The Noether number for the polynomial invariants of finite groups

Kálmán Cziszter

Central European University, Budapest

ICRA 2012

The polynomial invariants

- Let G be a finite group and $\mathbb{F}$ an algebraically closed field such that $|G| \in \mathbb{F}^\times$.
- Let V be an n-dimensional G-module over $\mathbb{F}$, i.e. a group homomorphism $\rho : G \to GL(V) \cong M_n(\mathbb{F})$ is given.
- Let $x_1, ..., x_n$ be a basis of the dual space V^*; then G acts on the polynomial ring $\mathbb{F}[V] := \mathbb{F}[x_1, ..., x_n]$ by substitutions:

$$(g \cdot f)(x_1, ..., x_n) = f(\rho(g)(x_1, ..., x_n)) \qquad g \in G, f \in \mathbb{F}[V]$$

- Let $\mathbb{F}[V]^G := \{f \in \mathbb{F}[V] : g \cdot f = f \text{ for all } g \in G\}$; this is the ring of polynomial invariants.
- By Hilbert's classical theorem $\mathbb{F}[V]^G$ is finitely generated as an $\mathbb{F}$-algebra.
- Noether's proved this a more constructive way: she gave an upper bound on the degrees of the generators

The Noether number

Definition

$$\beta(G,V) = \min\{s \in \mathbb{N} : \mathbb{F}[V]^G \text{ is generated by } \oplus_{d=0}^{s} \mathbb{F}[V]^G_d\}$$
$$\beta(G) = \sup\{\beta(G,V) : V \text{ is a } G\text{-module over } \mathbb{F}\}$$

- $\beta(G)$ might only depend on $\mathrm{char}(\mathbb{F})$, not on $\mathbb{F}$ (Knop 2004)
- if $\mathrm{char}(\mathbb{F})$ divides $|G|$ then $\beta(G) = \infty$ (Richman 1996)
- if $\mathrm{char}(\mathbb{F}) = 0$ then $\beta(G) = \beta(G, V_{\mathrm{reg}})$ (Schmid, Weyl)

Theorem (Noether 1916, Fleischmann, Fogarty 2001)

$$\beta(G) \leq |G| \qquad \textit{provided that } |G| \in \mathbb{F}^\times$$

For an abelian group $\beta(A) =$ **Davenport constant** $\mathrm{D}(A)$
$=$ the smallest integer n such that any sequence $a_1, \ldots, a_n \in A$ must contain a non-empty subsequence of sum 0

Theorem (Olson 1969)

If $n \mid m$ then $\quad \mathrm{D}(Z_n \times Z_m) = n + m - 1$

For a prime p $\quad \mathrm{D}(Z_{p^{n_1}} \times \ldots \times Z_{p^{n_k}}) = p^{n_1} + \ldots + p^{n_k} - k + 1$

Theorem (Schmid 1991)

$\beta(G) = |G|$ if and only if G is cyclic.

Theorem (Domokos-Hegedűs 2000, Sezer 2002)

$\beta(G) \leq \frac{3}{4}|G|$ if G is non-cyclic.

Main result: the groups with large $\beta(G)$

Theorem (CzK - Domokos, 2011)

Let $|G| \in \mathbb{F}^\times$; then $\beta(G) \geq \frac{1}{2}|G|$ holds if and only if G has a cyclic subgroup of index at most two, 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 $\tilde{A}_4$.*

Groups with cyclic subgroups of index two

By results of Burnside, these groups are of the form $Z_s \times H$ where H is a dihedral, semi-dihedral or dicyclic group and s is coprime to $|H|$

Theorem (CzK-Domokos, 2012)

If G is a non-cyclic group with a cyclic subgroup of index two then

$$\beta(G) = \frac{1}{2}|G| + \begin{cases} 2 & \text{if } G = Dic_{4n}, \ n \text{ even} \\ & \text{or } G = Z_r \rtimes_{-1} Z_4, \ r \text{ odd} \\ 1 & \text{otherwise} \end{cases}$$

Corollary

$$\limsup_{G \text{ non-cyclic}} \frac{\beta(G)}{|G|} = \frac{1}{2}$$

Structural induction

Schmid's reduction lemmata

1. If $H \leq G$ then $\beta(G) \leq [G : H]\beta(H)$
2. If $N \triangleleft G$ then $\beta(G) \leq \beta(G/N)\beta(N)$

   $\Rightarrow$ for any subquotient K $\frac{\beta(G)}{|G|} \leq \frac{\beta(K)}{|K|}$
3. $\beta(G) \geq \beta(H) \geq \max_{g \in G} \mathrm{ord}(g)$

Generalized Noether number

Definition

Let $\beta_k(G)$ be the maximal degree d such that $\mathbb{F}[V]^G_d \not\subseteq (\mathbb{F}[V]^G_+)^{k+1}$

Enhanced reduction lemmata

1. If $H \leq G$ then
2. If $N \triangleleft G$ then

Generalized Noether number

Definition

Let $\beta_k(G)$ be the maximal degree d such that $\mathbb{F}[V]^G_d \not\subseteq (\mathbb{F}[V]^G_+)^{k+1}$

