SUMMARY: Let $\varphi : G \hookrightarrow \text{GL}(n, \mathbb{F})$ 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 show how to refine Noether’s proof to yield a more general nonmodular result. In particular we prove that Noether’s bound holds for the alternating groups in the nonmodular case.
Let $G$ be a finite group and $\rho : G \to GL(n, IF)$ a faithful representation of $G$ over the field $IF$. Via $\rho$, the group $G$ acts on the vector space $V = IF^n$, and hence also on the graded algebra $IF[V]$ of homogeneous polynomial functions on $V$. The subalgebra of functions, $IF[V]^G$, fixed by the action of $G$ is called the \textbf{ring of invariants of} $G$. As a general reference on invariant theory see [3].

In [2] E. Noether proved that, whenever the characteristic of $IF$ is zero, then $IF[V]^G$ is a finitely generated as an algebra over $IF$. In addition she gave an algorithm to construct a system of generators using polarizations of elementary symmetric polynomials (see also [7] VII.B.15 or [3] §3.3). From this she deduced that $IF[V]^G$ 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 \textbf{Noether's bound}. This result has been extended to fields of characteristic $p \neq 0$ which satisfy $p \geq |G|$ (called the \textbf{strong nonmodular case}) in [6], and to solvable groups $G$, whose order $|G|$ is not divisible by $p$ (called the \textbf{nonmodular case}) in [4]. It is known that if Noether's bound fails in the nonmodular case then it fails for a finite nonabelian simple group (see [5]). For this reason the alternating groups have become a test case for the conjecture that Noether's bound holds for all finite groups in the nonmodular case.

In this note we show how to refine one of Noether's arguments in [2] using ideas coming from permutation representations. This leads to results in the nonmodular case, that, for example, apply to the alternating groups $A_n$. For a different discussion of Noether's bound for the alternating groups see [5].

This research was done while preparing a lecture on Noether's bound for a \textbf{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.

I am very grateful to Kay Magaard for a number of tutorials on permutation representations. In particular, the idea to use that the regular representation of a finite group preserves the partition coming from a subgroup is due to him.

\section{Review of Noether's Proof}

In this section we review the essential steps in one of E. Noether's proofs [2] of the finite generation of rings of invariants of finite groups over the complex numbers (see also [3] Chapter 3). So, let $\rho : G \to GL(n, IF)$ be a representation of a finite group over the field $IF$. Let $V = IF^n$ and $V^\ast$ its vector space dual, which we regard as the space of linear forms on $V$. Denote by $IF(G)$ the group algebra of $G$ over $IF$, and consider the action map

$$\alpha : IF(G) \otimes IF V^\ast \to V^\ast$$

defined by

$$\alpha(g \otimes z) = gz \quad g \in G, z \in V^\ast.$$ 

If we let $G$ act on $IF(G) \otimes IF V^\ast$ by

$$h(g \otimes z) = hg \otimes z \quad h, g \in G \text{ and } z \in V^\ast,$$

then the map $\alpha$ is $G$-equivariant. Let us write $W$ for the vector space dual of $IF(G) \otimes IF V^\ast$. Then

$$W = (IF(G) \otimes IF V^\ast)^\ast = (IF(G))^\ast \otimes IF V^{**} = (IF(G))^\ast \otimes IF V = \text{Hom}_IF (IF(G), V) = \text{map}(G, V),$$
where map(G, V) is the vector space of maps of G into V. Dual to the map \( \alpha \) is the Noether map

\[ \eta : V \rightarrow \text{map}(G, V) \]

which is a G-equivariant map, and hence, induces a G-equivariant map

\[ \eta^* : \text{IF}[W] \rightarrow \text{IF}[V], \]

which we also refer to as the Noether map, though no confusion should arise. This is the map induced by \( \alpha \) if we regard \( \text{IF}[V] \) as \( S(V^*) \), and similarly \( \text{IF}[W] \) as \( S(W^*) \), where \( S(\, \cdot \, ) \) is the symmetric algebra functor.

