Unspecified Journal
Volume 00, Number 0, Pages 000–000
S ????-????(XX)0000-0

# ON THE HILBERT IDEAL

MARA D. NEUSEL

Abstract. We prove the Hilbert number conjecture.

## 1. Introduction

Let $\mathbb{F}$ be a field, $G$ a finite group. Consider a faithful representation

$$\rho : G \hookrightarrow \mathsf{GL}(n, \mathbb{F}).$$

It induces a $G$-action on the vector space $V = \mathbb{F}^n$ by matrix multiplication and thus on the dual space $V^*$. We extend this action additively and multiplicatively to the symmetric algebra on $V^*$, denoted by $\mathbb{F}[V]$. Once we choose a basis $x_1, \ldots, x_n$ for $V^*$ we can identify

$$\mathbb{F}[V] \cong \mathbb{F}[x_1, \ldots, x_n]$$

as the ring of polynomial functions in $n$ indeterminates over the field $\mathbb{F}$. We are interested in the subalgebra

$$\mathbb{F}[V]^G \hookrightarrow \mathbb{F}[V]$$

of $G$-invariant polynomials. By a classical result due to E. Noether the ring of invariants $\mathbb{F}[V]^G$ is finitely generated as an $\mathbb{F}$-algebra. Furthermore, since our action is $\mathbb{F}$-linear we can assume that the generators of $\mathbb{F}[V]^G$ are homogeneous polynomials. We define $\beta(\mathbb{F}[V]^G)$ to be the maximal degree of an algebra generator in a minimal algebra generating set. This number is usually called the Noether number. If the group order, $|G|$, is invertible in $\mathbb{F}$, the nonmodular case, then $\beta(\mathbb{F}[V]^G) \leq |G|$, independent of the representation, see Theorem 2.3.3 in [8]. In the modular case, i.e., $|G| = 0 \in \mathbb{F}$, the value of $\beta(\mathbb{F}[V]^G)$ usually depends on the degree of the representation or the order of the field and the group order, see [3] for an overview on degree bounds, see [4] and [5] for recent results.

In this paper we consider not the ring of invariant polynomials but the Hilbert ideal

$$\mathfrak{h}(V, G) = (\overline{\mathbb{F}[V]^G}) \subseteq \mathbb{F}[V]$$

which is by definition generated by all homogeneous invariant polynomials of positive degree. The Hilbert number, denoted by $\beta(\mathfrak{h}(()V, G))$ is the maximal degree of an ideal generator in a minimal ideal generating set. In [1] it has been conjectured that the Hilbert ideal is, in contrast to the ring of invariants, always generated by invariants of degree at most group order. Of course, in the nonmodular case this

Received by the editors December 3, 2007.
2000 *Mathematics Subject Classification.* Primary 13A50 Commutative Rings.
*Key words and phrases.* invariant theory of finite groups, degree bounds, Hilbert ideal, Hilbert number.

follows from Noether's bound. Furthermore, this conjecure was proven for permutation representations in [2] and for indecomposable representations of $\mathbb{Z}/p$ in [9]. In this paper we prove this conjecture for all representations. While typing this manuscript I learned that the same conjecture has been proven simulteneously by Symonds, [10].

## 2. The Proof

Consider the induced $\mathbb{F}G$-module $\mathbb{F}G \otimes_{\mathbb{F}} V$ and the canonical inclusion

$$V \hookrightarrow \mathbb{F}G \otimes_{\mathbb{F}} V.$$

This induces a $G$-equivariant projection

$$\eta_G : \mathbb{F}[\mathbb{F}G \otimes_{\mathbb{F}} V] \longrightarrow \mathbb{F}[V]$$

of $\mathbb{F}$-algebras. Upon restriction to the respective rings of invariants we obtain the classical Noether map

$$\eta_G^G : \mathbb{F}[\mathbb{F}G \otimes_{\mathbb{F}} V]^G \longrightarrow \mathbb{F}[V]^G.$$

This map remains surjective in the classical nonmodular case. However in the modular case it often fails to be surjective, see [6] and [7] for a thorough study of the Noether map.

