Arch. Math. 74 (2000) 161–167
0003-889X/00/030161-07 $ 2.90/0

Archiv der Mathematik

Noether's bound for polynomial invariants of finite groups

By

MÁTYÁS DOMOKOS[1]) and PÁL HEGEDŰS[2])

Abstract. Let G be a finite group acting linearly on the polynomial algebra $\mathbb{C}[V]$. We prove that if G is the semi-direct product of cyclic groups of odd prime order, then the algebra of polynomial invariants is generated by its elements whose degree is bounded by $\frac{5}{8}|G|$. As a consequence we derive that $\mathbb{C}[V]^G$ is generated by elements of degree $\leqq \frac{3}{4}|G|$ for any non-cyclic group G. This sharpens the improved bound for Noether's Theorem due to Schmid.

1. Introduction. Let G be a finite group acting linearly on a finite dimensional complex vector space V, i.e. V is a right G-module. Consider the induced action of G on the polynomial algebra $\mathbb{C}[V]$, which is the direct sum of the symmetric tensor powers of V. For any $f \in \mathbb{C}[V]$ and $g \in G$ we put f^g for the image of f under g. We study

$$\mathbb{C}[V]^G = \{f \in \mathbb{C}[V] \mid \forall g \in G\ f^g = f\},$$

the *algebra of polynomial invariants*. It is a graded subalgebra of $\mathbb{C}[V]$, and Noether's Theorem [2] asserts that $\mathbb{C}[V]^G$ is generated as an algebra by its elements whose degrees are not greater than the order of G. Following [5] we put

$$\beta(G,V) = \min\{d \mid \mathbb{C}[V]^G \text{ is generated by its elements of degree } \leqq d\}$$

and

$$\beta(G) = \max\{\beta(G,V) \mid V \text{ is a finite dimensional representation of } G\}.$$

As it is pointed out in [5, Section 6], a theorem of Weyl implies that $\beta(G) = \beta(G, V_{reg})$, where V_{reg} denotes the *regular representation* of G. It follows that the number $\beta(G)$ does not change if we replace the base field $\mathbb{C}$ by any field of characteristic zero.

The bound in Noether's Theorem is sharp for cyclic groups. However, Schmid [5] (see also [4]) refined it by showing that $\beta(G) \leqq |G| - 1$ if G is non-cyclic. In the present paper we improve this result as follows.

Theorem 1.1. *If G is not cyclic, then $\beta(G) \leqq \frac{3}{4}|G|$.*

Remark. The cases of Klein's four group $Z_2 \times Z_2$ and the quaternion group of order 8 (see [5, 10.1. Lemma]) show that $c = \frac{3}{4}$ is the best possible constant in a bound $\beta(G) \leqq c|G|$ for non-cyclic G.

Mathematics Subject Classification (1991): 13A50.

[1]) Research supported by grants OTKA F023436 and the Bolyai Research Fellowship.
[2]) Research supported by grant OTKA T29132.

The proof is based on the reduction steps developed in [5]. Our main new contribution is a better bound for $\beta(G)$ when G is the semi-direct product of cyclic groups of odd order. In particular, we prove the following:

Proposition 1.2. *Let p, q be odd primes with q dividing $p-1$, and denote by $Z_p \rtimes Z_q$ the non-commutative semi-direct product of the cyclic groups of order p and q. Then we have the inequality $\beta(Z_p \rtimes Z_q) \leqq \frac{5}{8}pq$.*

2. The bound for the semi-direct product of cyclic groups. Throughout this section p, q are odd primes, $k = \dfrac{p-1}{2q}$ is a positive integer, $G = Z_p \rtimes Z_q$. The group G has the presentation

$$G = \langle a, b \mid a^p = b^q = 1,\ bab^{-1} = a^r \rangle,$$

where r is a primitive qth root of unity modulo p, fixed for the whole section. Let V be the regular representation of G. We shall study $\mathbb{C}[V]^G$. As we noted in the introduction, $\beta(G) = \beta(G, V)$. Recall that up to isomorphism G has q one-dimensional representations and k conjugate pairs of q-dimensional representations. For the purpose of our proof we choose a linear basis

$$\{x_1, \ldots, x_q, y_{i,n,j}, z_{i,n,j} \mid i = 1, \ldots, k,\ n, j = 1, \ldots, q\}$$

in V such that the generators a, b act on this basis as follows:

- $x_j^a = x_j$, $x_j^b = \eta^j x_j$, where η is a complex primitive qth root of unity;
- $y_{i,n,j}^a = \xi_i^{r^{j-1}} y_{i,n,j}$, where ξ_i is a primitive pth root of unity depending on i (and $\{\xi_i^{r^{j-1}}, \bar{\xi}_i^{r^{j-1}} \mid i = 1, \ldots, k,\ j = 1, \ldots, q\}$ are all the primitive pth roots of unity);
- $y_{i,n,j}^b = y_{i,n,j+1}$ $(j = 1, \ldots, q-1)$, $y_{i,n,q}^b = y_{i,n,1}$;
- $z_{i,n,j}^a = \xi_i^{-r^j} z_{i,n,j}$;
- $z_{i,n,j}^b = z_{i,n,j+1}$ $(j = 1, \ldots, q-1)$, $z_{i,n,q}^b = z_{i,n,1}$.

Note that $x_1, \ldots, x_q$ span pairwise non-isomorphic one-dimensional irreducible representations of G. For a fixed i and n

$$\mathrm{Span}_{\mathbb{C}}\{y_{i,n,j} \mid j = 1, \ldots, q\}$$

is a q-dimensional irreducible G-invariant direct summand of V, and

$$\mathrm{Span}_{\mathbb{C}}\{z_{i,n,j} \mid j = 1, \ldots, q\}$$

is its conjugate representation. The index i parametrizes the conjugate pairs of isomorphism classes of q-dimensional irreducible representations, and for a fixed i we have q isomorphic summands indexed by n. Observe that we have chosen the basis so that the eigenvalue of a on $z_{i,n,j}$ is the complex conjugate of the eigenvalue of a on $y_{i,n,j+1}$ ($y_{i,n,1}$, when $j = q$). This translation between the corresponding indices may seem unnatural now, but it will be relevant later (see the proof of Lemma 2.1).

The set of monomials in the above variables is denoted by $M(V)$. Consider a monomial

$$v = x_1^{\alpha_1} \cdots x_q^{\alpha_q} \prod_{i,n,j} y_{i,n,j}^{\gamma_{i,n,j}} \prod_{i,n,j} z_{i,n,j}^{\delta_{i,n,j}},$$

and define its *degrees* as

$$\gamma_j^i(v) = \sum_{n=1}^{q} (\gamma_{i,n,j} + \delta_{i,n,j}),\ (i = 1, \ldots, k,\ j = 1, \ldots, q).$$

We call a monomial v a *brick*, if there exists an $i \in \{1, \ldots, k\}$ such that $v = y_1 \cdots y_q$, where $y_j \in \{y_{i,n,j}, z_{i,n,j} \mid n = 1, \ldots, q\}$ for $j = 1, \ldots, q$.

Lemma 2.1. *A brick is either a-invariant or it has an a-invariant submonomial of degree two.*

Proof. Let $v = y_1 \cdots y_q$ be a brick, and denote by J the subset of indices j for which $y_j \in \{y_{i,n,j} \mid n = 1, \ldots, q\}$. Then we have

$$y_j^a = \begin{cases} \zeta_i^{rj-1} y_j, & \text{if } j \in J; \\ \zeta_i^{-rj} y_j, & \text{if } j \notin J. \end{cases}$$

It is easy to see that if v has no a-invariant subproduct of degree two, then the map $j \mapsto j - 1 \pmod q$ stabilizes J. It follows that J is either empty or $J = \{1, \ldots, q\}$. In both cases v itself is a-invariant. □

Now we introduce a partial ordering on $M(V)$. First for any monomial $v \in M(V)$ and $i \in \{1, \ldots, k\}$ we define the ith *degree counting series* of v as

$$\mu_d^i(v) = |\{j \mid \gamma_j^i(v) = d\}| \quad (d = 0, 1, 2, \ldots).$$

Let v, v' be two monomials. We say that v is *smaller* than v' ($v \prec v'$) if the total degree of v is smaller than the total degree of v', or if they have equal total degrees, and there exists an $s \in \{1, \ldots, k\}$ such that $\mu_d^i(v) = \mu_d^i(v')$ for $i = 1, \ldots, s-1$, $d = 0, 1, 2, \ldots$, and the series $(\mu_0^s(v), \mu_1^s(v), \mu_2^s(v), \ldots)$ is lexicographically smaller than $(\mu_0^s(v'), \mu_1^s(v'), \mu_2^s(v'), \ldots)$.