The action of G on map(G, V) = W is by permutation of the elements of the underlying set \( \Omega \) of G, and hence extends to an action of the full permutation group \( \Sigma_d \), where \( d = |G| \). Choose a basis \( z_1, \ldots, z_n \) for \( V^* \), then \( \{ g \otimes z_i \mid i = 1, \ldots, n, \text{ and } g \in G \} \) may be identified with a basis for \( W^* \). Define the operator

\[ E : \text{IF}[V] \rightarrow \text{IF}[W] \]

by the formulae

\[ E(f) = \sum_A \lambda_A E(z^A) \]

\[ E(z^A) = \sum_{g \in G} (g \otimes z_1)^{a_1} \cdots (g \otimes z_n)^{a_n} \]

where \( A = (a_1, \ldots, a_n) \in \mathbb{N}_0 \times \cdots \times \mathbb{N}_0 \) is a multiindex of nonnegative integers, and

\[ f = \sum \lambda_A z^A \]

expresses \( f \) as a sum of monomials \( z^A = z^{a_1} \cdots z^{a_n} \) with coefficients \( \lambda_A \in \text{IF} \). The following lemma is a direct consequence of the definitions (for a definition of the transfer homomorphism \( \text{Tr}^G \) and its properties see e.g., [3] Chapter 2).

**Lemma 1.1:** With the preceding notations, the operator \( E \) satisfies:

(i) \( E(f) \in \text{IF}[W]^\Sigma_d \) for all \( f \in \text{IF}[V] \), and

(ii) \( \eta^*(E(f)) = \text{Tr}^G(f) \) for all \( f \in \text{IF}[V] \).

As a consequence we obtain:

**Proposition 1.2:** Let \( \text{IF} \) be a field of characteristic \( p \) and \( G \) a group of order \( d = |G| \). Suppose that \( p \) does not divide \( d \). Then, with the preceding notations, we have that the composition

\[ \varphi : \text{IF}[W]^\Sigma_d \hookrightarrow \text{IF}[W]^G \xrightarrow{(\eta^*)^G} \text{IF}[V]^G \]

is onto.

**Proof:** Since \( |G| = d \in \text{IF}^X \) the averaging operator

\[ \pi := \frac{1}{|G|} \sum_{g \in G} g = \frac{1}{|G|} \text{Tr}^G : \text{IF}[V] \rightarrow \text{IF}[V]^G \]

is defined, and is a splitting for the inclusion \( \text{IF}[V]^G \hookrightarrow \text{IF}[V] \) (see e.g., [3] Section 2.4). Therefore the transfer

\[ \text{Tr}^G : \text{IF}[V] \rightarrow \text{IF}[V]^G \]

is onto, and the result follows from Lemma 1.1. \( \square \)
For a graded connected commutative Noetherean algebra $A$ over $\mathbb{F}$ let us introduce the notation $\beta(A)$ for the maximal degree of a a generator of $A$ in a minimal generating set. This is nothing but the degree of the Poincaré series, which in this case is a polynomial, of the module of indecomposables $QA := \bar{A} \otimes_\mathbb{F} \mathbb{F} = \bar{A}/(\bar{A})^2$,

where $\bar{A}$ denotes the augmentation ideal of $A$. (See for example [3] Chapter 4 and Section 5.1) For a representation $\rho : G \hookrightarrow GL(n, \mathbb{F})$ then we write $\beta(\rho)$ for $\beta(\mathbb{F}[V]^G)$, and set

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

Proposition 1.2 reduces finding an upper bound for $\beta(\rho)$ to finding one for $\beta(\mathbb{F}[W]^G)$. To do this, we note that $W$ regarded as a $\Sigma_d$-representation has the following description:

$$W = \text{map}(\Omega, V) = \text{map}(\Omega, F^n) = \bigoplus_i \text{map}(\Omega, \mathbb{F}),$$

(remember $\Omega$ denotes the underlying set of $G$) and $\text{map}(\Omega, \mathbb{F})$ is just the defining representation $\tau$ of $\Sigma_d$ over the field $\mathbb{F}$. If we denote this representation by $X$ then

$$\mathbb{F}[W]^G = \mathbb{F}[\bigoplus_i X]^G,$$

which is the ring of vector invariants of vectors of dimension $n$ for the defining representation of the symmetric group $\Sigma_d$. For these invariants we have the First Main Theorem of Invariant Theory for $\Sigma_d$ [3] Theorem 3.3.1 (the proof is in Section 3.4; for a proof in characteristic zero see [7] VIII.B.15), which we state here in a form directly applicable to our discussion of Noether’s proof.

