Math. Res. Lett. **17** (2010), *no.* 06, 1171–1182

DEGREE BOUNDS FOR SEPARATING INVARIANTS

Martin Kohls and Hanspeter Kraft

Abstract. If V is a representation of a linear algebraic group G, a set S of G-invariant regular functions on V is called *separating* if the following holds: *If two elements $v, v' \in V$ can be separated by an invariant function, then there is an $f \in S$ such that $f(v) \neq f(v')$.* It is known that there always exist finite separating sets. Moreover, if the group G is finite, then the invariant functions of degree $\leq |G|$ form a separating set. We show that for a non-finite linear algebraic group G such an upper bound for the degrees of a separating set does not exist.

If G is finite, we define $\beta_{\text{sep}}(G)$ to be the minimal number d such that for every G-module V there is a separating set of degree $\leq d$. We show that for a subgroup $H \subset G$ we have $\beta_{\text{sep}}(H) \leq \beta_{\text{sep}}(G) \leq [G : H] \cdot \beta_{\text{sep}}(H)$, and that $\beta_{\text{sep}}(G) \leq \beta_{\text{sep}}(G/H) \cdot \beta_{\text{sep}}(H)$ in case H is normal. Moreover, we calculate $\beta_{\text{sep}}(G)$ for some specific finite groups.

1. Introduction

Let K be an algebraically closed field of arbitrary characteristic. Let G be a linear algebraic group and X a G-variety, i.e. an affine variety equipped with a (regular) action of G, everything defined over K. We denote by $\mathcal{O}(X)$ the coordinate ring of X and by $\mathcal{O}(X)^G$ the subring of G-invariant regular functions. The following definition is due to Derksen and Kemper [4, Definition 2.3.8].

Definition 1. Let X be a G-variety. A subset $S \subset \mathcal{O}(X)^G$ of the invariant ring of X is called *separating* (or *G-separating*) if the following holds:

For any pair $x, x' \in X$, if $f(x) \neq f(x')$ for some $f \in \mathcal{O}(X)^G$ then there is an $h \in S$ such that $h(x) \neq h(x')$.

It is known and easy to see that there always exists a finite separating set (see [4, Theorem 2.3.15]).

If V is a *G-module*, i.e. a finite dimensional K-vector space with a regular linear action of G, we would like to know a priory bounds for the degrees of the elements in a separating set. We denote by $\mathcal{O}(V)_d \subset \mathcal{O}(V)$ the homogeneous functions of degree d (and the zero function), and put $\mathcal{O}(V)_{\leq d} := \bigoplus_{i=0}^{d} \mathcal{O}(V)_i$.

Definition 2. For a G-module V define

$$\beta_{\text{sep}}(G, V) := \min\{d \mid \mathcal{O}(V)^G_{\leq d} \text{ is } G\text{-separating}\} \in \mathbb{N},$$

and set

$$\beta_{\text{sep}}(G) := \sup\{\beta_{\text{sep}}(G, V) \mid V \text{ a } G\text{-module}\} \in \mathbb{N} \cup \{\infty\}.$$

The main results of this note are the following.

Received by the editors July 13, 2010.

Theorem A. *The group G is finite if and only if $\beta_{\mathrm{sep}}(G)$ is finite.*

In order to prove this we will show that $\beta_{\mathrm{sep}}(K^+) = \infty$, that $\beta_{\mathrm{sep}}(K^*) = \infty$, that $\beta_{\mathrm{sep}}(G) = \infty$ for every semisimple group G, and that $\beta_{\mathrm{sep}}(G^0) \leq \beta_{\mathrm{sep}}(G)$ where G^0 denotes the identity component of G (see Theorem 1 in section 3).

Theorem B. *Let G be a finite group and $H \subset G$ a subgroup. Then*

$$\beta_{\mathrm{sep}}(H) \leq \beta_{\mathrm{sep}}(G) \leq [G : H]\, \beta_{\mathrm{sep}}(H), \text{ and so } \beta_{\mathrm{sep}}(G) \leq |G|.$$

Moreover, if $H \subset G$ is normal, then

$$\beta_{\mathrm{sep}}(G) \leq \beta_{\mathrm{sep}}(G/H)\, \beta_{\mathrm{sep}}(H).$$

This will be done in section 4 where we formulate and prove a more precise statement (Theorem 2).

Finally, we have the following explicit results for finite groups.

Theorem C. (a) *Let* $\mathrm{char}\, K = 2$*. Then* $\beta_{\mathrm{sep}}(S_3) = 4$.
(b) *Let* $\mathrm{char}\, K = p > 0$ *and let G be a finite p-group. Then* $\beta_{\mathrm{sep}}(G) = |G|$.
(c) *Let G be a finite cyclic group. Then* $\beta_{\mathrm{sep}}(G) = |G|$.
(d) *Assume* $\mathrm{char}(K) = p$ *is odd, and $r \geq 1$. Then* $\beta_{\mathrm{sep}}(D_{2p^r}) = 2p^r$.

For a reductive group G one knows that the condition $f(x) \neq f(x')$ for some invariant f (in Definition 1) is equivalent to the condition $\overline{Gx} \cap \overline{Gx'} = \emptyset$, see [13, Corollary 3.5.2]. This gives rise to the following definition.

Definition 3. Let X be a G-variety. A G-invariant morphism $\varphi\colon X \to Y$ where Y is an affine variety is called *separating* (or *G-separating*) if the following condition holds: *For any pair $x, x' \in X$ such that $\overline{Gx} \cap \overline{Gx'} = \emptyset$ we have $\varphi(x) \neq \varphi(x')$.*

Remark 1. If $\varphi\colon X \to Y$ is G-separating and $X' \subset X$ a closed G-stable subvariety, then the induced morphism $\varphi|_{X'}\colon X' \to Y$ is also G-separating.