In the nonmodular case the ring of invariants and hence the Hilbert ideal is generated by polynomials of degree at most group order. Thus we restrict our attention to the modular case and obtain a commutative diagram as follows.

$$\begin{array}{ccc} \mathbb{F}[\mathbb{F}G \otimes_{\mathbb{F}} V] & \overset{\eta_G}{\twoheadrightarrow} & \mathbb{F}[V] \\ \cup & & \cup \\ & & \mathbb{F}[V]^G \\ & & \cup \\ \mathbb{F}[\mathbb{F}G \otimes_{\mathbb{F}} V]^G & \overset{\eta_G^G}{\twoheadrightarrow} & \mathrm{Im}(\eta_G^G) \end{array}$$

Note that $G$ acts by permutations on $\mathbb{F}G \otimes_{\mathbb{F}} V$. Thus by Fleischmann's result, [2], we have

$$\beta(\mathfrak{h}(\mathbb{F}G \otimes_{\mathbb{F}} V, G)) \leq |G|.$$

Therefore

$$(\star) \qquad \beta(\overline{\mathrm{Im}(\eta_G^G)}) \leq |G|,$$

where $\overline{\mathrm{Im}(\eta_G^G)} \subseteq \mathbb{F}[V]$ denotes the ideal generated by the invariants of positive degree in the image of the Noether map.

Furthermore, the kernel of $\eta_G$ is generated by linear forms. Moreover, $\mathrm{Ker}(\eta_G) \subseteq \mathbb{F}[\mathbb{F}G \otimes V]$ is a prime ideal of height $n|G| - |G|$. Thus we obtain the following chains of ideals

$$\begin{array}{rccc} & \mathbb{F}[\mathbb{F}G \otimes_{\mathbb{F}} V] & \overset{\eta_G}{\twoheadrightarrow} & \mathbb{F}[V] \\ & \cup & & \cup \\ \mathrm{Ker}(\eta_G) \subseteq & \eta_G^{-1}(\overline{\mathrm{Im}(\eta_G^G)}) & & \overline{\mathrm{Im}(\eta_G^G)} \\ & \cup & & \\ & \mathfrak{h}(\mathbb{F}G \otimes V, G) & & \end{array}$$

Let $I \subseteq \mathfrak{h}(V,G) \subseteq \mathbb{F}[V]$ be the ideal generated by all $G$-invariant polynomials of positive degree at most group order. We want to show that $I = \mathfrak{h}(V,G)$. By Inequality $(\star)$ we have

$$\overline{\mathrm{Im}(\eta_G^G)} \subseteq I \subseteq \mathfrak{h}(V,G) \subseteq \mathbb{F}[V].$$

Thus we can extend the above diagram to the following

$$\begin{array}{rccc} & \mathbb{F}[\mathbb{F}G \otimes_{\mathbb{F}} V] & \overset{\eta_G}{\twoheadrightarrow} & \mathbb{F}[V] \\ & \cup & & \cup \\ & \eta_G^{-1}(\mathfrak{h}(V,G)) & & \mathfrak{h}(V,G) \\ & \cup & & \cup \\ & \eta_G^{-1}(I) & & I \\ & \cup & & \cup \\ \mathrm{Ker}(\eta_G) \subseteq & \eta_G^{-1}(\overline{\mathrm{Im}(\eta_G^G)}) & & \overline{\mathrm{Im}(\eta_G^G)} \\ & \cup & & \\ & \mathfrak{h}(\mathbb{F}G \otimes V, G) & & \end{array}$$

We collect some properties of the ideals involved in the following lemma.

