PUTTING THE SQUEEZE ON THE NOETHER GAP
THE CASE OF THE ALTERNATING GROUPS $A_n$

LARRY SMITH

AND

SCHOOL OF MATHEMATICS
UNIVERSITY OF MINNESOTA

SUMMARY: Let $\varphi : G \hookrightarrow \mathrm{GL}(n, \mathbb{F})$ be a faithful representation of the finite group $G$ over the field $\mathbb{F}$. In 1916 E. Noether proved that for $\mathbb{F}$ of characteristic zero the ring of invariants $\mathbb{F}[V]^G$ is generated as an algebra by the invariant polynomials of degree at most $|G|$. This result has been generalized to the case where the characteristic of $\mathbb{F}$ is greater than $|G|$, or when the characteristic of $\mathbb{F}$ is prime to the order of $G$ and the group $G$ is solvable. In this note we prove that if Noether’s bound fails in the nonmodular case, then it fails for a finite nonabelian simple group. We then show how yet another reworking of Noether’s argument leads to a proof that Noether’s bound holds in the nonmodular case for the alternating groups.

MATHEMATICS SUBJECT CLASSIFICATION: 13A50 Invariant Theory

Typeset by \LaTeX
Let $G$ be a finite group and $\rho : G \hookrightarrow \text{GL}(n, \mathbb{F})$ a faithful representation of $G$ over the field $\mathbb{F}$. Via $\rho$ the group $G$ acts on the vector space $V = \mathbb{F}^n$, and hence also on the graded algebra $\mathbb{F}[V]^G$ of homogeneous polynomial functions on $V$. The subalgebra of functions $\mathbb{F}[V]^G$ fixed by the action of $G$ is called the ring of invariants of $G$. As a general reference on invariant theory see [3].

In [2] E. Noether proved that whenever the characteristic of $\mathbb{F}$ is zero then $\mathbb{F}[V]^G$ is a finitely generated as an algebra over $\mathbb{F}$. In addition she gave an algorithm to construct a system of generators using polarizations of elementary symmetric polynomials (see also [6] VIII.B.15 or [3] §3.3). From this she deduced that $\mathbb{F}[V]^G$ is generated by invariant polynomials of degree at most $|G|$. This upper bound for the degrees of the generators in a minimal generating set is referred to as Noether’s bound.

If the ground field $\mathbb{F}$ has characteristic $p$, then (see [5] or [3] Theorem 3.1.10) Noether’s bound is known to hold if $p > |G|$, where $|G|$ denotes the order of the group $G$. It may fail (see for example [3] §4.2 Example 2) if $p$ divides $|G|$. If $p$ does not divide $|G|$, but, $p < |G|$, then Noether’s bound is known to hold for solvable groups [4], and it has been conjectured to hold in general. The region, $p < |G|$, but $p / |G|$, where Noether’s bound is not known either to hold or to fail, is the Noether gap of the title. The first goal of this note is to show that if Noether’s bound fails in the nonmodular case, then it fails for a finite nonabelian simple group. We then show how yet another reworking of one of Noether’s argument leads to a proof for the alternating groups that Noether’s bound holds in the nonmodular case.

This research was done while preparing a lecture on Noether’s bound for a Crash Course on Invariant Theory given by the author as Ordway Visitor at the School of Mathematics of the University of Minnesota. I would like to thank the more than twenty participants in this lecture series for their attentive and critical attitude, and probing questions.