Remark 2. Choose a closed embedding $Y \subset K^m$ and denote by $\varphi_1, \ldots, \varphi_m \in \mathcal{O}(X)$ the coordinate functions of $\varphi\colon X \to Y \subset K^m$. *If φ is separating, then $\{\varphi_1, \ldots, \varphi_m\}$ is a separating set.* The converse holds if G is reductive, but not in general, as shown by the standard linear action of K^+ on K^2 given by $s(x, y) = (x + sy, y)$ which does not admit a separating morphism, but has $\{y\}$ as a separating set.

2. Some useful results

We want to recall some facts about the β_{sep}-values, and compare them with results for the classical β-values for generating invariants introduced by Schmid [15]: $\beta(G)$ *is the minimal $d \in \mathbb{N}$ such that, for every G-module V, the invariant ring $\mathcal{O}(V)^G$ is generated by the invariants of degree $\leq d$.*

By Derksen and Kemper [4, Corollary 3.9.14], we have $\beta_{\mathrm{sep}}(G) \leq |G|$. This is in perfect analogy to the Noether bound which says that $\beta(G) \leq |G|$ in the non-modular case (i.e. if $\mathrm{char}(K) \nmid |G|$), see [8, 9, 15]. Of course we have $\beta_{\mathrm{sep}}(G) \leq \beta(G)$, so every upper bound for $\beta(G)$ gives one for $\beta_{\mathrm{sep}}(G)$.

In characteristic zero and in the non-modular case there are the bounds by SCHMID [15] and by DOMOKOS, HEGEDÜS, and SEZER [6, 16] which improve the Noether bound. In particular, $\beta(G) \leq \frac{3}{4}|G|$ for non-modular non-cyclic groups G, by [16] .

For a linear algebraic group G it is shown by BRYANT, DERKSEN and KEMPER [2, 5] that $\beta(G) < \infty$ if and only if G is finite and $p \nmid |G|$ which is the analogon to our Theorem A. For further results on degree bounds, we recommend the overview article of WEHLAU [18].

The following results will be useful in the sequel.

Proposition 1. *Let $H \subset G$ be a closed subgroup, X an affine G-variety and Z an affine H-variety. Let $\iota\colon Z \to X$ be an H-equivariant morphism and assume that ι^* induces a surjection $\mathcal{O}(X)^G \twoheadrightarrow \mathcal{O}(Z)^H$. If $S \subset \mathcal{O}(X)^G$ is G-separating, then the image $\iota^*(S) \subset \mathcal{O}(Z)^H$ is H-separating.*

Proof. Let $f \in \mathcal{O}(Z)^H$ and $z_1, z_2 \in Z$ such that $f(z_1) \neq f(z_2)$. By assumption $f = \iota^*(\tilde{f})$ for some $\tilde{f} \in \mathcal{O}(X)^G$. Put $x_i := \iota(z_i)$. Then $\tilde{f}(x_1) = f(z_1) \neq f(z_2) = \tilde{f}(x_2)$. Thus we can find an $h \in S$ such that $h(x_1) \neq h(x_2)$. It follows that $\bar{h} := \iota^*(h) \in \iota^*(S)$ and $\bar{h}(z_1) = h(x_1) \neq h(x_2) = \bar{h}(z_2)$. □

Remark 3. In general, the inverse map $(\iota^*)^{-1}$ does not take H-separating sets to G-separating sets. Take $K^+ \subset \mathrm{SL}_2$ as the subgroup of upper triangular unipotent matrices, $X = K^2 \oplus K^2 \oplus K^2$ the sum of three copies of the standard representation of SL_2 and $Z = K^2 \oplus K^2$ the sum of two copies of the standard representation of K^+. Then $\iota\colon Z \to X$, $(v, w) \mapsto ((1, 0), v, w)$ is K^+-equivariant and induces an isomorphism $\mathcal{O}(X)^{\mathrm{SL}_2} \xrightarrow{\sim} \mathcal{O}(Z)^{K^+}$ (see [14]). In fact, choosing the coordinates $(x_0, x_1, y_0, y_1, z_0, z_1)$ on X and (y_0, y_1, z_0, z_1) on Y, we get from the classical description [3] of the invariants and covariants of copies of K^2:

$$\mathcal{O}(X)^{\mathrm{SL}_2(K)} = K[y_1x_0 - y_0x_1, z_1x_0 - z_0x_1, y_1z_0 - y_0z_1],$$

$$\mathcal{O}(Y)^{K^+} = K[y_1, z_1, y_1z_0 - y_0z_1],$$

and the claim follows, because $\iota^*(x_0) = 1, \iota^*(x_1) = 0$.

Now take $S := \{y_1, z_1, y_1(y_1z_0 - y_0z_1), z_1(y_1z_0 - y_0z_1)\} \subset \mathcal{O}(Z)^{K^+}$. We claim that S is a K^+-separating set, but $(\iota^*)^{-1}(S) \subset \mathcal{O}(X)^{\mathrm{SL}_2}$ is not SL_2-separating. For the first claim one has to use that if y_1 and z_1 both vanish, then the third generator $y_1z_0 - y_0z_1$ of the invariant ring $\mathcal{O}(Y)^{K^+}$ also vanishes. For the second claim we consider the elements $v = ((0, 0), (0, 0), (0, 0))$ and $v' = ((0, 0), (1, 0), (0, 1))$ of X, which are separated by the invariants, but not by $(\iota^*)^{-1}(S)$.

For the following application recall that for a closed subgroup $H \subset G$ of finite index the *induced module* $\mathrm{Ind}_H^G V$ of an H-module V is a finite dimensional G-module.

