On generators of modular invariant rings of finite groups

P. Fleischmann and W.Lempken

Institute for Experimental Mathematics

University of Essen

Ellernstr. 29, 45326 Essen, Germany

e-mail:

peter@exp-math.uni-essen.de

lempken@exp-math.uni-essen.de

Abstract

Let G be a finite group, let V be an $\mathbb{F}G$-module of finite dimension d, and denote by $\beta(V,G)$ the minimal number m such that the invariant ring $S(V)^G$ is generated by finitely many elements of degree at most m. A classical result of E. Noether says that $\beta(V,G) \leq |G|$ provided that $char\ \mathbb{F}$ is coprime to $|G|!$. If $char\ \mathbb{F}$ divides $|G|$ then no bounds for $\beta(V,G)$ are known except for very special choices of G. In this paper we present a constructive proof of the following: If $H \leq G$ with $[G:H] \in \mathbb{F}^*$ and if the restriction $V_{|H}$ is a permutation module (e.g. if V is a projective $\mathbb{F}G$ - module and $H \in Syl_p(G)$) then $\beta(V,G) \leq max\{|G|, d(|G|-1)\}$ regardless of $char\ \mathbb{F}$.

1 Introduction

For any (unitary) commutative ring R let ${}_RMod$ denote the category of left R - modules. Let G be a finite group, R a commutative ring and RG the group ring of G over R.

With ${}_{RG}mod$ we denote the full subcategory of ${}_{RG}Mod$ consisting of modules V such that V_R is also a free R - module of finite rank. Consider $T(V) := T_R(V) := \oplus_{i=1}^{\infty} V^{\otimes i}$, the graded tensor algebra over V. The R - linear action of G on V together with the universal property of tensor products induces a representation of G as automorphisms of the (non - commutative) graded ring $T(V)$. For any $v_1 \otimes ... \otimes v_n$ and $g \in G$ we have: $g(v_1 \otimes ... \otimes v_n) = gv_1 \otimes ... \otimes gv_n$. Let I be the homogeneous ideal of $T(V)$, generated by the tensors $v \otimes w - w \otimes v$ for $v, w \in V$ and $S_R(V) = S(V)$ the symmetric algebra $S(V) := T(V)/I$. Then $S(V) := \oplus_{i=1}^{\infty} S^i(V)$ is also a graded R - algebra with $S^i(V) := \langle v_1 \otimes ... \otimes v_i + I \rangle_R$ and $v_i \in V$. In particular the ideal I is G - stable and hence we also have a natural action of G on $S(V)$ as automorphisms of graded R - algebras.

Choosing an R - basis $\mathcal{B} := \{x_1, ..., x_d\}$ of V we can identify $S(V)$ with the polynomial ring $R[x_1, ..., x_d]$ in the indeterminates $x_1, ..., x_d$.

For $W \in {}_{RG}Mod$ and any subgroup $H \leq G$ we define $W^H := \{w \in W | hw = w \ \forall h \in H\}$ to be the submodule of H - fixed points in W. In particular A^H is the **algebra of invariants** in A.

If R is noetherian and $V \in_{RG} mod$, then a classical result of Emmy Noether states that the ring of invariants $S(V)^G$ is always finitely generated over R.

Moreover, if $R = \mathbb{F}$ is a field of characteristic bigger than the order $|G|$ of the group, then a full generating set for $S(V)^G$ can be found in degrees lower than or equal to $|G|$.

If $R = \mathbb{Z}$ or if R is a field of characteristic $p \mid |G|$, then this 'Noether bound' for the degrees of generators for the invariant ring is known to be false.
The easiest counterexample is the symmetric group Σ_2 on two letters acting on a k - fold direct sum $R^{2k} := \underline{R^2} \oplus \ldots \oplus \underline{R^2}$ where $\underline{R^2}$ denotes the canonical permutation module and $R = \mathbb{Z}$ or $\mathbb{F}_2$ and $k \geq 3$. It is not difficult to prove that the invariant ring $S(R^{2k})^{\Sigma_2}$ cannot be generated by elements of degree less than $max\{2, k\}$. In [2] this has been generalized to the ring of vector invariants for Σ_{p^m} in characteristic p which therefore provide a 'generic counterexample' to Noether's bound for modular fields.
In these cases Noether's proof of the finite generation of $S(V)^G$ is a mere existence proof, which runs as follows:

Let $A := S(V) = R[x_1, \dots, x_d]$. By Hilbert's theorem this is a noetherian ring. For $i = 1, \dots, d$ and $g := |G|$ let $f_i := \prod_{\sigma \in G}(T - \sigma(x_i)) =: T^g + \sum_{\ell=0}^{g-1} c_{i,\ell} T^\ell \in A^G[T]$; then $f_i(x_i) = 0$, hence A is integral over the noetherian subring $C := R[c_{i,\ell} \mid i = 1, \dots, d, \ \ell = 0, \dots, g-1]$. So A is finitely generated as **module** over C and hence is a noetherian module. Obviously $A^G \leq A$ is a C - submodule of A and hence it is finitely generated, i.e. $A^G = \langle a_1, \dots, a_m \rangle_C$. Now it is clear that $A^G = R[c_{i,\ell}, a_s \mid i = 1, \dots, d, \ \ell = 0, \dots, g-1, \ s = 1, \dots, m]$ is a finitely generated R - algebra.

Notice that even though C can be generated by the elements $c_{i,\ell}$ of degree at most $|G|$ and $A = \langle x_1^{a_1} x_2^{a_2} \dots x_d^{a_d} \mid a_i < |G| \rangle_C$, the previous arguments do not give a recipe how to construct the 'missing' invariants $a_1, \dots, a_m$.

If $|G|$ is contained in R^*, the group of units in R, then the **trace map** $T : A \to A^G, a \mapsto \sum_{\sigma \in G} \sigma(a)$ is a surjective homomorphism of A^G - modules. Using this together with some special arguments, valid if R is a field of characteristic $p > |G|$, Noether's bound can be proved (see [5]). If $|G|$ is not invertible in R, the trace map is no more surjective and in fact no bound on the degrees of generators of $S(V)^G$ seems to be known in the general case.

In this short note we will show how (relative) trace maps can still be used to obtain some information on the generators and their degrees in special instances of the non-coprime situation.

2 Relative trace maps and sets of generators

From now on A will be a commutative R - algebra.

Let $H \leq Aut_R(A)$ be a finite group with subgroup U. Then for $W \in {}_{RH}mod$ we have the following homomorphism of R - modules:

$$T_U^H : W^U \to W^H, \ w \mapsto \sum_{h \in H:U} hw,$$

where $H : U$ denotes an arbitrary cross section of (left) U - cosets in H.

This is called the **(relative) trace homomorphism**. If the index $[H:U]$ is invertible in R, then T_U^H is an epimorphism; if $W = A = S(V)$ with $V \in {}_{RH}mod$ then the trace homomorphism preserves degrees.

For any $a \in A^H$ and $b \in A^U$ we have $T_U^H(ab) = aT_U^H(b)$, showing that the image $A_U^H := T_U^H(A^U)$ is an ideal in A^H. If $A = S(V)$ then A_U^H is a homogeneous ideal.

If $\mathcal{X}$ is a set of subgroups of H, then we define $W_{\mathcal{X}}^H := \sum_{U \in \mathcal{X}} W_U^H$ and $W_<^H := \sum_{U<H} W_U^H$. Notice that $A_{\mathcal{X}}^H$ and $A_<^H$ are ideals in A^H and that they are homogenous if $A = S(V)$. The following easy observation will be useful for finding algebra generators of invariant rings:

Lemma 2.1 *Let $A = \oplus_{i=0}^{\infty} A_i$ be a commutative graded ring, $S \subseteq A^+ := \oplus_{i>0}^{\infty} A_i$ a set of homogeneous elements and $I = A\{i \mid i \in S\} \lhd A$ the (homogeneous) ideal generated by S. Then for any set $X \subseteq A$ of homogeneous elements we have*

$$A = A_0[X, S] \iff A/I = (A_0/A_0 \cap I)[\overline{X}].$$

Here $\overline{X} := \{x + I \mid x \in X\} \subseteq A/I$.