§1. Reducing the Noether Gap to Simple Groups

Let us begin by introducing some notation. If $A$ is a graded connected commutative Noetherian algebra over a field $\mathbb{F}$, denote by $\beta(A)$ the maximum degree of a (homogeneous) generator of $A$ in any minimal generating set for $A$ as an $\mathbb{F}$ algebra. This is nothing but the degree of the Poincaré polynomial $P(A,t)$ of the module of indecomposables $QA := \mathbb{F} \otimes_A \hat{A} = \hat{A}/(\hat{A})^2$, where $\hat{A} \subset A$ denotes the augmentation ideal. (See [3] Chapter 4 and Theorem 5.2.5.) Hence $\beta(A)$ does not depend on the choice of minimal generating set. If $G$ is a finite group and $\rho : G \hookrightarrow \text{GL}(n, \mathbb{F})$ a faithful representation of $G$ over the field $\mathbb{F}$, then we denote $\beta(\mathbb{F}[V]^G)$ by $\beta(\rho)$. We set

$$\beta_{\text{IF}}(G) = \max \{ \beta(\rho) \mid \rho : G \hookrightarrow \text{GL}(n, \mathbb{F}) \}.$$

The following proposition is proved by a simple linearization process as in [4].

**Proposition 1.1:** Let $A$ be a graded connected commutative algebra over a field $\mathbb{F}$ and $G \leq \text{Aut}_.(A)$ a finite group of grading preserving automorphisms of $A$. If $|G| \in \mathbb{F}^\times$ then

$$\beta(A^G) \leq \beta(A)\beta_{\text{IF}}(G).$$
PROOF: Let \( V = \bigoplus_{i=1}^{\beta(A)} A_i \), where \( A_i \) denotes the homogeneous component of \( A \) of degree \( i \). The group \( G \) acts on \( V \) by linear automorphisms, and the natural map

\[
S(V) \to A
\]

is a \( G \)-equivariant epimorphism, where \( S(V) \) denotes the symmetric algebra on the graded vector space \( A \). (Apart from the grading on \( V \) this is just \( IF[V^*] \), where \( V^* \) is the dual of \( V \).) Since the characteristic of \( IF \) does not divide the order of \( G \) the induced map

\[
S(V)^G \to A^G
\]

is also onto, and, taking account of the maximum degree of an element of \( V \), yields the result. \( \square \)

**COROLLARY 1.2:** Let \( G \) be a finite group, \( N \triangleleft G \) a normal subgroup, and \( IF \) a field of characteristic \( p \). Suppose \( \varphi : G \to GL(n, IF) \) is a representation of \( G \) over \( IF \) and \( \varphi|_N \) the restriction of \( \varphi \) to \( N \). Then \( G/N \) acts on \( IF[V]^N \) and, if \( p \nmid |G| \), then

\[
\beta(\varphi) \leq \beta(\varphi|_N)\beta_{IF}(G/N),
\]

and hence

\[
\beta_{IF}(G) \leq \beta_{IF}(N)\beta_{IF}(G/N).
\]

**PROOF:** This follows from the isomorphism (see [3] Proposition 1.5.1)

\[
IF[V]^G \cong (IF[V]^N)^G
\]

and Proposition 1.1. \( \square \)

**COROLLARY 1.3:** Let \( G \) be a finite group and \( IF \) a field. Suppose the characteristic of \( IF \) does not divide the order of \( G \). If \( G \) has a composition series whose composition factors \( K_1, \ldots, K_m \) satisfy \( \beta_{IF}(K_i) \leq |K_i| \), for \( i = 1, \ldots, m \), then \( \beta_{IF}(G) \leq |G| \).

**PROOF:** This follows from Corollary 1.2 by induction on \( m \). \( \square \)

**COROLLARY 1.4:** Let \( IF \) be a field of characteristic \( p \). If there is a finite group \( G \) with \( p \nmid |G| \) for which \( \beta_{IF}(G) > |G| \), then there is also a finite nonabelian simple group \( S \) with \( \beta_{IF}(S) > |S| \).