Corollary 1. *Let $H \subset G$ be a closed subgroup of finite index and let V be an H-module. Then $\beta_{\mathrm{sep}}(H, V) \leq \beta_{\mathrm{sep}}(G, \mathrm{Ind}_H^G V)$. In particular, $\beta_{\mathrm{sep}}(H) \leq \beta_{\mathrm{sep}}(G)$.*

Proof. By definition, $\mathrm{Ind}_H^G V$ contains V as an H-submodule in a canonical way. If $n := [G : H]$ and $G = \bigcup_{i=1}^n g_iH$, then $\mathrm{Ind}_H^G V = \bigoplus_{i=1}^n g_iV$. Moreover, the inclusion $\iota : V \hookrightarrow \mathrm{Ind}_H^G V$ induces a surjection $\iota^* : \mathcal{O}(\mathrm{Ind}_H^G(V))^G \twoheadrightarrow \mathcal{O}(V)^H,\ f \mapsto f|_V$. In fact, for $f \in \mathcal{O}(V)_+^H$, a preimage $\tilde{f}$ is given by $\tilde{f}(g_1v_1, \ldots, g_nv_n) := \sum_{i=1}^n f(v_i),\ v_i \in V$, which is easily seen to be G-invariant. Now the claim follows from Proposition 1 above, because the restriction map ι^* is linear and so preserves degrees. $\square$

Proposition 2 (Derksen and Kemper [4, Theorem 2.3.16])**.** *Let G be a reductive group, V a G-module und $U \subset V$ a submodule. The restriction map $\mathcal{O}(V) \to \mathcal{O}(U)$, $f \mapsto f|_U$ takes every separating set of $\mathcal{O}(V)^G$ to a separating set of $\mathcal{O}(U)^G$. In particular, we have*

$$\beta_{\mathrm{sep}}(G, U) \leq \beta_{\mathrm{sep}}(G, V).$$

Let us mention here that in positive characteristic the restriction map is in general not surjective when restriced to the invariants, and so a generating set is not necessarily mapped onto a generating set.

We finally remark that for finite groups there always exist G-modules V such that $\beta_{\mathrm{sep}}(G, V) = \beta_{\mathrm{sep}}(G)$. The same holds for the β-values in characteristic zero.

Proposition 3. *Let G be a finite group group and $V_{\mathrm{reg}} = KG$ its regular representation. Then*

$$\beta_{\mathrm{sep}}(G) = \beta_{\mathrm{sep}}(G, V_{\mathrm{reg}}).$$

In fact, every G-module V can be embedded as a submodule into $V_{\mathrm{reg}}^{\dim V}$. Since, by [7, Corollary 3.7], $\beta_{\mathrm{sep}}(G, V^m) = \beta_{\mathrm{sep}}(G, V)$ for any G-module V and every positive integer m, the claim follows from Proposition 2.

3. The case of non-finite algebraic groups

In this section we prove the following theorem which is equivalent to Theorem A from the first section.

Theorem 1. *For any non-finite linear algebraic group G we have $\beta_{\mathrm{sep}}(G) = \infty$.*

We start with the additive group K^+. Denote by $V = Ke_0 \oplus Ke_1 \simeq K^2$ the standard 2-dimensional K^+-module: $s \cdot e_0 := e_0,\ \ s \cdot e_1 := se_0 + e_1$ for $s \in K^+$. If $\operatorname{char} K = p > 0$ we can "twist" the module V with the Frobenius map $F^n \colon K^+ \to K^+, s \mapsto s^{p^n}$ to obtain another K^+-module which we denote by V_{F^n}.

Proposition 4. *Let $\operatorname{char} K = p > 0$ and consider the K^+-module $W := V \oplus V_{F^n}$. We write $\mathcal{O}(W) = K[x_0, x_1, y_0, y_1]$. Then $\mathcal{O}(W)^{K^+} = K[x_1, y_1, x_0^{p^n} y_1 - x_1^{p^n} y_0]$. In particular, $\beta_{\mathrm{sep}}(K^+, W) = p^n + 1$ and so $\beta_{\mathrm{sep}}(K^+) = \infty$.*

Proof. It is easy to see that $f := x_0^{p^n} y_1 - x_1^{p^n} y_0$ is K^+-invariant. Define the K^+-invariant morphism

$$\pi \colon W \to K^3, \quad w = (a_0, a_1, b_0, b_1) \mapsto (a_1, b_1, a_0^{p^n} b_1 - a_1^{p^n} b_0).$$

Over the affine open set $U := \{(c_1, c_2, c_3) \in K^3 \mid c_1 \neq 0\}$, the induced map $\pi^{-1}(U) \to U$ is a trivial K^+-bundle. In fact, the morphism $\rho \colon U \to \pi^{-1}(U)$ given by $(c_1, c_2, c_3) \mapsto (0, c_1, -c_1^{-p^n} c_3, c_2)$ is a section of π, inducing a K^+-equivariant isomorphism $K^+ \times U \xrightarrow{\sim} \pi^{-1}(U),\ (s, u) \mapsto s \cdot \rho(u)$. This implies that $\mathcal{O}(W)_{x_1}^{K^+} = K[x_1, x_1^{-1}, y_1, f]$, hence $\mathcal{O}(W)^{K^+} = K[x_0, x_1, y_0, y_1] \cap K[x_1, x_1^{-1}, y_1, f]$, and the claim follows easily. $\square$

If K has characteristic zero, we need a different argument. Denote by $V_n := S^nV$ the nth symmetric power of the standard K^+-module $V = Ke_0 \oplus Ke_1$ (see above). This module is cyclic of dimension $n+1$, i.e. $V_n = \langle K^+ v_n\rangle$ where $v_n := e_1^n$, and for any $s \in K^+, s \neq 0$, the endomorphism $v \mapsto sv - v$ of V_n is nilpotent of rank n. In particular, $V_n^{K^+} = Kv_0$ where $v_0 := e_0^n \in V_n$.

Remark 4. For $q \geq 1$ consider the *qth symmetric power* S^qV_n of the module V_n. Then the cyclic submodule $\langle K^+ v_n^q\rangle \subset S^qV_n$ generated by v_n^q is K^+-isomorphic to V_{qn}, and $\langle K^+ v_n^q\rangle^{K^+} = Kv_0^q$. One way to see this is by remarking that the modules V_n are $\mathrm{SL}_2(K)$-modules in a natural way, and then to use representation theory of $\mathrm{SL}_2(K)$.

