohen - Macaulay, if and only if it has an hsop of degrees $d_1, \cdots, d_n$ with exactly $d_1 d_2 \cdots d_n/|G|$ many secondary generators. The following results give a 'CM - criterion' that does not require information on hsops and generators:

Theorem 3.4.1 *Let $B \leq A$ be such that ${}_BA$ is a finitely generated B - module with ${}_BB$ as direct summand. Then B is a Cohen - Macaulay algebra.*

Proof: Let $\mathfrak{P} \leq B \leq A$ with $\mathfrak{P}$ generated by an hsop of B. Since A is Cohen - Macaulay, ${}_{\mathfrak{P}}A$ is finitely generated and free, hence ${}_{\mathfrak{P}}B$, as a summand of ${}_{\mathfrak{P}}A$ is projective. But for a graded connected algebra like $\mathfrak{P}$ all f.g. projective graded modules are free (see [1], Lemma 4.1.1) and we conclude that ${}_{\mathfrak{P}}B$ is free. Hence B is Cohen - Macaulay. $\diamond$

If $|G|$ is invertible in $\mathbb{F}$, then A^G is a direct summand of A as A^G - module and we immediately obtain the theorem of Eagon and Hochster:

Corollary 3.4.2 *If* char $\mathbb{F}$ *does not divide $|G|$, then A^G is a Cohen - Macaulay algebra.*

The CM - property plays a significant role in the description of an algebra by 'generators and syzygies': Let $\{h_1, \cdots, h_n\}$ be an hsop of B; then B is finitely generated, by $s_{n+1}, \cdots, s_{n+\ell}$ say, as $\mathfrak{P}$ - module. This gives rise to an obvious epimorphism of $\mathfrak{P}$ - modules $\chi : \mathfrak{P}^\ell \to B$. On the other hand one can pick a subset $\{a_{n+1}, \cdots, a_\mu\} \subseteq \{s_{n+1}, \cdots, s_{n+\ell}\}$ such that $B = \mathbb{F}[h_1, \cdots, h_n, a_{n+1}, \cdots, a_\mu]$. Then there is an obvious ring epimorphism $\phi : \mathbb{F}[X_1, \cdots, X_\mu] \to B$, giving B another structure as module over some polynomial ring. To find out what is 'intrinsic' about these module structures, let $\mathcal{F}$ be some polynomial algebra, $\theta : \mathcal{F} \to B$ an algebra homomorphism such that B is a finitely generated $\mathcal{F}$ - module via θ, and let $\theta_0 : \mathcal{F}^{r_0} \to B$ be an $\mathcal{F}$ - module epimorphism. Since $\mathcal{F}$ is Noetherian, the

[4] ann $M := \{b \in B \mid bm = 0, \ \forall m \in M\}$

kernel K of θ_0 is finitely generated and we can find an $\mathcal{F}$ - module epimorphism $\theta_1 : \mathcal{F}^{r_1} \to K$. The kernel of θ_1 is a finitely generated submodule of $\mathcal{F}^{r_1}$ and we can iterate the process, which leads to a **free resolution** $\mathcal{F}^*$ of B as $\mathcal{F}$ - module, i.e. to an exact sequence

$$\cdots \to \mathcal{F}^{r_t} \to \mathcal{F}^{r_{t-1}} \to \cdots \mathcal{F}^{r_1} \to \mathcal{F}^{r_0} \to B \to 0.$$

From Hilbert's syzygy - theorem it is known that the global dimension of $\mathcal{F}$ is equal to its Krull - dimension, which means that there is a 'minimal' free resolution

$$0 \to \mathcal{F}^{r_t} \to \mathcal{F}^{r_{t-1}} \to \cdots \mathcal{F}^{r_1} \to \mathcal{F}^{r_0} \to B \to 0$$

with $t \leq \mathrm{Dim}\ \mathcal{F}$. In fact the minimal number t_{min} is the **projective dimension** proj.dim $_{\mathcal{F}}B$ of B as an $\mathcal{F}$ - module. By the Auslander - Buchsbaum formula we get:

$$\mathrm{Dim}\ \mathcal{F} - \mathrm{proj.dim}\ _{\mathcal{F}}B = \mathrm{depth}\ B.$$

Thus the 'cohomological codimension' $\mathrm{Dim}\ \mathcal{F} - \mathrm{proj.dim}\ _{\mathcal{F}}B$ turns out to be an intrinsic property of B, namely the maximal length of a regular sequence in B^+. In other words, the **CM - defect** def $B := \mathrm{Dim}\ B - \mathrm{depth}\ B$ is equal to the projective dimension $\mathrm{proj.dim}_{\mathfrak{P}}\ B$ of B over any hsop. This of course is zero if and only if B is Cohen - Macaualay.