**PROOF:** Choose \( G \) of minimal order such that \( p \nmid |G| \) and \( \beta_{IF}(G) > |G| \). Then \( G \) is simple. For, if not, we may choose a nontrivial normal subgroup \( N \triangleleft G \). Since \( |N|, |G/N| < |G| \) it follows that \( \beta_{IF}(N) < |N| \) and \( \beta_{IF}(G/N) < |G/N| \), whence from Corollary 1.2 we obtain

\[
\beta_{IF}(G) \leq \beta_{IF}(N)\beta_{IF}(G/N) \leq |N| \cdot |G/N| = |G|,
\]

which would be a contradiction. Hence \( G \) is simple, and by [4] Lemma 1 it is not cyclic of prime order, so must be nonabelian. \( \square \)
§2. Closing the Noether Gap for the Alternating Groups

We begin with a generalization of [3] Theorem 2.4.2. For this we require some terminology. Suppose that $C \subseteq A$ is a finite integral extension of graded connected commutative Noetherian algebras over a field. If $a \in A$ then $a$ is a root of a monic polynomial of minimal degree $m_a(X) \in C[X]$, called the minimal polynomial of $a$ over $C$. We set

$$\deg(A | C) = \max \{ \deg(m_a(X)) | a \in A \}$$

and call it the degree of $A$ over $C$. As usual, if there is no maximum, we set $\deg(A | C) = \infty$.

Recall the following combinatorial lemma from [3] Lemma 2.4.1.

**Lemma 2.1**: Let $V$ be a vector space over a field $\text{IF}$ and $u_1, \ldots, u_j \in \text{IF}[V]$. If $j! \neq 0 \in \text{IF}$ then the monomial $u_1 \cdots u_j$ is a linear combination of $j$-th powers of sums of elements of $\{u_1, \ldots, u_j\}$.

**Proof**: This follows from the formula

$$(-1)^j j! u_1 \cdots u_j = \sum_{I \subseteq \{1, \ldots, j\}} (-1)^{|I|} \left( \sum_{i \in I} u_i \right)^j.$$ 

In this formula, $I$ runs over all subsets of $\{1, \ldots, j\}$ and $|I|$ is the cardinality of $I$.

**Theorem 2.2**: Let $C \subseteq A$ be a finite integral extension of graded connected commutative Noetherian algebras over the field $\text{IF}$ of characteristic $p$. Suppose

(i) $\deg(A | C)$ is finite,
(ii) $p > \deg(A | C)$, and
(iii) there exists a $C$-module splitting $\pi : A \to C$

Then $\beta(C) \leq \beta(A) \cdot \deg(A | C)$.

**Proof**: The proof is a minor modification of the proof of [3] Theorem 2.4.2, and as much as possible we employ the same notations.

Set $\beta(A) = m$ and $\deg(A | C) = d$. Let $B$ be the subalgebra of $C$ generated by elements of degree at most $md$. Our goal is to show that $B = C$. To this end introduce

$$N = \text{Span}_{\text{IF}} \{ a \in A | \deg(a) \leq m \}$$

$$M = \text{Span}_{\text{IF}} \{ a_1^{e_1} \cdots a_k^{e_k} | k, e_1, \ldots, e_k \in \text{IN}, e_1 + \cdots + e_k < d \}.$$ 

We are going to show that $B \cdot M = A$, i.e., that $M$ generates $A$ as a $B$-module.

If $a \in A$, then the minimal polynomial of $a$ has degree at most $d$. Hence we can find $b_1, \ldots, b_{d-1} \in C$ such that

$$a^d = -(b_1 a_1^{d-1} + \cdots + b_d).$$

If $\deg(a) \leq m$ then

$$\deg(b_1) \leq \deg(b_2) \leq \cdots \leq \deg(b_d) \leq d m$$

so $b_1, \ldots, b_d \in B$. The elements $a$, $a^2, \ldots, a^{d-1}$ belong to $M$ so ($*$) shows $a^d \in B \cdot M$ for any $a \in N$. 