Proposition 5. *Let* $\operatorname{char} K = 0$. *Consider the* K^+*-module* $W = V^* \oplus V_n$ *and the two vectors* $w := (x_0, v_0)$ *and* $w' := (x_0, 0)$ *of* W. *Then there is a* K^+*-invariant function* $f \in \mathcal{O}(W)^{K^+}$ *separating* w *and* w', *and any such* f *has degree* $\deg f \geq n+1$. *In particular,* $\beta_{\mathrm{sep}}(K^+, W) \geq n+1$, *and so* $\beta_{\mathrm{sep}}(K^+) = \infty$.

Proof. Let U_1, U_2 be two finite dimensional vector spaces. There is a canonical isomorphism

$$\Psi\colon\ \mathcal{O}(U_1^* \oplus U_2)_{(p,q)} \xrightarrow{\sim} \operatorname{Hom}(S^qU_2, S^pU_1)$$

where $\mathcal{O}(U_1^* \oplus U_2)_{(p,q)}$ denotes the subspace of those regular functions on $U_1^* \oplus U_2$ which are bihomogeneous of degree (p,q). If $F = \Psi(f)$, then for any $x \in U_1^*$ and $u \in U_2$ we have

$$f(x,u) = x^p(F(u^q)).$$

(Since we are in characteristic 0 we can identify $S^p(U_1^*)$ with $(S^pU_1)^*$.) Moreover, if U_1, U_2 are G-modules, then Ψ is G-equivariant and induces an isomorphism between the G-invariant bihomogeneous functions and the G-linear homomorphisms:

$$\Psi\colon\ \mathcal{O}(U_1^* \oplus U_2)^G_{(p,q)} \xrightarrow{\sim} \operatorname{Hom}_G(S^qU_2, S^pU_1).$$

For the K^+-module $W = V^* \oplus V_n$ we thus obtain an isomorphism

$$\Psi\colon\ \mathcal{O}(V^* \oplus V_n)^{K^+}_{(p,q)} \xrightarrow{\sim} \operatorname{Hom}_{K^+}(S^qV_n, S^pV).$$

Putting $p = n$ and $q = 1$ and defining $f \in \mathcal{O}(V^* \oplus V_n)^{K^+}_{(n,1)}$ by $\Psi(f) = \mathrm{Id}_{V_n}$, we get $f(w) = f(x_0, v_0) = x_0^n(v_0) = x_0^n(e_0^n) \neq 0$, and $f(w') = f(x_0, 0) = 0$. Hence w and w' can be separated by invariants.

Now let f be a K^+-invariant separating w and w' where $\deg f = d$. We can clearly assume that f is bihomogeneous, say of degree (p,q) where $p+q = d$. Because f must depend on V_n, we have $q \geq 1$. Hence $f(w') = f(x_0, 0) = 0$, and so $f(w) = f(x_0, v_0) \neq 0$. This implies for $F := \Psi(f)$ that $F(v_0^q) \neq 0$. Now it follows from Remark 4 above that F induces an injective map of $\langle K^+ v_n^q\rangle$ into S^pV, and so

$$p + 1 = \dim S^pV \geq \dim\langle K^+ v_n^q\rangle = qn + 1 \geq n + 1.$$

Hence $\deg f = p + q \geq n + 1$. □

To handle the general case we use the following construction. Let G be an algebraic group and $H \subset G$ a closed subgroup. We assume that H is reductive. For an affine H-variety X we define

$$G \times^H X := (G \times X)/\!\!/H := \operatorname{Spec}(\mathcal{O}(G \times X)^H)$$

where H acts (freely) on the product $G \times X$ by $h(g,x) := (gh^{-1}, hx)$, commuting with the action of G by left multiplication on the first factor. We denote by $[g,x]$ the image of $(g,x) \in G \times X$ in the quotient $G \times^H X$.

The following is well-known. It follows from general results from geometric invariant theory, see e.g. [12].

(a) The canonical morphism $G \times^H X \to G/H$, $[g,x] \mapsto gH$, is a fiber bundle (in the étale topology) with fiber X.
(b) If the action of H on X extends to an action of G, then $G \times^H X \xrightarrow{\sim} G/H \times X$ where G acts diagonally on $G/H \times X$ (i.e. the fiber bundle is trivial).
(c) The canonical morphism $\iota\colon X \hookrightarrow G \times^H X$ given by $x \mapsto [e,x]$ is an H-equivariant closed embedding.

Lemma 1. *If $\varphi\colon G \times^H X \to Y$ is G-separating, then the composite morphism $\varphi \circ \iota\colon X \to Y$ is H-separating. Moreover, if $S \subset \mathcal{O}(G \times^H X)^G$ is a G-separating set, then its image $\iota^*(S) \subset \mathcal{O}(X)^H$ is H-separating.*

Proof. For $x \in X$ we have $\overline{G[e,x]} = [G, \overline{Hx}]$. Therefore, if $\overline{Hx} \cap \overline{Hx'} = \emptyset$, then $\overline{G[e,x]} \cap \overline{G[e,x']} = \emptyset$ and so $\varphi \circ \iota(x) = \varphi([e,x]) \neq \varphi([e,x']) = \varphi \circ \iota(x')$. The second claim follows from Proposition 1, because $\mathcal{O}(G \times^H X)^G = \mathcal{O}(G \times X)^{G \times H} = \mathcal{O}(X)^H$ and so ι^* induces an isomorphism $\mathcal{O}(G \times^H X)^G \xrightarrow{\sim} \mathcal{O}(X)^H$. $\square$

Now let V be a G-module and $X := V|_H$, the underlying H-module. Let H act on G by right-multiplication with the inverse. As H is reductive, the categorical quotient $G/\!\!/H$ exists as an affine G-variety, and can be identified with the set of left cosets G/H (see [17, Exercise 5.5.9 (8)]). Choose a closed G-equivariant embedding $G/H \xrightarrow{\sim} Gw_0 \hookrightarrow W$ where W is a G-module (see [4, Lemma A.1.9]). Then we get the following composition of closed embeddings where the first one is H-equivariant and the remaining are G-equivariant:

$$\mu\colon V|_H \hookrightarrow G \times^H V \xrightarrow{\sim} G/H \times V \hookrightarrow W \times V.$$

The map μ is given by $\mu(v) = (w_0, v)$. It follows from Lemma 1 and Remark 1 that for any G-separating morphism $\varphi\colon W \times V \to Y$ the composition $\varphi \circ \mu\colon V|_H \to Y$ is H-separating. In particular, if G is reductive, then for any G-separating set $S \subset \mathcal{O}(W \times V)$ the image $\mu^*(S) \subset \mathcal{O}(V)^H$ is H-separating. Since $\deg \mu^*(f) \leq \deg f$ this implies the following result.

