FINITE GROUPS WITH LARGE NOETHER NUMBER ARE ALMOST CYCLIC

PÁL HEGEDŰS, ATTILA MARÓTI, AND LÁSZLÓ PYBER

Abstract. Noether, Fleischmann and Fogarty proved that if the characteristic of the underlying field does not divide the order $|G|$ of a finite group G, then the polynomial invariants of G are generated by polynomials of degrees at most $|G|$. Let $\beta(G)$ denote the largest indispensable degree in such generating sets. Cziszter and Domokos recently described finite groups G with $|G|/\beta(G)$ at most 2. We prove an asymptotic extension of their result. Namely, $|G|/\beta(G)$ is bounded for a finite group G if and only if G has a characteristic cyclic subgroup of bounded index. In the course of the proof we obtain the following surprising result. If S is a finite simple group of Lie type or a sporadic group then we have $\beta(S) \leq |S|^{39/40}$. We ask a number of questions motivated by our results.

1. Introduction

Let G be a finite group and V an FG-module of finite dimension over a field F. By a classical theorem of Noether [10], the algebra of polynomial invariants on V, denoted by $F[V]^G$, is finitely generated. Define $\beta(G, V)$ to be the smallest integer d such that $F[V]^G$ is generated by elements of degrees at most d. In case the characteristic of F does not divide $|G|$, the numbers $\beta(G, V)$ have a largest value as V ranges over the finite dimensional FG-modules. This number is called the *Noether number* and is denoted by $\beta(G)$. The notation $\beta(G)$ suppresses the dependence on the field but it should not cause misunderstanding. In fact, for fields of the same characteristic the Noether number is the same and we may assume that F is algebraically closed. See [9] for details.

Noether [10] also proved that $\beta(G) \leq |G|$ over fields of characteristic 0. This bound was verified independently by Fleischmann [5] and Fogarty [6] to hold also in positive characteristics not dividing $|G|$. For characteristics dividing $|G|$, a deep result of Symonds [16] states that $\beta(G, V) \leq \dim(V)(|G| - 1)$.

From now on throughout the whole paper, except in Question 8.3, we assume that the characteristic of the field F is 0 or is coprime to the order of G.

Date: September 30, 2018.

2010 *Mathematics Subject Classification.* 13A50, 20D06, (20D08, 20D99).

Key words and phrases. polynomial invariants, Noether bound, simple groups of Lie type.

The research was partly supported by the National Research, Development and Innovation Office (NKFIH) Grant No. K115799. The second and third authors were also funded by the National Research, Development and Innovation Office (NKFIH) Grant No. ERC_HU_15 118286. The second author received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No. 648017) and was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

Schmid [14] proved that over the field of complex numbers $\beta(G) = |G|$ holds only when G is cyclic. This was sharpened by Domokos and Hegedűs [4] (and later by Sezer [15] in positive coprime characteristic) to $\beta(G) \leq \frac{3}{4}|G|$ unless G is cyclic.

An important ingredient in Schmid's argument was to show that $\beta(G) \geq \beta(H)$ holds for any subgroup $H \leq G$. In particular, $\beta(G)$ is bounded from below by the maximal order of the elements in G, that is, the *Noether index* $n(G) = |G|/\beta(G)$ of a finite group G is at most the minimal index of a cyclic subgroup in G.

Recently Cziszter and Domokos [3] described finite groups G with $n(G)$ at most 2. Their deep result [3, Theorem 1.1] states that for a finite group G (with order not divisible by the characteristic of F) we have $n(G) \leq 2$ if and only if G has a cyclic subgroup of index at most 2, or G is isomorphic to $Z_3 \times Z_3$, $Z_2 \times Z_2 \times Z_2$, the alternating group A_4, or the binary tetrahedral group $\widetilde{A_4}$. In particular, the inequality $n(G) \leq 2$ implies that G has a cyclic subgroup of index at most 4.

Our main result is as follows.

Theorem 1.1. *Let G be a finite group with Noether index $n(G)$. Then G has a characteristic cyclic subgroup of index at most $n(G)^{10\log_2 k}$ where k denotes the maximum of 2^{10} and the largest degree of a non-Abelian alternating composition factor of G, if such exists. Furthermore if G is solvable, then G has a characteristic cyclic subgroup of index at most $n(G)^{10}$.*

In view of Theorem 5.2 and Section 6, the bound $n(G)^{10}$ holds even for a large class of non-solvable groups.

Theorem 1.1 has a consequence which can be viewed as an asymptotic version of the afore-mentioned result of Cziszter and Domokos.

Corollary 1.2. *Let G be a finite group with Noether index $n(G)$. If G is nonsolvable, then $n(G) > 2.7$ and G has a characteristic cyclic subgroup of index at most $n(G)^{100+10\log_2\log_2 n(G)}$. If G is solvable then G contains a characteristic cyclic subgroup of index at most $n(G)^{10}$.*

It is an open question whether there exists a polynomial bound in $n(G)$ for the index of a characteristic cyclic subgroup in an arbitrary finite group G. Theorem 1.1 is a major step in answering this question.

As a step in our proofs we obtain a result which may be of independent interest.

Theorem 1.3. *Let S be a finite simple group of Lie type or a sporadic simple group. Then $n(S) \geq |S|^{1/40}$.*

It would be interesting to know if the bound in Theorem 1.3 holds for alternating groups of arbitrarily large degrees. Our methods are sufficient only for degrees up to 17. For degrees no greater than 17 (but at least 5) the claim follows from the remark after Lemma 4.1.

Assume that, for some fixed constant $\epsilon > 0$, we have $n(S) \geq |S|^{\epsilon}$ for every alternating group S of degree at least 5. Then our proofs show that, for some other (computable) fixed constant $\epsilon' > 0$ with $\epsilon' \leq 0.1$, any finite group G has a characteristic cyclic subgroup of index at most $n(G)^{1/\epsilon'}$.

2. Affine groups

Our main aim in the present section is to give upper bounds on $\beta(G)$ for the Frobenius group $G \cong Z_p \rtimes Z_n$, where p is a prime and $n \mid p-1$.