**Theorem 1.3:** Let $d \in \mathbb{N}$ be a positive integer and $\mathbb{F}$ a field of characteristic $p$. Let $\tau : \Sigma_d \hookrightarrow GL(d, \mathbb{F})$ be the defining representation of $G$ over the field $\mathbb{F}$. If $p > d$ then for any positive integer $n$, $\beta(\bigoplus_i \tau) = d$. \(\square\)

Since

$$\varphi : \mathbb{F}[W]^G = \mathbb{F}[\bigoplus_i X]^G \longrightarrow \mathbb{F}[V]^G$$

is onto we therefore conclude: if $p > d$ then $\beta(\rho) \leq \beta(\bigoplus_i \tau) = d = |G|$. 

§2. Refining Noether’s Proof

In this section we show how to refine Noether’s proof to yield an improved condition on the characteristic of the ground field for the validity of $\beta_{IF}(G) \leq |G|$ (Noether’s bound). We continue to employ the notations of Section 1, in particular, $\rho : G \hookrightarrow GL(n, \mathbb{F})$ is a fixed representation of a finite group $G$ of order $d = |G|$ over the field $\mathbb{F}$ of characteristic $p$. For the moment we make no assumptions about the relation between $p$ and $d$. As in Section 1 we let $W = \text{map}(\Omega, V)$, where $\Omega$ is the underlying $G$ set of $G$, and we have the composite

$$\varphi : \mathbb{F}[W]^G \hookrightarrow \mathbb{F}[W]^G \overset{(\tau^*)^G}{\longrightarrow} \mathbb{F}[V]^G,$$

where $G$ has been embedded in $\Sigma_d$ via the regular representation $\text{reg}(G) : G \hookrightarrow \Sigma_d$. Notice that if $S$ is any subgroup of $\Sigma_d$ that contains the image of $G$ under $\text{reg}(G)$ in $\Sigma_d$, then the factorization of $\varphi$

$$\varphi : \mathbb{F}[W]^G \hookrightarrow \mathbb{F}[W]^S \hookrightarrow \mathbb{F}[W]^G \overset{(\tau^*)^G}{\longrightarrow} \mathbb{F}[V]^G,$$
shows that the map
\[ \text{IF}[W]^S \rightarrow \text{IF}[V]^G \]
is onto for \( |G| \in \text{IF}^\times \). Thus in Noether’s argument we could replace \( \Sigma_d \) by \( S \), if only we could find an \( S \) for which we could show \( \beta(\text{IF}[W]^S) \leq d \). We proceed to show how to do this.

Call a subgroup \( K \leq \Sigma_d \) **regular** if \( K \) acts transitively on \( \Omega \) and the isotropy groups \( K_\omega \) are all trivial, \( \omega \in \Omega \). Regular subgroups of \( \Sigma_d \) cannot sit arbitrarily in \( \Sigma_d \). To explain what is meant by this, choose a chain of maximal subgroups
\[ \{1\} = G_k < G_{k-1} < \cdots < G_1 < G_0 = G \]
in \( G \), i.e., \( G_i \) is a maximal subgroup of \( G_{i-1} \) for \( i = 1, \ldots, k - 1 \). Let \( d_i = |G_i| \) and \( e_i = |G_i : G_{i+1}| \) for \( i = 0, \ldots, k - 1 \). Note that \( |G| = d = \prod_{i=1}^{k-1} e_i \).