Proposition 6. *Let G be a reductive group, $H \subset G$ a closed reductive subgroup and V' an H-module. If V' is isomorphic to an H-submodule of a G-module V, then*

$$\beta_{\text{sep}}(H, V') \leq \beta_{\text{sep}}(G).$$

Now we can prove the main result of this section,

Proof of Theorem 1. By Corollary 1 we can assume that G is connected.

(a) Let G be semisimple, $T \subset G$ a maximal torus and $B \supset T$ a Borel subgroup. If $\lambda \in X(T)$ is dominant we denote by E^λ the Weyl-module of G of highest weight λ, and by $D^\lambda \subset E^\lambda$ the highest weight line. Choose a one-parameter subgroup $\rho\colon K^* \to T$ and define $k_0 \in \mathbb{Z}$ by $\rho(t)u = t^{k_0} \cdot u$ for $u \in D^\lambda$. For any $n \in \mathbb{N}$ put

$$V_n' := (D^\lambda)^* \oplus D^{n\lambda} \subset V_n := (E^\lambda)^* \oplus E^{n\lambda}.$$

Then V_n' is a two-dimensional K^*-module with weights $(-k_0, nk_0)$. Hence $\mathcal{O}(V_n')^{K^*}$ is generated by a homogeneous invariant of degree $n+1$ and so $\beta_{\text{sep}}(K^*, V_n') = n+1$. Now Proposition 6 implies

$$n + 1 = \beta_{\text{sep}}(K^*, V_n') \leq \beta_{\text{sep}}(G)$$

and the claim follows. In addition, we have also shown that $\beta_{\text{sep}}(K^*) = \infty$.

(b) If G admits a non-trivial character $\chi\colon G \to K^*$ then the claim follows because $\beta_{\text{sep}}(G) \geq \beta_{\text{sep}}(K^*) = \infty$, as we have seen in (a).

(c) If the character group of G is trivial, then either G is unipotent or there is a surjective homomorphism $G \to H$ where H is semisimple (use [17, Corollary 8.1.6 (ii)]). In the first case there is a surjective homomorphism $G \to K^+$ and the claim follows from Proposition 4 and Proposition 5. In the second case the claim follows from (a). □

4. Relative degree bounds

In this section all groups are finite. We want to prove the following result which covers Theorem B from the first section.

Theorem 2. *Let G be a finite group, $H \subset G$ a subgroup, V a G-module and W an H-module. Then*

$$\beta_{\text{sep}}(H, W) \leq \beta_{\text{sep}}(G, \operatorname{Ind}_H^G W) \quad \textit{and} \quad \beta_{\text{sep}}(G, V) \leq [G : H]\, \beta_{\text{sep}}(H, V).$$

In particular

$$\beta_{\text{sep}}(H) \leq \beta_{\text{sep}}(G) \leq [G : H]\, \beta_{\text{sep}}(H), \ \textit{and so}\ \beta_{\text{sep}}(G) \leq |G|.$$

Moreover, if $H \subset G$ is normal, then

$$\beta_{\text{sep}}(G) \leq \beta_{\text{sep}}(G/H)\, \beta_{\text{sep}}(H).$$

Note that the inequalities $\beta_{\text{sep}}(G, V) \leq [G : H]\beta_{\text{sep}}(H, V)$ and $\beta_{\text{sep}}(G) \leq |G|$ were already proved by Derksen and Kemper ([11, Corollary 24], [4, Corollary 3.9.14]).

The proof needs some preparation. Let V, W be finite dimensional vector spaces and $\varphi\colon V \to W$ a morphism, i.e. a polynomial map.

Definition 4. The *degree of* φ is defined in the following way, generalizing the degree of a polynomial function. Choose a basis $(w_1, \ldots, w_m)$ of W, so that $\varphi(v) = \sum_{j=1}^m f_j(v) w_j$ for $v \in V$. Then

$$\deg \varphi := \max\{\deg f_j \mid \quad j = 1, \ldots, m\}.$$

It is easy to see that this is independent of the choice of a basis.

If V is a G-module and $\varphi\colon V \to W$ a separating morphism, then $\beta_{\text{sep}}(G, V) \leq \deg \varphi$. Moreover, there is a separating morphism $\varphi\colon V \to W$ for some W such that $\beta_{\text{sep}}(G, V) = \deg \varphi$.

For any (finite dimensional) vector space W we regard $W^d = W \otimes K^d$ as the direct sum of $\dim W$ copies of the standard $\mathcal{S}_d$-module K^d. In this case we have the following result due to Draisma , Kemper and Wehlau [7, Theorem 3.4].

Lemma 2. *The polarizations of the elementary symmetric functions form an $\mathcal{S}_d$-separating set of W^d. In particular, there is an $\mathcal{S}_d$-separating morphism $\psi_W \colon W^d \to K^N$ of degree $\leq d$.*

Recall that the polarizations of a function $f \in \mathcal{O}(U)$ to n copies of U are defined in the following way. Write

$$f(t_1u_1 + t_2u_2 + \cdots + t_nu_n) = \sum_{i_1,i_2,\ldots,i_n} t_1^{i_1}t_2^{i_2}\cdots t_n^{i_n} f_{i_1i_2\ldots i_n}(u_1,u_2,\ldots,u_n)$$

Then the functions $f_{i_1i_2\ldots i_n}(u_1,u_2,\ldots,u_n) \in \mathcal{O}(U^n)$ are called *polarizations of f*. Clearly, $\deg f_{i_1i_2\ldots i_n} \leq \deg f$. Moreover, if U is a G-module and f a G-invariant, then all $f_{i_1i_2\ldots i_n}$ are G-invariants with respect to the diagonal action of G on U^n.