Enhanced reduction lemmata

1. If $H \leq G$ then $\beta(G) \leq [G : H]\beta(H)$
2. If $N \triangleleft G$ then $\beta(G) \leq \beta(G/N)\beta(N)$

Generalized Noether number

Definition

Let $\beta_k(G)$ be the maximal degree d such that $\mathbb{F}[V]^G_d \not\subseteq (\mathbb{F}[V]^G_+)^{k+1}$

Enhanced reduction lemmata

1. If $H \leq G$ then $\beta(G) \leq \beta_{[G:H]}(H)$
2. If $N \triangleleft G$ then $\beta(G) \leq \beta_{\beta(G/N)}(N)$

Generalized Noether number

Definition

Let $\beta_k(G)$ be the maximal degree d such that $\mathbb{F}[V]^G_d \not\subseteq (\mathbb{F}[V]^G_+)^{k+1}$

Enhanced reduction lemmata

1. If $H \leq G$ then $\beta_k(G) \leq \beta_{k[G:H]}(H)$
2. If $N \triangleleft G$ then $\beta_k(G) \leq \beta_{\beta_k(G/N)}(N)$

Generalized Noether number

Definition

Let $\beta_k(G)$ be the maximal degree d such that $\mathbb{F}[V]^G_d \not\subseteq (\mathbb{F}[V]^G_+)^{k+1}$

Enhanced reduction lemmata

1. If $H \leq G$ then $\beta_k(G) \leq \beta_{k[G:H]}(H)$
2. If $N \triangleleft G$ then $\beta_k(G) \leq \beta_{\beta_k(G/N)}(N)$
3. If $G' \leq N \triangleleft G$ then $\beta_k(G) \geq \beta_k(N) + \mathrm{D}(G/N) - 1$

The new reductions give better results since typically $\beta_k(G) \ll k\beta(G)$

Theorem

For any G-module V there are non-negative integers $\beta_0(G, V)$ and $k_0(G, V)$ s.t.

$$\beta_k(G, V) = k\sigma(G, V) + \beta_0(G, V) \quad \text{for every } k \geq k_0(G, V)$$

Definition

Let $R_d \subseteq F[V]^G$ denote the subalgebra generated by all elements of degree at most d. Then $\sigma(G, V)$ is the smallest integer d such that $\mathbb{F}[V]^G$ is a finitely generated as a module over R_d.

Examples

1. Let $G = Z_4 \rtimes Z_4$; this has a normal subgroup s.t. $N \cong G/N \cong Z_2 \times Z_2$.
   From Schmid's lemma we get $\beta(G) \leq 9$.
   It is easily seen that $\beta_k(Z_2 \times Z_2) = 2k + 1$, so

$$\beta(G) \leq \beta_{\beta(Z_3)}(Z_2 \times Z_2) = \beta_3(Z_2 \times Z_2) = 7$$

2. Let G be group with $\beta(G) \geq \frac{1}{2}|G|$ which has a subgroup $H \cong Z_2 \times Z_2 \times Z_2$.

$$\beta_k(Z_2 \times Z_2 \times Z_2) = \begin{cases} 4 & \text{if } k = 1 \\ 2k+3 & \text{if } k > 1 \end{cases}$$

   Let $k = [G : H]$ then we have:

$$4k = \frac{1}{2}|G| \leq \beta(G) \leq \beta_k(Z_2 \times Z_2 \times Z_2) \leq 2k + 3 \Rightarrow \quad G = H$$

A structure theorem

Theorem

For any finite group G one of the following holds:

1. G *contains a cyclic subgroup of index at most* 2
2. G *has a subgroup* $H \leq G$ *isomorphic to one of the groups*
   1. $Z_p \times Z_p$, *where* p *is an odd prime*
   2. $Z_2 \times Z_2 \times Z_2$
   3. A_4 *or* $\tilde{A}_4$
3. G *has a subquotient* K *isomorphic to one of the following:*
   1. *an extension of* $Z_2 \times Z_2$ *by itself*
   2. *an extension of* D_{2p} *by* $Z_2 \times Z_2$
   3. $D_{2p} \times D_{2q}$ *where* p, q *are distinct odd primes*
   4. $Z_p \rtimes Z_q$ *where* p, q *are odd primes,* $q \mid p - 1$
   5. $Z_p \rtimes Z_4$, *where* Z_4 *acts faithfully*
   6. $(Z_2 \times Z_2) \rtimes Z_9$

Theorem

$$\beta_k(A_4) = 4k + 2$$

Conjecture (Pawale)

$$\beta(Z_p \rtimes Z_q) = p + q - 1$$

This is currently proven only for the following cases:

1. $q = 2$ (dihedral groups)
2. $q = 3$ and $\mathrm{char}(\mathbb{F}) = 0$
3. $Z_7 \rtimes Z_3$

References

1. K. Cziszter, M. Domokos: *Groups with large Noether bound* (arXiv:1105.0679)
2. K. Cziszter, M. Domokos: *The Noether number for the groups with a cyclic subgroup of index two* (arXiv:1205.3011)
3. K. Cziszter, M. Domokos: *On the generalized Davenport constant and the Noether number* (arXiv:1205.3416)
4. K. Cziszter: *The Noether number of the non-abelian group of order 3p* (arXiv:1205.5834)

Thank you for your attention!