It is an open conjecture of Pawale [13] that $\beta(Z_p \rtimes Z_q) = p+q-1$ for a prime q. This is verified for $q = 2$ [14] (where $\beta(D_{2n}) = n+1$ is shown for composite n, as well) and for $q = 3$ [2]. Cziszter and Domokos obtain an upper bound which we extend to a more general one if q is not a prime. See Lemma 2.6, Theorem 2.7 and Corollary 2.9.

In this section we rely heavily on the techniques developed by Cziszter and Domokos. For convenience and completeness we include here those that we need. However, we try to simplify and not include them in full generality.

Let G be the Frobenius group of order pn with $Z_p \leq G \leq \mathrm{Aff}_p$. Then every G-module has a Z_p-eigenbasis permuted up to scalars by G. The regular module is relevant because every irreducible Z_p-character occurs in it. For every Z_p-module V the polynomial invariants are linear combinations of Z_p-invariant monomials. The Z_p-invariant monomials correspond to 0-sum sequences of irreducible Z_p-characters. These motivate all the definitions below.

Let $\mathcal{Y} = \{y_1, \ldots, y_p\}$ be the set of variables from $F[Z_p]$ that are Z_p-eigenvectors and y_1 is Z_p-invariant. For a monomial $f = \prod_{i=1}^{p} y_i^{a_i}$ let us define $b(f) = \prod_{a_i>0} y_i$. Let $g_1 = b(f)$ and construct recursively the finite list of monomials $g_1, g_2, \ldots$ in such a way that $g_{k+1} = b(f/\prod_{j=1}^{k} g_j)$ for every k, stopping if $f = \prod g_j$. We call this list the *row decomposition* of f. (In [3] the corresponding list of irreducible Z_p-characters is considered and called the row decomposition.) This list consists of monomials each dividing the previous one and the exponent of every variable y_i is at most 1.

Let l be a positive integer. Suppose a set of variables $\{x_1, \ldots, x_l\}$ consists of Z_p-eigenvectors on which G/Z_p acts by permutation, but not necessarily transitively. For each x_i there is a corresponding unique $y_{\bar{i}} \in \mathcal{Y}$ having the same Z_p-action on them. This defines a map $m \mapsto f_m$ from the monomials in $\{x_1, \ldots, x_l\}$ to the monomials in $\mathcal{Y}$ by $m = \prod x_i^{a_i} \mapsto m_f = \prod y_{\bar{i}}^{a_i}$. This map is G/Z_p-equivariant. Moreover, the Z_p-action on m is the same as on f_m, so m is Z_p-invariant if and only if f_m is.

Given a monomial m we determine the row decomposition $g_1, \ldots, g_h$ of f_m. Suppose that for every G-orbit $\mathcal{O} \subseteq \mathcal{Y}$ and every index $i < h$ the following holds. If g_i involves some variables from $\mathcal{O}$, but not all then g_{i+1} involves fewer variables than g_i does. Such a monomial m is called *gapless* in [3, Definition 2.5]. If $g_i = g_{i+1}$ for a gapless monomial m then g_i is G/Z_p-invariant. In particular, as nontrivial G/Z_p-orbits on $\mathcal{Y}$ are of length n,

$$\text{if } y_1 \nmid g_i \text{ and } \deg(g_i) < n \text{ then } \deg(g_{i+1}) < \deg(g_i). \tag{1}$$

Let $M = \oplus_{d=0}^{\infty} M_d$ be a graded module over a commutative graded F-algebra $R = \oplus_{d=0}^{\infty} R_d$. We also assume that $R_0 = F$ when $1 \in R$ and $R_0 = 0$ otherwise. Define $M_{\leq s} = \oplus_{d=0}^{s} M_d$, a subspace of M, and $R_+ = \oplus_{d=1}^{\infty} R_d \lhd R$ a maximal ideal. The subalgebra of R generated by $R_{\leq s}$ is denoted by $F[R_{\leq s}]$. Define $\beta(M, R) =$

$\min\{s \mid M = \langle M_{\leq s}\rangle_{R_+}\}$, the highest degree needed for an R_+-generating set of M. In other words, it is the highest degree of nonzero components of M/MR_+ (the factor space M/MR_+ inherits the grading).

The following three propositions from [3] will be used in the proof of Theorem 2.7. They are paraphrased and not stated in their full generality.

Proposition 2.1. [3, Proposition 2.7] *Let G be the Frobenius group of order pn with $Z_p \leq G \leq \mathrm{Aff}_p$. Let V be an FG-module, $L = F[V]$ the polynomial algebra, $R = L^G$ its invariants. Suppose the variables of L are permuted by G up to non-zero scalar multiples. Then the vector space L_+/L_+R_+ is spanned by monomials of the form $b_1 \cdots b_r m$, where the b_i are Z_p-invariant of degree 1 or of prime degree $q_i|n$ and m has a gapless divisor of degree at least $\deg(m) - (p-1)$.*

(Note that the so-called *bricks* mentioned in the original version of Proposition 2.1 are Z_p-invariant.)

Proposition 2.2. [3, Lemma 1.11] *Let G be the Frobenius group of order pn with $Z_p \leq G \leq \mathrm{Aff}_p$. Let V be an FG-module, $L = F[V]$ the polynomial algebra, $R = L^G$ and $I = L^{Z_p}$ its invariants. Then for every $s \geq 1$ the following bound is valid:*

$$\beta(L_+, R) \leq (n-1)s + \max\{\beta(L_+/L_+R_+, I), \beta(L_+/L_+R_+, F[I_{\leq s}]) - s\}.$$

(The original version of Proposition 2.2 holds for the generalized Noether numbers β_r, however we only use the case $r = 1$.)

Lemma 2.3. [3, Lemma 2.10] *Let S be a sequence over Z_p with maximal multiplicity h. If $|S| \geq p$ then S has a zero-sum subsequence $T \subseteq S$ of length $|T| \leq h$.*

The following proposition is a simple corollary.