3.5 Non - CM Invariant Rings

In the modular situation, i.e. if the characteristic of $\mathbb{F}$ divides $|G|$, then A^G will in general not be a Cohen - Macaulay algebra. Following [6], this can be seen in the following way, which has been described in [6]:

Assume that $N \triangleleft G$ is a normal subgroup such that $G/N = \langle \bar{g} \rangle \cong C_p$ with $p = \mathrm{char}\ \mathbb{F}$. Then for $1 \leq i \leq p-1$ there is $j \in \mathbb{N}$ with $ij \equiv 1 \bmod p$ and we have

$$(\bar{g}^i - 1)A^N = (\bar{g}-1)(1+\bar{g}+\cdots+\bar{g}^{i-1})A^N \subseteq (\bar{g}-1)A^N = ((\bar{g}^i)^j - 1)A^N \subseteq (\bar{g}^i - 1)A^N,$$

hence the ideal $\mathcal{J} := (\bar{g}-1)A^N \cap A^G \triangleleft A^G$ is independent of the choice of the generator $\bar{g} \in G/N$. Moreover $\mathcal{J}$ is nonzero. To see this, note that by Galois theory $\mathrm{Quot}(A)^G < \mathrm{Quot}(A)^N$, hence $A^G < A^N$ and A^G is the kernel of the operator $\bar{g}-1$ on A^N. In particular there is $a \in A^N$ with $(\bar{g}-1)a \neq 0$. Since $(\bar{g}-1)^p a = (\bar{g}^p - 1)a = 0$, there is some $i \in \mathbb{N}$ with $(\bar{g}-1)^{i+1}a = 0 \neq (\bar{g}-1)^i a \in \mathcal{J}$.

Lemma 3.5.1 *([6])*

$$\mathrm{grade}(\mathcal{J}, A^G) = \min\{2, \mathrm{ht}(\mathcal{J})\}.$$

Proof: By contradiction we assume that $f_1, f_2, f_3 \in \mathcal{J}$ form a regular sequence. Then there are $a_1, a_2, a_3 \in A^N$ with $\bar{g}(a_i) - a_i = f_i$ for $i = 1, 2, 3$ and we have

$$0 = \begin{vmatrix} f_1 & f_2 & f_3 \\ f_1 & f_2 & f_3 \\ a_1 & a_2 & a_3 \end{vmatrix} = u_{23}f_1 + u_{31}f_2 + u_{12}f_3 \text{ with } u_{ij} := \begin{vmatrix} f_i & f_j \\ a_i & a_j \end{vmatrix}.$$

It is easy to see that $\bar{g}(u_{ij}) = u_{ij} \in A^G$ and the regularity of f_1, f_2, f_3 implies that $u_{12} \in (f_1, f_2)A^G$, so $a_2 f_1 - a_1 f_2 = u_{12} = r f_1 + s f_2$ with $r, s \in A^G$ which gives $(a_2 - r) f_1 = (a_1 + s) f_2$. Since the polynomial ring A is Cohen - Macaulay and finite over A^G, f_1, f_2 are part of a system of parameters for A and therefore regular. It is easy to see that this implies that f_1 and f_2 are coprime as polynomials. Hence f_1 divides $a_1 + s$ in A, i.e. $a_1 = q f_1 - s$. From this we get $f_1 = \bar{g}(a_1) - a_1 = f_1(\bar{g} - 1)(q)$, hence $(\bar{g} - 1)(q) = 1$ which is impossible. This shows that $\mathrm{grade}(\mathcal{J}, A^G) \leq 2$. In general one knows that $\mathrm{grade}(\mathcal{J}, A^G) \leq \mathrm{ht}(\mathcal{J})$. If $\mathrm{ht}(\mathcal{J}) = 1$, then $\mathcal{J}$ contains a regular element of A^G and $\mathrm{grade}(\mathcal{J}, A^G) = 1$. So assume that $\mathrm{ht}(\mathcal{J}) \geq 2$. Then there are homogeneous elements $f_1, f_2 \in \mathcal{J}$ with $\mathrm{ht}(f_1, f_2)A^G = 2 = \mathrm{ht}(f_1, f_2)A$ (the equality of heights, because A is finite over A^G). This implies that f_1 and f_2 are coprime in A, otherwise $f_i = d\tilde{f}_i$, $i = 1, 2$, with greatest common divisor $d \in A$, hence $(f_1, f_2)A \subseteq (d)A$ which would imply the contradiction $\mathrm{ht}(f_1, f_2)A^G \leq 1$. Now it follows that $(f_1, f_2) \subseteq A^G$ is a regular sequence: indeed a relation $r f_1 + s f_2 = 0$ in A^G implies that f_1 divides s in A but also in A^G. Hence $\mathrm{grade}(\mathcal{J}, A^G) \geq 2$ and the proof is complete. $\diamond$

