ON A THEOREM OF BARBARA SCHMID

LARRY SMITH

(Communicated by Wolmer V. Vasconcelos)

Abstract. Let $G$ be a finite group and $\rho: G \to GL(n, \mathbb{C})$ a complex representation. Barbara Schmid has shown that the algebra of invariant polynomial functions $\mathbb{C}[V]^G$ on the vector space $V = \mathbb{C}^n$ is generated by homogeneous polynomials of degree at most $\beta$, where $\beta$ is the largest degree of a generator in a minimal generating set for $\mathbb{C}[\text{reg}_{\mathbb{C}}(G)]^G$, and $\text{reg}_{\mathbb{C}}(G)$ is the complex regular representation of $G$. In this note we give a new proof of this result, and at the same time extend it to fields $\mathbb{F}$ whose characteristic $p$ is larger than $|G|$, the order of the group $G$.

Let $\rho: G \to GL(n, \mathbb{F})$ be a representation of a finite group $G$ over the field $\mathbb{F}$. Then $G$ acts on the vector space $V = \mathbb{F}^n$, and hence also on the algebra $\mathbb{F}[V]$ of polynomial functions on $V$. The algebra fixed by this action is called the ring of invariants, and is denoted by $\mathbb{F}[V]^G$. Note that $\mathbb{F}[V]^G$ depends on $\rho$, but $\rho$ does not appear in the notation. Despite this, no confusion should arise.

By theorems of D. Hilbert [1] and E. Noether [2, 3] it is known that $\mathbb{F}[V]^G$ is finitely generated as an algebra over $\mathbb{F}$ (see also [5], Chapter 2, to which we refer for basic facts from invariant theory). The maximal degree of a generator in any minimal generating set for $\mathbb{F}[V]^G$ is denoted by $\beta(\rho)$. This is nothing but the degree of the Poincaré polynomial $P(\mathbb{F}[V]^G, t)$ of the module of indecomposable elements

$$Q\mathbb{F}[V]^G = \mathbb{F} \otimes_{\mathbb{F}[V]} \mathbb{F}[V]^G = \mathbb{F}[V]^G / (\mathbb{F}[V])^2,$$

where $\mathbb{F}[V]$ denotes the augmentation ideal of $\mathbb{F}[V]^G$. (See for example [4], Chapter 4 and Section 5.1.) In [4] Barbara Schmid proved, among other things, that for a complex representation $\rho: G \to GL(n, \mathbb{C})$

$$\beta(\rho) \leq \beta(\text{reg}_{\mathbb{C}}(G)),$$

where $\text{reg}_{\mathbb{C}}(G): G \to GL(|G|, \mathbb{C})$ is the complex regular representation of $G$. The purpose of this note is to provide what I feel is a more conceptual proof of this theorem, which, at the same time extends the result to the strong nonmodular case [7]. Specifically, we will prove:

Theorem. Let $G$ be a finite group of order $d$ and $\mathbb{F}$ a field of characteristic $p$. If $p > d$, then $\beta(\rho) \leq \beta(\text{reg}_{\mathbb{F}}(G))$ for any representation $\rho: G \to GL(n, \mathbb{F})$, where $\text{reg}_{\mathbb{F}}(G): G \to GL(d, \mathbb{F})$ is the regular representation of $G$ over the field $\mathbb{F}$.

Received by the editors July 1, 1998 and, in revised form, September 8, 1998.

1991 Mathematics Subject Classification. Primary 13A50.

1It is perhaps worthwhile to note that the proof of [4] uses the complete reducibility of $GL(n, \mathbb{C})$ in an essential way, so it cannot be extended to arbitrary ground fields. In particular, it does not extend to the strong non-nonmodular case.
This research was done in the course of preparing a series of lectures on the invariant theory of finite groups which were presented at the University of Minnesota School of Mathematics in the spring quarter of 1998 when the author was an Ordway Visitor. I would like to thank the participants in the lecture series for their attentive, critical attitude, and their often penetrating questions, and the School of Mathematics for providing an atmosphere conducive to productive research and study.

The proof of the theorem relies on the main result of [8] (see also [5], Theorem 3.1.10) and the following Proposition. Taken together I think these results explain conceptually why the regular representation provides a universal upper bound for \( \beta(\rho) \).