Proposition 2.4. *Suppose f is a monomial in $\mathcal{Y}$ of degree at least p such that the exponent of each $y_i \in \mathcal{Y}$ is at most h. Then f has a Z_p-invariant submonomial f' such that $\deg(f') \leq h$.*

Proof. Let $f = \prod y_i^{a_i}$. Fix a generator element $z \in Z_p$ and a primitive p-th root of unity, $\mu \in F$. Define S to be the sequence over $\mathbb{Z}/\mathbb{Z}_p$ consisting of a_i copies of the exponent of μ as the eigenvalue of z on y_i. This satisfies the assumptions of the previous lemma. Let then f' be the product of the elements of T, it is a submonomial of degree $|T| \leq h$. That T is zero-sum means exactly that f' is Z_p-invariant. □

The following upper bound is used frequently.

Lemma 2.5. *Let $E = (Z_p)^k$ be a non-cyclic elementary Abelian p-group for some prime p. Then $\beta(E) = kp - k + 1$. Thus $\beta(E) < |E|^{0.8}$. Furthermore if $|E| \neq 2^2$, 3^2, 5^2, then $\beta(E) < |E|^{0.67}$.*

Proof. The first statement is the combination of Olson's Theorem [11] and a "folklore result" of invariant theory [15, Proposition 8]. We have $\beta(E) < |E|^{0.8}$ since $k \geq 2$. The other statement follows from an easy calculation. □

We reformulate the result of [3] for affine groups in a form that can be applied in inductive arguments. For our purposes the following lemma is sufficient. However, as the proof shows, $\beta(G) \leq (1+\varepsilon)p\sqrt{q}$ is true for fixed $\varepsilon > 0$ and for p, q large enough.

Lemma 2.6. *Let $q \mid p-1$ for primes p, q and let $G \leq \mathrm{Aff}_p$ be of order pq. Then $\beta(G) \leq pq^{0.8}$.*

Proof. If $q = 2$, then $\beta(G) = p+1 < p2^{0.8}$ (see [14, (7.1)] and [15, Proposition 13]). Let $q > 2$. By [3, Proposition 2.15] we have $\beta(G) \leq \frac{3}{2}(p + q(q-2)) - 2 < 3p - 2$ if $p > q(q-2)$. If here $q \geq 5$ then $3p - 2 < pq^{0.8}$. If $q = 3$ then $\beta(G)$ is at most $\frac{3}{2}(p + q(q-2)) - 2 = \frac{3}{2}p + 2.5 < p3^{0.8}$, as required.

So let $p < q(q-2)$, in particular $q > 3$. In this case [3, Proposition 2.15] concludes $\beta(G) \leq 2p + (q-2)q - 2$ and $\beta(G) \leq 2p + (q-2)(c-1) - 2$ if there exists $c \leq q$ such that $c(c-1) < 2p < c(c+1)$. Note that if $q(q-1) < 2p$ then $q < \sqrt{2p}$ and if $q(q-1) > 2p$ then there exists $c \leq q$ such that $c(c-1) < 2p < c(c+1)$ and $c - 1 < \sqrt{2p}$. So in both cases $\beta(G) \leq 2p + (q-2)\sqrt{2p} - 2$. If $q = 5$ then $p < 15$ and $5 \mid p-1$ imply $p = 11$. We have $\beta(G) \leq 22 + 3\sqrt{22} - 2 < 11 \cdot 5^{0.8}$.

Finally let $q \geq 7$. Using $q - 2 < \sqrt{q}\sqrt{p/2}$ we get

$$\beta(G) < p(2 + \frac{\sqrt{q}\sqrt{p/2}\sqrt{2p}}{p}) = p(2 + \sqrt{q}).$$

As $q^{0.8} - q^{0.5}$ is increasing and $7^{0.8} - 7^{0.5} > 2$ we get the claimed bound. □

Theorem 2.7. *Let G be the Frobenius group of order pn with $Z_p \leq G \leq \mathrm{Aff}_p$. Suppose that $n \geq 6$ has no prime divisor larger than $p/\sqrt{n}$. Then $\beta(G) < 2p\sqrt{n}$.*

Proof. Let V be an arbitrary FG-module, $L = F[V]$ the polynomial algebra and $R = L^G$ and $I = L^{Z_p}$ the respective group invariants. Put $s = [p/\sqrt{n}]$. As $\beta(Z_p) = p$ we have $\beta(L_+/L_+R_+, I) \leq p$. Hence by Proposition 2.2,

$$\beta(G, V) \leq (n-1)s + \max\{p, \beta(L_+/L_+R_+, F[I_{\leq s}]) - s\}.$$

The first term of this sum is smaller than $p\sqrt{n}$ so it is enough to prove that

$$\beta(L_+/L_+R_+, F[I_{\leq s}]) \leq p\sqrt{n} + s. \tag{2}$$

We assume that the basis of the dual module V^* is a Z_p-eigenbasis $\{x_1, x_2, \ldots, x_l\}$ permuted by G/Z_p. Now apply Proposition 2.1. The space L_+/L_+R_+ is spanned by monomials m that either have a Z_p-invariant divisor of degree at most s or have a gapless monomial divisor of degree at least $\deg(m) - (p-1)$. The former kind are in $F[I_{\leq s}]$ so we need an upper bound for the degrees of the latter kind. More precisely, we have that if m' is the largest degree gapless monomial with no Z_p-invariant divisor of degree at most s then

$$\beta(L_+/L_+R_+, F[I_{\leq s}]) \leq p - 1 + \deg(m'). \tag{3}$$

Consider now the row decomposition $g_1, \ldots, g_h$ of $f_{m'}$. In the submonomial $f = g_1 + g_2 + \cdots + g_s$ of $f_{m'}$ all the exponents are at most s, so by Proposition 2.4,

$\deg f \leq p-1$. This implies that $\deg(g_s) \leq (p-1)/s$. It is below $\sqrt{n}+1$ because if $s = (p/\sqrt{n}) - \varepsilon$ then

$$(\frac{p}{\sqrt{n}} - \varepsilon)(\sqrt{n}+1) = p + \frac{p}{\sqrt{n}} - \varepsilon\sqrt{n} - \varepsilon > p-1.$$

So $\deg(g_s) \leq \sqrt{n}+1$. In particular, $\deg(g_s) < n$ and by (1), $\deg(g_{i+1}) < \deg(g_i)$ for $i \geq s$. Hence we have the following bound on the degree.