**Lemma 2.1.** *The ideals $I \subseteq \mathfrak{h}(V,G) \subseteq \mathbb{F}[V]$ as well as the ideals $\eta_G^{-1}(I) \subseteq \eta_G^{-1}(\mathfrak{h}(V,G)) \subseteq \mathbb{F}[\mathbb{F}G \otimes V]$ are closed under the action of the group $G$.*

*Proof.* The first two ideals are by definition generated by invariant polynomials. Thus they are closed under the $G$-action. Since the map $\eta_G$ is $G$-equivariant, the latter two are also closed under the $G$-action. □

Next we present a series a reduction arguments. The first one shows that it is enough to prove that the inverse images of $I$ and $\mathfrak{h}(V,G)$ in $\mathbb{F}[\mathbb{F}G \otimes V]$ are equal.

**Lemma 2.2.** *If $\eta_G^{-1}(\mathfrak{h}(V,G)) = \eta_G^{-1}(I)$ then $\mathfrak{h}(V,G) = I$.*

*Proof.* By construction we have $I \subseteq \mathfrak{h}(V,G)$. To prove the reverse inclusion let $f \in \mathfrak{h}(V,G)$. Then there exists an element $F \in \eta_G^{-1}(\mathfrak{h}(V,G)) = \eta_G^{-1}(I)$ with

$$f = \eta_G(F) \in \eta_G(\eta_G^{-1}(\mathfrak{h}(V,G))) = \eta_G(\eta_G^{-1}(I)) = I$$

as desired. □

The third lemma shows that it is enough to consider elements that map onto $G$-invariant polynomials under the Noether map.

**Lemma 2.3.** *If $F \in \eta_G^{-1}(I)$ for all $F \in \mathbb{F}[\mathbb{F}G \otimes V]$ with $\eta_G(F) = f \in \mathbb{F}[V]^G$, then $\eta_G^{-1}(I) = \eta_G^{-1}(\mathfrak{h}(V,G))$.*

*Proof.* The inclusion $\subseteq$ is true by construction. To prove the reverse inclusion let $H \in \eta_G^{-1}(\mathfrak{h}(V,G))$ be an arbitrary element. Then

$$\eta_G(H) = \sum \alpha_i f_i \in \mathfrak{h}(V,G),$$

where $f_i \in \mathbb{F}[V]^G$ have positive degree and $\alpha_i \in \mathbb{F}[V]$. By assumption for each $i$ there exists an $F_i \in \eta_G^{-1}(I)$ such that $\eta_G(F_i) = f_i$. Thus

$$H = \sum A_i F_i + K \in \eta_G^{-1}(I),$$

for some $\eta_G(A_i) = \alpha_i$ and $K \in \mathrm{Ker}(\eta_G)$. □

We write

$$\mathbb{F}G \otimes V = \operatorname{span}_{\mathbb{F}} \begin{Bmatrix} x_{1g_1} & \dots & x_{1g_{|G|}} \\ x_{2g_1} & \dots & x_{2g_{|G|}} \\ \vdots & & \vdots \\ x_{ng_1} & \dots & x_{ng_{|G|}} \end{Bmatrix}$$

for some enumeration of the group elements $G = \{g_1, \dots, g_{|G|}\}$. Withoutloss of generality we assume that $g_1 = 1 \in G$ is the identity element. Then the group $G$ acts on the first index, and the Noether map is given by

$$\eta_G(x_{ig_j}) = g_j x_i \in \mathbb{F}[V].$$

We choose the reverse lexicographic order $x_{1g_1} < \dots < x_{1g_{|G|}} < x_{2g_1} < \dots < x_{ng_{|G|}}$.

We note that for any polynomial $f = \sum a_i x_1^{i_1} \cdots x_n^{i_n} \in \mathbb{F}[V]$, where $a_i \in \mathbb{F}$, there exists an inverse image

$$F = \eta_G^{-1}(f) = \sum a_i x_{11}^{i_1} \cdots x_{n1}^{i_n} \in \mathbb{F}[\mathbb{F}G \otimes V]$$

whose terms are monomials in the elements of the first column of $(x_{ig_j})_{ig_j}$.