As an application we get the following beautiful result

Theorem 3.5.2 *[Campbell, Hughes, Kemper, Shank, Wehlau][6] Let* $\mathrm{char}\, \mathbb{F} = p > 0$ *and let N be a normal subgroup of G with cyclic factor group $G/N \cong C_p$. Then for every $\mathbb{F}G$ - module V the ring of m - fold vector - invariants $\mathbb{F}[V^m]^G$ is not Cohen - Macaulay for $m \geq 3$.*

Proof: Using the notation above, the discussion in the beginning of this section shows that there is $a \in \mathbb{F}[V]^N$ with $0 \neq \bar{g}a - a \in \mathbb{F}[V]^G$. Let $a_1, \cdots, a_m$ be the elements in $\mathbb{F}[V^m]^N$ corresponding to a, with $f_i := \bar{g}a_i - a_i$. Then the sequence $(f_1, \cdots, f_m)$ is a partial hsop of $\mathbb{F}[V^m]^G$ whose elements lie in $\mathcal{J}$. From 3.5.1 we know that $(f_1, \cdots, f_m)$ cannot be regular if $m \geq 3$. Since in a CM - algebra each partial hsop forms a regular sequence, we conclude that $\mathbb{F}[V^m]^G$ is not CM for $m \geq 3$. $\diamond$

It has been shown by Gregor Kemper that for every finite group G of order divisible by $p = \mathrm{char}\ \mathbb{F}$ and for every finite - dimensional $\mathbb{F}G$ - module V there is some $m \in \mathbb{N}$ such that the ring of m - fold vector invariants $\mathrm{Sym}((V^*)^m)^G$ is not Cohen

- Macaulay (see [19], Corollary 2.4).

The following "Three Copies Conjecture" is still open:

Conjecture 3.5.3 *If V is a faithful $\mathbb{F}G$-module and* $\mathrm{char}\mathbb{F}$ *divides $|G|$, then for W the direct sum of three copies of V, the invariant ring $\mathbb{F}[W]^G$ is not Cohen-Macaulay.*

3.6 On the Depth of Invariant Rings

We have seen that modular invariant rings are in general not Cohen - Macaulay. Therefore we will refine our initial question to the following one

- How 'far away' is A^G from being a Cohen - Macaulay algebra?

It is known that the length of a maximal regular sequence in $A^{G,+}$ is less or equal to the Krull - dimension with equality if and only if A^G is CM. Hence the parameters $\mathrm{depth}(A^G) = \mathrm{grade}(A^{+G}, A^G)$ or $\mathrm{def}(A^G) := \mathrm{Dim}(A^G) - \mathrm{depth}(A^G)$ provide a natural measure for the distance of A^G to being CM. The following is a generalization of 3.4.1:

Lemma 3.6.1 *Let $C \leq B$ be graded connected over $\mathbb{F}$ such that ${}_CB$ is finite. Assume $\theta : B \to C$ is a* **Reynolds - operator***, i.e. a C - module homomorphism which is a right inverse to the embedding $C \hookrightarrow B$. Then*

$$\mathrm{depth}(B) \leq \mathrm{depth}(C).$$

Corollary 3.6.2 *Let $p =$ char $\mathbb{F}$ and P a Sylow p - group, if $p > 0$. Then the following hold:*