3
Next suppose that $a^E = a_1^{e_1} \cdots a_k^{e_k}$ with $a_1, \ldots, a_k \in \mathbb{N}$ and $e_1 + \cdots + e_k = d$. From lemma 2.1 we obtain

\[
(-1)^d \cdot a^E = \sum_{I \subseteq \{1, \ldots, d\}} (-1)^{|I|} \left( \sum_{i \in I} a_i \right)^d = \sum_{I \subseteq \{1, \ldots, d\}} (-1)^{|I|} h_I^d,
\]

where $h_I \in \mathbb{N}$. Since $d! \neq 0 \in \mathbb{IF}$ it follows that $a^E \in B \cdot M$.

Assume inductively that all monomials $a^E = a_1^{e_1} \cdots a_k^{e_k}$ with $k, e_1, \ldots, e_k \in \mathbb{N}, a_1, \ldots, a_k \in \mathbb{N}$ and $e_1 + \cdots + e_k \leq d$ belong to $B \cdot M$. Consider a monomial $a^E = a_1^{e_1} \cdots a_k^{e_k}$ with $k, e_1, \ldots, e_k \in \mathbb{IN}, a_1, \ldots, a_k \in \mathbb{IN}$ and $e_1 + \cdots + e_k = d + i + 1$. Without loss of generality we may suppose $a^E = a^{E'} \cdot a_k$. By the induction hypothesis we have $a^{E'} \in B \cdot M$ and therefore we may choose $h_1, \ldots, h_l \in \mathbb{N}$ and $d_1, \ldots, d_l \in \mathbb{IN}$ with $d_1 + \cdots + d_l < d$ and $c_D \in B$ so that

\[
a^{E'} = \sum_{|D|<d-1} c_D h^D = \sum_{|D|<d-1} c_D h^D + \sum_{|D|=d-1} c_D h^D,
\]

where

\[
h^D = \prod_{i=1}^l h_i^{d_i}.
\]

If $|D| < d - 1$ then $h^D a_k \in M$ for degree reasons and hence

\[
\sum_{|D|<d-1} c_D h^D a_k \in B \cdot M.
\]

If $|D| = d - 1$ then by (**) $h^D a_k \in B \cdot M$ and hence

\[
\sum_{|D|=d-1} c_D h^D a_k \in B \cdot M.
\]

Combining these inclusions gives

\[
a^E = a^{E'} \cdot a_k = \sum_{|D|<d-1} c_D h^D a_k = \sum_{|D|<d-1} c_D h^D a_k + \sum_{|D|=d-1} c_D h^D a_k \in B \cdot M.
\]

Therefore, by induction, any monomial $a^E = a_1^{e_1} \cdots a_k^{e_k}$, with $a_1, \ldots, a_k \in \mathbb{N}$, belongs to $B \cdot M$. Since $\mathbb{N}$ generates $A$ as an algebra we have shown that $B \cdot M = A$ as required.

To complete the proof that $B = C$ we apply the projection $\pi$ to $A$ and obtain

\[
C = \pi(A) = \pi(B \cdot M) = B
\]

since $\pi(M) \subseteq B$. \(\square\)

**Theorem 2.3**: Let $\varphi : G \hookrightarrow \text{GL}(n, \mathbb{IF})$ be a representation of a finite group $G$ over the field $\mathbb{IF}$ of characteristic $p$. If $H \leq G$ is a subgroup such that $p > |G : H|$, then

\[
\beta(\varphi) \leq \beta(\varphi|_H) \cdot |G : H|.
\]
PROOF: Consider the inclusion $\text{IF}[V]_G \subseteq \text{IF}[V]_H$. This is a finite extension, and every $f \in \text{IF}[V]_H$ is a root of the polynomial

$$\Phi_f(X) = g \in \text{G/H} \cdot (X - gf),$$

where the product is taken over a set of coset representatives of $H$ in $G$. The polynomial $\Phi_f(X)$ has degree $|G:H|$ and therefore $\deg(\text{IF}[V]_G) \leq |G:H|$. Since $p$ does not divide $|G:H|$, there is the averaging operator, derived from the relative transfer $\text{Tr}_{\text{G/H}}$, $\frac{1}{\text{char}_g \in \text{G/H}} = 1 \frac{1}{|G:H|} \text{Tr}_{\text{G/H}}: \text{IF}[V]_G \rightarrow \text{IF}[V]_G$, (see [3] Section 4.2) which splits the inclusion $\text{IF}[V]_G \hookrightarrow \text{IF}[V]_H$. Therefore the hypotheses of Theorem 2.2 are satisfied, and, applying this theorem yields the desired conclusion.