Proof: 'only if' is clear. So suppose A/I is generated by $\overline{X}$ and the image of A_0 in A/I. Then any homogeneous element $a \in A$ of degree d can be written as $a = \tilde{a} + \sum_j a_j s_j$ with homogeneous element $\tilde{a} \in A_0\langle x \mid x \in X\rangle$ of degree d and homogeneous elements $a_j \in A$ and $s_j \in S$. Since $S \subseteq A^+$, the s_j's have positive degree, hence the degrees of the a_j are strictly less than d. Now, by induction, a_j and hence a belong to $A_0\langle y \mid y \in X \cup S\rangle$. $\circ$

Now recall that the algebra A^U is an integral extension of A^H. In fact each homogeneous $a \in (A^U)^+$ is a zero of the polynomial $f_a(T) := \prod_{\{h \in H:H_a\}}(T - ha) = T^{|H:H_a|} + \sum_{i=1}^{|H:H_a|} c_i(a) T^{|H:H_a|-i}$ with $c_i(a) \in A^H$ homogeneous of degree $deg(a) \cdot i$. Now put $\mathcal{C}_U(a) := \{c_i(a) \mid 1 \leq i \leq |H:H_a|\}$.

For any finite non-empty subset $S_U = \{s_1, \ldots, s_k\} \subseteq (A^U)^+$ of homogeneous elements and $n \in \mathbb{N}_0 \cup \{\infty\}$ we define

$$S_U^{(n)} := S_U \cup \{s_1^{a_1} \cdot \ldots \cdot s_k^{a_k} \mid s_i \in S_U,\ 0 \leq a_i < n, \sum_i a_i > 0\} \cup \bigcup_{i=1}^{k} \mathcal{C}_U(s_i).$$

Notice that $S_U^{(n)} \subseteq (A^U)^+$ and $\mathcal{C}_U(s_i) \subseteq (A^H)^+$; moreover, if all elements in S_U have degree at most m, then the elements in $S_U^{(|H:U|)}$ and $T_U^H(S_U^{(|H:U|)}) =$

$$\{T_U^H(s_i), T_U^H(s_1^{a_1}\dots s_k^{a_k}), cT_U^H(1) \mid s_i \in S_U, 0 \le a_i < |H:U|, \sum_i a_i > 0, c \in \mathcal{C}_U(s_i)\}$$

are homogeneous of degree at most $max\{m \cdot |H:U|, k \cdot m(|H:U|-1)\}$.

Using the relations $f_{s_i}(s_i)$ we can now reduce exponents greater than $|H:U|-1$ and conclude for any ideal $\mathcal{I} \lhd A$:

$$\mathcal{I}^H \cdot T_U^H(\langle S_U^{(\infty)}\rangle_R) = \mathcal{I}^H \cdot T_U^H(\langle S_U^{(|H:U|)}\rangle_R).$$

Together with the previous lemma we get the following result:

Theorem 2.2 *Let A be an $\mathbb{N}_0$ - graded, commutative R - algebra, A^+ the ideal of elements of positive degree and G be a finite group of degree preserving R - algebra automorphisms of A. For each $H \le G$ let $S_H \subseteq (A^+)^H$ be a subset consisting of homogeneous elements such that $A^H/(A^+)^H_< = R[\overline{S}_H]$. Then for each $U \le G$:*

$$(A^+)^G_{<U\ \ (\le U)} = \sum_{X<U\ \ (X \le U)} T_X^G(S_X^{(|G:X|)}) \cdot A^G.$$