$$\deg(m') = \sum_{i=1}^{s} \deg(g_i) + \sum_{i=s+1}^{h} \deg(g_i) < p-1+\frac{1}{2}\sqrt{n}(\sqrt{n}+1) = p-1+\frac{n+\sqrt{n}}{2}.$$

Now (3) and $2 + \frac{n}{2(p-1)} \leq 2.5 < \sqrt{n} + \frac{1}{\sqrt{n}}$ (as $n > 5$) imply that

$$\begin{aligned}\beta(L_+/L_+R_+, F[I_{\leq s}]) &\leq p-1+\deg(m') \leq 2(p-1)+\frac{n+\sqrt{n}}{2} = \\ &= (p-1)\left(2+\frac{n}{2(p-1)}\right)+\frac{\sqrt{n}}{2} < \\ &< (p-1)\left(\sqrt{n}+\frac{1}{\sqrt{n}}\right)+\sqrt{n}-1 < p\sqrt{n}+s,\end{aligned}$$

which is exactly (2). □

We continue with a useful tool.

Lemma 2.8 (Schmid [14] and Sezer [15])**.** *Let H be a subgroup and N a normal subgroup in a finite group G. Then $\beta(G) \leq \beta(N)\beta(G/N)$ and $\beta(G) \leq |G:H|\beta(H)$.*

Proof. See Schmid [14, (3.1), (3.2)] and Sezer [15, Propositions 2 and 4]. □

Corollary 2.9. *Let N be a normal subgroup of prime order p in a finite group G. Assume that $N = C_G(N)$ and that G/N is cyclic of order m prime to p. Then $\beta(G) \leq pm^{0.9}$.*

Proof. The group G is an affine Frobenius group. If m is prime, then the claim follows from Lemma 2.6. For $m = 4$ we have $\beta(G) \leq p+6 < 4^{0.9}p$ by [3, Corollary 2.9]. If m has a prime divisor $q > p/\sqrt{m}$ then first, $m < p < q\sqrt{m}$ implies $q > \sqrt{m}$. Second, $Z_p \rtimes Z_q \leq G$, so by Lemma 2.6 and Lemma 2.8, $\beta(G) \leq \frac{m}{q}pq^{0.8} = mpq^{-0.2} < pm^{0.9}$. Finally, if $m \geq 6$ has no prime divisor larger than $p/\sqrt{m}$ then by Theorem 2.7 we have $\beta(G) \leq 2p\sqrt{m} \leq pm^{0.9}$. □

3. Solvable groups

In this section we will give a general upper bound for $\beta(G)$ in case G is a finite solvable group.

Proposition 3.1. *Let C be a characteristic cyclic subgroup of maximal order in a finite nilpotent group G. Then $\beta(G) \leq |C|^{0.2}|G|^{0.8}$.*

Proof. Suppose that G is a counterexample with $|G|$ minimal. By the aforementioned result of Noether [10], Fleischmann [5] and Fogarty [6], G must be non-cyclic. By Lemma 2.8, G must also be a p-group for some prime p. Then $G/\Phi(G)$ must be a non-cyclic elementary Abelian p-group where $\Phi(G)$ denotes the Frattini subgroup of G. By Lemma 2.5, $\beta(G/\Phi(G)) < |G/\Phi(G)|^{0.8}$. By minimality, there exists a characteristic cyclic subgroup C in $\Phi(G)$, characteristic in G, such that $\beta(\Phi(G)) \leq |C|^{0.2}|\Phi(G)|^{0.8}$. We get a contradiction using Lemma 2.8. □

We repeat the following result from the Introduction.

Theorem 3.2 (Domokos and Hegedűs [4] and Sezer [15])**.** *For any non-cyclic finite group G we have $\beta(G) \leq \frac{3}{4}|G|$.*

The next bound holds for every finite solvable group, but it is slightly weaker than the one in Proposition 3.1.

Theorem 3.3. *Let C be a characteristic cyclic subgroup of maximal order in a finite solvable group G. Then $\beta(G) \leq |C|^{0.1}|G|^{0.9}$.*

Proof. By Proposition 3.1, we may assume that G is not nilpotent. Consider the Fitting subgroup $F(G)$ and the Frattini subgroup $\Phi(G)$ of G. Since $F(G)$ is normal in G, we have, by [8, Page 269], that $\Phi(F(G)) \leq \Phi(G) \leq F(G)$. Thus $F(G)/\Phi(G)$ is a product of elementary Abelian groups. The socle of the group $G/\Phi(G)$ is $F(G)/\Phi(G)$ on which $G/F(G)$ acts completely reducibly (in possibly mixed characteristic) and faithfully (see [8, III. 4.5]).

Let N be the product of $O_p(G) \cap \Phi(F(G))$ for all primes p for which $O_p(G)$ is cyclic, together with the subgroups $O_p(G) \cap \Phi(F(G))$ for all primes p for which p divides $|F(G)/\Phi(G)|$ but p^2 does not, together with $O_p(G) \cap \Phi(G)$ for all primes p for which p^2 divides $|F(G)/\Phi(G)|$. Clearly, $F(G)/N$ is a faithful $G/F(G)$-module (of possibly mixed characteristic) with a completely reducible, faithful quotient.

We claim that the bound in the statement of the theorem holds when C is taken to be the product of the (direct) product of all cyclic Sylow subgroups of $F(G)$ and a characteristic cyclic subgroup of maximal order in N. By our choice of C and Proposition 3.1, we have $\beta(N) \leq (|C|/s)^{0.1}|N|^{0.9}$, where s denotes the product of the primes for which $O_p(G)$ is cyclic. In order to finish the proof of the theorem, it is sufficient to show that $\beta(G/N) \leq s^{0.1}|G/N|^{0.9}$.

This latter bound will follow from the following claim. Let H be a finite solvable group with a normal subgroup V that is the direct product of elementary Abelian normal subgroups of H. Let π be the set of prime divisors of $|V|$ and write V in the form $\times_{p\in\pi}O_p(V)$. Assume that V is self-centralizing in H and that the H/V-module V has a completely reducible, faithful quotient module. We claim that $\beta(H) \leq s^{0.1}|H|^{0.9}$ where s denotes the product of all primes p for which $|O_p(V)| = p$.