As an easy consequence we obtain inductively that Noether's bound holds for the alternating groups in the nonmodular case.

COROLLARY 2.4:

Let $A_n$ be the alternating group on $n$ letters and $\text{IF}$ a field of characteristic prime to $|A_n|$, then $b_\text{IF}(A_n) \leq |A_n|\cdot|A_{n-1}|\cdot\ldots\cdot|A_1|/|A_n|\cdot|A_{n-1}|\cdot\ldots\cdot|A_1|.$

PROOF: The alternating group $A_3$ is cyclic, and $A_4$ is solvable, so the result holds for them by [4]. Let the characteristic of $\text{IF}$ be $p$, and note that $p$ does not divide $|A_n| = n!/2$ if and only if $p > n = |A_n|/|A_{n-1}| = n/(n-1)$. Hence, proceeding inductively on $n$, and applying Theorem 2.3, we obtain $b_\text{IF}(A_n) \leq b_\text{IF}(A_{n-1}) \cdot|A_n|\cdot|A_{n-1}|\cdot\ldots\cdot|A_1|/|A_n|\cdot|A_{n-1}|\cdot\ldots\cdot|A_1|$ and the result follows.

Theorem 2.3 has a number of other consequences, among which we note the following.

COROLLARY 2.5:

Let $\text{IF}$ be a field of characteristic $p$, $G$ a finite group, and $H < G$ a subgroup. If $p > |G:H|$ and $b_\text{IF}(H) \leq |H|$, then $b_\text{IF}(G) \leq |G|$. This can be applied to some of the sporadic simple groups to almost close the Noether gap for them. For example, looking at the entries for the Mathieu groups in the ATLAS [1], one can derive the following result.

PROPOSITION 2.6:

Let $M_i$ be one of the Mathieu groups, $i=10, 11, 12, 22, 23, 24$, and $\text{IF}$ a field of characteristic $p$ with $p > i$. Then $b_\text{IF}(M_i) \leq |M_i|$. The following little table lists the primes that do not divide the order of a Mathieu group but are excluded by this proposition, so for which the Noether gap is not yet closed.

<table>
<thead>
<tr>
<th>GROUP</th>
<th>PRIMES EXCLUDED</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_{10}, M_{11}, M_{12}$</td>
<td>7</td>
</tr>
<tr>
<td>$M_{22}, M_{23}, M_{24}$</td>
<td>17, 19</td>
</tr>
</tbody>
</table>

Finally, we note that Theorem 2.3 can be applied iteratively to obtain:
COROLLARY 2.7: Let $\mathbb{F}$ be a field of characteristic $p$, $G$ a finite group and
\[
\{1\} < G_k < G_{k-1} < \cdots < G_1 < G_0 = G
\]
a chain of subgroups of $G$ such that:
(i) $\beta_{\mathbb{F}}(G_i) \leq |G_i|$, for $i = 1, \ldots, k - 1$, and
(ii) $p > \max \{ |G_i : G_{i-1}| \mid i = 1, \ldots, k - 1 \}$,
then $\beta_{\mathbb{F}}(G) \leq |G|$. $\square$

References


Larry Smith
School of Mathematics
University of Minnesota
Minneapolis, MN 55455
USA

and

AG-Invariantentheorie

Mathematisches Institut der Universität
D 37073 Göttingen
Federal Republic of Germany