If $A^G/(A^+)^G_{<U\ \ (\le U)} = R[\overline{Y}]$ for some $Y \subseteq A^G$ consisting of homogeneous elements, then

$$A^G = R[Y, T_X^G(S_X^{(|G:X|)}) \mid X < U\ \ (X \le U)]$$

in particular

$$A^G = R[T_X^G(S_X^{(|G:X|)}) \mid X \le G].$$

Proof: For any $U \le G$ let $< U$ be the set of proper subroups of U. Then by the previous lemma $A^U = R[S_U, (A^+)^U_<]$ hence $(A^+)^U = \langle S_U^{(\infty)}\rangle_R + (A^+)^U_<$. We get

$$(A^+)^G_{<U} = \sum_{V<U} T_V^G((A^+)^V) = \sum_{V<U} T_V^G(\langle S_V^{(\infty)}\rangle_R + (A^+)^V_<)A^G$$

$$\subseteq \sum_{V<U} T_V^G(S_V^{(|G:V|)}) \cdot A^G + (A^+)^G_{<V} \subseteq \ldots \subseteq \sum_{X<U} T_X^G(S_X^{(|G:X|)}) \cdot A^G \subseteq (A^+)^G_{<U}.$$

Notice that $(A^+)^G_{<1} = 0$. Similarly we get

$$(A^+)^G_{\leq U} = \sum_{V \leq U} T^G_V((A^+)^V) = \sum_{V \leq U} T^G_V(\langle S_V^{(\infty)} \rangle_R + (A^+)^V_<) A^G$$

$$\subseteq \sum_{V \leq U} T^G_V(S_V^{(|G:V|)}) \cdot A^G + (A^+)^G_{<V} \subseteq \ldots \subseteq \sum_{X \leq U} T^G_X(S_X^{(|G:X|)}) \cdot A^G \subseteq (A^+)^G_{\leq U}.$$

In particular we have $(A^+)^G_< = \sum_{X<G} T^G_X(S_X^{(|G:X|)}) \cdot A^G$. Now the result follows directly from the previous lemma. $\circ$

Corollary 2.3 *We keep the assumptions of the previous theorem.*

(i) *If $|G|$ is invertible in R and $A = R[S]$ with $S \subseteq A^+$ consisting of homogeneous elements, then*

$$A^G = R[T^G_1(S^{(|G|)})];$$

(ii) *Let $|G : H| \in R^*$ then*

$$A^G = R[T^G_X(S_X^{(|G:X|)}) \mid X \leq H].$$

Proof: Case (i) is a speciality of (ii) for $H = 1$; in case (ii) the result follows from $A^G/(A^+)^G_{\leq H} = R$. $\circ$

3 Invariant rings of 'restricted' permutation modules

Now let G be a finite group and Ω a finite G - set. We consider the permutation module $V_\Omega := R^\Omega \cong \oplus_{\omega\in\Omega} R \cdot e_\omega$, where $e_\omega(\omega') = 1$ if and only if $\omega = \omega'$ and zero otherwise. Now let $A = A(R) := S_R(V_\Omega) = \oplus_{f \in \mathbb{N}^\Omega} R\pi(f)$, where for each $f \in \mathbb{N}^\Omega$ we define $\pi(f) := \prod_{\omega\in\Omega} e_\omega^{f(\omega)}$.

Notice that for $a, b \in \mathbb{N}^\Omega$ we have $\pi(a) \cdot \pi(b) = \pi(a + b)$ where $(a + b)(\omega) = a(\omega) + b(\omega)$, hence we can view $S(V_\Omega)$ as the semigroup - algebra $R[\mathbb{N}^\Omega]$.

We define $supp(a) := \{\omega \in \Omega \mid a(\omega) \neq 0\}$; for each $s \subseteq \Omega$ we denote by 1_s the characteristic function of s in Ω, which takes the value 1 on s and 0 on $\Omega \backslash s$.

The group Σ_Ω and with it the group G acts on A by permuting the monomials $\pi(f)$ according to the rule:

$$\sigma(\pi(f)) = \prod_{\omega\in\Omega} e_{\sigma(\omega)}^{f(\omega)} = \prod_{\omega\in\Omega} e_{\omega}^{f\circ\sigma^{-1}(\omega)} = \pi(f\circ\sigma^{-1}).$$

Hence the RG -module $S(V_\Omega)$ is isomorphic to the permutation module $V_{\mathbb{N}^\Omega}$ and in each degree i the module $S(V_\Omega)^i$ is isomorphic to the permutation module $V_{(\mathbb{N}^\Omega)^i}$, where $(\mathbb{N}^\Omega)^i := \{f\in\mathbb{N}^\Omega \mid \sum_\omega f(\omega)=i\}$ with the natural action of Σ_Ω and G.