We prove the claim by induction on $|\pi|$. Let $p \in \pi$. Assume that $|\pi| = 1$. If $|V| = p$ then Corollary 2.9 gives the claim. Assume that $|V| \geq p^2$. By a result of Pálfy [12] and Wolf [18], $|H/V| < |V|^{2.3}$. First assume that $|V|$ is different from 2^2,

3^2, 5^2. By Lemma 2.5 and Lemma 2.8,

$$\beta(H) < |V|^{0.67}|H/V| < |H|^{0.9}.$$

Thus assume that $|V| = 2^2$, 3^2, or 5^2. If $|H| < |V|^2$, then

$$\beta(H) < |V|^{0.8}|H/V| < |H|^{0.9},$$

again by Lemmas 2.5 and 2.8. So assume also that $|H| \geq |V|^2$, in particular that H/V is not cyclic. By Theorem 3.2, we have $\beta(H) < \frac{3}{4}|V|^{0.8}|H/V| \leq |H|^{0.9}$, since H is solvable.

Assume that $|\pi| > 1$. The group H can be viewed as a subdirect product in $Y = Y_p \times Y_{p'}$ where Y_p and $Y_{p'}$ are solvable groups with the following properties. There is an elementary Abelian normal p-subgroup V_p in Y_p and a direct product $V_{p'}$ of elementary Abelian normal p'-subgroups in $Y_{p'}$ such that both the Y_p/V_p-module V_p and the $Y_{p'}/V_{p'}$-module $V_{p'}$ have a completely reducible, faithful quotient module. Let N be the kernel of the projection of H onto Y_p. Clearly, N satisfies the inductive hypothesis with the set $\pi \setminus \{p\}$ of primes. Thus Lemma 2.8 gives the bound of the claim. □

4. Finite simple groups of Lie type

The following is inherent in [3] without being explicitly stated. We reproduce their argument with a slight modification.

Lemma 4.1. *If G is a nonsolvable finite group then $n(G) > 2.7$.*

Proof. By Lemma 2.8, it is enough to prove this for minimal non-Abelian simple groups. By a theorem of Thompson [17, Corollary 1] these are $\mathrm{PSL}(3,3)$, Suzuki groups $\mathrm{Sz}(2^p)$, for $p > 2$ prime and $\mathrm{PSL}(2,q)$, where $q = 2^p$, 3^p (p a prime, $p > 2$ for $q = 3^p$) or $q > 3$ is a prime such that $q \equiv \pm 2 \pmod 5$.

If $G \cong \mathrm{Sz}(2^p)$ or $G \cong \mathrm{PSL}(2, 2^p)$, for $p > 2$ then G has an elementary Abelian subgroup $H \cong Z_2^3$ of index $k = |G : H| \geq 63$. So $n(G) \geq \frac{8k}{2k+3} = 4 - \frac{12}{2k+3} > 3.9$. (See the proof of [3, Theorem 1.1 case (2a)].)

If $G \cong \mathrm{PSL}(3,3)$ or $G \cong \mathrm{PSL}(2, 3^p)$, for $p > 2$ then G has an elementary Abelian subgroup $H \cong Z_3^2$ of index $k = |G : H| \geq 624$. So $n(G) \geq \frac{9k}{3k+2} = 3 - \frac{6}{3k+2} > 2.9$. (See the proof of [3, Theorem 1.1 case (2b)].)

If $G \cong \mathrm{PSL}(2,4) \cong A_5$ or $G \cong \mathrm{PSL}(2,p)$ then G contains a subgroup $H \cong A_4$ of index $k = |G : H| \geq 5$. So $n(G) \geq \frac{6k}{2k+1} = 3 - \frac{3}{2k+1} > 2.7$. (See the proof of [3, Theorem 1.1 case (2c)].) □

This implies that if G is a nonsolvable group with order less than 2.7^{40} then $\beta(G) < |G|/2.7 < |G|^{39/40}$. The following theorem claims this bound for every finite simple group of Lie type.

Theorem 4.2. *Let S be a finite simple group of Lie type. Then $\beta(S) \leq |S|^{39/40}$, in other words, $n(S) \geq |S|^{1/40}$.*

TABLE 1. Elementary Abelian groups in finite simple groups of Lie type

type	order bound	lower bound for $\lvert E\rvert$	lower bound for $\log_{\lvert S\rvert} n(E)$
$A_m(q)$	q^{m^2+2m}	$q^{[(\frac{m+1}{2})^2]}$	0.11 ($m=3$, $q=2$), 0.051 ($m=2$, $q=2$)
${}^2A_m(q)$	q^{m^2+2m}	$q^{[\frac{m+1}{2}]^2(+1)}$	0.11 ($m=3$, $q=2$), 0.066 ($m=2$, $q=3$)
$B_m(q)$	q^{2m^2+m}	q^{2m-1}, $q^{1+\binom{m}{2}}$	0.12 ($m=2$, $q=3$)
$C_m(q)$	q^{2m^2+m}	$q^{\binom{m+1}{2}}$	0.15 ($m=3$, $q=2$), 0.15 ($m=2$, $q=4$)
$D_m(q)$	q^{2m^2-m}	$q^{\binom{m}{2}}$	0.11 ($m=4$, $q=2$)
${}^2D_m(q)$	q^{2m^2-m}	$q^{\binom{m}{2}}$, $q^{2+\binom{m-1}{2}(+1)}$	0.11 ($m=4$, $q=2$), 0.15 ($m=4$, $q=3$)
${}^2B_2(q)$	q^5	q	0.066 ($q=8$)
${}^3D_4(q)$	q^{28}	q^5	0.086 ($q=2$)
$G_2(q)$	q^{14}	q^3, q^4	0.1 ($q=5$), 0.14 ($q=3$)
${}^2G_2(q)$	q^7	q^2	0.17 ($q=27$)
$F_4(q)$	q^{52}	q^{11}, q^9	0.14 ($q=2$), 0.12 ($q=3$)
${}^2F_4(q)$	q^{26}	q^5	0.14 ($q=8$)
$E_6(q)$	q^{78}	q^{16}	0.15 ($q=2$)
${}^2E_6(q)$	q^{78}	q^{12}, q^{13}	0.11 ($q=3$), 0.11 ($q=2$)
$E_7(q)$	q^{133}	q^{27}	0.16 ($q=2$)
$E_8(q)$	q^{248}	q^{36}	0.12 ($q=2$)

Proof. The proof requires a case by case check of the 16 families of simple groups of Lie type. In each case we find a subgroup $E \leq S$ with Noether index $n(E)$ relatively large, more precisely $n(E) \geq |S|^{1/40}$ and hence $n(S) \geq n(E) \geq |S|^{1/40}$ as required.