We call an a-invariant monomial v *expressible* if

$$v + v^b + \cdots + v^{b^{q-1}} \in \mathbb{C}[w + w^b + \cdots + w^{b^{q-1}} \mid w \in M(V), w^a = w, w \prec v].$$

The above definition is motivated by the fact that $\mathbb{C}[V]^G$ is generated as an algebra by the elements $w + w^b + \cdots + w^{b^{q-1}}$ as w runs over the set of a-invariant monomials.

For $v \in M(V)$ and $i \in \{1, \ldots, k\}$ we define the number

$$h_i(v) = \min\{d \mid \mu_d^i(v) \neq 0,\ \mu_{d+1}^i(v) = 0\}.$$

In other words, put the degrees $\gamma_1^i(v), \ldots, \gamma_q^i(v)$ in an increasing sequence. Then $h_i(v)$ is the first member of this sequence such that the next member jumps at least by two (if there is no such a jump then $h_i(v)$ is the largest degree in the sequence).

Lemma 2.2. *Let v be an a-invariant monomial with a non-trivial decomposition $v = wz$, such that $w^a = w$, $z^a = z$, and z contains a variable different from $x_1, \ldots, x_q$. Let $s \in \{1, \ldots, k\}$ be the minimal index for which z contains a variable from $\{y_{s,n,j}, z_{s,n,j} \mid n, j = 1, \ldots, q\}$. Assume that*

$\gamma_j^s(z) > 0$ if and only if $\gamma_j^s(v) > h_s(v)$,
and $\gamma_j^s(w) \geqq h_s(v) + 1$ if $\gamma_j^s(v) > h_s(v)$.

Then v is expressible.

Proof. Consider

$$(w + w^b + \cdots + w^{b^{q-1}})(z + z^b + \cdots + z^{b^{q-1}}) = \sum_{t,u=0}^{q-1} w^{b^t} z^{b^u} = \sum_{t,u=0}^{q-1} (wz^{b^t})^{b^u}. \tag{1}$$

We claim that $wz^{b^t} \prec wz$ for $t = 1, \ldots, q-1$. Since z and z^{b^t} do not depend on variables contributing to $\mu_d^i(v)$ for $i < s$, we have

$$\mu_d^i(wz^{b^t}) = \mu_d^i(w) = \mu_d^i(v) \text{ if } i < s.$$

The conditions on w and z imply that $(\mu_0^s(w), \ldots, \mu_h^s(w)) = (\mu_0^s(v), \ldots, \mu_h^s(v))$, where $h = h_s(v)$.

Since q is a prime number, the non-empty set of indices $\{j \mid \gamma_j^s(v) > h_s(v)\}$ is not stabilized by the map $j \mapsto j + t \pmod q$. Therefore there exists a variable y of z^{b^t} such that for the unique index l with $\gamma_l^s(y) = 1$ we have $f := \gamma_l^s(v) \leqq h$, thus

$$\gamma_l^s(wz^{b^t}) > \gamma_l^s(w) = f.$$

It follows that $(\mu_0^s(wz^{b^t}), \ldots, \mu_f^s(wz^{b^t}))$ is lexicographically smaller than $(\mu_0^s(w), \ldots, \mu_f^s(w)) = (\mu_0^s(v), \ldots, \mu_f^s(v))$. This means that $wz^{b^t} \prec wz = v$, and $wz + (wz)^b + \cdots + (wz)^{b^{q-1}}$ is expressible by (1). □

Corollary 2.3. *Let v be an a-invariant monomial. We decompose it as a product $v = v_0 w$, where w does not contain any variable x_j, v_0 is a product of variables x_j and bricks (see Lemma 2.1), and $\mu_0^i(w) \neq 0$ for $i = 1, \ldots, k$ (i.e. w is not divisible by any bricks). If $\deg(w) \geqq k(1 + 2 + \cdots + (q-1)) + p$, then v is expressible.*

Proof. The assumption on $\deg(w)$ implies that $\gamma_1^i(w) + \cdots + \gamma_q^i(w) > 0 + 1 + 2 + \cdots + (q-1)$ holds for some i, and therefore there is a jump by two in the increasing sequence of the degrees $0 = \gamma_{\pi(1)}^i(w) \leqq \cdots \leqq \gamma_{\pi(q)}^i(w)$. Let $s \in \{1, \ldots, k\}$ be minimal with $h_s(w) < \max\{\gamma_j^s(w) \mid j = 1, \ldots, q\}$.