**Lemma 2.4.** *Let $f \in \mathfrak{h}(V,G)$, and assume that the inverse image $F$ of $f$ consisting of terms in the first column is an element in $\eta_G^{-1}(I)$. Then all inverse images of $f$ lie in $\eta_G^{-1}(I)$.*

*Proof.* Since two elements $F$ and $F'$ of $\eta_G^{-1}(f)$ differ by an element in the kernel of $\eta_G$ which in turn is contained in $\eta_G^{-1}(I)$, the result follows. □

We want to prove our statement degree-wise by induction on the term order. The next result constitutes the induction start for every degree.

**Proposition 2.5.** *Let $F \in \eta_G^{-1}(\mathfrak{h}(V,G))$ have degree $d$. Let $F$ be minimal with respect to the reverse lexicographic order. Assume that the ideals $\eta_G^{-1}(I)$ and $\eta_G^{-1}(\mathfrak{h}(V,G))$ coincide in degree less than $d$. Then $F \in \eta_G^{-1}(I)$.*

*Proof.* The unique minimal monomial in $\mathbb{F}[\mathbb{F}G \otimes V]$ of degree $d$ is $x_{11}^d$. If $G$ is a $p$-group we assume without loss of generality that $G$ fixes $x_1$, then $x_1 \in I$ and thus $x_{11} \in \eta_G^{-1}(I)$.

Now, let $G$ be an arbitrary group with $p$-Sylow subgroup $P$ fixing $x_1$. Order the elements of $G$ such that $g_2 \in P$ is a nontrivial element. Then $\eta_G(x_{1g_2}) = g_2 x_1 = x_1$. We have to consider two cases:

CASE: $x_{11}^d \notin \eta_G^{-1}(\mathfrak{h}(V,G))$

In this case we have

$$F = x_{11}^{d-1}(x_{11} - x_{1g_2}) \in \operatorname{Ker}(\eta_G) \subseteq \eta_G^{-1}(\mathfrak{h}(V,G)).$$

Its leading term is $x_{11}^{d-1}x_{1g_2}$ and is thus the smallest leading term of an element of degree $d$ in $\eta_G^{-1}(\mathfrak{h}(V,G))$. Furthermore, $\eta_G^{-1}(I)$ contains the kernel of $\eta_G$ and hence it contains $x_{11}^{d-1}(x_{11} - x_{1g_2})$. Finally, note that $F$ is the unique polynomial in $\eta_G^{-1}(\mathfrak{h}(V,G))$ with this leading term.

CASE: $x_{11}^d \in \eta_G^{-1}(\mathfrak{h}(V,G))$

Then $\eta_G(x_{11}^d) = x_1^d \in \mathfrak{h}(V,G)$. Thus if $d \leq |G|$ it follows that $x_1^d \in I$ by definition of $I$, and hence $x_{11} \in \eta_G^{-1}(I)$. Otherwise we have

$$x_1^d = \sum_i \alpha_i f_i$$

for some $G$-invariant polynomials $f_i$. If the degree of the $\alpha_i$'s is positive, we have $f_i \in I$ by assumption, and thus

$$x_{11}^d = \sum_i A_i F_i + K \in \eta_G^{-1}(I)$$

for $\eta_G(F_i) = f_i$, $\eta_G(A_i) = \alpha_i$, and an element $K$ in the kernel. Finally assume we have

$$x_1^d = f_0 + \sum_i \alpha_i f_i.$$

Then the relative transfer gives

$$\mathrm{Tr}_P^G(x_1^d) = |G:P| f_0 + \sum_i \mathrm{Tr}_P^G(\alpha_i) f_i.$$

Since $d > |G|$ we can apply Lemma 2.2 in [2] and obtain

$$\mathrm{Tr}_P^G(x_1^d) \in I.$$

Hence

$$f_0 = \frac{1}{|G:P|}(\mathrm{Tr}_P^G(x_1^d) - \sum_i \mathrm{Tr}_P^G(\alpha_i) f_i) \in I.$$