In particular the R - module A^G has a basis consisting of the orbit sums $\pi(f)^+ := \sum_{g\in G:G_f} g\pi(f) = T_{G_f}^G(\pi(f))$ for $f\in\mathbb{N}^\Omega$.

Lemma 3.1 *Let $\mathcal{X}$ be any set of subgroups of G. For any $f\in\mathbb{N}^\Omega$ let $g_{\mathcal{X}}(f) :=$ g.c.d.$(\frac{|G_f|}{|H_f|}\mid H\in\mathcal{X})$. Then*

$$A(R)^G_{\mathcal{X}} = \langle g_{\mathcal{X}}(f)\pi(f)^+ \mid f\in\mathbb{N}^\Omega\rangle_R.$$

Proof: $x\in A^G_{\mathcal{X}} \iff x=\sum_{H\in\mathcal{X},f\in\mathbb{N}^\Omega} r_{(H,f)}T^G_{H_f}(\pi(f))$
$=\sum_{H\in\mathcal{X},f\in\mathbb{N}^\Omega} r_{(H,f)}\frac{|G_f|}{|H_f|}(T^G_{G_f}(\pi(f))$ with $r_{(H,f)}\in R$. Hence

$$A^G_{\mathcal{X}} = \langle\frac{|G_f|}{|H_f|}\pi(f)^+ \mid H\in\mathcal{X}, f\in\mathbb{N}^\Omega\rangle_R.$$

This proves the lemma. $\circ$

Notice that $\pi(f)^+\in A^G_<$ if and only if $\frac{|G_f|}{|H_f|}$ is invertible in R for some proper subgroup $H<G$ (e.g. if $G_f<G$). Hence $A^G/A^G_<$ is generated by the images of the $\pi(f)^+$ with $G_f=G$.

Let $\Omega\backslash G$ denote the set of G - orbits on Ω. Then $G=G_f$ if and only if f is constant on these G - orbits, hence induces a function $\overline{f}\in\mathbb{N}^{\Omega\backslash G}$. For such an f the corresponding monomial $\pi(f)$ is given by $\prod_{\omega\in\Omega} e_\omega^{f(\omega)} = \prod_{\omega^G\in\Omega\backslash G}\pi(\omega^G)^{\overline{f}(\omega^G)}$. Where $\pi(\omega^G) := \pi(1_{\omega^G}) = \prod_{\omega\in\omega^G} e_\omega$ denotes the orbit - product of ω under G. Since different G - orbits are disjoint, the $\pi(\omega^G)$'s are algebraically independent. We conclude $R[X_1,...,X_{|\Omega\backslash G|}]\cong R[\pi(\omega^G)\mid\omega^G\in\Omega\backslash G]$ is a subalgebra of A^G and

$$A^G/A^G_< \cong R[\pi(\omega^G)+A^G_< \mid \omega^G\in\Omega\backslash G].$$

Now let $V \in {}_{RG}mod$ and $H \leq G$ a subgroup such that the index $|G:H|$ is invertible in R and V_H is a permutation module. Then $V_H \cong R^\Omega$ with H acting on the basis $\{e_\omega \mid \omega \in \Omega\}$. Thus we have $A^X/A^X_< \cong R[\pi(\omega^X) + A^X_< \mid \omega^X \in \Omega\backslash X]$.

We get the following result

Theorem 3.2 *Let G be a finite group, $V \in {}_{RG}mod$ and let $H \leq G$ be a subgroup with $|G:H| \in R^*$ such that $V_H \cong R^\Omega$ is a permutation module.*
For each subgroup $X \leq H$ let $\mathcal{P}_X$ be the set of X - orbit products $\{\pi_X(\omega^X) \mid \omega^X \in \Omega\backslash X\}$. Then we have:

$$S(V)^G = R[T_X^G(\mathcal{P}_X^{(|G:X|)}) \mid X \leq H].$$

In particular $S(V)^G$ can be generated by finitely many invariants of degree at most

$$max\{|G|, rank_R(V)(|G|-1)\}.$$

(Here the subgroups X of H have to be taken only up to G - conjugacy.)