**Proposition.** Let \( \mathbb{F} \) be a field, \( G \) a finite group, and \( \Omega \) a finite transitive \( G \)-set. Then \( \Omega \) occurs as an orbit in the regular representation of \( G \) defined over \( \mathbb{F} \).

**Proof.** Identify the regular representation of \( G \) over \( \mathbb{F} \) with the action of \( G \) from the left on the group ring \( \mathbb{F}(G) \) of \( G \) over \( \mathbb{F} \). If \( H \subset G \) is the isotropy group of a point of \( \Omega \), then we may identify \( \Omega \) as a \( G \)-set with the left action of \( G \) on the left cosets of \( H \) in \( G \), so \( \Omega \cong G/H \) as \( G \)-sets. Let

\[
\sigma_H = \sum_{h \in H} h \in \mathbb{F}(G).
\]

Then the isotropy group of \( \sigma_H \) in \( \mathbb{F}(G) \) is \( H \), so the orbit of \( \sigma_H \) is also isomorphic to \( G/H \) as a left \( G \)-set. \( \square \)

**Proof of the Theorem.** Since \( d = |G| < p \), it follows from [8] (see also [5], Theorem 3.1.10) that \( \mathbb{F}[V]^G \) is generated by orbit Chern classes. Write \( V^* \) for the space of linear forms on \( V \). If \( B \subset V^* \) is an orbit of \( G \), then, by the Proposition, we may find a \( G \)-equivariant embedding \( B \hookrightarrow \mathbb{F}(G) \). This in turn induces an epimorphism

\[
\alpha_B : \mathbb{F}[\mathbb{F}(G)] \to \mathbb{F}[B],
\]

where \( \mathbb{F}[B] \) is the polynomial algebra in the formal variables \( \{b \in B\} \). Since \( p \nmid d \), passing to fixed subalgebras yields an epimorphism

\[
\alpha_B^G : \mathbb{F}[\mathbb{F}(G)]^G \to \mathbb{F}[B]^G.
\]

If \( k \) denotes the number of elements in \( B \), then the action of \( G \) on \( B \), being by permutations, leaves the elementary symmetric polynomials \( e_1, \ldots, e_k \) in the elements \( b \in B \) invariant, i.e.,

\[
\mathbb{F}[e_1(B), \ldots, e_k(B)] \subseteq \mathbb{F}[B]^G.
\]

The inclusion \( B \subset V^* \) induces a \( G \)-equivariant map

\[
\lambda_B : \mathbb{F}[B] \to \mathbb{F}[V],
\]

and, per definition [8],

\[
\lambda(e_i(B)) = c_i(B), \quad i = 1, \ldots, k,
\]

where \( c_1(B), \ldots, c_k(B) \in \mathbb{F}[V]^G \) are the Chern classes of the orbit \( B \). Therefore the composite

\[
\gamma_B : \mathbb{F}[\mathbb{F}(G)]^G \xrightarrow{\alpha_B^G} \mathbb{F}[B]^G \xrightarrow{\lambda_B} \mathbb{F}[V]^G
\]

contains the characteristic subalgebra of the orbit \( B \) in its image, i.e., \( \text{Im}(\gamma_B) \) contains the subalgebra of \( \mathbb{F}[V]^G \) generated by the orbit Chern classes \( c_1(B), \ldots, c_k(B) \in \mathbb{F}[V]^G \).
$F[V]^G$ of the orbit $B$. Since $F[V]^G$ is generated by orbit Chern classes, this means we can find a finite number $B_1, \ldots, B_m$ of orbits of $G$ in $V^*$ such that the map

$$\bigotimes_{i=1}^m F[F(G)]^G \to \bigotimes_{i=1}^m F[V]^G \to F[V]^G$$

is an epimorphism, where $\mu$ is the multiplication map. Since $\bigotimes_{i=1}^m F[F(G)]^G$ is generated by forms of degree at most $\beta_2(\text{reg}_G(G))$ the result follows. 

**References**


School of Mathematics, University of Minnesota, Minneapolis, Minnesota 55455

E-mail address: smith@math.umn.edu

Mathematisches Institut der Universität, D 37073 Göttingen, Germany

E-mail address: larry@sunrise.uni-math.gwdg.de