So, finally we get

$$x_{11}^d \in \eta_G^{-1}(x_1^d) = \eta_G^{-1}(f_0 + \sum_i \alpha_i f_i) \subseteq \eta_G^{-1}(I)$$

as desired. □

We need one more preparation:

**Lemma 2.6.** *Let $M, M' \in \mathbb{F}[\mathbb{F}G \otimes V]$ be monomials of the same degree. Assume that $M$ consists of elements in the first column, and assume that $M > M'$ in the reverse lexicographic order. Then for all $g \in G$ we have that $gM > gM'$.*

*Proof.* $M$ is a monomial in the first column, say

$$M = x_{1,1}^{i_1} \cdots x_{n,1}^{i_n}.$$

Thus

$$gM = x_{1,g}^{i_1} \cdots x_{n,g}^{i_n}$$

is a monomial in the $g$th column.

We turn to the monomial $M'$. Since $M'$ is smaller it must look like

$$M' = x_{n,1}^{i_n} \ldots x_{j+1,1}^{i_{j+1}} x_{j,1}^{k_j} N$$

where $N$ is a monomial avoiding the columns $j$ through $n$ and $k_j < i_j$. Thus $gM'$ looks like

$$gM' = x_{n,g}^{i_n} \ldots x_{j+1,g}^{i_{j+1}} x_{j,g}^{k_j} gN$$

where $gN$ still avoids columns $j$ through $n$. Thus $gM' < gM$. □

The following result proves the Hilbert ideal conjecture for $p$-groups in characteristic $p$.

**Theorem 2.7.** *Let $P$ be a $p$-group, and assume that $\rho(P) \subseteq \mathsf{GL}(n, \mathbb{F})$ is in lower triangular form, i.e., $gx_i \in \mathrm{span}_{\mathbb{F}}\{x_1, \ldots, x_n\}$. Then*

$$\mathfrak{h}(V, P) = I.$$

*Proof.* By Lemma 2.2 it is enough to show that $\eta_G^{-1}(\mathfrak{h}(()V,G)) = \eta_G^{-1}(I)$. The inclusion " $\supset$ " is valid by construction. To show the reverse inclusion we proceed by double induction on degree and term order.

Let $F \in \eta_P^{-1}(\mathfrak{h}(V,P))$ be an element of degree $d$. If $d \leq |G|$ there is nothing to show. Thus we assume that the degree of $F$ is strictly larger than the group order.

By Lemma 2.4 we can assume that $F$ lives in the first column and by Lemma 2.3 we can assume that $\eta_P(F)$ is invariant.

Since the induction start is proven in Proposition 2.5 we assume that for all elements of smaller degree or same degree and lower in term order we have shown that it is in $\eta_G^{-1}(I)$. We write $F$ as a sum of monomials

$$F = M_0 + M_1 + \cdots + M_k$$

and without loss of generality we assume that $M_0 > M_1 > \cdots > M_k$.

Let $r = \max\{1,\dots,n\}$ such that the variable $x_{r1}$ appears in $F$.

CASE: $M_0 = x_{r1}^d$

We consider the top orbit Chern class of $x_r$

$$c_{\text{top}}(x_r) \in \mathbb{F}[V]^P$$

which is a polynomial of degree, say, $t$ with leading term $x_r^d$. Note that $t$ cannot exceed the group order. We find an inverse image $C \in \eta_P^{-1}(c_{\text{top}}(x_r))$ in the first column

$$C \in \mathbb{F}[x_{11}, x_{21}, \dots, x_{r1}].$$

We note that this polynomial is by construction in $\eta_P^{-1}(I)$. Then

$$F - C^{d-t}$$

lies in $\eta_P^{-1}(\mathfrak{h}(V,P))$ and has lower leading term than $F$. Thus by induction

$$F - C^{d-t} \in \eta_P^{-1}(I)$$

and thus $F \in \eta_P^{-1}(I)$ as desired.