\[ \Omega = \Omega_1 \sqcup \cdots \sqcup \Omega_{e_0} \]
be the decomposition of \( \Omega \) into the left cosets of \( G_1 \) in \( G \). This partition of \( \Omega \) must be preserved by the action of \( G \) on \( \Omega \) via the regular representation, and therefore \( \text{reg}(G)(G) \) must sit in the largest subgroup of \( \Sigma_d \) that preserves this partition. This subgroup is
\[ \Sigma_{d_1} \times \cdots \times \Sigma_{d_k} \times \Sigma_{e_0} = \Sigma_{d_1} \wr \Sigma_{e_0} \]
If we denote by \( \Gamma \) the underlying set of \( G_1 \) then the representation \( W \) as \( \Sigma_{d_1} \wr \Sigma_{e_0} \)-representation may be described as follows: Note
\[ W = \text{map}(\Omega, V) = \text{map}(\bigcup_{\Omega_1} \cdots \bigcup_{\Omega_{e_0}}, V) = \bigoplus_{\Omega_{e_0}} \text{map}(\Gamma, V) \]
and that map(\( \Gamma, V \)) is just the direct sum of \( n \) copies of the defining representation of \( \Sigma_{d_1} \) over \( \text{IF} \). Therefore
\[ \text{IF}[W]^\Sigma_{d_1} \times \cdots \times \Sigma_{d_k} = \bigoplus_n \text{IF}[Y]^\Sigma_{d_1} \]
where \( Y \) is the linear representation defined over \( \text{IF} \) from the representation of \( \Sigma_{d_0} \) as the permutations of \( \Gamma \). Let us write \( A = \text{IF}[Y]^\Sigma_{d_1} \) so that
\[ \text{IF}[W]^\Sigma_{d_1} \wr \Sigma_{e_0} = \left( \bigoplus_n \text{IF}[W]^\Sigma_{d_1} \right)^\Sigma_{e_0} = \left( \bigoplus_n \text{IF}[Y]^\Sigma_{d_1} \right)^\Sigma_{e_0} = \left( \bigoplus n \right)^\Sigma_{e_0} \]
Notice that
\[ \left( \bigoplus n \right)^\Sigma_{e_0} \]
are just the invariants of \( \Sigma_{e_0} \) acting by permutation of the tensor factors. We can employ the linearization process of [4] and [5] to obtain information on \( \beta\left( \bigoplus n \right)^\Sigma_{e_0} \) provided \( p \nmid |\Sigma_{e_0}| \), which is equivalent to \( p > e_0 \). Here is how this works.

Let \( A \) be generated by homogeneous forms of degree less than or equal to \( b = \beta(A) \) say. Let \( Z \) be the vector space dual of \( \bigoplus_{i=1}^{b} A_i \), where \( A_i \) denotes the homogeneous component of \( A \) in degree \( i \). Note that the natural map \( Z^* \rightarrow A \) extends to an epimorphism \( \text{IF}[Z] \rightarrow A \). Hence there is an induced map of algebras with \( \Sigma_{e_0} \) action
\[ \bigoplus_{\Sigma_{e_0}} \text{IF}[Z] \rightarrow \bigoplus_{\Sigma_{e_0}} A \]
and, if \( p > e_0 \), i.e., \( |\Sigma_{e_0}| \) is not divisible by \( p \), then the induced map of the invariant subalgebras

\[
\left( \otimes_{\mathbb{Z}} \right)^{\Sigma_{e_0}} \rightarrow \left( \otimes_{\mathbb{A}} \right)^{\Sigma_{e_0}}
\]

is also surjective. Finally, if \( U \) denotes the \( \mathbb{K} \)-linear representation corresponding to the defining representation of \( \Sigma_{e_0} \), then

\[
\left( \otimes_{\mathbb{Z}} \right)^{\Sigma_{e_0}} \rightarrow \left( \otimes_{\mathbb{A}} \right)^{\Sigma_{e_0}}
\]

