

AG-Invariantentheorie

ON A THEOREM OF BARBARA SCHMID

LARRY SMITH

AG-Invariantentheorie

AND

SCHOOL OF MATHEMATICS
UNIVERSITY OF MINNESOTA

ORDWAY LECTURE

SUMMARY : *Let G be a finite group and $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{C})$ 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 β , where β is the largest degree of a generator in a minimal generating set for $\mathbb{C}[\mathrm{reg}_{\mathbb{C}}(G)]^G$, and $\mathrm{reg}_{\mathbb{C}}(G)$ 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 $\rho : G \hookrightarrow \text{GL}(n, \mathbb{F})$ 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 ρ , but ρ 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 $P(Q\mathbb{F}[V]^G, t)$ of the module of indecomposable elements

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

where $\overline{\mathbb{F}[V]}^G$ denotes the augmentation ideal of $\mathbb{F}[V]^G$. (See for example [5] Chapter 4 and Section 5.1) In [4] Barbara Schmid proved, among other things, that for a complex representation $\rho : G \hookrightarrow \text{GL}(n, \mathbb{C})$

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

where $\text{reg}_{\mathbb{C}}(G) : G \hookrightarrow \text{GL}(|G|, \mathbb{C})$ 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 $\rho : G \hookrightarrow \text{GL}(n, \mathbb{F})$, where $\text{reg}_{\mathbb{F}}(G) : G \hookrightarrow \text{GL}(d, \mathbb{F})$ is the regular representation of G over the field \mathbb{F} .*

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 be a finite group, and Ω a finite transitive G -set. Then Ω 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 $H \leq G$ is the isotropy group of a point of Ω then we may identify Ω 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 σ_H in $\mathbb{F}(G)$ is H , so the orbit of σ_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

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

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

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

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, \dots, e_k in the elements $b \in B$ invariant, i.e.,

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

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

$$\beta_B : \mathbb{F}[B] \longrightarrow \mathbb{F}[V],$$

and, per definition [8],

$$\beta_B(e_i(B)) = c_i(B) \quad i = 1, \dots, k,$$

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

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

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 $c_1(B), \dots, c_k(B) \in \mathbb{F}[V]^G$ of the orbit B . Since $\mathbb{F}[V]^G$ is generated by orbit Chern classes, this means we can find a finite number B_1, \dots, B_m of orbits of G in V^* such that the map

$$\bigotimes_{i=1}^m : \bigotimes_{i=1}^m \mathbb{F}[\mathbb{F}(G)]^G \xrightarrow{\bigotimes_{i=1}^m \gamma_{B_i}} \bigotimes_{i=1}^m \mathbb{F}[V]^G \xrightarrow{\mu} \mathbb{F}[V]^G,$$

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

References

- [1] D. Hilbert, *Über die Theorie der Algebraischen Formen*, Math. Ann. 36 (1890), 473–534.
- [2] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. 77 (1916), 89–92.
- [3] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p* , Nachr. v. d. Ges. d. Wiss. zu Göttingen (1926), 28–35.
- [4] B. J. Schmid, *Finite Groups and Invariant Theory*, Séminaire d'Algèbre P. Dubriel et M.-P. Malliavin 1989-1990, Lecture Notes in Math. 1478, Springer-Verlag, Heidelberg, Berlin, 1991.
- [5] L. Smith, *Polynomial Invariants of Finite Groups*, (second printing), A.K. Peters Ltd., Wellesley, MA 1995, 1997.
- [6] L. Smith, *Noether's Bound in the Invariant Theory of Finite Groups*, Arch. der Math. 66 (1996), 89 – 92.
- [7] L. Smith, *Polynomial Invariants of Finite Groups, A Survey of Recent Results*, Bull. of the Amer. Math. Soc. 34 (1997), 211 – 250.
- [8] L. Smith and R. E. Stong, *On the Invariant Theory of Finite Groups: Orbit Polynomials and Splitting Principles*, J. of Algebra 110 (1987), 134–157.

Larry Smith
 School of Mathematics
 University of Minnesota
 Minneapolis, MN 55455
 USA
 e-mail: SMITH@MATH.UMN.EDU
 and

AG-Invariantentheorie

Mathematisches Institut der Universität
 D 37073 Göttingen
 Federal Republic of Germany
 e-mail: LARRY@SUNRISE.UNI-MATH.GWDG.DE