ON DEGREE BOUNDS FOR INVARIANT RINGS OF FINITE GROUPS OVER FINITE FIELDS

PETER FLEISCHMANN AND WOLFGANG LEMPKEN

ABSTRACT. Let G be a finite group acting as algebra automorphisms on $A := \mathbb{F}[X_1, \dots, X_n]$. If $\mathbb{F}$ is a field of characteristic zero, then, due to classical results of Emmy Noether one knows that the invariant ring A^G can be generated in degrees less or equal to $|G|$. If $\mathbb{F}$ an arbitrary commutative ring (e.g. a finite field), the situation is much less satisfying. In this paper we give an outline on known results (with some new proofs) on degree bounds for arbitrary rings and arbitary finite groups. It turns out that for the finite field $\mathbb{F}_q$ with $q = p^s$, A^G can be constructed explicitly from A^P, if P is a Sylow - p group of G. We also present some new results on the range of finite fields over which Noether's bound holds for subgroups of classical groups.

1. Introduction

Let R be a commutative ring, A a finitely generated (unitary) commutative R -algebra and G a group acting on A as R - algebra automorphisms. Then the **invariant ring** A^G is defined to be the R - algebra of fixed points

$$A^G := \{a \in A \mid g(a) = a\}.$$

For example R can be the field of complex numbers and A the polynomial ring $\mathbb{C}[X_1, \dots, X_n]$ where the G - action on A is derived from a linear action on the space $V := \langle X_1, \dots, X_n \rangle_{\mathbb{C}}$ of homogeneous polynomials with degree one. This situation had been considered by Hilbert in his famous address on occasion of the first International Congress of Mathematics 1900 in Paris. There he posed the problem to prove or disprove that $\mathbb{C}[V]^G$ is finitely generated for arbitrary G. Today this is known as **Hilbert's 14^{th} problem**. By that time a positive answer was already known for $G = SL_2$ by explicit work of Gordan on binary forms and for GL_n by Hilbert himself, as an important application of his famous 'basis theorem'. These results could later be extended by Hermann Weyl who proved finite generation for the invariant rings of what are known today as 'linearly reductive' groups, i.e. groups G whose category of finite - dimensional $\mathbb{C}G$ - modules is semisimple.

In general the answer to Hilbert's 14^{th} problem is **'no'**: In (1958) a counterexample consisting of a group $G \cong (\mathbb{C}^+)^m$ was given by Nagata.

This cannot occur if G is a finite group because of the following fundamental result of Emmy Noether

Theorem 1.1. (Emmy Noether, 1926 [9]) If G is a finite group, R a Noetherian ring and A a finitely generated R - algebra, then A^G is finitely generated.

1991 *Mathematics Subject Classification.* Primary 20C20.

Noether's proof of this result uses the fact that A is integral over the subalgebra $B \leq A^G$, generated by the coefficients of all the polynomials $f_i(T) := \prod_{g\in G}(T-g(a_i)) \in A^G[T]$, where the a_i are chosen such that $A = R[a_1,\dots,a_n]$ and G acts on $\sum_{i=1}^n Ra_i$. By Hilbert's basis theorem B is a Noetherian ring and by finite integrality, A is a Noetherian B - module, containing A^G as a submodule. Since submodules of finitely generated modules over a Noetherian ring are again finitely generated, A^G is a finitely generated B - module and, a fortiori, finitely generated as an A - algebra.
Notice that, although we can easily describe a finite set of algebra generators for B, the above argument does not indicate any constructive method of choosing the 'missing' module generators for A^G over B.

Throughout the paper $\mathbf{N}_0$ denotes the set of nonnegative integers; for $n \in \mathbf{N}$, $\underline{n}$ denotes the set $\{1,2,\cdots,n\}$ and $\mathbf{N}_0^{\underline{n}}$ denotes the set of functions from $\underline{n}$ to $\mathbf{N}_0$.