1. *If $H \leq G$ with $[G : H]1_{\mathbb{F}} \neq 0$, then* $\mathrm{depth}\ A^H \leq \mathrm{depth}\ A^G$ *(*Kemper *[17]).*
2. *If A^P is CM, so is A^G (*Campbell-Hughes-Pollack *[3]).*

Proof: 1.) follows from 3.6.1 with $\theta := t_H^G : A^H \to A^G$. Now 2.) follows from the fact that, since G is finite, the extensions $A^G \leq A^P \leq A$ are finite and therefore all of equal dimension. $\diamond$

It is known that in 1. equality is not true in general: for $G = \Sigma_5$, $P = \langle(12345)\rangle$, $p = 5$ and $V = \mathbb{F}^5$ with natural permutation action, one knows that $\mathbb{F}[V]^P$ is not CM, whereas $\mathbb{F}[V]^{\Sigma_5}$ is even a polynomial ring.

In 1980 G. Ellingsrud and T. Skjelbred proved the celebrated result that, if P is a Sylow p - group of G with fixed point space V^P, one has

$$\text{depth } \mathrm{Sym}(V^*)^G \geq 2 + \dim(V^P) \tag{3}$$

if $\dim(V) \geq \dim(V^P) + 2$, with equality if G is a cyclic p - group (see [5]). For almost two decades this has been the only general result on the depth of modular invariant rings, which remains to be one of their most interesting, but difficult to determine parameters. In particular the classification of modular Cohen - Macaulay - invariant rings is an open problem. The result of Ellingsrud and Skjelbred was achieved using homological algebra, in particular a Grothendieck spectral sequence. During the last five years or so, these techniques have been revitalized (see e.g. [19], [33], [22]), most notably by Gregor Kemper who was able to classify all groups, whose modular regular representation has a Cohen - Macaulay ring of invariants:

Theorem 3.6.3 *[G Kemper, [18]] For a finite group G with group algebra $\Lambda := \mathbb{F}G$ the following are equivalent:*

1. $\mathrm{Sym}(\Lambda)^G$ *is Cohen - Macaulay;*
2. $\mathrm{char}\mathbb{F}$ *does not divide* $|G|$ *or* $G \in \{\mathbb{Z}_2,\ \mathbb{Z}_3,\ \mathbb{Z}_2 \times \mathbb{Z}_2\}$.

Due to constraints in length and time we have not mentioned the use of Steenrod - operations in modular invariant rings. An extensive account can be found in chapter 8 of [23]. Without doubt the most striking success of these techniques in modular invariant is the proof by Bourguiba and Zarati of an earlier conjecture of Landweber and Stong:

Theorem 3.6.4 *(Bourguiba - Zarati, [2] and [16]) Let $A = \mathbb{F}_q[V]$ with $\mathbb{F}_qG$ - module V. Then one can use the Dickson invariants (see 3.3) as a test sequence to measure the depth of A^G. More precisely the depth of A^G is the largest ℓ such that the sequence of Dickson - invariants $d_{1,n}, \ldots, d_{\ell,n}$ is A^G-regular.*

3.7 Relative Transfer and Depth

With regard to the techniques laid out in the previous sections of these notes, some recent results show that the relative transfer ideal $\mathcal{I}^G_{<P}$ and its radical ideal $\sqrt{\mathcal{I}^G_{<P}}$ [5] shed some new light on the problem of determining the depth of modular

[5] for an ideal $\mathcal{I}$ in A: $\sqrt{\mathcal{I}} := \{a \in A \mid a^m \in I,\ \text{for some } m \in \mathbb{N}\}$.

invariant rings. Let $P \leq G$ be a fixed Sylow p - group of G and assume that $\mathbb{F}$ is algebraically closed of characteristic $p > 0$. This allows us to consider $A := \mathrm{Sym}(V^*)$ as the algebra of polynomial functions on V, and A^G as the algebra of polynomial functions on the orbit space V/G. Hence for an ideal $\mathcal{I} \triangleleft A^G$, the variety $\mathcal{V}(\mathcal{I})$ consists of all orbits v^G in V such that $f(x) = 0$ for every $f \in \mathcal{I}$ and $x \in v^G$. On the other hand for each subset $S \subseteq V$ there is the ideal

$$\mathcal{I}(S) := \{f \in A \mid f(s) = 0 \ \forall s \in S\}$$

and $\mathcal{I}^G(S) := \mathcal{I}(S) \cap A^G \triangleleft A^G$. In [8] relative transfer ideals have been investigated geometrically, which led to the following description of $\sqrt{\mathcal{I}^G_{<P}}$ in terms of its variety in the orbit space V/G:

Theorem 3.7.1 *([8]) 1.)* $\mathcal{V}(\mathcal{I}^G_{<P}) = \{v^G \in V/G \mid p \not| \ |v^G|\}$;
2.) $\sqrt{\mathcal{I}^G_{<P}} = \mathcal{I}^G(V^P)$ *is a prime ideal of height* $\mathrm{codim}_{\mathbb{F}}(V^P)$, *where* V^P *denotes the space of* P *- fixed points in* V.

Note that for a permutation module of a p - group Q, the previous result $A^Q = \mathcal{I}^Q_{<Q} \oplus \mathbb{F}[\mathfrak{n}_1, \cdots, \mathfrak{n}_s]$ implies that $\sqrt{\mathcal{I}^Q_{<Q}} = \mathcal{I}^Q_{<Q}$ with $A^Q/\mathcal{I}^Q_{<Q} \cong \mathbb{F}[\mathfrak{n}_1, \cdots, \mathfrak{n}_s]$ being a polynomial ring. In general the quotient $A^G/\mathcal{I}^G(V^P)$ is still Cohen - Macaulay, which was proved in [8] for p - permutation modules. A second proof in that paper, designed to work under slightly more general hypotheses, contains a gap and I am indebted to Jim Shank for pointing that out to me. I take this occasion to present a proof that works without any additional hypotheses. We will make use of a very useful technique to extend regular sequences, which was developed by Gregor Kemper [19]:

Proposition 3.7.1 *(G Kemper) Let* $W \leq V^*$ *be an* $\mathbb{F}G$ *- submodule such that the kernel* N *of the* G *- action on the quotient* V^*/W *has an index coprime to* p*. Then there exist homogeneous* $g_1, g_2, \cdots, g_m \in A^G$ *with the following two properties:*

- *(a) The images* $\overline{g_1}, \overline{g_2}, \cdots, \overline{g_m}$ *form an hsop in the quotient ring* $A^G/[(W)A \cap A^G]$.
- *(b) For each* i*, multiplication with* g_i *has a left inverse in the endomorphism ring* $\mathrm{End}_{A_iG}(A)$*, where* A_i *is the subalgebra*

$$A_i := \mathrm{Sym}(W)^G[g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_m] \subseteq A^G,$$

generated by $\mathrm{Sym}(W)^G$ *and all* g_j *with* $j \neq i$.

Any $g_1, g_2, \cdots, g_m$ *having property (a) also have property (b) and* $m = \mathrm{codim}(W)$.

Let $W := (V^G)^\perp = \{f \in V^* \mid f(V^G) = 0\}$ with $\mathbb{F}$ - basis $\{y_1, \cdots, y_r\}$, let $\mathcal{I} := \mathcal{I}(V^G) = ((V^G)^\perp)A$ and $\mathfrak{i} := \mathcal{I} \cap A^G = \mathcal{I}^G(V^G)$. Note that G acts trivially on the quotient V^*/W, hence we can take $N = G$ in Proposition 3.7.1. The proof in [19] shows, that there always exists a sequence $g_1, g_2, \cdots, g_m \in A^G$, $m = \dim(V^G)$, with $\overline{g_1}, \overline{g_2}, \cdots, \overline{g_m}$ being an hsop in $\overline{A^G} := A^G/\mathfrak{i}$, such that

1. for each i there is a map $\Psi_i : A \to A$, commuting with the G $(= N)$ - action and with elements in $\mathbb{F}[g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_m, y_1, y_2, \cdots, y_r]$;
2. $\Psi_i(g_i a) = a$ for every $a \in A$.