Proof of Theorem 2. The first inequality $\beta_{\text{sep}}(H,W) \leq \beta_{\text{sep}}(G, \operatorname{Ind}_H^G W)$ is shown in Corollary 1.

Let V be a G-module, $v,w \in V$, and let $\varphi \colon V \to W$ be an H-separating morphism of degree $\beta_{\text{sep}}(H,V)$. Consider the partition of G into H-right cosets: $G = \bigcup_{i=1}^d Hg_i$ where $d := [G:H]$. Define the following morphism

$$\bar{\varphi} \colon V \xrightarrow{\tilde{\varphi}} W^d \xrightarrow{\psi_W} K^N$$

where $\tilde{\varphi}(v) := (\varphi(g_1v),\ldots,\varphi(g_dv))$ and $\psi_W \colon W^d \to K^N$ is the separating morphism from Lemma 2.

We claim that $\bar{\varphi}$ is G-separating. In fact, for $g \in G$ define the permutation $\sigma \in \mathcal{S}_d$ by $Hg_ig = Hg_{\sigma(i)}$, i.e. $g_ig = h_ig_{\sigma(i)}$ for a suitable $h_i \in H$. Then $\varphi(g_igv) = \varphi(h_ig_{\sigma(i)}v) = \varphi(g_{\sigma(i)}v)$ and so $\tilde{\varphi}(gv) = \sigma^{-1}\tilde{\varphi}(v)$. This shows that $\bar{\varphi}$ is G-invariant.

Assume now that $gv \neq w$ for all $g \in G$. This implies that $hg_iv \neq w$ for all $h \in H$ and $i = 1,\ldots d$, and so $\varphi(g_iv) \neq \varphi(w)$ for $i = 1,\ldots,d$, because φ is H-separating. As a consequence, $\tilde{\varphi}(v) \neq \sigma\tilde{\varphi}(w)$ for all permutations $\sigma \in \mathcal{S}_d$, hence $\bar{\varphi}(v) \neq \bar{\varphi}(w)$, because ψ_W is $\mathcal{S}_d$-separating, and so $\bar{\varphi}$ is G-separating.

For the degree we get $\deg\bar{\varphi} \leq \deg\psi_W \cdot \deg\tilde{\varphi} \leq d \cdot \deg\varphi = [G:H]\beta_{\text{sep}}(H,V)$. This shows that

$$\beta_{\text{sep}}(G,V) \leq [G:H]\beta_{\text{sep}}(H,V).$$

If $H \subset G$ is normal we can find an H-separating morphism $\varphi \colon V \to W$ of degree $\beta_{\text{sep}}(H,V)$ such that W is a G/H-module and φ is G-equivariant. Now choose an G/H-separating morphism $\psi \colon W \to U$ of degree $\beta_{\text{sep}}(G/H,W)$. Then the composition $\psi \circ \varphi \colon V \to U$ is G-separating of degree $\leq \deg\psi \cdot \deg\varphi$. Thus

$$\beta_{\text{sep}}(G,V) \leq \beta_{\text{sep}}(G/H,W)\,\beta_{\text{sep}}(H,V) \leq \beta_{\text{sep}}(G/H)\,\beta_{\text{sep}}(H),$$

and the claim follows. □

5. Degree bounds for some finite groups

In principle, Proposition 3 allows to compute $\beta_{\text{sep}}(G)$ for any finite group G. Unfortunately, the invariant ring $\mathcal{O}(V_{\text{reg}})^G$ does not behave well in a computational sense. We have been able to compute $\beta_{\text{sep}}(G)$ with Magma [1] and the algorithm of [10] in just one case (computation time about 20 minutes):

Proposition 7 (MAGMA and Proposition 3)**.** *Let* $\operatorname{char} K = 2$*. Then* $\beta_{\text{sep}}(S_3) = 4$*.*

Proposition 8. *Let* $\operatorname{char} K = p > 0$ *and let* G *be a* p*-group. Then* $\beta_{\text{sep}}(G) = |G|$*.*

Proof. Let us start with a general remark. Let G be an arbitrary finite group, and let V be a *permutation module of* G, i.e. there is a basis $(v_1, v_2, \ldots, v_n)$ of V which is permuted under G. Then the invariants are linearly spanned by the *orbit sums* s_m of the monomials $m = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \in \mathcal{O}(V) = K[x_1, x_2, \ldots, x_n]$ which are defined in the usual way:

$$s_m := \sum_{f \in Gm} f$$

The value of s_m on the fixed point $v := v_1 + v_2 + \cdots + v_n \in V$ equals $|Gm|$. Hence, $s_m(v) = 0$ if p divides the index $[G : G_m]$ of the stabilizer G_m of m in G. It follows that for a p-group G we have $s_m(v) \neq 0$ if and only if m is invariant under G.

If, in addition, G acts transitively on the basis $(v_1, v_2, \ldots, v_n)$, then an invariant monomial m is a power of $x_1 x_2 \cdots x_n$, and thus has degree $\ell n \geq \dim V$. If we apply this to the regular representation, the claim follows. □

With Corollary 1 we get the next result.