Definition 1.2. Let R, A and G be as above and let $RG-mod$ denote the category of finitely generated RG - modules which are free over R. With R^* we denote the group of units of R. For $n \in \mathbf{N}$, $a_1,\dots,a_n \in A$ and $\alpha \in \mathbf{N}_0^{\underline{n}}$ we denote with $\underline{a}^\alpha$ the element $a_1^{\alpha_1}a_2^{\alpha_2}\dots a_n^{\alpha_n} \in A$ and with $\mathcal{M}_k(\underline{(a_i)})$ the R - span $\langle \underline{a}^\alpha \mid |\alpha| := \sum_{i=1}^n \alpha_i \leq k\rangle$.
Suppose that $A = R[a_i, i = 1,\dots,n]$ for some $n \in \mathbf{N}$ such that G acts linearly on $\sum_{i=1}^n Ra_i$. We define the **degree bound** $\beta(A^G,(a_1,\dots,a_n))$ to be the infimum of the set of all $k \in \mathbf{N}$ satisfying $A^G = R[b_1,\dots,b_m]$ with $\{b_1,\dots,b_m\} \subseteq \mathcal{M}_k(\underline{(a_i)})$. Notice that $\beta(A^G,(a_1,\dots,a_n)) \in \mathbb{Z}\cup\{\infty\}$.
If $A = R[X_1,\dots,X_n]$ is a polynomial ring with R - linear action of G on $V := \oplus_{i=1}^n RX_i$ then we will also write $A = R[V]$ and call $\beta(R[V]^G) := \beta(R[V],(X_1,\dots,X_n))$ a **local degree bound** of the pair (G,V). The supremum

$$\beta_R(G) := \sup\{\beta(R[V]^G) \mid V \in \ RG-mod\} \in \mathbb{Z}\cup\infty$$

will be called the **global (linear) degree bound** of the pair (R,G).

Remark 1.3. (i) Suppose that G is finite and $A = R[a_1,\dots,a_n]$ as above. Extending $\{a_i\}$, if necessary, we can assume that G permutes this set of generators. Consider $W := \oplus_{i=1}^n RX_i$ as a G - permutation module where G permutes the X_i in the same way as the a_i. Then the epimorphism $c:\ R[W] \to A,\ X_i \mapsto a_i$ is G - equivariant, i.e. c commutes with the G - actions on $R[W]$ and A. If $|G|$ is invertible in R, then the restriction $c_| : R[W]^G \to A^G$ is easily seen to be surjective as well, since $f = c(h) \in A^G$ with $h \in R[W]$ implies that $f = |G|^{-1}\sum_{g\in G} gf = c(|G|^{-1}\sum_{g\in G} gh) \in c(R[W]^G)$. We see that $\beta(A^G,(a_1,\dots,a_n)) \leq \beta(R[W]^G)$ (notice that the 'additional a_i's ' can be linearly expressed in the 'original' ones). The argument above shows that $\beta_R(A^G,(a_1,\dots,a_n)) \leq \beta_R(G)$, whenever $|G| \in R^*$. It also shows that if $|G|$ is invertible, a 'global' degree bound **for permutation modules** is a global degree bound for invariant rings of arbitrary modules.
(ii) By 1.1, $\beta := \beta(A^G,(a_1,\dots,a_n)) < \infty$ if R is Noetherian, but the proof does not give any bound for β.

The significance of degree bounds for constructive invariant theory has the following reason: Let $G :=\ \langle g_1,\dots,g_m\rangle$ with generators g_i and $A := R[V] = R[X_1,\dots,X_n]$. If $\beta(A^G)$ is a known finite number, then the following 'linear algebra' - procedure leads to a system of algebra generators of A^G:

Procedure 1.1. (Constructing algebra generators of $R[V]^G$)
(1) For $i = 1,2,\dots,\beta := \beta(R[V]^G)$ do
(2) find all homogeneous $f \in R[V]$ of degree i with $g_\ell(f) = f$ for all $\ell = 1,\dots,m$;
(3) od;

Denoting the i - th homogeneous component of $R[V]$ by $R[V]_i$ we have

$$R[V]_i = \oplus_{\alpha\in\mathbb{N}^{\underline{n}},|\alpha|=i}\ \underline{X}^\alpha$$

for $i \in \mathbf{N}$; hence step (2) consists of the solution of the following system of linear equations over R:

$$\Sigma_{\alpha\in\mathbb{N}^{\underline{n}},|\alpha|=i}\ c_\alpha(g_\ell(\underline{X}^\alpha) - \underline{X}^\alpha) = 0,\ \ell = 1, \dots, m$$

of format $m \times \begin{pmatrix} n+i-1 \\ i \end{pmatrix} \times \begin{pmatrix} n+i-1 \\ i \end{pmatrix}$. If $R = \mathbb{F}$ is a field, the complexity of this procedure will be $\mathcal{O}(m \cdot n^{3\beta})$ in elementary $\mathbb{F}$ - operations.