CASE: Assume that $M_0 = x_{r1}^i N_0$, where $N_0$ has positive degree and $x_{r1}$ does not divide $N_0, M_1, \dots, M_k$.

Since $\eta_P(F)$ is invariant we have that $gF - F \in \text{Ker}(\eta_P) \subseteq \eta_P^{-1}(I)$ for all $g \in P$. Since $x_{r1}$ appears solely in $M_0$, we have that $x_r | \eta_P(M_0) = m_0$ but it does not divide any of the other $\eta_P(M_i)$ for $i = 1, \dots, k$. Since $\eta_P(gF - F) = g\eta_P(F) - \eta_P(F) = 0$ the terms with the same $x_r$-degree must cancel. Thus

$$\eta_P(gM_0 - M_0) = g(x_r)^i g n_0 - x_r^i n_0 = x_r^i(gn_0 - n_0) + R,$$

where the remainder $R$ has lower $x_r$-degree and $\eta_G(N_0) = n_0$. Thus $gn_0 - n_0 = 0$ and $n_0$ is an invariant of strictly smaller degree than $m_0$. Thus $N_0 \in \eta_P^{-1}(I)$, therefore $M_0 \in \eta_P^{-1}(I)$. Hence

$$F - M_0 \in \eta_P^{-1}(\mathfrak{h}(V,P))$$

has strictly smaller term-order, and is by induction in $\eta_P^{-1}(I)$. Thus $F \in \eta_P^{-1}(I)$.

CASE: $x_{r1}$ divides $M_0, \dots, M_j$ but none of the other terms of $F$

Write

$$M_0 = x_{r1}^{i_1} N_0, \ \dots, \ M_j = x_{r1}^{i_j} N_j$$

If $i_1 > \max\{i_2, \dots, i_j\}$, then the preceding argument goes through without change. Thus we assume that $i_1 = i_2 = \cdots = i_l$ for some $1 < l \leq j$. Since $M_0 > M_1 >$

$\cdots > M_l$ there exists a largest index $s$, $1 \leq s \leq r-1$, such that the monomials differ. Hence we can write

$$M_0 = x_{r1}^{i_r} x_{r-1,1}^{i_{r-1}} \cdots x_{s+1,1}^{i_{s+1,1}} x_{s1}^{i_{s,1}} N_0, \ \ldots, \ M_l = x_{r1}^{i_r} x_{r-1,1}^{i_{r-1}} \cdots x_{s+1,1}^{i_{s+1,1}} x_{s1}^{j_{s,1}} N_l.$$

Similar to the above we obtain that

$$x_{s1}^{i_{s,1}} N_0 + \cdots + x_{s1}^{j_{s,1}} N_l$$

maps under $\eta_P$ to an invariant. By construction it has lower degree than $F$ and is thus in $\eta_P^{-1}(I)$. Here we can apply the argument of the preceding case to find that $N_0 \in \eta_P^{-1}(I)$. □

Finally, we are prepared to prove the Hilbert number conjecture for all groups and representations.

**Theorem 2.8.** *Let $\rho : G \hookrightarrow \mathsf{GL}(n, \mathbb{F})$ be a faithful representation of a finite group over an arbitrary field $\mathbb{F}$. Then*

$$\mathfrak{h}(V, G) = I$$

*and hence the Hilbert number is bounded above by the group order*

$$\beta(\mathfrak{h}(V, G)) = \beta(I) \leq |G|.$$

*Proof.* By Lemma 2.2 it is enough to show that $\eta_G^{-1}(\mathfrak{h}(()V, G)) = \eta_G^{-1}(I)$. The inclusion " $\supset$ " is valid by construction. To show the reverse inclusion we proceed as above by double induction on degree and term order.

Let $F \in \eta_G^{-1}(\mathfrak{h}(V, G))$.If degree if $F$ is at most group order then $F \in \eta_G^{-1}(I)$ by construction. Thus we assume that $\deg(F) = d > |G|$.