Let w_1 denote a submonomial of w such that

$$\gamma_j^i(w_1) = \begin{cases} \gamma_j^i(w), & \text{if } i < s; \\ \gamma_j^s(w), & \text{if } i = s \text{ and } \gamma_j^s(w) \leqq h_s(w); \\ h_s(w) + 1, & \text{if } i = s \text{ and } \gamma_j^i(w) > h_i(w); \\ 0, & \text{otherwise.} \end{cases}$$

For any j with $\gamma_j^s(w) > h_s(w)$ take a variable y of $\dfrac{w}{w_1}$ with $\gamma_j^s(y) = 1$, and denote by w_2 the product of these variables. Then we have $w = w_1 w_2 w'$. It is easy to see that $\deg(w_1 w_2) \leqq s(1 + 2 + \cdots + (q-1)) + 1$, hence $d = \deg(w') \geqq p - 1$ by the assumption on $\deg(w)$. Now write $w' = y_1 \cdots y_d$ as a product of variables. We have $y_j^a = \zeta^{c_j} y_j$, where ζ is a complex primitive pth root of unity, and c_j are positive integers smaller than p. Consider the two-element subsets $C_j = \{\bar{c}_j, \bar{0}\}$ of the additive group of the residue classes modulo p. Recall the Cauchy–Davenport Lemma [1], which states that for any subsets C, D of the additive group of the residue classes modulo p we have that the cardinality of their sum $C + D$ is at least $\min\{p, |C| + |D| - 1\}$. It follows that $C_1 + \cdots + C_d$ contains all the residue classes modulo p, which means that w' has a submonomial w_3 such that $w_2 w_3$ is a-invariant. Thus we get a decomposition of v as a product of a-invariant monomials $v = (v_0 w_1 w_4)(w_2 w_3)$ such that the conditions of Lemma 2.2 are fulfilled, and so v is expressible. □

Proof of Proposition 1.2. The algebra $\mathbb{C}[V]^G$ is generated by $v + v^b + v^{b^2} + \cdots + v^{b^{q-1}}$ as v runs over the set of a-invariant monomials in $M(V)$. Moreover, by definition it is clearly sufficient to take v from the set of monomials which are not expressible. The proof will be concluded by giving an upper bound for the degree of a non-expressible monomial. We shall use the fact that if an a-invariant monomial v is the product of more than q non-trivial a-invariant monomials, then $v + v^b + \cdots + v^{b^{q-1}}$ is contained in the algebra generated by the elements $w + w^b + \cdots + w^{b^{q-1}}$ with $w^a = w$ and $\deg(w) < \deg(v)$ (c.f. [5, 4.2. Lemma, line 5]), in particular, v is expressible.

Let v be a non-expressible a-invariant monomial. Then we write it as

$$v = x_{i_1} \cdots x_{i_s} v_1 \cdots v_t w, \tag{2}$$

where $x_{i_j} \in \{x_1, \ldots, x_q\}$, $v_1, \ldots, v_t$ are bricks, w does not contain more a-invariant variables and $\mu_0^i(w) \neq 0$ for $i = 1, \ldots, k$. By Corollary 2.3 we have $\deg(w) \leqq k(1 + \cdots + (q-1)) + p - 1 = A$, so (2) implies

$$\deg(v) \leqq s + tq + A. \tag{3}$$

On the other hand, by Lemma 2.1 each v_j contains an a-invariant submonomial v_j', so we have

$$v = x_{i_1} \cdots x_{i_s} v_1' \cdots v_t' w'. \tag{4}$$

Let u denote the maximal number such that w' is the product of u non-trivial a-invariant monomials. Since v cannot be written as a product of more than q non-trivial a-invariant monomials, we have

$$s + t + u \leqq q. \tag{5}$$

By the Cauchy–Davenport Lemma any monomial of degree $\geqq p$ contains non-trivial a-invariant submonomials, hence we have $\deg(w') \leqq up$, and (4) implies

$$\deg(v) \leqq s + tq + up. \tag{6}$$

If $up \geqq A$, then we use the bound (3), while if $up \leqq A$, then we use the bound (6). The biggest value with (3) is obtained when $u = \lceil A/p \rceil$, $s = 0$ and $t = q - u$. Similarly, the biggest value with (6) is obtained when $u = \lfloor A/p \rfloor$, $s = 0$, $t = q - u$.