In 1916 Emmy Noether had already given two constructive proofs for the fact that for a finite group and a field $\mathbb{F}$ of characteristic zero, $\beta_{\mathbb{F}}(G) \leq |G|$. This is usually referred to as 'Noether's bound'. Unfortunately, both of these proofs fail in positive characteristics. In fact both proofs have two different steps where the characteristic of $\mathbb{F}$ comes into play: in one of these steps one needs that $|G|$ is invertible in $\mathbb{F}$ whereas in the other step one even needs that $|G|!$ is invertible in $\mathbb{F}$.
As we see soon Noether's bound does not hold in general if $|G|$ is not invertible in R. If $|G|$ is invertible in R, Noether's bound holds for solvable groups. This has been proved by L. Smith in 1995 for the case that R is a field [12] and by D. Richman in 1990 for arbitrary R with $|G| \in R^*$ (see [10] which appeared posthumously).

In [5] a constructive proof has been given for $\beta(R[V]^G) \leq max\{|G|,\ rank_R(V)(|G|-1)\}$ whenever there is a subgroup $H \leq G$ such that the index $|G:H|$ is invertible in R and the restriction $V_{|H}$ is a permutation module (i.e. H permutes an R - basis of V.) In [4] a degree bound has been given for so called 'vector invariants' of symmetric groups over arbitrary commutative rings. Each of these results give as a corollary the degree bound

$$\beta(R[V]^G) \leq max\{|G|,\ rank_R(V)(|G|-1)\} \quad (*)$$

for finite groups having a group order $|G|$ which is invertible in the ring R. Recently A. Broer proved the bound (*) to hold if R is field and $R[V]^G$ is a Cohen-Macaulay ring [2].
In case V is a permutation module of rank n over an arbitrary commutative ring R, M. Goebel ([6]) proved

$$\beta(R[V]^G) \leq \frac{n(n-1}{2}.$$

Moreover, a result of Richman ([11]) shows that $\beta_F(G) = \infty$ whenever the characteristic of the field F divides the order of G.

In this paper we use the result of [4] to extend the idea of Emmy Noether's first proof in [8] to arbitrary rings and in particular finite fields. In general this will not give a degree bound as good as Noether's bound for arbitrary finite groups with invertible order; but for special groups we will either obtain Noether's bound globally or at least significantly extend the range of rings where Noether's bound holds. In any case the proofs will be constructive, which means that they will provide a method to find a generating system of invariants within the given bound.

2. Constructing generators

From now on all groups considered will be assumed to be finite!

Let $R[X(n,k)]$ be the polynomial ring $R[X_{11},...,X_{n1},...,X_{1k},...,X_{nk}]$ in $n \times k$ variables and define the action of Σ_n on $R[X(n,k)]$ by extending the permutation action $\sigma(X_{ij}) := X_{\sigma(i)j}$ on $X(n,k) := \sum_{ij}^{\oplus} RX_{ij}$. Let $\underline{Y} := (Y_1,\ldots,Y_k)$ be a 'vector of variables'; then the multivariate polynomial

$$G(\underline{X}_1,\ldots,\underline{X}_n;\underline{Y}) := \prod_{i=1}^{n}(1+\sum_{j=1}^{k} X_{i,j}Y_j) \in R[X(n,k)]^{\Sigma_n}[Y_1,\ldots,Y_k]$$

is called **Galois - resolvent**. In the famous book 'Classical groups' of Hermann Weyl [14] one can find a proof of the following

Theorem 2.1. (Weyl) If $\mathbf{Q} \subseteq R$ then $R[X(n,k)]^{\Sigma_n}$ is generated by the coefficients of the Galois - resolvent $G(\underline{X}_1,\ldots,\underline{X}_n;\underline{Y})$. All of these have total degree $\le n$, so $\beta(R(n,k)^{\Sigma_n}) \le n$.