Corollary 2. *Let* $\operatorname{char} K = p > 0$ *and* G *be a group of order* rp^k *with* $(r, p) = 1$*. Then* $\beta_{\text{sep}}(G) \geq p^k$*.*

Proposition 9. *Let* G *be a cyclic group. Then* $\beta_{\text{sep}}(G) = |G|$*.*

Proof. Let $|G| = rp^k$ where $(r, p) = 1$, $p = \operatorname{char} K$, and choose two elements $g, h \in G$ of order r and $q := p^k$, respectively, so that $G = \langle g, h \rangle$. We define a linear action of G on $V := \bigoplus_{i=1}^{q} K v_i$ by

$$g v_i := \zeta \cdot v_i \text{ and } h v_i := v_{i+1} \text{ for } i = 1, \ldots, q$$

where $\zeta \in K$ is a primitive rth root of unity and $v_{q+1} := v_1$. We claim that the G-invariants $\mathcal{O}(V)^G$ are linearly spanned by the orbit sums s_m where $r | \deg m$. In fact, $\mathcal{O}(V)^{\langle g \rangle}$ is linearly spanned by the monomials of degree ℓr ($\ell \geq 0$), and the subgroup $H := \langle h \rangle \subset G$ permutes these monomials.

Now look again at the element $v := v_1 + v_2 + \cdots + v_q \in V$. If $r | \deg m$ then $s_m(v) = |Hm|$, and this is non-zero if and only if the monomial m is invariant under H. This implies that m is a power of $x_1 x_2 \cdots x_q$. Since the degree of m is also a multiple of r we finally get $\deg s_m \geq rq = |G|$. □

Corollary 3. *Let* G *be a finite group. Then we have*

$$\beta_{\text{sep}}(G) \geq \max_{g \in G} (\operatorname{ord} g).$$

Let $D_{2n} = \langle \sigma, \rho \rangle$ denote the dihedral group of order $2n$ with $\operatorname{ord}(\sigma) = 2$, $\operatorname{ord}(\rho) = n$ and $\sigma \rho \sigma^{-1} = \rho^{-1}$.

Proposition 10. *Assume that* $\operatorname{char}(K) = p$ *is an odd prime, and let* $r \geq 1$*. Then* $\beta_{\text{sep}}(D_{2p^r}) = 2p^r$*.*

Note that if $\operatorname{char}(K) = p = 2$, then D_{2p^r} is a 2-group, so $\beta_{\text{sep}}(D_{2^{r+1}}) = 2^{r+1}$ by Proposition 8. We conjecture that for $\operatorname{char}(K) = 2$ and p an odd prime, we have $\beta_{\text{sep}}(D_{2p}) = p + 1$, which would fit with Proposition 7.

Proof. Put $q = p^r$ and define a linear action of D_{2p^r} on $V := \bigoplus_{i=0}^{q-1} Kv_i$ by

$$\rho v_i = v_{i+1} \text{ and } \sigma v_i = -v_{-i} \text{ for } i = 0, 1, \ldots, q-1$$

where $v_j = v_i$ if $j \equiv i \mod q$ for $i, j \in \mathbb{Z}$. As before, the invariants under $H := \langle \rho \rangle$ are linearly spanned by the orbit sums $s_m := \sum_{f \in Hm} f$ of the monomials $m = x_0^{i_0} x_1^{i_1} \cdots x_{q-1}^{i_{q-1}} \in \mathcal{O}(V) = K[x_0, x_1, \ldots, x_{q-1}]$. Thus, the D_{2p^r}-invariants are linearly spanned by the functions $\{s_m + \sigma s_m \mid m \text{ a monomial}\}$.

For $v := v_0 + v_1 + \cdots + v_{q-1}$ we get $\sigma s_m(v) = s_m(\sigma v) = (-1)^{\deg m} s_m(v)$. Therefore, $s_m + \sigma s_m$ is non-zero on v if and only if $s_m(v) \neq 0$ and the degree of m is even. As in the proof of Proposition 9, $s_m(v) \neq 0$ implies that m is a power of $x_0 x_1 \cdots x_{q-1}$ which has to be an even power since q is odd. Thus, for $m := (x_0 x_1 \cdots x_{q-1})^2$, $s_m + \sigma s_m = 2m$ is an invariant of smallest possible degree, namely $2q$, which does not vanish on v. □

Let $I_H := \mathcal{O}(V)_+^G \mathcal{O}(V)$ denote the *Hilbert-ideal*, i.e. the ideal in $\mathcal{O}(V)$ generated by all homogeneous invariants of positive degree. It is conjectured by Derksen and Kemper that I_H is generated by invariants of positive degree $\leq |G|$, see [4, Conjecture 3.8.6 (b)]. The following corollary shows that this conjectured bound can not be sharpened in general.

Corollary 4. *Let* $\operatorname{char} K = p$ *and* G *a* p*-group (with* $p > 0$*), or a cyclic group, or* $G = D_{2p^r}$ *with* p *odd. Then there exists a* G*-module* V *such that* I_H *is not generated by homogeneous invariants of positive degree strictly less than* $|G|$.

Proof. In the proofs of the Propositions 8, 9 and 10 respectively, we constructed a G-module V and a non-zero $v \in V$ such that $f(v) = 0$ for all homogeneous $f \in \mathcal{O}(V)^G$ of positive degree strictly less than $|G|$, but such that there exists a homogeneous $f \in \mathcal{O}(V)^G$ of degree $|G|$ with $f(v) \neq 0$. This shows that $f \notin \mathcal{O}(V)^G_{+,<|G|} \mathcal{O}(V)$. □

Now we use relative degree bounds for separating invariants and good degree bounds for generating invariants of non-modular groups, that appear as a subquotient, to get improved degree bounds for separating invariants in the modular case.