The polynomial of minimal leading term of degree $d$ in $\eta_G^{-1}(\mathfrak{h}(V, G))$ is contained in $\eta_G^{-1}(I)$ by Proposition 2.5.

Thus assume that the leading term of $F$ is not minimal, and all polynomials of degree less than $d$ or of degree $d$ with smaller leading term than $F$ are in $\eta_G^{-1}(I)$.

We denote the leading term of $F$ by $\mathsf{LT}(F)$. We note that by Lemmata 2.3 and 2.4 we may assume that $F$ is a polynomial in the first column mapping under $\eta_G$ onto an invariant polynomial.

We note also that the leading term of $gF$ is strictly larger than $F$ for all $g \neq 1$, because $F$ lives in the first column, while $gF$ lives in the $g$th column.

Since $F$ maps to an invariant polynomial under $\eta_G$ we have that $gF - F \in \mathrm{Ker}(\eta_G) \subseteq \eta_G^{-1}(I)$. Thus

$$\mathsf{LT}(gF - F) = \mathsf{LT}(gF) \in \mathsf{LT}(\mathrm{Ker}(\eta_G)) \subseteq \mathsf{LT}(\eta_G^{-1}(I)),$$

where $\mathsf{LT}(I)$ denotes the ideal of leading terms of the ideal $I$.

Hence there exists an element $H \in \eta_G^{-1}(I)$ such that $\mathsf{LT}(H) = \mathsf{LT}(gF)$. If $H = gF$ we are done by Lemma 2.3.

Otherwise, consider $gF - H \in \eta_G^{-1}(\mathfrak{h}(V, G))$ with $\mathsf{LT}(gF - H) < \mathsf{LT}(gF)$.

If $\mathsf{LT}(gF - H) < \mathsf{LT}(F)$, then $gF - H \in \eta_G^{-1}(I)$ by induction on the term order, and thus $gF \in \eta_G^{-1}(I)$. Hence $F \in \eta_G^{-1}(I)$. Otherwise, we consider the polynomial $(gF - F) - H$ which is an element in $\eta_G^{-1}(I)$.

If $\mathsf{LT}(gF - F - H) > \mathsf{LT}(F)$, we pick an element $K_1 \in \eta_G^{-1}(I)$ such that $\mathsf{LT}(K_1) = \mathsf{LT}(gF - F - H)$. Then

$$\mathsf{LT}(gF - F - H - K_1) < \mathsf{LT}(gF - F - H)$$

and we can proceed inductively and find $K_1, \dots, K_l \in \eta_G^{-1}(I)$ such that

$$\mathsf{LT}(gF - F - H - K_1 - \cdots - K_l) \leq \mathsf{LT}(F).$$

Thus we may assume without loss of generality that $\mathsf{LT}(gF - F - H) \leq \mathsf{LT}(F)$. If there exists an element $H$ such that $\mathsf{LT}(gF - F - H) = \mathsf{LT}(F)$, we have

$$\mathsf{LT}(gF - F - H - F) < \mathsf{LT}(gF - F - H) = \mathsf{LT}(F).$$

By construction $gF - F - H - F \in \eta_G^{-1}(\mathfrak{h}(V, G))$ and thus by induction on the term order in $\eta_G^{-1}(I)$. Since $H$ as well as $gF - F$ are in $\eta_G^{-1}(I)$ we conclude that $F \in \eta_G^{-1}(I)$.

Finally we have to take care of the case $\mathsf{LT}(gF - F - H) < \mathsf{LT}(F)$ for all $H \in \eta_G^{-1}(I)$ and all $g \in G$.