which are the vector invariants of the defining representation of \( \Sigma_{e_0} \) on vectors of dimension \( n \). Therefore, since we have already assumed that \( p > e_0 \), we can apply Theorem 1.3 to conclude that \( \beta \left( \left( \otimes_{\mathbb{Z}} \right)^{\Sigma_{e_0}} \right) = be_0 \), where we have reaccounted for the fact that \( b = \beta(A) \) is the maximal degree of an element in \( Z \). Hence \( \beta \left( \left( \otimes A \right)^{\Sigma_{e_0}} \right) \leq be_0 \). We therefore obtain

\[
\beta \left( \left( \otimes_{\mathbb{Z}} \right)^{\Sigma_{e_0}} \right) \leq \beta(A)e_0
\]

provided only that \( p > e_0 \).

If, in addition, \( p > d_1 \), we could apply Theorem 1.3 to \( \Sigma_{d_1} \) also, and could conclude that \( \beta \left( \left( \otimes_{\mathbb{Z}} \right)^{\Sigma_{d_1}} \right) \leq d_1 \). Combining all this would then give

\[
\beta(\rho) \leq \beta \left( \left( \otimes_{\mathbb{Z}} \right)^{\Sigma_{d_1}} \right) \leq d_1e_0 = d.
\]

If \( k > 1 \) the partition

\[
\Omega = \Omega_1 \sqcup \cdots \sqcup \Omega_{e_0}
\]

can be refined further by using the maximal subgroup \( G_2 < G_1 \) to partition the sets \( \Omega_i \), (Recall that the \( \Omega_i \) are the left cosets of \( G_1 \) in \( G_0 = G \) ) into the left cosets of \( G_2 \) in \( G_1 \). Denote the resulting partition of \( \Omega_i \) by

\[
\Omega_i = \Omega_{i,1} \sqcup \cdots \sqcup \Omega_{i,e_0}.
\]

note that the action of \( G \) on \( \Omega \) must preserve the multipartition

\[
\Omega = \bigsqcup_{i=1}^{e_0} \bigsqcup_{j=1}^{e_i} \Omega_{i,j},
\]

so \( \text{reg}(G)(G) \) must belong to the subgroup of \( \Sigma_d \) consisting of all permutations preserving this multipartition. This subgroup is:

\[
(\Sigma_{d_2} \wr \Sigma_{e_0}) \wr \Sigma_{e_0}.
\]

Continuing in this way, we find that the image in \( \Sigma_d \) of \( G \) under the regular representation preserves the multipartition

\[
\Omega = \bigsqcup_{i_k=1}^{e_{k-1}} \bigsqcup_{i_{k-1}=1}^{e_{k-2}} \cdots \bigsqcup_{i_1=1}^{e_0} \Omega_{i_{k-1} \cdots i_1}
\]

obtained from the full chain of maximal subgroups, and therefore is a subgroup of

\[
(\cdots (\Sigma_{e_{k-1}} \wr \Sigma_{e_{k-2}}) \wr \cdots) \wr \Sigma_{e_0} \wr \Sigma_{e_0}).
\]

Inductively applying the preceding arguments, we obtain the degree bound

\[
\beta \left( \left( \otimes_{\mathbb{Z}} \right)^{\cdots (\Sigma_{e_{k-1}} \wr \Sigma_{e_{k-2}}) \cdots \wr \Sigma_{e_0}} \right) \leq \prod_{i=0}^{k-1} e_i = d,
\]

provided that \( e_0, e_1, \ldots, e_{k-1} \) are invertible in \( \mathbb{K} \). Therefore we have shown:
**Theorem 2.1:** Let $IF$ 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 maximal subgroups in $G$, i.e., $G_i$ is a maximal subgroup of $G_{i-1}$ for $i = 1, \ldots, k - 1$. Let $e_i = |G_i : G_{i+1}|$ for $i = 0, \ldots, k - 1$. If

$$p > \max\{e_{k-1}, \ldots, e_0\},$$

then $\beta_{IF}(G) \leq |G|$. \(\square\)

**Remark:** Note that the condition $p > \max\{e_{k-1}, \ldots, e_0\}$ in the preceding theorem implies that $p \not| |G|$.