If the rank of the group is at least 2 then we find a non-cyclic elementary Abelian p-subgroup E in the defining characteristic p satisfying $|E|^8 > |S|$. The relevant data can be found for example in [7, Tables 3.3.1 and 2.2] which we summarise below. By Lemma 2.5 we have $n(S) \geq n(E) > |S|^{1/40}$ which implies our statement in this case. However Table 1 gives the best bounds for each type that can be obtained this way. (For notational ease $C_2(2^a)$ is used instead of $B_2(2^a)$ below. The Tits group is not in the list, but using a Sylow 2-subgroup we can easily obtain $n(S) > |S|^{0.2}$ for that S.)

So this method gives a better bound $\log_{|S|} n(E) \geq 0.051 > 1/20$, the worst group being $S \cong \mathrm{PSL}(3,2)$, with $|E| = 4$.

The rank 1 case remains. First let $p > 3$ be a prime and $S = \mathrm{PSL}(2,p)$. Then S contains a Frobenius subgroup $H \cong Z_p \rtimes Z_{(p-1)/2}$ of index $|S:H| = p+1$. By Corollary 2.9, we have the bound $\beta(H) \leq p(\frac{p-1}{2})^{0.9}$. It follows by Lemma 2.8 that $\beta(S) \leq (p+1)\beta(H) \leq (p+1)p(\frac{p-1}{2})^{0.9}$. This implies $\beta(S) < |S|^{1-1/40}$ for $p \geq 13$.

For $S \cong \mathrm{PSL}(2,p)$ with $p = 5$, 7, 11 the order of the group S is less than 2.7^{40}, so the theorem holds by the remark after Lemma 4.1.

Finally let $S = \mathrm{PSL}(2,q)$ where $q = p^f$, p a prime and $f > 1$. Then $S = \mathrm{PSL}(2,q)$ contains an elementary Abelian subgroup E of order p^f for which, by Lemma 2.5,

$\beta(E) = (p-1)f + 1 < p^{0.8f}$. Since $|S| < q^3 = p^{3f}$, we have

$$n(E) = \frac{p^f}{(p-1)f+1} > p^{0.2f} > |S|^{1/15}.$$

This finishes the proof. □

5. A reduction to almost simple groups

We will proceed to prove the following result.

Theorem 5.1. *Let G be a finite group and C a characteristic cyclic subgroup in G of largest size. Then $\beta(G) \leq |C|^{\epsilon}|G|^{1-\epsilon}$ with $\epsilon = (10\log_2 k)^{-1}$, where k denotes the maximum of 2^{10} and the largest degree of a non-Abelian alternating composition factor of G, if such exists. If G is solvable, then $\beta(G) \leq |C|^{0.1}|G|^{0.9}$.*

The second statement of Theorem 5.1 is Theorem 3.3. The following result reduces the proof of Theorem 5.1 to a question on almost simple groups.

Theorem 5.2. *Let G be a finite group. Let ϵ be a constant with $0 < \epsilon \leq 0.1$ such that $\beta(H) \leq 2^{-\epsilon}|H|^{1-\epsilon}$ for any (if any) almost simple group H whose socle is a composition factor of G. Let C be a characteristic cyclic subgroup of maximal order in G. Then $\beta(G) \leq |C|^{\epsilon}|G|^{1-\epsilon}$.*

Note that for any finite group G the ϵ in Theorem 5.2 can be taken to be positive by Theorem 3.2.

Proof. Let G be a counterexample to the statement of Theorem 5.2 with $|G|$ minimal. By Theorem 3.3, G cannot be solvable. Let R be the solvable radical of G. By Theorem 3.3 there exists a characteristic cyclic subgroup C of R (which is also characteristic in G) such that $\beta(R) \leq |C|^{\epsilon}|R|^{1-\epsilon}$. If $R \neq 1$, then, by minimality, $\beta(G/R) \leq |G/R|^{1-\epsilon}$, and so Lemma 2.8 gives a contradiction. Thus $R = 1$.

Let S be the socle of G. This is a direct product of, say $r \geq 1$, non-Abelian simple groups. Let K be the kernel of the action of G on S. By our hypothesis on almost simple groups and by Lemma 2.8, $\beta(K) \leq |K|^{1-\epsilon}/2^{\epsilon \cdot r}$.

Let $T = G/K$. We claim that $\beta(T) \leq 2^{\epsilon(r-1)}|T|^{1-\epsilon}$. By Lemma 2.8 this would yield $\beta(G) \leq |G|^{1-\epsilon}$, giving us a contradiction.

To prove our claim we will show that if P is a permutation group of degree n such that $|P| \leq |T|$, $n \leq r$, and every non-Abelian composition factor (if any) of P is also a composition factor of T, then $\beta(P) \leq 2^{\epsilon(n-1)}|P|^{1-\epsilon}$. Suppose that P acts on a set Ω of size n. Let P be a counterexample to the bound of this latter claim with n minimal. Then $n > 1$. Suppose that P is not transitive. Then P has an orbit Δ of size, say k, with $k < n$. Let B be the kernel of the action of P on Δ. Then $\beta(P/B) \leq 2^{\epsilon(k-1)}|P/B|^{1-\epsilon}$ and $\beta(B) \leq 2^{\epsilon((n-k)-1)}|B|^{1-\epsilon}$. We get a contradiction using Lemma 2.8. So P must be transitive. Suppose that P acts imprimitively on Ω. Let Σ be a (non-trivial) system of blocks with each block of size k with $1 < k < n$. Let B be the kernel of the action of P on Σ. By minimality, $\beta(P/B) \leq 2^{\epsilon((n/k)-1)}|P/B|^{1-\epsilon}$. By minimality and Lemma 2.8, we also have $\beta(B) \leq 2^{\epsilon(k-1)(n/k)}|B|^{1-\epsilon}$. Again, Lemma 2.8 gives a contradiction. Thus P

must be primitive. If the solvable radical of P is trivial, we get $\beta(P) \leq |P|^{1-\epsilon}$ by $|P| < |G|$. In fact, the same conclusion holds unless n is prime and P is meta-cyclic. In this latter case Corollary 2.9 gives $\beta(P) \leq n^{\epsilon}|P|^{1-\epsilon}$. We get a contradiction by $n \leq 2^{n-1}$. □