Hence Ψ_i is a left - inverse to the multiplication - map $\mu_{g_i} : A \to A, \ a \mapsto g_i a$. Moreover we see that $\Psi_i(\mathcal{I}) \subseteq \mathcal{I}$ and $\Psi_i(\mathfrak{i}) \subseteq \mathfrak{i}$, therefore the Ψ_i's induce left - inverses in $\mathrm{End}_{\mathbb{F}[g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_m]}(\overline{A^G})$ to the multiplication - map $\mu_{\overline{g_i}}$. Now assume that $(\overline{g_1}, \overline{g_2}, \cdots, \overline{g_s})$ is a regular sequence on $\overline{A^G}$ with $s < m$, and $\overline{a} \in \overline{A^G}$ with $\overline{g_{s+1} a} \in (\overline{g_1}, \overline{g_2}, \cdots, \overline{g_s})\overline{A^G}$. Then $\overline{a} = \Psi_{s+1}(\overline{g_{s+1} a}) \in (\overline{g_1}, \overline{g_2}, \cdots, \overline{g_s})\overline{A^G}$, proving that $(\overline{g_1}, \overline{g_2}, \cdots, \overline{g_{s+1}})$ is regular as well. Hence $m = \dim(V^G) \le \mathrm{depth}(\overline{A^G}) \le \mathrm{Dim}(\overline{A^G})$.

Theorem 3.7.2 *Let G be a finite group, P a Sylow p - subgroup of G and $A = \mathbb{F}[V]$ with $\mathbb{F}G$ - module V. Then $\overline{A^G} := A^G/\mathcal{I}^G(V^P)$ is Cohen - Macaulay of Krull - dimension $\dim_{\mathbb{F}}(V^P)$.*

Proof: Taking $U := V^P$ and $\overline{A^P} := A^P/\mathcal{I}^P(V^P)$, we get from from the above: $\mathrm{Dim}(\overline{A^P}) \ge \mathrm{depth}(\overline{A^P}) \ge \dim_{\mathbb{F}}(V^P)$. Since A and A^P are finite over A^G, the (prime) ideals $\mathcal{I}(V^P) \triangleleft A$, $\mathcal{I}^P(V^P) \triangleleft A^P$ and $\mathcal{I}^G(V^P) \triangleleft A^G$ have the same height and $\overline{A^P}$ is finite over $\overline{A^G}$ with the same Krull - dimension $\dim_{\mathbb{F}}(V^P)$. In particular we see that $\mathrm{depth}(\overline{A^P}) = \mathrm{Dim}(\overline{A^P}) = \dim_{\mathbb{F}}(V^P)$, and $\overline{A^P}$ is Cohen - Macaulay. The Mackey - formula from section 1 shows that

$$t_P^G(\mathcal{I}^P(V^P)) = \mathcal{I}^P(V^P) \cap A^G = \mathcal{I}^G(V^P),$$

hence the relative transfer t_P^G induces a Reynolds operator $\overline{A^P} \to \overline{A^G}$. Now Lemma 3.6.1 yields

$$\dim_{\mathbb{F}}(V^P) = \mathrm{depth}(\overline{A^P}) \le \mathrm{depth}(\overline{A^G}) \le \mathrm{Dim}(\overline{A^G}) = \dim_{\mathbb{F}}(V^P).$$

$\diamond$

The theorems 3.7.1 and 3.7.2 indicated that the ideal $\sqrt{\mathcal{I}^G_{<P}} = \mathcal{I}^G(V^P)$ might 'measure the depth' of $\mathrm{Sym}(V^*)^G$ in general: the formula (3) of Ellingsrud - Skjelbred shows, that $\dim(V^P)$ is a lower bound for the depth of A^G, so it was conceivable that the 'missing part' of the depth is provided by regular elements in the

ideal $\mathcal{I}^G_{<P}$[6]. In the case of p - groups this is a consequence of Theorem 1.5 in [19] and for arbitrary finite groups it is a consequence of the following

Theorem 3.7.3 *(P. Fl., R.J. Shank, [10])*

$$\text{depth } A^G = \text{grade}(\mathcal{I}^G_{<P}, A^G) + \dim(V^P).$$

Moreover, if V is defined over $\mathbb{F}_q$, one can apply Theorem 3.6.4 and at least in principle use the 'Dickson invariants' $d_{i,n} \in \text{Sym}(V^*)^{\text{GL}_n(q)} \leq \text{Sym}(V^*)^G$ to determine the grade of $\mathcal{I}^G_{<P}$ on A^G.