Proposition 11. *Let* $\operatorname{char} K = p$ *and* G *be a finite group. Assume there exists a chain of subgroups* $N \subset H \subset G$ *such that* N *is a normal subgroup of* H *and such that* H/N *is non-cyclic of order* s *coprime to* p*. Then*

$$\beta_{\text{sep}}(G) \leq \begin{cases} \frac{3}{4}|G| & \text{in case } s \text{ is even} \\ \frac{5}{8}|G| & \text{in case } s \text{ is odd.} \end{cases}$$

Proof. By Sezer [16], for a non-cyclic non-modular group U, we have $\beta(U) \leq \frac{3}{4}|U|$ in case $|U|$ is even, and $\beta(U) \leq \frac{5}{8}|U|$ in case $|U|$ is odd. We now assume s is even; the other case is essentially the same. Since $\beta_{\text{sep}}(U) \leq \beta(U)$ always holds, we get by using Theorem 2

$$\begin{aligned} \beta_{\text{sep}}(G) &\leq \beta_{\text{sep}}(H)[G:H] \leq \beta_{\text{sep}}(N)\beta_{\text{sep}}(H/N)[G:H] \\ &\leq \beta(H/N)[G:H]|N| \leq \frac{3}{4}[H:N][G:H]|N| = \frac{3}{4}|G|. \end{aligned}$$

□

Example 1. Assume $p = 3$ and $G = A_4$. The Klein four group is a non-cyclic non-modular subgroup of even order. We get $\beta_{\mathrm{sep}}(A_4) \le \frac{3}{4}|A_4| = 9$. Application of Theorem 2 shows $\beta_{\mathrm{sep}}(A_4 \times A_4) \le \beta_{\mathrm{sep}}(A_4)^2 \le 81$.

Example 2. Let D_{2n} be the dihedral group of order $2n$. We know $n \le \beta_{\mathrm{sep}}(D_{2n})$ by Corollary 3. Assume $\operatorname{char} K = p \ne 2$ and $n = p^r m$ with p, m coprime and $m > 1$. Then D_{2n} has the non-cyclic subgroup D_{2m} of even order, so $\beta_{\mathrm{sep}}(D_{2n}) \le \frac{3}{4}2n = \frac{3}{2}n$. So the only dihedral groups, to which the proposition above does not apply, are those of the form D_{2p^r}, which are covered by Proposition 10.

We end this section with two questions:

Question 1. *Which finite groups G satisfy $\beta_{\mathrm{sep}}(G) = |G|$?*

Question 2. *Which finite groups G do not have a non-cyclic non-modular subquotient?*

The dihedral groups of Proposition 10 satisfy this property, and we get $\beta_{\mathrm{sep}}(G) = |G|$ for those groups. But in characteristic 2, $\beta_{\mathrm{sep}}(S_3) < |S_3|$ by Proposition 7, so the answer to the second question only partially helps to solve the first one.

Note added in proof: The conjecture following Proposition 10 claiming that in characteristic 2 we have $\beta_{\mathrm{sep}}(D_{2p}) = p + 1$ for an odd prime p was recently proved by the first author jointly with Müfit Sezer: *Invariants of the dihedral group D_{2p} in characteristic two,* Preprint 2010.

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993).

[2] R. M. Bryant and G. Kemper, *Global degree bounds and the transfer principle for invariants*, J. Algebra **284** (2005), no. 1, 80–90.

[3] C. de Concini and C. Procesi, *A characteristic free approach to invariant theory*, Advances in Math. **21** (1976), no. 3, 330–354.

[4] H. Derksen and G. Kemper, Computational invariant theory, Invariant Theory and Algebraic Transformation Groups, I, Springer-Verlag, Berlin (2002), ISBN 3-540-43476-3. Encyclopaedia of Mathematical Sciences, 130.

[5] ———, *On global degree bounds for invariants*, in Invariant theory in all characteristics, Vol. 35 of *CRM Proc. Lecture Notes*, 37–41, Amer. Math. Soc., Providence, RI (2004).

[6] M. Domokos and P. Hegedűs, *Noether's bound for polynomial invariants of finite groups*, Arch. Math. (Basel) **74** (2000), no. 3, 161–167.

[7] J. Draisma, G. Kemper, and D. Wehlau, *Polarization of separating invariants*, Canad. J. Math. **60** (2008), no. 3, 556–571.

[8] P. Fleischmann, *The Noether bound in invariant theory of finite groups*, Adv. Math. **156** (2000), no. 1, 23–32.

[9] J. Fogarty, *On Noether's bound for polynomial invariants of a finite group*, Electron. Res. Announc. Amer. Math. Soc. **7** (2001) 5–7 (electronic).

[10] G. Kemper, *Computing invariants of reductive groups in positive characteristic*, Transform. Groups **8** (2003), no. 2, 159–176.

[11] ———, *Separating invariants*, J. Symbolic Comput. **44** (2009), no. 9, 1212–1222.

[12] D. Mumford, J. Fogarty, and F. Kirwan, Geometric invariant theory, Vol. 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)]*, Springer-Verlag, Berlin, third edition (1994), ISBN 3-540-56963-4.

[13] P. E. Newstead, Introduction to moduli problems and orbit spaces, Vol. 51 of *Tata Institute of Fundamental Research Lectures on Mathematics and Physics*, Tata Institute of Fundamental Research, Bombay (1978), ISBN 0-387-08851-2.

[14] M. Roberts, *On the Covariants of a Binary Quantic of the n^{th} Degree*, The Quarterly Journal of Pure and Applied Mathematics **4** (1861) 168–178.

[15] B. J. Schmid, *Finite groups and invariant theory*, in Topics in invariant theory (Paris, 1989/1990), Vol. 1478 of *Lecture Notes in Math.*, 35–66, Springer, Berlin (1991).

[16] M. Sezer, *Sharpening the generalized Noether bound in the invariant theory of finite groups*, J. Algebra **254** (2002), no. 2, 252–263.

[17] T. A. Springer, Linear algebraic groups, Vol. 9 of *Progress in Mathematics*, Birkhäuser Boston Inc., Boston, MA, second edition (1998), ISBN 0-8176-4021-5.

[18] D. L. Wehlau, *The Noether number in invariant theory*, C. R. Math. Acad. Sci. Soc. R. Can. **28** (2006), no. 2, 39–62.

Zentrum Mathematik - M11, Technische Universität München, Boltzmannstrasse 3, D-85748 Garching, Germany

E-mail address: kohls@ma.tum.de

Mathematisches Institut, Universität Basel, Rheinsprung 21, CH-4051 Basel, Switzerland

E-mail address: Hanspeter.Kraft@unibas.ch