So we conclude from (3), (5) and (6) that

$$\beta(G) \leqq \min\{q(q - \lceil A/p \rceil) + A, q(q - \lfloor A/p \rfloor) + \lfloor A/p \rfloor p\}, \tag{7}$$

where $\lceil - \rceil$ ($\lfloor - \rfloor$, resp.) denotes the upper (lower, resp.) integral part of the rational number in the argument. Note that the difference of the two numbers on the right hand side of (7) is $A - p\lfloor A/p \rfloor - q$.

In the remaining part of the proof we demonstrate that $\frac{5}{8}$ is the best upper bound for $\dfrac{\beta(G)}{|G|}$ which can be derived from (7). Indeed, since $A = \frac{1}{2}kq(q+3)$, we have

$$\frac{q+2}{4} < \frac{A}{p} = \frac{kq\dfrac{q+3}{2}}{2kq+1} < \frac{q+3}{4}.$$

Hence if $q \equiv 1 \bmod 4$, then $\left\lceil \frac{A}{p} \right\rceil = \frac{q+3}{4}$. One can easily check that the number in (7) coming from (6) gives the better bound, which is

$$\frac{\beta(G)}{|G|} \leqq \frac{3q+1}{4p} + \frac{q-1}{4q} \leqq \frac{5q^2-1}{8q^2+4} < \frac{5}{8}$$

($k = 1$ yields $\frac{5q^2-1}{8q^2+4}$, which tends to $\frac{5}{8}$ as q goes to infinity).

If $q \equiv 3 \bmod 4$, then $\left\lceil \frac{A}{p} \right\rceil = \frac{q+5}{4}$, and the number in (7) coming from (3) gives

$$\frac{\beta(G)}{|G|} \leqq \frac{q\left(q - \frac{q+5}{4}\right) + \frac{kq(q+3)}{2}}{pq} \leqq \frac{5q+1}{8q+4} < \frac{5}{8}. \quad \square$$

3. Noether's bound in general. Let G be a finite group. Then $\beta(G) \leqq \beta(G/N)\beta(N)$ for any normal subgroup N of G, and $\beta(G) \leqq \beta(H)[G:H]$ for any subgroup H of G, where $[G:H]$ denotes the index of H in G (c.f. [5, 3.1., 3.2. Lemma]). Therefore by induction it is sufficient to prove Theorem 1.1 for the direct products of two cyclic groups (which are non-cyclic), and for non-abelian groups whose all proper subquotients are cyclic, and these non-abelian groups are precisely the semi-direct products of groups of prime order (see for example [5, 3.4. Proposition]).

Now we have

(i) $\beta(Z_p \times Z_2) = p + 1 \leqq \frac{2}{3}2p$ for any odd prime p by [5, 7.1. Theorem].

(ii) If a is a divisor of b, then $\beta(Z_a \times Z_b) = a + b - 1$ by [3] (see [5, Section 2, 8] why Olson's Theorem is relevant here), and obviously $a + b - 1 \leqq \frac{3}{4}ab$. We would like to note that [5, 8.2. Conjecture] is false in general, the first counterexample was given in [6].

(iii) The only missing case is that of the groups $Z_p \times Z_q$, which is covered by our Proposition 1.2.

Thus $\beta(G) \leqq \frac{3}{4}|G|$ holds for any non-cyclic group G.

Acknowledgement. We thank Pálfy Péter Pál for his helpful comments on the manuscript.

References

[1] H. DAVENPORT, On the addition of residue classes. J. London Math. Soc. **10,** 30–32 (1935).

[2] E. NOETHER, Der Endlichkeitssatz der Invarianten endlicher Gruppen. Math. Ann. **77,** 89–92 (1916).

[3] J. E. OLSON, A combinatorial problem on finite abelian groups II. J. Number Theory **1,** 195–199 (1969).

[4] B. J. SCHMID, Generating invariants of finite groups. C. R. Acad. Sci. Paris **308,** Série I, 1–6 (1989).

[5] B. J. SCHMID, Finite groups and invariant theory. "Topics in Invariant Theory". LNM **1478,** 35–66. Berlin-Heidelberg-New York 1991.

[6] D. KRUYSWIJK and P. VAN EMDE BOAS, A combinatorial problem on finite abelian groups III. Report ZW-34-1969-008, Math. Centre Amsterdam.

Eingegangen am 14. 12. 1998

Anschrift der Autoren:

Mátyás Domokos
Mathematical Institute of the Hungarian
Academy of Sciences
P.O. Box 127
H-1364 Budapest
Hungary

Pál Hegedűs
Department of Algebra and Number Theory
Eötvös University
Budapest
Múzeum krt 6–8
H-1088
Hungary