**Corollary 2.2:** Let $IF$ be a field of characteristic $p$, $n \in \mathbb{N}$ a positive integer, and $A_n$ the alternating group on $n$ letters. If $p > n$ then $\beta_{IF}(A_n) \leq |A_n|$, i.e., Noether's bound holds for the alternating groups $A_n$, $n \in \mathbb{N}$, in the nonmodular case.

**Proof:** Apply Theorem 2.1 to the chain of maximal subgroups

$$\{1\} = A_2 < A_3 < \cdots < A_{n-1} < A_n$$

and note that $p > n$ is equivalent to $p \not| |A_n| = \frac{n!}{2}$. \(\square\)

§3. The Fine Structure of Orbits and Orbit Chern Classes

The method employed in Section 2 leads to a refinement of the orbit Chern classes, a tool introduced in [6] for constructing invariants. (We make use of several standard constructions for permutation representations, and refer to [8] for basic facts about permutation representations.) To explain this, suppose that $G$ is a finite group and $\Omega$ is a finite transitive $G$ set. A **system of imprimitivity** for $\Omega$ is a partition of $\Omega$,

$$\Omega = \Omega_1 \sqcup \ldots \sqcup \Omega_e,$$

that is preserved by the action of $G$. This means, for each $g \in G$ and $1 \leq i \leq e$, that $g(\Omega_i) = \Omega_{g(i)}$, where $1 \leq g(i) \leq e$, and the correspondence $i \mapsto g(i)$ is a permutation of the set $\{1, 2, \ldots, e\}$. The subsets $\Omega_i$, $i = 1, \ldots, e$, are called the **blocks** of the system of imprimitivity. Since $G$ acts transitively on $\Omega$, it is easy to see that the blocks all have the same number of elements, say $c$. In fact, if $K = G_{x_1}$ is the isotropy group of a fixed point $x_1 \in \Omega_1$, then $\Omega$ may be identified with the $G$-space $G/K$, and the blocks with the cosets of $K$ in $H$, where

$$H = \{\ h \in G \mid h(\Omega_1) = \Omega_1 \}.$$

So a system of imprimitivity for $\Omega$ corresponds to a chain of subgroups $K < H < G$.

Next, let $\rho : G \hookrightarrow GL(n, IF)$ be a representation of a finite group $G$ and $B \subset V^*$ an orbit of $G$ in the space of linear forms $V^*$ on $V = IF^n$. Suppose the permutation representation of $G$ on $B$ is imprimitive and

$$B = B_1 \sqcup \cdots \sqcup B_e$$

is a system of imprimitivity for $B$. For each integer $j$, $1 \leq j \leq c$ introduce the polynomial

$$\varphi_{B_j}(X) = \prod_{b \in B_j} (X + b_j) \in IF[V][X]$$
and write
\[ \varphi_{B_j}(X) = \sum_{r+s = c} c_r(B_j)X^r, \]
where \( c \) is the block size. Call the forms \( c_r(B_j) \) the **block Chern classes**. If \( \mathbf{l} = (i_1, \ldots, i_c) \) is a multiindex of nonnegative integers let \( \sigma_1 \) denote the \( \mathbf{l} \)-th polarized elementary symmetric polynomial in \( e \) vector variables, each of dimension \( c \). Then
\[ c_i(B_1, \ldots, B_e) := \sigma_1(c_i(B_1), \ldots, c_i(B_e)) \in \text{IF}[V]^G, \]
and is called the \( \mathbf{l} \)-th **Chern class of the system of imprimitivity**
\[ B = B_1 \sqcup \cdots \sqcup B_e, \]
or a **fine orbit Chern class** of \( B \). The proof of Theorem 2.1 shows:

**Theorem 3.1**: Let \( \text{IF} \) 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 maximal subgroups in \( G \), i.e., \( G_i \) is a maximal subgroup of \( G_{i+1} \) for \( i = 1, \ldots, k-1 \).
Let \( e_i = |G_i : G_{i+1}| \) for \( i = 0, \ldots, k-1 \). If
\[ p > \max\{e_{k-1}, \ldots, e_0\}, \]
then, for any representation \( \rho : G \to \text{GL}(n, \text{IF}) \), the ring of invariants \( \text{IF}[V]^G \) is generated as an algebra by fine orbit Chern classes.