6. Almost simple groups

Let H be an almost simple group. In view of Theorem 5.2 in this section we will give a bound for $\beta(H)$ of the form $2^{-\epsilon}|H|^{1-\epsilon}$ where ϵ is such that $0 < \epsilon \leq 0.1$. Let S be the socle of H.

6.1. **The case when S is a finite simple group of Lie type.** We first show that we may take $\epsilon = 0.01$. By Theorem 4.2, $\beta(S) \leq |S|^{39/40}$. By this and Lemma 2.8, we get

$$\beta(H) \leq |H : S| \cdot |S|^{39/40} = |H : S|^{0.01} \cdot |S|^{0.01-(1/40)} \cdot |H|^{0.99}.$$

Thus it is sufficient to see that $|H : S|^{0.01} \cdot |S|^{0.01-(1/40)} \leq 2^{-0.01}$. But this is clear since $|H : S| \leq |\mathrm{Out}(S)| < |S|^{1.5}/2$.

For the remainder of this subsection set $\epsilon = 0.1$. In order to prove the bound for this ϵ, by the previous argument, it would be sufficient to show that $\beta(S) \leq |S|^{0.8}$. We claim that this holds once the Lie rank m of S is sufficiently large. Let E be an elementary Abelian subgroup in S of maximal size. By Lemma 2.5 and by Table 1, if $m \to \infty$, we have $\log_2 |E|/\log_2 \beta(E) \to \infty$. Again by Table 1, $\log_2 |S|/\log_2 |E| = 4 + o(1)$ as $m \to \infty$. Thus we have

$$\log_2 \beta(S) \leq \log_2 \beta(E) - \log_2 |E| + \log_2 |S| = (-1 + o(1)) \log_2 |E| + \log_2 |S| =$$
$$= (-(1/4) + o(1)) \log_2 |S| + \log_2 |S| = ((3/4) + o(1)) \log_2 |S| < 0.8 \log_2 |S|,$$

as $m \to \infty$.

Let p be a defining characteristic for S and let $q = p^f$ be the size of the field of definition. Unfortunately we cannot prove the bound $\beta(H) \leq 2^{-0.1}|H|^{0.9}$ for all groups H with q large enough, but we can establish this bound in case f is sufficiently large. By Table 1, if the Lie rank m is at least 2 then S contains an elementary Abelian p-subgroup E such that $|E|^8 > |S|$. Notice that this bound also holds for $m = 1$, at least for sufficiently large groups S. Thus $\log_2 |S|/\log_2 |E| < 8$. If $f \to \infty$, then $\log_2 |E|/\log_2 \beta(E) \to \infty$. In a similar way as in the previous paragraph, we obtain $\log_2 \beta(S) < ((7/8) + o(1)) \log_2 |S|$, that is, $\beta(S) < |S|^{0.89}$, for sufficiently large S. Since $|H : S|$ is at most a universal constant multiple of f, we certainly have $|H : S| < |S|^{o(1)}$, as $f \to \infty$. The claim follows by Lemma 2.8.

6.2. **The case when S is a sporadic simple group or the Tits group.** In this subsection we set $\epsilon = 0.1$ and try to establish the proposed bound in as many cases as possible. Here we also complete the proof of Theorem 1.3.

In this paragraph for a prime p and a positive integer k let p^k denote the elementary Abelian p-group of rank k and let 2^{1+4} denote a group of order 2^5 with center of size 2. By the Atlas [1], the groups $S = \mathrm{J}_4$ and $S = \mathrm{Co}_1$ contain a section isomorphic to 2^{12}. Furthermore the groups $S = \mathrm{Co}_2$, Co_3, $\mathrm{M^cL}$, Fi_{22}, Fi_{23}, Fi_{24}, B

and M contain a section isomorphic to 2^{10}, 3^5, $3^4:\mathrm{M}_{10}$, 2^{10}, 2^{10}, 2^{12}, 2^{22}, and 2^{24} respectively and the group $S=\mathrm{O'N}$ contains a subgroup isomorphic to $3^4:2^{1+4}$. If S is any of these previously listed groups, we may use Lemmas 2.8 and 2.5 together with the estimate $\beta(\mathrm{M}_{10})/|\mathrm{M}_{10}|\leq 3/4$ in one case (see Theorem 3.2) to obtain the bound $\beta(H)\leq 2^{-\epsilon}|H|^{1-\epsilon}$ with $\epsilon=0.1$. The same estimate holds in case S is the Tits group, as shown in the proof of Theorem 4.2.

If S is not a group treated in the previous paragraph, then $|H|<2.7^{40}$. Thus, by the remark after Lemma 4.1, we have $\beta(H)<|H|/2.7<|H|^{39/40}$. This and Theorem 4.2 complete the proof of Theorem 1.3. Notice also that for $\epsilon=0.01$ we have $|H|^{39/40}<2^{-\epsilon}|H|^{1-\epsilon}$.

6.3. **The case when S is an alternating group.** Let $S=A_k$ be the alternating group of degree k at least 5.

Assume first that $k>10$. Put $s=[k/4]\geq 2$. There exists an elementary Abelian 2-subgroup $P\leq A_k$ of rank $2s$. By Lemma 2.5, we have $\beta(P)=2s+1$. By Lemma 2.8, this gives $n(S)\geq n(P)=2^{2s}/(2s+1)$. Thus $\log_2(n(S))>k\log_2 1.11>k/10$. This gives $\beta(H)<|H|/2^{k/10}$. Thus if

$$\epsilon=\frac{k}{10+10\log_2|H|}>\frac{1}{(10/k)+10(\log_2(k)-1)}>\frac{1}{10\log_2 k},$$

then $\beta(H)<2^{-\epsilon}|H|^{1-\epsilon}$.