Proof: At this point only the degree bound has to be checked: for any $X \leq H$ there are $|\Omega\backslash X| \leq d := rank_R(V)$ many orbit products each having degree at most $|X|$. Hence whenever $X < G$, any element $\alpha \in T_X^G(\mathcal{P}_X^{(|G:X|)})$ has degree at most $|\Omega\backslash X|\,|X|\cdot(|G:X|-1) \leq d\cdot(|G|-1)$. If $X = H = G$ any element $\alpha \in T_X^G(\mathcal{P}_X^{(|G:X|)}) = \mathcal{P}_G$ has degree $\leq |G|$. $\circ$

Suppose that R is a local ring with unique maximal ideal $Rad\ R$ and residue class field $F = R/Rad\ R$ of characteristic p (R itself can be a field of characteristic p). Then for any finite p - group P, the ring RP is local and any finitely generated projective module $M \in {}_{RP}mod$ is free ([1] 5.25 pg. 115), so it is a direct sum of finitely many copies of the regular module RP. In particular M is a permutation module. Notice that a module $V \in {}_{RG}mod$ is projective if and only it is projective when restricted to any Sylow p - subgroup, so we conclude:

Corollary 3.3 *Let R be a local ring with $R/Rad\ R$ a field of characteristic p and $P \leq G$ a Sylow p - subgroup. Then for any projective module $V \in {}_{RG}mod$ we have:*

$$S(V)^G = R[T_X^G(\mathcal{P}_X^{(|G:X|)}) \mid X \leq P].$$

In particular the invariant ring is generated by elements of degree at most

$$max\{|G|, rank_R V \cdot (|G|-1)\}.$$

Final remarks: (i) Even if R is a field of characteristic p not dividing the order of G but less than $|G|$, it is not known yet if $\beta(V,G) \leq |G|$ holds. Proofs in the case of solvable groups have been given in [5] and [6].

(ii) If V is already a permutation module for G , a recent result of Göbel [3] shows that $S(V)^G$ can be generated by elements of degree at most $\frac{d(d-1)}{2}$ where $d = rank_R(V)$.

(iii) Notice that by 3.2 at least $max\{|G|, rank_R(V)(|G|-1)\}$ is an upper bound for generator degrees in the general coprime case. Moreover R does not have to be noetherian.

(iv) Suppose that V is a nontrivial absolutely irreducible and projective FG - module of dimension d. It is well known that V is liftable to characteristic zero and forms a block of defect zero. Therefore $d^2 \leq |G|-1$ (independent of the characteristic of $\mathbb{F}$). In particular we get

$$\beta(V,G) \leq (|G|-1)^{\frac{3}{2}}.$$

(v) If G is a finite group of Lie type, defined over a finite field $\mathbb{F}_q$ with $q = p^s$, then G has an irreducible projective $\mathbb{F}_q G$- module ST (the so called 'Steinberg module') whose dimension coincides with $|G|_p$, the order of a Sylow p - subgroup. Thus $\beta(ST,G) \leq |G|_p \cdot (|G|-1)$.

References

[1] C. W. Curtis, I. Reiner, *Methods of Representation Theory I*, John Wiley and Sons, New York (1981).

[2] P. Fleischmann, *A new degree bound for Vector Invariants of Symmetric Groups*, to appear in Transactions of the AMS.

[3] M. Göbel, *Computing bases for rings of permutation- invariant polynomials*, J. Symb. Comp. **19** (1995), 285-291.

[4] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p*, Nachr. Ges. Wiss. Göttingen (1926), 28-35, in 'Collected Papers', pp.485-492, Springer Verlag, Berlin (1983).

[5] D. Richman, *Explicit generators of the invariants of finite groups*, Adv. Math. **124** (1997), 49-76.

[6] L. Smith, *E. Noether's bound in the invariant theory of finite groups*, Arch. Math. **66** (1995), 89-92.