Theorem 3.7.3, in connection with Lemma and Conjecture 1.3.6, shows that the relative transfer ideal $\mathcal{I}^G_{<P}$ contains the clues for many important structural and constructive properties of modular invariant rings. Therefore an efficient algorithm to find minimal generating sets for the ideal $\sqrt{\mathcal{I}^G_{<P}}$ is very much needed as an important step to determine its grade and henceforth the depth of A^G.

Connecting 3.7.3 with the cohomological methods developed by Gregor Kemper, a substantial generalization of G. Ellingsrud and T. Skjelbred's depth formula could be achieved. Note that the following result has purely group-theoretic hypotheses: the group G is called p - nilpotent if it has a normal p - complement, i.e. a normal subgroup N of order coprime to p, such that G/N is a p - group (which then has to be isomorphic to a Sylow p - group of G.)

Theorem 3.7.4 *[11] If G is p-nilpotent with cyclic Sylow p-subgroup $P \leq G$, then*

$$\text{depth}(A^G) = \min\left\{\dim_{\mathbb{F}}(V^P) + 2, \dim_{\mathbb{F}}(V)\right\}.$$

[6]note that the grade of an ideal always coincides with the grade of its radical.

Notation

A^G, pg. 7, ring of G - invariants
$|\alpha| := \sum_{i=1}^n \alpha_i$, for $\alpha \in \mathbb{N}_0^n$
$\underline{a}^\alpha$, pg. 8
$A(k,n)$, pg. 20
ann M, pg. 34
$A(\Omega)$, pg. 17
$\beta(A^G)$, pg.8, Noether number
$\mathrm{Dim}(A)$, pg. 28
Dim M, pg. 34
e_i, pg. 20
$\mathbb{F}G$, group algebra over $\mathbb{F}$
$\mathbb{F}[V]$, pg. 29
$[G:H]$, pg.12, index of H in G
$H(M,t)$, pg. 29
hsop, pg. 31
$\mathcal{I}^H_{<U}$, pg.13, relative transfer ideal
$\mathcal{I}^G_{<P}$, $\sqrt{\mathcal{I}^G_{<P}}$, pg. 38
$\mathcal{I}(S)$, pg. 39
$\mathbb{N}_0 := \{0,1,2,\ldots\}$
$\underline{n} := \{1,2,\ldots,n\}$
$\underline{n}_0 := \{0,1,2,\ldots,n\}$
$N_G(P)$ pg.13, normalizer of P in G
$\mathrm{orb}_{\Sigma_n}(\underline{X}^\alpha)$, pg. 6
$\mathcal{P}$, pg. 17
$\mathrm{Pol}(f)$, pg. 23
Σ_Ω, symmetric group on set Ω
Σ_n, symmetric group on $\underline{n}$
$\mathrm{soc}(V)$, pg.40
$\mathrm{Sym}(V^*)$, pg. 19
t_1^G, pg.9
t_H^G, pg.11
$\mathcal{V}(\mathcal{I})$, pg. 39
$\underline{X}^\alpha$, pg. 5
Y^X, the set of functions from X to Y

Bibliography

[1] D.J. Benson. *Polynomial Invariants of Finite Groups.* Number 190 in Lond. Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1993.

[2] D. Bourguiba and S. Zarati. Depth and the Steenrod algebra. *Invent. math.*, 128:589–602, 1997.

[3] H.E.A. Campbell, I. Hughes, and R.D. Pollack. Rings of invariants and p-Sylow subgroups. *Canad. Math. Bull*, 34:42 – 47, 1991.

[4] H. Derksen and G. Kemper. *Computational Invariant Theory.* Encyclopaedia of Mathematical Sciences. Springer-Verlag, Berlin, Heidelberg, New York, 2002. 241 pages.

[5] G. Ellingsrud and T. Skjelbred. Profondeur d'anneaux d'invariants en caractéristique p. *Compos. Math.*, 41:233–244, 1980.

[6] H.E.A. Campbell et al. Depth of modular invariant rings. *Transformation Groups*, 5(1):21 – 34, 2000.

[7] P. Fleischmann. A new degree bound for vector invariants of symmetric groups. *Transactions of the Amer. Math. Soc.*, 350(4):1703–1712, 1998.