Now let $k\leq 10$. Then $|H|<2.7^{16}$. By the remark after Lemma 4.1 we have $\beta(H)<|H|/2.7<|H|^{15/16}$. This is certainly less than $2^{-\epsilon}|H|^{1-\epsilon}$ for $\epsilon=0.01$.

7. Proofs of three main results

Proof of Theorem 5.1. Let G be a finite group. By Theorem 3.3, we may assume that G is nonsolvable. Let H be an almost simple group whose socle S is a composition factor of G. By Sections 6.1, 6.2, and 6.3, we see that $\beta(H)\leq 2^{-0.01}|H|^{0.99}$ provided that S is not an alternating group of degree at least 2^{10}. If S is an alternating group of degree k at least 2^{10}, then $\beta(H)\leq 2^{-\epsilon}|H|^{1-\epsilon}$ with $\epsilon=(10\log_2 k)^{-1}$. The result now follows from Theorem 5.2. □

Proof of Theorem 1.1. Let G be a finite group with Noether index $n(G)$. Let k denote the maximum of 2^{10} and the largest degree of a non-Abelian alternating composition factor of G, if such exists. Let C be a characteristic cyclic subgroup in G of largest possible size. Put $f=|G:C|$. By Theorem 5.1, $\beta(G)\leq|C|^{\epsilon}|G|^{1-\epsilon}$ with $\epsilon=(10\log_2 k)^{-1}$. In other words, $n(G)\geq f^{\epsilon}$. Thus G has a characteristic cyclic subgroup of index at most $n(G)^{10\log_2 k}$. If G is solvable, then $\beta(G)\leq|C|^{0.1}|G|^{0.9}$ by Theorem 5.1. In other words, $n(G)\geq f^{0.1}$ and so $f\leq n(G)^{10}$. □

Proof of Corollary 1.2. Let G be a finite group with Noether index $n(G)$. By Theorem 1.1 we may assume that G is nonsolvable. Thus $n(G)>2.7$ by Lemma 4.1. By Theorem 1.1 we may also assume that G has an alternating composition factor A_k with $k\geq 2^{10}$. From Section 6.3 we have $k<10\log_2(n(A_k))$. Since $n(A_k)\leq n(G)$

by Lemma 2.8, we get $10 \leq \log_2 k < \log_2 10 + \log_2 \log_2(n(G))$. The result now follows from Theorem 1.1. □

8. Questions

We close with three questions which suggest another connection between the Noether number of a group and the Noether numbers of its special subgroups.

Question 8.1. *Is it true that* $\beta(S) \leq \max\{o(g)^2 | g \in S\}$ *for a finite simple group* S*?*

Question 8.2. *Is it true that* $\beta(G) \leq \max\{\beta(A)^{100} | A \leq G,\ A \text{ Abelian}\}$ *for a finite group* G*?*

Question 8.3. *Let* V *be a finite dimensional* FG*-module for a field* F *and finite group* G*. Is it true that* $\beta(G, V) \leq \dim(V)|G : H|\beta(H, V)$ *for every subgroup* H *of* G*?*

Acknowledgements

The authors are grateful to Mátyás Domokos for comments on an earlier version of the paper.

References

[1] Conway, J. H.; Curtis, R. T.; Norton, S. P.; Parker, R. A.; Wilson, R. A. Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. *Oxford University Press*, Eynsham, (1985).

[2] Cziszter, Kálmán. The Noether number of the non-Abelian group of order $3p$. *Period. Math. Hungar.* **68** (2014), no. 2, 150–159.

[3] Cziszter, Kálmán and Domokos, Mátyás. Groups with large Noether bound. *Ann. Inst. Fourier (Grenoble)* **64** (2014), no. 3, 909–944.

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

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

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

[7] Gorenstein, Daniel; Lyons, Richard; Solomon, Ronald. The classification of the finite simple groups. Number 5. Part III. Chapters 1–6. The generic case, stages 1–3a. Mathematical Surveys and Monographs, 40.5. American Mathematical Society, Providence, RI, 2002.

[8] Huppert, B. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134 Springer-Verlag, Berlin-New York, 1967.

[9] Knop, Friedrich. On Noether's and Weyl's bound in positive characteristic. Invariant theory in all characteristics, 175–188, CRM Proc. Lecture Notes, 35, Amer. Math. Soc., Providence, RI, 2004.

[10] Noether, Emmy. Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.* **77** (1915), no. 1, 89–92.

[11] Olson, John E. A combinatorial problem on finite Abelian groups. I. *J. Number Theory* **1** (1969) 8–10.

[12] Pálfy, P. P. A polynomial bound for the orders of primitive solvable groups. *J. Algebra* **77** (1982), 127–137.

[13] Pawale, Vivek M. Invariants of semidirect product of cyclic groups. Ph.D. Thesis, Brandeis University. 1999.

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

[15] Sezer, Müfit. Sharpening the generalized Noether bound in the invariant theory of finite groups. *J. Algebra* **254** (2002), no. 2, 252–263.
[16] Symonds, Peter. On the Castelnuovo-Mumford regularity of rings of polynomial invariants. *Ann. of Math.* (2) **174** (2011), no. 1, 499–517.
[17] Thompson, John G. Nonsolvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.* **74** (1968) 383–437.
[18] Wolf, Thomas R. Solvable and nilpotent subgroups of $GL(n, q^m)$. *Canad. J. Math.* **34** (1982), 1097–1111.

Department of Mathematics, Central European University, Nádor utca 9, H-1051 Budapest, Hungary

E-mail address: hegedusp@ceu.edu

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Reáltanoda utca 13-15, H-1053, Budapest, Hungary

E-mail address: maroti.attila@renyi.mta.hu

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Reáltanoda utca 13-15, H-1053, Budapest, Hungary

E-mail address: pyber.laszlo@renyi.mta.hu