The analogue of Weyl's theorem is false if $R = \mathbf{Z}$ or a field of characteristic $p \le n$. Already in the smallest nontrivial case $n = 2$ and $R = \mathbb{F}_2$ it is an easy exercise to show that the invariant $X_{11}X_{12}\ldots X_{1k} + X_{21}X_{22}\ldots X_{2k}$ is indecomposable, i.e. cannot be written as a sum of products of invariants with degrees less than k. Hence $\beta(\mathbb{F}_2(X(2,k)))^{\Sigma_2} \ge k$ and $\beta_{\mathbb{F}_2}(\Sigma_2) \ge \lim_{k\to\infty} k = \infty$. In particular, this shows that Noether's bound does not hold in the case of finite fields in general.
In [10] it was proved by D. Richman, that the analogue of Weyl's theorem holds if $n!$ is invertible in R. For arbitrary R the following has been shown in [4]

Theorem 2.2. $\beta(R[X(n,k)]^{\Sigma_n}) \le max\{n, k\cdot(n-1)\}$. with equality if $n = p^s$ and $char\ R = p$.

Now let $H \le G$ with $n := |G : H|$ and $G/H := \{H := g_1H, g_2G, \ldots, g_nH\}$ the set of H cosets in G. Consider the Cayley - homomorphism $c: G \to \Sigma_n, g \mapsto (g_iH \mapsto g_jH := gg_iH)$. Suppose that $A := R[a_1,\ldots,a_m]$ with $G(\sum_{i=1}^m Ra_i) \subseteq \sum_{i=1}^m Ra_i$ and $A^H = R[b_1,\ldots,b_k]$ with $b_i \in \mathcal{M}_b(\underline{(a_i)})$. Then

$$\nu : R[X(n,k)] \to A, X_{i\ell} \mapsto g_i(b_\ell)$$

is a G - equivariant R - algebra morphism. In fact, it does not depend on the choice of the g_i and

$$\nu(g(X_{i\ell})) = \nu(X_{j\ell}) = g_j(b_\ell) = gg_ih(b_\ell) = gg_i(b_\ell) = g\nu(X_{i\ell}),$$

because $gg_i = g_jh^{-1}$ for a suitable $h \in H$. The map ν (for $H = 1$) had been used in Noether's original 1916 - proof. We can use her original argument to show that that the restriction

$$\nu_| : R[X(n,k)]^{\Sigma_n} \to A^G$$

is surjective, whenever n is invertible in R: In this case, for any $f = f(b_1,\ldots,b_k) \in A^G \le A^H$ we can define

$$F := \frac{1}{n}(f(X_{11},X_{12},\ldots,X_{1k}) + \cdots + f(X_{n1},X_{n2},\ldots,X_{nk})) \in R[X(n,k)]^{\Sigma_n} \text{ and get}$$

$$\nu(F) = \frac{1}{n}(f(g_1(b_1),g_1(b_2),\ldots,g_1(b_k)) + \cdots + f(g_n(b_1),g_n(b_2),\ldots,g_n(b_k))$$

$= \frac{1}{n}(g_1f(b_1,b_2,\ldots,b_k) + \cdots + g_nf(b_1,b_2,\ldots,b_k)) = f$. Let $\beta(n,k) := \beta(R[X(n,k)]^{\Sigma_n})$ then $R[X(n,k)^{\Sigma_n}] = R[F_1,\ldots,F_s]$ with $F_i \in \mathcal{M}_{\beta(n,k)}(\underline{(X_{ij})})^{\Sigma_n}$ and hence

$A^G = R[\nu(F_1), \ldots, \nu(F_s)]$ with $\nu(F_i) \in \mathcal{M}_{\beta(n,k)}(\underline{(g_i(b_j))})^G \leq \mathcal{M}_{\beta(n,k)b}(\underline{(a_i)})^G$. So $|G:H| \in R^*$ implies

$$\beta(A^G) \leq \beta(n,k)\beta(A^H).$$

On the other hand, since $c(G) = G/\cap_{g\in G}^g H \leq \Sigma_n$, we have $R[X(n,k)]^{\Sigma_n} \subseteq R[X(n,k)]^{c(G)}$, hence

$$\beta(A^G) \leq \beta(R[X(n,k)]^{c(G)}\beta(A^H).$$

Together with 2.1 (or [10]) and 2.2 we get:

Theorem 2.3. Let A be an R - algebra as above and $H \leq G$ with $|G:H|$ invertible in R and $A^H = R[b_1, \ldots, b_k]$ with $b_i \in A^H \cap \mathcal{M}_b(\underline{(a_i)})$. Then

$$\beta(A^G, (a_1, \ldots, a_m)) \leq \ max\{|G:H|, k \cdot (|G:H| - 1)\}\beta(A^H, (a_1, \ldots, a_m)), \text{ and}$$

$$\beta(A^G, (a_1, \ldots, a_m)) \leq \ \beta_R(c(G))\beta(A^H, (a_1, \ldots, a_m)), \text{ and.}$$