Recall that $F$ is a polynomial in the first column and that $\eta_G(F) = f$ is invariant. We write it as a sum of monomials

$$F = M_0 + M_1 + \cdots + M_k$$

and assume without loss of generality that $M_0 > M_1 > \cdots > M_k$ in the term-order. Then

$$gF = gM_0 + gM_1 + \cdots + gM_k$$

has leading term $gM_0$ by Lemma 2.6. Since the leading term of $gF - F - H$ is strictly smaller than the leading term of $F$ we have

$$H = gM_0 - M_0 + \sum_{K_i < M_0} K_i \in \eta_G^{-1}(I),$$

where the $K_i$'s are monomials smaller than $M_0$.

We choose an element $g \in G$ of maximal order $s$. We order the group elements such that

$$x_{i1} < x_{ig} < x_{ig^2} < \cdots < x_{ig^{s-1}}.$$

We consider

$$g^{s-1}F = g^{s-1}M_0 + \cdots + g^{s-1}M_k$$

and note that

$$\eta_G(g^{s-1}F) = g^{s-1}\eta_G(F) = g^{s-1}f = f = \eta_G(F).$$

Thus there exists a polynomial $\tilde{H} \in \eta_G^{-1}(I)$ with the same leading term as $g^{s-1}F$. Moreover,

$$\tilde{H} = g^{s-1}M_0 - M_0 + \sum_{K_i < M_0} K_i,$$

because $\mathsf{LT}(g^{s-1}F - \tilde{H} - F) < \mathsf{LT}(F)$ by assumption. Thus

$$g^{s-1}\tilde{H} = g^{s-2}M_0 - g^{s-1}M_0 + \sum_{K_i < M_0} g^{s-1}K_i$$

has leading term $g^{s-1}M_0$, the same leading term as $g^{s-1}F$. Hence

$$g^{s-1}F - (-g^{s-1}H) - F =$$
$$g^{s-1}M_1 + \cdots + g^{s-1}M_k + \sum_{K_i < M_0} g^{s-1}K_i + g^{s-2}M_0 - M_0 - \cdots - M_k.$$

By assumption this polynomial must be smaller than $F$. However, $M_0 < g^{s-2}M_0$ unless $g^{s-2} = 1$. Thus the element $g$ must have order 2. Since $g$ was an element of maximal order in $G$, it follows that $G$ is an elementary abelian 2-group. Thus

if the characteristic of the ground field is not two, we are in the nonmodular case, and the result follows from Noether's bound. If the characteristic is two, then the result follows from the preceding Theorem 2.7. □

## References


1. Harm Derksen and Gregor Kemper, *Computational Invariant Theory*, Encyclopaedia of Mathematical Sciences Vol. 130, Springer Verlag, Berlin 2002.
2. Peter Fleischmann, On Invariant Theory of Finite Groups, *Centre de Recherches Mathématiques Proceedings and Lecture Notes* Vol 35 (2004), 43-69.
3. Mara D. Neusel, Degree Bounds - An Invitation to Postmodern Invariant Theory -, *Topology and its Applications* 154 (2007), 792-814.
4. Mara D. Neusel, Degree Bounds and the Regular Representation, preprint, 2007.
5. Mara D. Neusel and Müfit Sezer, The Invariants of Modular Indecomposable Representations of $\mathbb{Z}_{p^2}$, *Mathematische Annalen*, to appear.
6. Mara D. Neusel and Müfit Sezer, The Noether Map I, *Forum Mathematicum*, to appear.
7. Mara D. Neusel and Müfit Sezer, The Noether Map II, *Proceedings of the AMS* 135 (2007), 2347-2354.
8. Mara D. Neusel and Larry Smith, *Invariant Theory of Finite Groups*, Math. Surveys and Monographs Vol. 94, AMS, Providence RI 2002.
9. Müfit Sezer, A Note on the Hilbert Ideal of a Cyclic Group of Prime Order, *Journal of Algebra*, to appear.
10. Peter Symonds, On Castelnuovo-Mumford of Rings of Invariants, preprint, 2007.


Department of Mathematics and Statistics, MS 1042, Texas Tech University, Lubbock, Texas 79409

*E-mail address*: Mara.D.Neusel@ttu.edu