[8] P. Fleischmann. Relative trace ideals and Cohen-Macaulay quotients of modular invariant rings. In P. Dräxler, G.O. Michler, and C. M. Ringel, editors, *Computational Methods for Representations of Groups and Algebras, Euroconference in Essen, April 1-5 1997*, number 173 in Progress in Mathematics, Basel, 1999. Birkhäuser.

[9] P. Fleischmann. The Noether bound in invariant theory of finite groups. *Adv. in Math.*, 156:23–32, 2000.

[10] P. Fleischmann and J.Shank. The relative trace ideal and the depth of modular rings of invariants. *to appear in: Archiv der Mathematik.*

[11] P. Fleischmann, G. Kemper, and J. Shank. Work in progress ...

[12] P. Fleischmann and W. Lempken. On generators of modular invariant rings of finite groups. *Bull. London Math. Soc.*, 29:585–591, 1997.

[13] P. Fleischmann and W. Lempken. On degree bounds for invariant rings of finite groups over finite fields. *Contemporary Mathematics*, 225:31–41, 1999.

[14] J. Fogarty. On Noether's bound for polynomial invariants of a finite group. *Electron. Res. Announc. Amer. Math. Soc.*, 7:5–7, 2001.

[15] M. Göbel. Computing bases for rings of permutation- invariant polynomials. *J. Symbolic Comput.*, 19:285 – 291, 1995.

[16] H-W. Henn. A variant of the proof of the Landweber - Stong conjecture. *Proceedings of Symposia in Pure Mathematics*, 63:271–275, 1998.

[17] G. Kemper. Calculating invariant rings of finite groups over arbitrary fields. *J. Symb. Comp.*, 21:351 – 366, 1996.

[18] G. Kemper. Die Cohen-Macaulay-Eigenschaft in der modularen Invariantentheorie. Habilitationsschrift, Universität Heidelberg, 1999.

[19] G. Kemper. On the Cohen-Macaulay property of modular invariant rings. *J. of Algebra*, 215:330–351, 1999.

[20] G. Kemper. The depth of invariant rings and cohomology, with an appendix by Kay Magaard. *J. of Algebra*, 245:463–531, 2001.

[21] P. Landrock. *Finite Group Algebras and their Modules.* Number 84 in Lond. Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1983.

[22] M. Lorenz and J. Pathak. On Cohen-Macaulay rings of invariants. *J. of Algebra*, 245:247–264, 2001.

[23] M.Neusel and L. Smith. *Invariant Theory of Finite Groups*, volume 94. AMS, 2001.

[24] E. Noether. Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.*, 77:89–92, 1916.

[25] E. Noether. Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p. *Nachr. Ges. Wiss. Göttingen*, pages 28–35, 1926.

[26] D. Richman. Explicit generators of the invariants of finite groups. *Adv. Math.*, 124:49–76, 1996.

[27] D. Richman. Invariants of finite groups over fields of characteristic p. *Adv. in Math.*, 124:25–48, 1996.

[28] B. J. Schmid. Generating invariants of finite groups. *C. R. Acad. Sci. Paris*, 308:1–6, 1989.

[29] R. J. Shank and D.L. Wehlau. Computing modular invariants of p - groups. *J. Symbolic Comput.*, 34(5):307–327, 2002.

[30] R. J. Shank and D.L. Wehlau. Noether numbers for subrepresentations of cyclic groups of prime order. *Bull. London Math. Soc.*, 4:438–450, 2002.

[31] L. Smith. *Polynomial Invariants of Finite Groups.* A K Peters, 1995.

[32] L. Smith. Noether's bound in the invariant theory of finite groups. *Arch. der Math.*, 66:89–92, 1996.

[33] L. Smith. Homological codimension of modular rings of invariants and the Koszul complex. *J. Math. Kyoto Univ.*, 38:727–747, 1998.

[34] J. Thevenaz. *G-Algebras and Modular Representation Theory.* Clarendon Pres, Oxford, 1995.

[35] H. Weyl. *The Classical Groups.* Princeton Univ. Press, 1953.

[36] C.W. Wilkerson. A primer on the Dickson invariants. *Amer. Math. Soc. Contemp. Math. Series*, 19:421–434, 1983.