In particular, if A^H is finitely generated then so is A^G. If moreover $|G:H|!$ is invertible in R, then

$$\beta(A^G, (a_1, \ldots, a_m)) \leq \ |G:H|\beta(A^H, (b_1, \ldots, b_\ell)).$$

In the case $H = 1$ and $|G|$ invertible we recover the bound (*) above and if $|G|!$ is invertible, we get Noether's bound.
If $R = \mathbb{F}_q$ is the finite field of order $q = p^s$, then we can take $H = P$, a Sylow - p group of G. Since the index $|G:P|$ is invertible in $\mathbb{F}$, we can apply 2.3 and construct $\mathbb{F}[V]^G$ from $\mathbb{F}[V]^P$ via vector invariants. So in modular invariant theory the most serious problem is to construct invariant rings of p - groups in characteristic $p > 0$. For this task there are algorithms available due to Gregor Kemper (see [7]).

By an obvious induction we get from 2.3:

Corollary 2.4. Let $G = H_0 > H_1 > H_2 > \cdots > H_m$ with $|G|$ and $(|H_{i-1} : H_i|)! \in R^*$ for $i = 1, \ldots, m$. Then

$$\beta_R(G) \leq \beta_R(H_m) \cdot |G : H_m|.$$

Recall that a subgroup $G \leq \Sigma_n$ is called k **- fold transitive** (for $1 \leq k \leq n$), if the induced action $g(\alpha) = g \circ \alpha$ of G on the set $Inj(\underline{n}^{\underline{k}})$ of injective maps $\underline{k} \to \underline{n}$ is transitive. If $G \leq \Sigma_n$ is k - fold transitive, then the stabilizer $G_{i_1,i_2,\ldots,i_\ell} \leq \Sigma_{\underline{n}\setminus i_1,i_2,\ldots,i_\ell}$ of any $\ell \leq k$ ciphers is $k - \ell$ - fold transitive. Consider the chain of subgroups

$$G > G_{i_1} > G_{i_1,i_2} > \cdots > G_{i_1,i_2,\ldots,i_\ell}$$

then $n,\ n-1,\ \ldots,\ n-\ell+1$ is the corresponding sequence of indices and we get from 2.4:

Corollary 2.5. Let $G \leq \Sigma_n$ be k - fold transitive and $n! \in R^*$ then for any $\ell \leq k$ ciphers of $\underline{n}$:

$$\beta_R(G) \leq \beta_R(G_{i_1,i_2,\ldots,i_\ell}) \cdot \frac{n!}{(n-k)!} = \beta_R(G_{i_1,i_2,\ldots,i_\ell}) \cdot |G : G_{i_1,i_2,\ldots,i_\ell}|.$$

From the well known theorem of symmetric polynomials one knows that the local degree bound $\beta(R[V]^{\Sigma_n}) \leq n$ holds for the 'natural permutation module' $V \in R\Sigma_n - mod$; $(R[V]^{\Sigma_n}$ is generated by the elementary symmetric polynomials). Since $n < n!$ (for $n > 2$) this is much better than Noether's bound. But using 2.5 we obtain Noether's bound globally for the symmetric and alternating groups whenever the group order is invertible in R.

Corollary 2.6. Let $G \in \{\Sigma_n, Alt_n\}$ and $|G| \in R^*$ then $\beta_R(G) \leq |G|$.

Proof: The groups Σ_n and Alt_n are n - fold and $n-2$ - fold transitive on $\underline{n}$ respectively, with trivial n and $n-2$ - fold stabilisers. Now the claim follows immediately from 2.5.