Let us illustrate this with an example. The example is chosen because it is a generic example (see [3] Section 3.2 Example 1 and the discussion preceding Example 2) of a ring of invariants that is not generated by orbit Chern classes.

**Example 1** (L. E. Dickson): Consider the subgroup of \( \text{GL}(2, \text{IF}_3) \) generated by the matrices
\[ A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix} \in \text{GL}(2, \text{IF}_3). \]
Set
\[ C = AB = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \]
Since
\[ A^2 = B^2 = C^2 = -I, \]
where \( I \) is the identity matrix, the subgroup of \( \text{GL}(2, \text{IF}_3) \) generated by \( A \) and \( B \) is isomorphic to the quaternion group \( Q_8 \) of order 8.

Inspection of the 8 matrices in \( Q_8 \) shows that every nonzero vector in \( \text{IF}_3^2 \) occurs exactly once as a first column, so that \( Q_8 \) acts transitively on \( \text{IF}_3^2 \setminus \{0\} \). There are only two orbits of \( Q_8 \) acting on \( V^* \), and they are \( \{0\} \), and \( V^* \setminus \{0\} \). The only Chern classes are therefore the two Dickson polynomials
\[ d_{2,1} = \frac{xy^9 - x^9 y}{xy^3 - x^3 y^3}, \quad d_{2,0} = (xy^3 - x^3 y)^2, \]
where \( \{x, y\} \) is the dual of the canonical basis of \( \text{IF}_3^2 \). These polynomials cannot generate \( \text{IF}[x, y]^{Q_8} \), which therefore is not generated by ordinary orbit Chern classes.
Denote by $\Omega$ the orbit $V^* \mod \text{char} 8 \mod \text{char} 9$ of $G$. This orbit is imprimitive, and the system of imprimitivity corresponding to the subgroup $\mathbb{Z}/4$ in $\mathbb{Q}/8$ generated by $A$ consists of the two blocks $\Omega_1 = \pm x, \pm (x+y)$, $\Omega_2 = \pm x, \pm (x-y)$.

Each block has two nonzero block Chern classes:

$c^2(\Omega_1) = -(x^2 + y^2)$
$c^4(\Omega_1) = x^2y^2$
$c^2(\Omega_2) = (x^2 + y^2)$
$c^4(\Omega_2) = (x^2 - y^2)^2$.

These give the following fine Chern classes for the orbit $\Omega$:

$\Phi = c^4(\Omega_1) + c^4(\Omega_2) = (x^2 + y^2)^2$
$\Theta = c^4(\Omega_1)c^2(\Omega_2) + c^2(\Omega_1)c^4(\Omega_2) = -(x^2 + y^2)(x^4 - y^4)$.

There is another system of imprimitivity for $\Omega$ corresponding to the subgroup $\mathbb{Z}/4$ generated by $B$, whose blocks are $\Lambda_1 = \pm x, \pm (x-y)$, $\Lambda_2 = \pm y, \pm (x+y)$.

From the block Chern classes of this system of imprimitivity we obtain the fine orbit Chern class $\Psi = c^4(\Lambda_1) + c^4(\Lambda_2) = x^2(x-y)^2 + y^2(x+y)^2$.

The fine orbit Chern classes $\Phi, \Psi \in \mathbb{Q}/8$ form a system of parameters and (see the discussion in [3] of Example 1 in Section 3.2)

$\mathbb{Q}/8 = \mathbb{Q}[\Phi, \Psi] \oplus \mathbb{Q}[\Phi, \Psi]' \Theta$.

Therefore the fine orbit Chern classes $\Phi, \Psi, \Theta$ generate $\mathbb{Q}[x, y]$ as an algebra.
References


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