3. Normal subgroups and Factor groups

Theorem 3.1. Let $N \triangleleft G$, $|G/N|$ invertible in R. Then

$$\beta_R(A^G, (a_1, \ldots, a_n)) \leq \beta_R(A^N, (a_1, \ldots, a_n)) \cdot \beta_R(G/N).$$

Proof: If $N \triangleleft G$, then the image $c(G)$ of the Cayley homomorphism is isomorphic to G/N and the result follows immediately from 2.3. $\circ$

If $|G|$ is invertible in R and we know a global degree bound for any composition factor of G, then 3.1 yields a global degree bound for G. Thus a proof of the Noether bound (for invertible $|G|$) is in principle reduced to simple groups. For the simple groups of a prime order which is invertible in R, the Noether bound holds due to a result of Richman:

Theorem 3.2. (D. Richman,[10]) Let $A = R[a_1, \ldots, a_n]$ with $G(\sum_{i=1}^n Ra_i) \subseteq \sum_{i=1}^n Ra_i$. Assume that $|G|$ is a prime and is invertible in R. Then A^G is generated as an R - algebra by

$$\{\sum_{g \in G} g(\underline{a}^\gamma) \mid \gamma \in \mathbf{N}_0^{\underline{k}},\ |\gamma| \leq |G|\}.$$

The following theorem can be viewed as a further motivation to prove Noether's bound in general for groups with invertible order:

Theorem 3.3. Let $\mathcal{K} := \{\mathbb{Z}/n\mathbb{Z}, Alt_n \mid n \in \mathbb{N}\}$ be the class consisting of cyclic and alternating groups. If G is a finite group with all composition factors isomorphic to an element of $\mathcal{K}$ and assume that $|G|$ is invertible in R. Then $\beta(A^G, (a_1, \ldots, a_n)) \leq |G|$; in particular

$$\beta_R(G) \leq |G|.$$

Proof: By 3.1, 2.6 and 3.2 a minimal counterexample cannot exist. $\circ$

Remark 3.4. We have been informed that this result has also been obtained by Ming-chang Kang, but we do not have any further details.

As a corollary we get:

Corollary 3.5. (D. Richman ([10]) , L. Smith ([12])) If G is solvable and $|G| \in R^*$, then $\beta_R(G) \leq |G|$.

Examples 3.6. i) The simple Mathieu group M_{11} has order $2^4 \cdot 3^2 \cdot 5 \cdot 11$ and contains a maximal subgroup $H \cong M_{10} := A_6.2$ of index 11. If we define $\tilde{\mathcal{K}} := \mathcal{K} \cup \{M_{11}\}$, then similar to 3.3 one can prove Noether's bound for all groups with composition factors in $\tilde{\mathcal{K}}$, as long as R is a field of characterisic $p \neq 7$ and not dividing $|G|$.

ii) As another example consider $G = SL_2(7)$, which has order $6 \cdot 7 \cdot 8 = 336$. From 2.3 we know that Noether's bound holds for G over any field of characteristic $p > 336$. But for classical groups like G we can do much better. In fact we will see that in case of $SL_2(7)$ Noether's bound already holds for $p > 7$.

So let us now consider the finite Chevalley groups of classical type $G(q)$, which are defined over finite fields $\mathbb{F}_q$. For details on these groups refer to [3]

The orders of these groups are given by polynomials in q of the following form

$$|G(q)| = |B(q)| \prod_{i=1}^{\ell} \frac{q^{d_i} - 1}{q - 1}$$

with $2 \leq d_1 \leq d_2 \leq \cdots \leq d_\ell \in \mathbf{N}$. The numbers $d_i - 1$ are the degrees of the fundamental invariants in the 'reflection representation' of the 'Weyl group' associated with $G(q)$, ℓ is the so called 'semisimple rank' of $G(q)$ and $B(q) \leq G(q)$ is the 'Borel subgroup' which is solvable. Let $d(G(q)) := max\{d_i \mid i = 1, \ldots, \ell\}$.
Then $d((G(q)) = \ell + 1$ for quasisimple $G(q)$ of Dynkin type A_ℓ, e.g. $GL_{\ell+1}(q), SL_{\ell+1}(q)$ or $PGL_{\ell+1}(q)$; $d((G(q)) = 2\ell$ for quasisimple $G(q)$ of Dynkin type B_ℓ, e.g. $Sp_{2\ell}(q)$ or $SO_{2\ell+1}(q)$ and $d((G(q)) = 2(\ell - 1)$ for quasisimple $G(q)$ of Dynkin type D_ℓ, e.g. $SO^{\pm}_{2\ell}(q)$.

Theorem 3.7. Suppose that $(\frac{q^{d(G(q))}-1}{q-1})!$ is invertible in R (e.g. R is a field of characteristic $p > \frac{q^{d(G(q))}-1}{q-1}$), then Noether's bound $\beta_R(G) \leq |G|$ holds for every $G \leq G(q)$.

Proof: From the order formulae for $|G(q)|$ we see immediately that all prime divisors of $|G(q)|$ are less or equal to $\frac{q^{d(G(q))}-1}{q-1}$, so $|G(q)|$ is invertible in R. Let $(G, G(q))$ be a counterexample with $|G| + |G(q)|$ minimal. Then we can assume that $G(q)$ is quasisimple: Indeed otherwise $G(q) = G_1(q) * G_2(q)$ with $|G_i(q)| < |G(q)|$ and $d(G_i(q)) \leq d(G(q))$. Consider the short exact sequence $1 \to G \cap G_2(q) \to G \to H \to 1$ with $H \cong GG_2(q)/G_2(q) \leq G_1(q)/Z$ and Z a central subgroup of $G_1(q)$. Since $G_1(q)/Z$ is a again a Chevalley group of classical type, the induction hypotheses together with 3.1 yield a contradiction.
It is well known, that $G(q)$ contains a maximal parabolic subgroup $P(q)$ which can be written as a semidirect product $UL(q)$, where $U := O_r(P(q))$ with $q = r^s$, r a prime and $L(q) < G(q)$ a Chevalley group of classical type. Moreover $P(q)$ can be chosen such that $|G(q) : P(q)|$ divides $\frac{q^{d(G(q))}-1}{q-1}$ and $d(L(q)) \leq d(G(q))$. Since $|G : G \cap P(q)|$ divides $|G(q) : P(q)|$, its factorial is in R^* and we get from 2.4:

$$\beta_R(G) \leq |G : G \cap P(q)| \beta_R(G \cap P(q)). \quad (*)$$

Now $G \cap U \triangleleft G \cap P(q)$ and $G \cap P(q)/G \cap U \leq P(q)/U \cong L(q)$. Since $G \cap U$ is solvable we get $\beta_R(G \cap P(q)) \leq |G \cap U| \cdot |G \cap P(q)/G \cap U| = |G \cap P(q)|$. Together with $(*)$ this gives the final contradiction. $\circ$

Corollary 3.8. If $n > 1$ and $\mathbb{F}$ is a field of characteristic $p > \frac{q^n-1}{q-1}$, then

$$\beta_{\mathbb{F}}(G) \leq |G|$$

for each $G \leq GL_n(q)$.

References

[1] D. Benson, *Representations and cohomology I*, Cambridge Univ. Press 1991.
[2] A. Broer, *Remarks on Invariant Theory of Finite Groups*, preprint, Université de Montréal, 1997.
[3] R.W.Carter *Finite Groups of Lie Type*, J.Wiley and Sons, (1985)
[4] P. Fleischmann, *A new degree bound for Vector Invariants of Symmetric Groups*, Trans. Amer. Math. Soc. **350** (1998), 1703-1712.
[5] P. Fleischmann, W. Lempken, *On generators of modular invariant rings of finite groups*, Bull. London Math. Soc. **29** (1997), 585-591.
[6] M. Goebel, *Computing bases for rings of permutation- invariant polynomials*, J. Symb. Comp. **19** (1995), 285-291.

[7] G. Kemper, *Calculating Invariant Rings of Finite Groups over Arbitrary Fields*, J.Symbolic Computation, **21** (1996), 351–366.
[8] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77** (1916), 89-92.
[9] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p*, Nachr. Ges. Wiss. Göttingen (1926), 28-35, in 'Collected Papers', pp.485-492, Springer Verlag, Berlin (1983).
[10] D. Richman, *Explicit generators of the invariants of finite groups*, Adv. Math. **124** (1996), 49-76.
[11] D. Richman, *Invariants of finite groups over fields of charact eristic p*, Adv. Math. **124** (1996), 25-48.
[12] L. Smith, *E. Noether's bound in the invariant theory of finite groups*, Arch. Math. **66** (1995), 89-92.
[13] L. Smith, *Polynomial Invariants of Finite Groups*, A.K. Peters Ltd., (1995).
[14] H. Weyl, *The Classical Groups*, 2^{nd} Edition, Princeton Univ. Press, Princeton (1953).

Institute for Experimental Mathematics, University of Essen, Ellernstr. 29, 45326 Essen, G ermany

E-mail address: `peter@exp-math.uni-essen.de`

Institute for Experimental Mathematics, University of Essen, Ellernstr. 29, 45326 Essen, Germany

E-mail address: `lempken@exp-math.uni-essen.de`